UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Los registros informáticos como medidas de investigación tecnológica limitativas de derechos fundamentales y su eficacia probatoria en el proceso penal

D. Isidoro Espín López

2020

UNIVERSIDAD DE MURCIA

DEPARTAMENTO DE DERECHO FINANCIERO, INTERNACIONAL Y PROCESAL

Los registros informáticos como medidas de investigación tecnológica limitativas de derechos fundamentales y su eficacia probatoria en el proceso penal

Doctorando: D. Isidoro Espín López

Director: Dr. D. Fernando Castillo Rigabert

A mis padres e hijos, quienes, en todo momento, no dejaron de infundirme ánimo.

Y a mi esposa, Patricia. Sin su ayuda, no hubiera sido posible concluir esta tesis doctoral.

También quiero agradecer sinceramente a Fernando Castillo Rigabert que aceptara ser mi tutor y director de tesis, así como todo el valioso tiempo que me ha dedicado.

ÍNDICE

RESUMEN

Los registros informáticos, como medidas de investigación tecnológica en el proceso penal, han sido incorporados a nuestra legislación con 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 esta reforma, se han establecido dos modalidades principales de registros informáticos que han sido reguladas en los capítulos VIII y IX del título VIII del libro II del citado texto legal y que llevan respectivamente como títulos «Registro de dispositivos de almacenamiento masivo de información» y «Registros remotos sobre equipos informáticos».

Con la presente tesis, se pretende efectuar un estudio completo de estas medidas de investigación partiendo del tratamiento que por la jurisprudencia se dio a las mismas con anterioridad a la citada reforma legal, con un completo análisis de la suficiencia de la nueva regulación y un estudio de la doctrina y jurisprudencia que en este breve espacio de tiempo se ha pronunciado sobre la materia.

Para ello, serán planteadas, además de las peculiaridades propias de esta modalidad de diligencias de investigación, cuestiones como los derechos fundamentales que pudieran quedar limitados, así como los problemas probatorios que se plantearán desde la obtención de las fuentes de prueba mediante la ejecución de la medida hasta su válida incorporación al juicio oral.

ABSTRACT

Computer inspections, as technological research measures in criminal proceedings, have been incorporated into our legislation with Organic Law 13/2015 of 5 October amending the Criminal Procedure Act to strengthen procedural guarantees and regulate technological research measures. With this reform, two main types of computer inspections have been established, which have been regulated in chapters VIII and IX of Title VIII of Book II of the aforementioned legal text and which are entitled respectively «Inspections of information mass storage devices» and «Remote records on computer equipment».

The present thesis aims to make a complete study of these measures of investigation of the crime based on the treatment given to them by the jurisprudence

prior to the aforementioned legal reform, with a complete analysis of the sufficiency of the new regulation and a study of the doctrine and jurisprudence that has been pronounced on the subject in this brief period of time.

To this end, in addition to the peculiarities of this type of investigative proceedings, questions will be raised such as the fundamental rights that may be limited, as well as the evidentiary problems that will arise from obtaining the sources of evidence through the execution of the measure until its valid incorporation into the oral trial.

ABREVIATURAS

apdo.	apartado
art.	artículo
AAP	Auto Audiencia Provincial
AP	Audiencia Provincial
ATC	Auto Tribunal Constitucional
ATS	Auto Tribunal Supremo (Sala de lo Penal)
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CENDOJ	Centro de Documentación Judicial del CGPJ
CGPJ	Consejo General del Poder Judicial
cit.	obra citada
coord.	coordinador
CP	Código Penal
dir.	director
DRAE	Diccionario de la Real Academia Española
EOMF	Estatuto Orgánico del Ministerio Fiscal
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FGE	Fiscalía General del Estado
FJ	Fundamento jurídico
LEC	Ley de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOFCS	Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

LOPD 1999	Ley Orgánica de Protección de Datos de Carácter Personal 15/1999
LOPD 2018	Ley Orgánica de Protección de Datos Personales 3/2018
LOPJ	Ley Orgánica del Poder Judicial
n.º	número
p. (pp.)	página (páginas)
RD	Real Decreto
RGPD UE	Reglamento General de Protección de Datos de la Unión Europea
ROJ	Repertorio Oficial de Jurisprudencia
SAP	Sentencia Audiencia Provincial
ss.	siguientes
STC	Sentencia Tribunal Constitucional
STEDH	Sentencia Tribunal Europeo de Derechos Humanos
STS	Sentencia Tribunal Supremo (Sala de lo Penal)
TC	Tribunal Constitucional
TIC	Nuevas Tecnologías de la Información y Comunicación
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
vid.	véase
vol.	volumen

INTRODUCCIÓN

La rápida evolución de las nuevas tecnologías, fundamentalmente por la aparición de internet y el constante progreso de los sistemas informáticos y de telecomunicaciones, provocó la aparición de nuevas formas de delincuencia organizada que, valiéndose de complejos sistemas tecnológicos, han venido a constituir lo que ha sido denominado como el fenómeno de la «ciberdelincuencia».

Este progreso tecnológico ha exigido que los ordenamientos jurídicos establezcan medidas de investigación como reacción a dicho fenómeno delictivo aprovechando los avanzados sistemas de comunicación, imagen, audio, video e informáticos en general. Estos medios, que hasta no hace mucho tiempo eran desconocidos, han proporcionado a los poderes públicos unas valiosísimas herramientas para la persecución, investigación y prueba de las conductas delictivas, y no solo de aquellas conductas en cuya comisión se utilizan medios relacionados con las nuevas tecnologías, sino en general de todas las conductas constitutivas de delito, y ello dado que la prueba de cualquier delito podría ser localizada en un archivo digital ubicado en cualquier sistema informático.

Estas medidas de investigación ya se venían llevando a cabo desde hace unos años bajo una legalidad precaria y al amparo de una jurisprudencia que, mediante formas de habilitación comunes, venía permitiendo estas novedosas formas de intromisión en la esfera privada. No obstante, no es menos cierto que, ya desde finales del siglo XX, se venía reclamando jurisprudencialmente el primero de los requisitos que debe cumplirse para que puedan tener lugar este tipo de injerencias como es una previsión legal suficiente que cubra todos sus aspectos esenciales. Con ello, no se hacía otra cosa que reclamar el cumplimiento del mandato de la Constitución Española de 1978 (CE) relativo a que toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ya incida directamente sobre su desarrollo (art. 81.1 CE) o limite o condicione su ejercicio (art. 53.1 CE), se encuentre regulada legalmente.

De este modo, la reforma procesal para llenar este vacío legal resultaba inaplazable. Tras algunos intentos de una nueva Ley de Enjuiciamiento Criminal (LECrim), como los Anteproyectos de 2011 y 2013 —que no prosperaron por razones políticas—, el legislador decidió finalmente incorporar a nuestro derecho positivo la

regulación de las medidas de investigación tecnológica por medio de una nueva reforma de la más que centenaria LECrim, que tuvo lugar con la Ley Orgánica (LO) 13/2015 de 5 de octubre de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Esta nueva normativa ha incorporado una amplia regulación de tales medidas que se han concretado en la interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; el registro de dispositivos de almacenamiento masivo de información; y los registros remotos sobre equipos informáticos.

Con la investigación tecnológica, resulta incuestionable la limitación de los derechos fundamentales regulados en el art. 18 de la CE, denominados doctrinalmente los derechos de la vida privada. Así, los derechos a la intimidad personal y familiar (art. 18.1 CE), inviolabilidad del domicilio (art. 18.2 CE), secreto de las comunicaciones (art. 18.3 CE) o protección de datos de carácter personal o derecho a la autodeterminación informativa (art. 18.4 CE) se ven restringidos con la práctica de alguna de las diligencias reguladas en la LECrim (arts. 588bis-588octies). Junto a ellos, jurisprudencialmente se ha invocado como nuevo derecho el llamado «derecho al entorno virtual» respecto del que, como analizaremos en su momento, para un completo reconocimiento estimamos necesaria su incorporación a la legislación vigente.

No obstante, esta limitación de los derechos fundamentales de la vida privada tiene su contrapeso en los requisitos que deben cumplirse para que, válidamente, pueda llevarse a efecto la injerencia. Estos requisitos, que han sido incorporados a la LECrim con la mencionada reforma legal, ya habían sido desarrollados jurisprudencialmente. El primero de ellos se centra en la necesidad de una «previsión normativa», la cual venía siendo reclamada reiteradamente por el Tribunal Europeo de Derechos Humanos (TEDH) y por el TC. Pero, además, la intromisión debe cumplir con el requisito de la «jurisdiccionalidad»; es decir, la medida ha de ser acordada —salvo puntuales excepciones— por un órgano jurisdiccional en el marco de un proceso judicial, lo que exigirá, a su vez, una resolución motivada (art. 588 bis a.1 LECrim) que deberá respetar la tercera y fundamental exigencia de la «proporcionalidad», principio mediante el cual el juez o tribunal, tomadas en consideración todas las circunstancias del caso, verificará

que el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros (art. 588 bis a.5 LECrim).

Otro de los presupuestos incorporados con la LO 13/2015 ha sido el relativo a la «especialidad», principio conforme al que la medida deberá estar relacionada con la investigación de un delito concreto, sin que puedan ser acordadas medidas con carácter prospectivo (art. 588 bis a.2 LECrim). Asimismo se introducen en la LECrim tres principios que son considerados como integrantes del principio de proporcionalidad, como son: la «idoneidad» que servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad; la «excepcionalidad», que exige que se adopte la medida concreta cuando no estén a disposición de la investigación, en atención a sus características otras medidas menos gravosas; y la «necesidad», conforme a la cual se llevará a efecto la intromisión cuando la investigación se vea gravemente dificultada sin el recurso a esta medida (art. 588 bis a.3 y 4 LECrim).

La incorporación legal de las medidas de investigación, ha sido afrontada por el legislador incorporando un nuevo título VIII en el libro II de la LECrim, el cual lleva como rúbrica «De las medidas de investigación limitativas de los derechos reconocidos en el art. 18 de la Constitución» que ha sustituido al originario título VIII de 1882[1], que se dedicaba a la entrada y registro en lugar cerrado, del de libros y papeles y de la detención y apertura de la correspondencia escrita y telegráfica.

En este novedoso título se incluyen diez capítulos, de los cuales los tres primeros —con la relevante modificación del art. 579 relativo a la correspondencia escrita y telegráfica, e inclusión de un nuevo art. 579 bis referido a la utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales—, reproducen la anterior regulación[2]. Es en los siguientes siete capítulos donde se produce la incorporación de las nuevas medidas, iniciándose la regulación con el capítulo IV dedicado a unas disposiciones comunes a todas ellas, para continuar los restantes

[1] El texto original de la LECrim aprobado por RD de 14 de septiembre de 1882 puede ser consultado en https://www.boe.es/datos/pdfs/BOE/1882/260/R00803-00085.pdf. Consultado el 12 de junio de 2019.

[2] Afirma MARCHENA GÓMEZ que «son muchos los temas controvertidos abarcados por esos tres grandes bloques sistemáticos. Algunos de ellos, además, siguen necesitados de una actualización terminológica y conceptual que les despoje de su sabor decimonónico». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuellar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, p. 173.

capítulos sucesivamente con cada una de las medidas de investigación, dedicándose el X y último a las medidas de aseguramiento en relación con la conservación y protección de datos o informaciones incluidas en sistemas informáticos.

Por lo que respecta a las disposiciones comunes a todas las medidas de investigación tecnológica, además de los principios rectores anteriormente mencionados son diversos los elementos a los que nos referiremos. Serán examinadas cuestiones reguladas en la LECrim tales como los aspectos concernientes a la autorización judicial de la medida, secreto de las actuaciones, duración, prórroga, control de la medida, afectación de terceras personas, utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales, cese de la medida, deber de colaboración de terceros, destrucción de registros y orden de conservación de datos como medida de aseguramiento.

Una vez analizados los anteriores apartados, nos ocuparemos de los registros informáticos propiamente dichos, los cuales se concretan en dos modalidades distintas como son: el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim) y los registros remotos sobre equipos informáticos (art. 588 septies LECrim). Si bien se trata en ambos casos del registro de un sistema informático, son diligencias de naturaleza distinta, habida cuenta de las especiales características de los registros remotos, en los que se precisa la utilización de datos de identificación o códigos, o la instalación de un programa informático en el sistema del investigado denominado «troyano»[3], que permite captar información y transmitirla a otro equipo externo mientras el investigado desconoce que se está llevando a efecto la injerencia. El legislador ha tenido en cuenta las circunstancias de esta especial intromisión llevada a cabo por los registros remotos, estableciendo una lista cerrada de delitos en el marco de cuya investigación podrán ser acordados los mismos, vedando asimismo para esta medida la posibilidad de que la Policía Judicial o el Ministerio Fiscal puedan actuar en supuestos de urgencia, siendo esta una de las notables diferencias con el registro de dispositivos de almacenamiento masivo de información.

Por otra parte, para el estudio de la eficacia probatoria de los registros informáticos en el proceso penal, se hace necesario el estudio de cuestiones relacionadas con el tema de la prueba, como son las siguientes:

[3] El DRAE en su 23.ª edición de 2014 incorpora como tercera acepción de troyano la siguiente: «Dicho de un virus: Capaz de alojarse en una computadora para captar información y transmitirla a usuarios ajenos».

a) Las relativas a la preconstitución de las fuentes de prueba obtenidas con los registros informáticos.

b) Los aspectos relacionados con la prueba ilícita.

c) Las medidas a adoptar a fin de asegurar la integridad de los datos obtenidos tras los registros informáticos y las garantías de su preservación, cobrando en este punto especial importancia los aspectos referentes al volcado de los datos y la debida cadena de custodia de los mismos. Esto nos lleva a otro aspecto como es el de la intervención del letrado de la Administración de Justicia durante el volcado de datos, habida cuenta de que este funcionario carece de conocimientos informáticos. Como consecuencia de ello, surge a su vez, la cuestión relativa a la necesidad de intervención para las tareas de volcado y análisis, de un experto informático —respecto de lo que propondremos que se trate de un informático forense al servicio de la Administración de Justicia—, así como la de la existencia de un organismo adecuado para el depósito y análisis de los equipos informáticos y la prueba digital en general.

d) La aportación de las pruebas obtenidas, su valor probatorio y los eventuales casos de impugnación de la prueba digital. Para la regular incorporación al juicio oral de la misma, ha de tenerse en cuenta la premisa fundamental de su válida obtención a fin de que la misma no incurra en la ilicitud del art. 11.1 LOPJ, así como una adecuada cadena de custodia, a lo que ha de añadirse que la incorporación habrá de realizarse a través de cualquiera de los medios probatorios admitidos en derecho y siempre con absoluto respeto al principio de contradicción.

Todo ello posibilitará la práctica en el juicio oral de las pruebas obtenidas con los registros informáticos, a fin de que, con el debido respeto a los principios de publicidad, oralidad, inmediación, contradicción y concentración, y con base en el principio de libre valoración de la prueba proclamado en el art. 741, puedan servir para fundar una sentencia condenatoria.

Son principalmente estas cuestiones las que serán abordadas en esta tesis. Se tendrán en cuenta los principales tratados de Derecho Procesal Penal, monografías y artículos doctrinales relacionados con los distintos apartados de la investigación, y siendo, obviamente, de imprescindible análisis la jurisprudencia de nuestros más altos tribunales. También la del TEDH y, en su caso, la denominada «jurisprudencia menor» de las Audiencias Provinciales.

En cualquier caso, todos estos aspectos no serán los únicos analizados, dado que se pretende igualmente un completo análisis de la suficiencia de la nueva regulación legal así como un exhaustivo examen de la doctrina que en este breve espacio de tiempo se ha pronunciado sobre la materia.

En definitiva, se pretende lograr un completo, sistemático y crítico estudio de los registros informáticos como medidas de investigación tecnológica limitativas de derechos fundamentales y su eficacia probatoria en el proceso penal.

CAPÍTULO I. INVESTIGACIÓN TECNOLÓGICA Y DERECHOS FUNDAMENTALES

I. Introducción

No cabe duda, y así es admitido por todos, que las nuevas tecnologías de la información y comunicación (TIC), y muy especialmente la revolución tecnológica que tuvo lugar con la aparición de internet, ha ido paulatinamente transformando nuestra forma de comunicarnos así como nuestras relaciones sociales, fundamentalmente por la mayor facilidad para acceder a cualquier tipo de información y la inmediatez que ofrecen las comunicaciones telemáticas.

Pero del mismo modo, estos avances tecnológicos permitieron la proliferación de nuevas formas de delinquir y la aparición de un nuevo grupo de delincuentes que, teniendo en cuenta las dificultades iniciales de la investigación en la red, unido a la volatilidad[4] de la información que circula por la misma y la falta de regulación en nuestros textos legales de estas nuevas formas delictivas, hacía muy complicada la identificación y detención de los responsables de estos novedosos delitos. Ante tal situación, los poderes públicos, a través de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), fueron haciendo uso de las TIC para la investigación, no solo de los ciberdelitos, sino en general de cualquier delito.

Debe señalarse, no obstante, que con anterioridad a estos acontecimientos, ya contábamos en nuestro ordenamiento jurídico con una concreta diligencia de investigación tecnológica: la intervención de las comunicaciones telefónicas. Esta medida de investigación fue incorporada al art. 579 de la LECrim por Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, existiendo en relación a la misma una copiosa jurisprudencia, que ha resultado igualmente aplicable a las demás diligencias de investigación tecnológica que paulatinamente se han incorporado a la investigación criminal, entre las que merecen ser destacados los registros informáticos por el elevado grado de intromisión que los mismos suponen en la esfera de los derechos fundamentales.

Las diligencias de investigación (también denominadas actos instructorios o actos de investigación), en general, constituyen el cauce para la aportación de hechos al proceso, con la finalidad de acreditar ante el juez de instrucción la participación del investigado en los hechos y, como señala GIMENO SENDRA, sirven a las partes para

[4] Al hablar de volatilidad de la información, queremos expresar que la misma es fácilmente mudable o alterable.

instar el sobreseimiento o formular su escrito de acusación, pero no permiten fundar una sentencia de condena. Por ello, no deben confundirse las diligencias de investigación con los actos de prueba, los cuales sí están dirigidos a poder fundar, en su día, una sentencia de condena[5]. De la problemática de los actos de prueba en relación con los registros informáticos nos ocuparemos en el último capítulo de este trabajo.

En cuanto a la intromisión o injerencia en los derechos fundamentales llevada a cabo con la investigación penal en general, «resulta innecesario destacar», como así lo afirma CASTILLO RIGABERT, «que los principios y derechos reconocidos en la Constitución han de ser respetados en todo tipo de procedimientos»[6]. No obstante, es igualmente cierto que para poder dar cumplimiento al art. 299 de la LECrim[7] y en consecuencia descubrir la comisión de los delitos y la culpabilidad de los presuntos autores, se hace necesario el uso de medios de investigación indefectiblemente limitativos de determinados derechos fundamentales proclamados en la CE, por cuanto no tratándose de derechos absolutos, conforme precisa MORENO CATENA, «cabe que su protección resulte exceptuada al enfrentarse al interés público por la persecución de los delitos»[8].

Pues bien, esta inevitable injerencia, conforme hemos mencionado anteriormente, se vio incrementada con el desarrollo de las TIC y el crecimiento de su uso por la sociedad para fines de todo tipo, incluido lamentablemente el delictivo. En este sentido, las novedosas medidas de investigación tecnológica han originado un

[5] Afirma GIMENO SENDRA que «debido a la función esencial de la fase instructora, consistente en preparar adecuadamente el juicio oral (art. 299), el juez ha de realizar toda una serie de actos instructorios o de investigación a fin de comprobar la existencia y tipicidad de la "notitia criminis", así como la de su autoría […]. Los actos de investigación sirven, como se ha dicho, para facilitar a las partes la fundamentación fáctica de sus respectivos escritos de calificación o acusación, pero no permiten al juez o Tribunal sentenciador extender sobre ellos su conocimiento en la declaración de hechos probados de la sentencia». Vid. GIMENO SENDRA, J. V., *Manual de Derecho Procesal Penal*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, p. 239 y 307.

[6] CASTILLO RIGABERT, F., «Derechos fundamentales e investigación en las diligencias previas (Estudio de la reciente jurisprudencia de la Sala II del TS)», *Anales de Derecho (Universidad de Murcia)*, n.º 13, 1995, p. 14.

[7] Dispone el art. 299 de la LECrim: «Constituyen el sumario las actuaciones encaminadas a preparar el juicio y practicadas para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación, y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos».

[8] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., *Derecho Procesal Penal*, Valencia, Tirant Lo Blanch, 2019, p. 265.

incremento del grado de intromisión en los llamados derechos a la vida privada, que fueron declarados con dicha rúbrica en el art. 8 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950 (CEDH)[9], y que en nuestro derecho se concretan en el art. 18 de la CE.

En todo caso, como se verá en su momento, dicha injerencia será legítima, siempre que se respeten las garantías procesales y principios rectores establecidos para este tipo de medidas de investigación, siendo de destacar que, igualmente, la intromisión será necesaria cuando su adopción suponga un beneficio al interés público y de terceros superior al perjuicio que pueda sufrir el investigado con la intromisión en sus derechos fundamentales.

II. Investigación tecnológica: una necesidad del siglo XXI

1. El inicio de la era digital

La era digital, también conocida como sociedad de la información y el conocimiento[10], es el nombre que recibe el período de la historia de la humanidad que va ligado a las tecnologías de la información y la comunicación. El comienzo de este período aunque tiene sus antecedentes en tecnologías como el teléfono, la radio o la televisión, que indudablemente potenciaron la rapidez de la información, se asocia con la aparición de internet y la irrupción en nuestras vidas de los dispositivos electrónicos, los cuales han puesto a disposición de la ciudadanía en general nuevas formas de comunicación impensables hace unos pocos años.

[9] El art. 8 del CEDH bajo la rúbrica: «Derecho al respeto a la vida privada y familiar», dispone: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

[10] ORTIZ PRADILLO afirma que aunque el calificativo comúnmente utilizado para designar la etapa actual en que vivimos es el de la «sociedad de la información y el conocimiento» —vista como la sucesora de la sociedad industrial o postmoderna, y caracterizada por el trascendental papel que juegan las tecnologías de la información y la comunicación en las actividades sociales, culturales y económicas—, decide utilizar de modo genérico y sin pretensiones sociológicas la expresión "Era Digital", para tratar de aunar en dicho término todo lo que ha significado la revolución informática, e internet en particular, para el desarrollo de la sociedad de la información y el conocimiento. Vid. ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, Madrid, Colex, 2013, p. 15.

Tal y como señala ORTIZ PRADILLO «la investigación aplicada a las denominadas "nuevas tecnologías" ha generado un continuo desarrollo, que ha desembocado en la miniaturización y la reducción de costes en la fabricación y venta de todo tipo de dispositivos electrónicos, lo cual ha provocado la universalización del empleo de la informática en todos los ámbitos de nuestras vidas»[11], de tal modo que «usamos la tecnología para comunicarnos, pero también para crear, educar, aprender, sanar, fabricar, contratar, jugar, y lamentablemente, también para dañar y cometer todo tipo de actos delictivos»[12].

Por otra parte, esta acelerada evolución de la tecnología no parece que vaya a estabilizarse, sino que, al contrario, la sensación general es que la misma mantendrá un mismo o incluso mayor ritmo de progreso. En este sentido, afirma MIRÓ LLINARES que «el desarrollo de todo el conjunto de tecnologías informáticas que empezó en los sesenta y setenta y que tuvo su espaldarazo definitivo con la creación de Internet y su posterior universalización hasta su conversión en el medio de intercomunicación social más importante de la actualidad, no tiene visos de haber firmado sus últimos avances, sino que, más bien al contrario, parece que la rapidez con la que aparecen nuevas tecnologías se ha ido incrementando exponencialmente»[13].

El inicio de esta nueva era, puede situarse entre las postrimerías del siglo XX y los albores del presente siglo XXI. En ella, el uso de las TIC para la investigación del delito debe calificarse como una exigencia, dado que, por cuestiones lógicas, sin tal uso no sería posible luchar eficazmente contra la delincuencia llevada a cabo a través de las TIC. A ello debe añadirse la dificultad que supone la investigación del delito informático por circunstancias tales como la posibilidad de los delincuentes de cometer delitos de forma simultánea en lugares muy distantes, que en muchas ocasiones se producen más allá de nuestras fronteras, no encontrándose nunca físicamente el delincuente donde se produce el daño; así como por la complejidad derivada del uso profesional de las TIC llevado a cabo por grupos y organizaciones criminales.

Ante tal situación, en el año 1995 se crea el Grupo de Delitos Informáticos en el seno de la Brigada de Delincuencia Económica y Financiera, de la Comisaría General de

[11] ORTIZ PRADILLO, J. C., «*Problemas procesales de la ciberdelincuencia*», cit., p. 15.
[12] ORTIZ PRADILLO, J. C., «*Problemas procesales de la ciberdelincuencia*», cit., p. 15.
[13] MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, p. 26.

Policía Judicial, tratando de dar respuesta a los ataques y vulneraciones de derechos que empezaba a plantear la piratería de software y determinadas estafas bancarias en internet.

Se da un importante impulso en el año 2000, cuando se crea la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, y en el año 2002 evolucionará hasta establecerse como Brigada de Investigación Tecnológica, dependiente inicialmente de la Unidad Central de Delincuencia Económica y Fiscal[14].

Posteriormente, mediante la hoy derogada Orden INT/2103/2005, de 1 de julio, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía [Boletín Oficial del Estado (BOE) de 2 de julio de 2005], pasó a depender de la Unidad de Delincuencia Especializada y Violenta.

Finalmente, con la Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía (BOE de 24 de enero de 2013), se crea una propia unidad para la investigación de los delitos relacionados con las TIC, dependiente de la Comisaría General de la Policía Judicial, que conforme al art. 7.6 de la citada Orden, recibe el nombre de Unidad de Investigación Tecnológica, de la cual dependen la Brigada Central de Investigación Tecnológica y la Brigada Central de Seguridad Informática[15].

---

[14] COMISARÍA GENERAL DE POLICÍA JUDICIAL, «La investigación de los delitos cometidos a través de las TIC'S por el CNP», p. 1, Consultado en http://www5.poderjudicial.es/CVdi/TEMA06-ES.pdf. Consultado el 14 de agosto de 2018.

[15] Dispone el art. 7.6 de la Orden INT/28/2013, de 18 de enero, por la que se desarrolla la estructura orgánica y funciones de los Servicios Centrales y Periféricos de la Dirección General de la Policía que la Unidad de Investigación Tecnológica: «Asume la investigación y persecución de las actividades delictivas que impliquen la utilización de las tecnologías de la información y las comunicaciones (TIC) y el ciberdelito de ámbito nacional y transnacional, relacionadas con el patrimonio, el consumo, la protección al menor, la pornografía infantil, delitos contra la libertad sexual, contra el honor y la intimidad, redes sociales, fraudes, propiedad intelectual e industrial y seguridad lógica. Actuará como Centro de Prevención y Respuesta E-Crime del Cuerpo Nacional de Policía. De esta Unidad dependerán:
a) La Brigada Central de Investigación Tecnológica, a la que corresponde la investigación de las actividades delictivas relacionadas con la protección de los menores, la intimidad, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones. b) La Brigada Central de Seguridad Informática la que corresponde la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes».

Se produce de esta forma, por una obligada adaptación a las necesidades que surgen como consecuencia de los cambios sociales, una especialización de las FCSE para la investigación del crimen a través de la TIC.

Ello no es nada excepcional si tenemos en cuenta que el art. 3.1 del Código Civil (CC) establece como uno de los criterios para la interpretación de las normas «la realidad social del tiempo en que ha de ser aplicadas atendiendo fundamentalmente al espíritu y finalidad de aquéllas», y que el art. 282 de la LECrim, ya desde su redacción original de 1882, establece en su primer inciso que será obligación de la Policía Judicial practicar las diligencias necesarias para averiguar y comprobar los delitos y descubrir a los delincuentes, todo ello sin perjuicio, como veremos, de la intervención previa de la autoridad judicial cuando se trate de garantizar el respeto a los derechos fundamentales.

Asimismo, el art. 11.1 g) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad (LOFCS), establece que las FCSE tienen, en garantía de la seguridad ciudadana, la función, entre otras, de «investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes».

Por lo que atañe al ámbito internacional, el primer instrumento que aborda de una forma completa el fenómeno del crimen a través de las TIC, se aprobó en el marco del Consejo de Europa, precisamente en los inicios del siglo XXI. En efecto, y como se señala en su preámbulo, la preocupación «por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes», condujo a la aprobación, y abrió a la firma, el Convenio sobre la Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001 (en adelante, Convenio de Budapest). Asimismo, en su preámbulo se reconoce «la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información»[16].

[16] Cabe señalar no obstante, como así lo hace ORTUÑO NAVALÓN, que los inicios del Convenio de Budapest se fraguaron con la Convención del Consejo de la UE de 17 de noviembre de 1997, en la que se nombró un comité de expertos del ciberespacio, sobre contenido ilícito en la red, con el que se consiguió poner de acuerdo a la Comunidad Internacional en relación con la ciberdelincuencia. Vid. ORTUÑO

El Convenio de Budapest fue ratificado por España por Instrumento de 20 de mayo de 2010 (BOE de 17 de septiembre de 2010), constando en la actualidad llevada a cabo la ratificación por 64 países.

Debe resaltarse que, aunque el convenio se firmó en el marco del Consejo de Europa, participaron en su elaboración países no pertenecientes al mismo, estableciéndose además en el art. 37 la posibilidad de que el Comité de Ministros pueda invitar a cualquier país que no hubiese participado en su elaboración[17]. Asimismo, España ratificó el Protocolo Adicional al Convenio de Budapest, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo, el 28 de enero de 2003, el cual entró en vigor el 1 de abril de 2015 (BOE de 30 de enero de 2015).

Posteriormente, se han firmado otros convenios internacionales, si bien con carácter fundamentalmente regional[18], por lo que puede afirmarse que el Convenio de Budapest es el único instrumento internacional que nace con vocación vinculante, sirviendo como una guía para cualquier país que desarrolle una legislación nacional integral contra el delito cibernético y como un marco para la cooperación internacional entre los estados parte y aquellos que instaran adherirse al mismo previa invitación del Comité de Ministros del Consejo de Europa.

NAVALÓN, M. C., *La prueba electrónica ante los tribunales*, Valencia, Tirant Lo Blanch, 2014, p. 41, nota al pie n.º 56.

[17] Información obtenida de la web del Consejo de Europa: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Cabe reseñar que de los países del Consejo de Europa, el Convenio no fue firmado inicialmente por Rusia y se encuentra pendiente de ratificación por Irlanda y Suecia. Participaron en su elaboración como países no pertenecientes al Consejo de Europa, Canadá, Japón, República de Sudáfrica y Estados Unidos de América, siendo las últimas ratificaciónes de países invitados que no participaron en su elaboración, la de Perú con fecha 26 de agosto de 2019 y la de Colombia con fecha 16 de marzo de 2020.

[18] CABEZUDO RODRÍGUEZ cita otros convenios internacionales, como el Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de pruebas en materia de cibercriminalidad de 2014, el Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001), el Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009), la League of Arab States Convention on Combating Information Technology Offences (2010) o el proyecto africano, African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012). Vid. CABEZUDO RODRÍGUEZ, N., «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín del Ministerio de Justicia*, n.º 2186, 2016, nota al pie n.º 21, p. 15.

2. La ciberdelincuencia

2.1. Concepto de ciberdelito

Si pretendemos definir el término «ciberdelito», debemos señalar en primer lugar que dicho término no figura en el Diccionario de la Real Academia Española (DRAE), que sí reconoce el vocablo «ciber-», definiéndolo como un elemento compositivo que «indica relación con redes informáticas», reconociendo igualmente el término «ciberespacio», que define como «el ámbito artificial creado por medios informáticos»[19].

En virtud de lo anterior, podría definirse «ciberdelito» como aquella infracción criminal que se comete a través de las redes informáticas, pudiendo entenderse igualmente, siguiendo a DELGADO MARTÍN, como «aquellas infracciones penales que se cometen en el ciberespacio»[20].

Nos parece, sin embargo, más acertada la definición que también de una forma concisa facilita MIRÓ LLINARES al considerar que estaremos ante un «ciberdelito o cibercrimen» únicamente «cuando se trate de un comportamiento delictivo realizado en el ciberespacio cuya esencia de injusto no podría haberse dado de ninguna otra forma fuera de él»[21].

2.2. Tipos de ciberdelitos

Aun cuando el objeto de nuestro estudio no forma parte del Derecho Penal sustantivo, realizaremos unas breves consideraciones en relación con la ciberdelincuencia como detonante de la investigación a través de las nuevas tecnologías de la información y comunicación (TIC), las cuales a día de hoy, dado su carácter dinámico han experimentado una gran evolución[22].

---

[19] Tanto la presente como las sucesivas menciones que se hagan de definiciones obrantes en el DRAE, se refieren a su 23.ª edición de 2014.

[20] DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Las Rozas (Madrid), Wolters Kluwer, 2016, p. 280.

[21] MIRÓ LLINARES, F., «*El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*», cit., p. 42.

[22] Ha de tenerse en cuenta que las TIC constituyen un concepto dinámico, ya que algunas invenciones como el teléfono o la televisión, que en los años 50 del siglo pasado fueron consideradas sin duda como nuevas tecnologías, hoy ya no pueden ser consideradas como tales. Podríamos incluso afirmar que un ordenador sin conexión a internet para tareas ofimáticas o un teléfono móvil sin servicio de datos tampoco tienen la consideración a día de hoy de nuevas tecnologías, las cuales hemos de identificar con los

Una ordenación de las distintas tipologías de ciberdelitos se lleva a cabo en el documento elaborado por la Secretaría de Estado de Seguridad del Ministerio del Interior denominado «Estudio sobre la Cibercriminalidad en España»[23], el cual realiza una clasificación en determinados grupos de tipos delictivos detallando las conductas ilícitas siguiendo la clasificación adoptada por el Convenio de Budapest[24], así como la de la Directiva Europea 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que fue promulgada teniendo en cuenta el contenido del Convenio de Budapest, considerando al mismo como el marco jurídico de referencia para la lucha contra la ciberdelincuencia, incluidos los ataques contra los sistemas de información[25].

---

modernos servicios de la comunicación e información a través de la proliferación de redes creadas a partir de internet, de tal forma que, a medida que se ha ido ampliando la llamada banda ancha de internet, son considerados principalmente nuevas tecnologías todos los contenidos (impensables hace unos años y de los que sería imposible ocuparnos, además de por no ser objeto de nuestro estudio por su amplísimo contenido) que se ofrecen a los ciudadanos a través de dichas redes así como la forma de acceder a los mismos.

[23] MINISTERIO DEL INTERIOR, S. DE E. DE S., *Estudio sobre la Cibercriminalidad en España*, 2017, p. 55, Consultado en http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+España.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70, el 8 de marzo de 2019.

[24] El Convenio realizó una primera clasificación de delitos en sus arts. 2 a 10 con el siguiente orden:

A) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

a) Acceso ilícito

b) Interceptación ilícita

c) Interferencia en los datos

d) Interferencia en el sistema

e) Abuso de los dispositivos

B) Delitos informáticos

a) Falsificación informática

b) Fraude informático

C) Delitos relacionados con el contenido

a) Delitos relacionados con la pornografía infantil

D) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

[25] La Directiva Europea 2013/40/UE declaró en su considerando n.º 33: «Dado que los objetivos de la presente Directiva, a saber, garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros con penas efectivas, proporcionadas y disuasorias, y mejorar y fomentar la cooperación judicial entre las autoridades judiciales y otras autoridades competentes, no pueden ser alcanzados de manera suficiente por los Estados miembros, y que, por consiguiente, debido a sus dimensiones o efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la UE. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos», estableciendo en su art. 1 al definir el objeto de la

Como consecuencia de dicha directiva, España, cumpliendo el mandato expreso fijado en la misma aprobó la LO 1/2015 de 30 de marzo que modificó el Código Penal (CP) mediante la introducción de nuevas infracciones penales en relación a la ciberdelincuencia[26].

3. La necesidad de la investigación tecnológica para cualquier tipología delictiva

Aun cuando la investigación tecnológica surge como respuesta a la irrupción de la cibercriminalidad, no tardó en utilizarse la misma en el marco de cualquier investigación criminal, aun cuando la infracción penal no tuviese por objeto un ciberdelito.

No obstante, es cierto, como se verá en su momento, que el principio de proporcionalidad no sería respetado si se utilizasen determinadas medidas de investigación altamente lesivas de derechos fundamentales en la investigación de cualquier delito, con independencia de su gravedad. Pero, en todo caso, por lo que ahora nos interesa, lo relevante se circunscribe a la circunstancia de que, en el contexto social y con el estado de la tecnología existente en los inicios del siglo XXI, se hizo indispensable el recurso a las TIC para la investigación del delito en general.

En tal sentido, ha de tenerse en cuenta que determinadas investigaciones no serían posibles sin el recurso a las TIC. Piénsese que, sin recurrir a tales medios, no sería posible combatir eventualmente cualquier tipo delictivo, dado que, en muchos casos, la única prueba incriminatoria que facilitara la localización y detención de los presuntos culpables podría localizarse en un equipo informático, o bien por medio de la grabación de comunicaciones orales o de imágenes o la utilización de los modernos dispositivos

---

directiva: «La presente Directiva establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes».

[26] Cabe señalar que, de acuerdo con el Estudio sobre la Cibercriminalidad en España, además de las conductas que introduce el Convenio de Budapest, nuestra realidad en materia de criminalidad denota que existen otras categorías distintas que conviene reseñar, encuadrando dentro de los delitos tecnológicos otras conductas delictivas, teniendo en cuenta, el volumen y la importancia de la cifra registrada, como son los delitos contra el honor y las amenazas y coacciones. MINISTERIO DEL INTERIOR, SECRETARÍA DE ESTADO DE SEGURIDAD, «*Estudio sobre la Cibercriminalidad en España*», cit., p. 5.

técnicos de seguimiento. En definitiva, cualquier prueba digital podría determinar la culpabilidad de los autores de un delito.

Baste señalar, por su relevancia, que el Convenio de Budapest no pretirió esta posibilidad, sino que se refirió expresamente a ella, dado que, después de establecer en su art. 14.2 su aplicación a los delitos que se establecen en el mismo así como a otros delitos cometidos por medio de un sistema informático, termina disponiendo en su apartado c) que será aplicable igualmente a «la obtención de pruebas electrónicas de un delito».

III. Derechos fundamentales susceptibles de ser limitados por la investigación tecnológica

1. Consideraciones previas

No es posible, por evidentes razones de extensión así como por no ser objeto de la disciplina que nos ocupa, llevar a cabo un estudio de los derechos fundamentales con carácter general. No obstante, con la finalidad de sistematizar adecuadamente este trabajo, y a fin de adentrarnos en el examen de los derechos fundamentales afectados por la investigación tecnológica, realizaremos unas breves consideraciones acerca de los mismos, para lo cual se hace necesario, en primer lugar, referirnos a la doble naturaleza de los derechos fundamentales.

1.1. La doble naturaleza de los derechos fundamentales

Una de las primeras sentencias del TC ya se refirió a la doble naturaleza de los derechos fundamentales al declarar que «en primer lugar, los derechos fundamentales son derechos subjetivos, derechos de los individuos no sólo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia. Pero al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho…»[27].

[27] Sentencia del Tribunal Constitucional (STC) 25/1981, de 14 de julio, fundamento jurídico (FJ) 5.º

Así, desde el punto de vista subjetivo, siguiendo a GARCÍA-ATANCE Y GARCÍA DE MORA «su carácter público les confiere la condición de que son exigibles frente al Estado y frente a los poderes públicos»[28], mientras que en relación al aspecto objetivo de los mismos ha señalado ÁLVAREZ CONDE que «los derechos fundamentales, además de su condición de derechos subjetivos, cumplen una función unificadora del ordenamiento jurídico, al que dotan de sus contenidos básicos, estableciendo una vinculación directa entre los individuos y el Estado»[29], refiriéndose a una obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales e igualmente a una obligación positiva de contribuir a la efectividad de los derechos fundamentales aun cuando no exista una pretensión subjetiva por parte del ciudadano[30].

1.2. Los derechos fundamentales a la vida privada reconocidos en el art. 18 CE

Lo dicho anteriormente, no obsta para que el Estado pueda llevar a cabo determinadas injerencias en la esfera de los derechos fundamentales cuando ello resulte necesario para la investigación del delito, lo cual, cuando se utilizan medios de investigación tecnológicos, nos lleva a la necesaria mención de los derechos fundamentales reconocidos en el art. 18 CE.

En relación a los mismos, señala DÍEZ-PICAZO GIMÉNEZ que «el artículo 18 CE consagra una pluralidad de derechos cuya finalidad última común es proteger la vida privada»[31]. Esta denominación fue dada por la rúbrica del art. 8 del CEDH, al referirse al

---

[28] GARCÍA-ATANCE Y GARCÍA DE MORA, M. . V., «La Constitución Dogmática (I). Estado de Derecho y naturaleza de los derechos», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, p. 41.

[29] ÁLVAREZ CONDE, E., «El sistema constitucional español de derechos fundamentales», *Corts: Anuario de derecho parlamentario*, n.º 15, 2004, p. 118.

[30] ÁLVAREZ CONDE, E., «El sistema constitucional español de derechos fundamentales», cit., pp. 119-120.

[31] Dice este autor que «se trata de lo que Louis BRANDEIS, un gran jurista norteamericano que llegó a ser miembro del Tribunal Supremo, bautizó hace cien años como la *privacy*. Esta privacidad consistiría, sintéticamente, en el derecho «a ser dejado en paz» *(to be let alone)*. La existencia de una esfera privada, en la que los demás (poderes públicos o particulares) no pueden entrar sin el consentimiento de la persona, no implica sólo un reconocimiento del altísimo valor que tiene la faceta privada de la vida humana, sino que constituye también una garantía básica de libertad: en un mundo donde toda la actividad de los hombres fuera pública, no cabría la autodeterminación individual. El constitucionalismo, así, exige diferenciar entre las esferas pública y privada y, por tanto, entre lo visible y lo reservado». Vid. DÍEZ-

respeto a los derechos a la vida privada y familiar, con la única salvedad de que en este precepto no se contempla, al menos de manera expresa, el derecho al honor ni tampoco el derecho a la protección de datos. Esta última carencia, se explica por la época en la que fue adoptado el CEDH, siendo prueba de ello que no se produjo tal circunstancia en la Carta de derechos fundamentales, aprobada por el Parlamento Europeo, el Consejo de la Unión y la Comisión Europea el 7 de diciembre de 2000 en Niza, la cual si establece en su art. 7 el respeto a la vida privada y familiar y en su art. 8 reconoce el derecho a la protección de datos de carácter personal[32].

Finalmente, como veremos más adelante, los derechos a la vida privada reconocidos en el art. 18 CE que pueden resultar restringidos por las medidas de investigación tecnológica, se concretan en el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos de carácter personal.

1.3. Derechos fundamentales e investigación tecnológica

En cuanto a la confrontación de los derechos fundamentales a la vida privada y la investigación tecnológica, todas las diligencias de este tipo, incorporadas por la LO 13/2015 a la LECrim, es decir, la interceptación de comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización, el registro de dispositivos de almacenamiento masivo de información y el registro remoto sobre equipos informáticos, pueden resultar limitativas de los derechos a la vida privada reconocidos en el artículo 18 CE, como así se establece en la rúbrica del título VIII del libro II de la LECrim.

Realizaremos a continuación un estudio de los aspectos relevantes en el contexto de la posible vulneración de los citados derechos fundamentales como consecuencia de la investigación tecnológica para obtener pruebas de la comisión de un delito, mientras que en el capítulo V, dedicado a los registros informáticos, nos ocuparemos de las particularidades, que por la injerencia en los derechos fundamentales afectados, se derivan de estas singulares diligencias de investigación.

PICAZO GIMÉNEZ, L. M., *Sistema de Derechos Fundamentales*, Cizur Menor (Navarra), Editorial Aranzadi, 2013, p. 279.

[32] Vid. DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., pp. 279-280.

2. Derecho a la intimidad

2.1. Concepto de intimidad

Aunque se suele afirmar que el término intimidad adolece de una vaguedad e imprecisión que lo lleva al terreno de aquellos conceptos difícilmente definibles[33], nuestro TC nos ha facilitado, a los efectos que nos interesan, una correcta definición del derecho fundamental a la intimidad al declarar que «el derecho fundamental a la intimidad reconocido por el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 CE), frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares»[34]. Asimismo, ha declarado que «tratándose de un derecho fundamental estrictamente vinculado a la propia personalidad […] implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana»[35].

Este concepto ha sido tratado tanto doctrinal como jurisprudencialmente desde dos puntos de vista o criterios: objetivo y subjetivo[36], también denominados material o formal[37].

Conforme a un criterio subjetivo o formal, el derecho a la intimidad comprendería aquéllos ámbitos reservados de la vida privada y familiar que conforme a la voluntad del interesado deben quedar excluidos del conocimiento e intromisiones de los demás. Desde un punto de vista objetivo o material estarán protegidas por el derecho a la intimidad todas aquellas facetas de la vida privada que según el sentimiento mayoritario de una concreta sociedad sean consideradas privadas y ajenas a los demás.

---

[33] LUCENA CID, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2014, p. 18.

[34] Vid. STC 115/2000, de 5 de mayo, FJ 4.º

[35] Vid. STC 186/2000, de 10 de julio, FJ 5.º

[36] REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 180-181.

[37] DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., p. 281.

El problema a resolver se centra en determinar cuál de las concepciones indicadas ha de prevalecer. Como indica DIEZ-PICAZO GIMÉNEZ «ni que decir tiene que, si se adopta un criterio formal, la extensión de la esfera privada variará de una persona a otra, dependiendo de cuán celoso de la propia intimidad sea cada uno; si se adopta un criterio material, en cambio, la extensión de la esfera privada será tendencialmente la misma para todos»[38]. Se plantea entonces el interrogante de si cada persona puede decidir qué aspectos de la vida privada han de quedar excluidos del conocimiento de los demás.

La jurisprudencia constitucional, aunque se ha inclinado más a favor de un criterio objetivo o material[39], se ha pronunciado a favor de ambos conceptos, entendiendo que desde el punto de vista subjetivo cada persona puede reservarse un espacio resguardado de la curiosidad ajena[40].

Doctrinalmente, se han defendido ambas posturas igualmente, existiendo autores que señalan que, en todo caso, en el en el derecho a la intimidad subsiste un acentuado carácter subjetivo que podría cambiar dependiendo de la persona e incluso de una sociedad a otra, llegándose a denominar a la intimidad como el elemento de la desconexión social[41]. Otros autores, sin embargo, se han inclinado por un criterio objetivo o material, entendiendo que el derecho a la intimidad se ha de entender en clave predominantemente objetiva o material, considerando que una construcción de índole formal o subjetiva se encuentra llena de riesgos[42].

---

[38] DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., p. 281.

[39] Pueden mencionarse entre otras las SSTC 143/1994, de 9 de mayo, FJ 6.º y 207/1996, de 16 de diciembre FJ 3.º en las que con cita de otras numerosas sentencias se declaró que el derecho a la intimidad «implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana».

[40] La STC 134/1999, de 15 de julio, FJ 5.º con cita de numerosas sentencias declaró que «el derecho a la intimidad salvaguardado en el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad», así como que «el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida. El art. 18.1 C.E. no garantiza una "intimidad" determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público».

[41] Vid. REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», cit., p. 183.

[42] Vid. DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., p. 282.

Sin embargo, para modular ambos criterios, finalmente nuestra jurisprudencia acogió la doctrina de la «idea de la expectativa razonable de la privacidad».

2.2. Idea de la expectativa razonable de la privacidad

Ante la confrontación entre los criterios objetivo y subjetivo del derecho a la intimidad, esta teoría constituye un criterio válido para establecer si nos encontramos ante una manifestación de la vida privada que ha de ser protegida ante cualquier intromisión. Se trata de la «expectativa razonable» que toda persona tiene sobre si se encuentra amparada ante cualquier observación ajena. Este concepto fue establecido por la jurisprudencia de EEUU en el caso Katz v. United States[43] y ha sido recogida por el TEDH[44].

El fundamento que sustenta esta doctrina radica en la circunstancia de que no pueden abrigarse expectativas razonables de privacidad cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean pueden ser claramente objeto de registro o de información pública. De este modo, la protección constitucional del derecho a la intimidad se dará en las situaciones en las no es razonable que la propia persona, o cualquier otra en similares circunstancias, considere que sus acciones se someten al conocimiento ajeno, mientras que no gozará de protección el ciudadano que sea consciente de que su actividad puede trascender a terceros.

Dicho en palabras de RODRÍGUEZ LAINZ «el enunciado de esta doctrina podía resumirse en la siguiente máxima: Un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables»[45].

---

[43] En el caso Katz v. United States, resuelto por Sentencia del Tribunal Supremo de EEUU el 18 de diciembre de 1967, quedó acreditado que Charles Katz usó una cabina telefónica pública para transmitir información sobre apuestas ilegales desde Los Angeles a Miami y Boston. Sin que Katz lo supiera, el FBI estaba grabando sus conversaciones a través de un dispositivo de escucha electrónico conectado al exterior de la cabina. Katz fue condenado con base en estas grabaciones. Argumentó en su recurso que las grabaciones se obtuvieron con violación de los derechos de la Cuarta Enmienda. El Tribunal Supremo estimó el recurso considerando que hubo intromisión ilegítima por parte del FBI, dado que, al haber cerrado la puerta de la cabina, se mantenía intacta la expectativa razonable del Sr. Katz de que su intimidad se encontraba preservada.

[44] Vid. Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido § 57, y STEDH de 28 de enero de 2003, Peck c. Reino Unido, § 58.

[45] RODRÍGUEZ LAINZ, J. L., «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley - Sección Doctrina*, n.º 8122, 2013, p. 2.

También el TC ha seguido esta doctrina, declarando qué ámbito de cobertura del derecho a la intimidad viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad[46].

Por su parte, el TS en la Sentencia 610/2016, de 7 de julio, se refirió a la expectativa razonable de privacidad al realizar un completo estudio de la jurisprudencia del TEDH dictada en relación con el derecho a la intimidad, así como de la STEDH citada anteriormente, del derecho comparado y de las resoluciones del TC relativas al derecho a la intimidad[47].

2.3. Derecho a la intimidad e investigación tecnológica

La necesidad de intervención de la sociedad y de los sistemas que gobiernan la misma ya se hizo necesaria en el ámbito del derecho a la intimidad en 1890 a propósito de la publicación por Warren y Brandeis del artículo «The Right to Privacy», en el cual denunciaban la captura de imagen a distancia y sin permiso a través de fotografías y la distribución de las mismas en la prensa[48].

Un siglo después, de una forma similar, como consecuencia del desarrollo de las TIC, surgieron nuevos contenidos del derecho a la intimidad, concretados en los

[46] STC 170/2013, de 7 de octubre, FJ 5.º entre otras, la cual declaró que «hemos tenido ocasión de precisar que el ámbito de cobertura de este derecho fundamental viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad. En concreto, hemos afirmado que un "criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno. Así, por ejemplo, cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública (SSTEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, § 57, y de 28 de enero de 2003, Peck c. Reino Unido, § 58)».

[47] En su FJ 1.º la STS 610/2016 declaró: «Son la intensidad de la injerencia y el factor tiempo los que hacen que la medida afecte claramente a esa expectativa razonable de privacidad que inspira la doctrina del caso Katz».

[48] Citado por LUCENA CID, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», cit., p. 16. Señalaron estos autores en 1890 que «es un principio tan viejo como el *common law* que el individuo debe gozar de total protección en su persona y en sus bienes, sin embargo, resulta necesario, de vez en cuando, redefinir con precisión la naturaleza y la extensión de esta protección. Los cambios políticos, sociales y económicos imponen el reconocimiento de nuevos derechos, y el *common law*, en su eterna juventud, evoluciona para dar cabida a las demandas de la sociedad».

aspectos de la vida privada a los que eventualmente podrían tener acceso no autorizado terceras personas a través de la tecnología digital. Tales accesos indebidos a la vida privada de los demás, se mostraron como consecuencia de la aparición de internet y las redes sociales, así como por otras tecnologías como la videovigilancia, el conocimiento de la ubicación de una persona a través de GPS (Global Positioning Systems) y también como no, en los casos de diligencias de investigación tecnológica del delito, que, como hemos venido exponiendo, hicieron necesaria igualmente la intervención de la sociedad, dando lugar a una revisión de la definición del derecho a la intimidad.

En efecto, como consecuencia de la irrupción de las TIC, se produce una ampliación en el contenido del derecho a la intimidad. Como declaró el TC, al resolver un recurso de amparo en el que se planteaba la vulneración del derecho a la intimidad como consecuencia de una investigación policial, «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.» [49].

En cualquier caso, el derecho a la intimidad, tal y como ha declarado el TC, no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes siempre que el recorte que aquel haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y proporcionado para alcanzarlo, siendo en todo caso respetuoso con el contenido esencial del derecho[50].

Respecto a los intereses constitucionalmente relevantes, el TC ha considerado incluida dentro de los mismos a la investigación del delito, declarando que la intromisión es imprescindible para asegurar la defensa del interés público que se pretende defender mediante el ejercicio del *ius puniendi*[51].

[49] Vid. STC 173/2011, de 7 de noviembre, FJ 3.º
[50] Vid. SSTC 57/1994, de 28 de febrero, FJ 5.º; y 143/1994, de 9 de mayo, FJ 6.º entre muchas otras.
[51] Vid. SSTC 37/1989, de 15 de febrero, FJ 8.º; y 207/1996, de 16 de diciembre, FJ 4.º

Asimismo, el TEDH ha declarado, al resolver un caso en el que se denunciaba la violación del derecho a la intimidad como consecuencia de una diligencia de investigación tecnológica, que para la legítima injerencia se han de cumplir los requisitos del apartado 2 del art. 8 del CEDH, es decir, se ha de determinar si la medida está prevista por la ley y si es necesaria en una sociedad democrática[52].

Cuando concurran tales exigencias, o, en su caso, cuando medie el consentimiento del interesado, no será ilegítima la afectación o injerencia en el derecho a la intimidad, y, como ha declarado nuestro TC, «tampoco podrá ser calificada de ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos, siempre y cuando se respete el contenido esencial del derecho»[53].

3. Derecho al secreto de las comunicaciones

El derecho al secreto de las comunicaciones se encuentra protegido, junto con los demás derechos que en general comprenden el derecho a la vida privada, por el art. 12 de la Declaración Universal de Derechos Humanos de 19 de diciembre de 1948, el art. 8 CEDH y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966, y ampara a toda persona física o jurídica contra cualquier injerencia en el ámbito de su libertad a comunicarse libremente con los demás, impidiendo que el contenido de la comunicación sea conocido por terceros.

Asimismo, el derecho se encuentra reconocido en el art 7 de la Carta de Derechos Fundamentales de la UE, que dispone que «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

El art. 18.3 de nuestra Constitución dispone que «se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

Afirma REBOLLO DELGADO que el texto constitucional realiza una precisión, a su juicio improcedente, al referirse, en especial, a las comunicaciones postales, telegráficas

[52] Vid. STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España, apdo. 28.
[53] Vid. STC 159/2009, de 29 de junio, FJ 3.º

y telefónicas, señalando que «hubiera sido mejor no haber delimitado los tipos de comunicaciones, sobre todo por lo vertiginoso de la evolución de estos, y haber hecho una protección genérica del secreto de las comunicaciones o de las telecomunicaciones»[54]. No obstante, como también afirma el referido autor, el precepto constitucional ha de interpretarse de forma «amplia y flexible»[55] y por tanto de forma extensiva a las comunicaciones que tengan lugar a través de cualquier medio tecnológico, habiéndose pronunciado el TS en idéntico sentido[56].

En cualquier caso, de conformidad con las disposiciones citadas, es lo cierto que nos encontramos ante un derecho fundamental de todas las personas, cuya restricción supondría una invasión en la esfera privada del afectado y, por tanto, un ataque a su intimidad. Ello lleva, en primer lugar, a indagar acerca de la delimitación entre el derecho a la intimidad y el derecho al secreto de las comunicaciones.

3.1. Delimitación entre los derechos a la intimidad y secreto de las comunicaciones

Cabe reseñar, como así lo hace REBOLLO DELGADO, que, como derecho, el secreto de las comunicaciones «tuvo un reconocimiento en los textos constitucionales muy anterior al derecho a la intimidad, quedando recogido por primera vez en los arts. 7 y 8 de la Constitución de 1869, y reconocido de nuevo en las de 1876 (art. 7) y 1931

[54] REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», cit., p. 193.

[55] REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», cit., p. 193.

[56] Vid. STS 714/2016, de 26 de septiembre, FJ 6.º que declaró que «el derecho al secreto de las comunicaciones puede considerarse una plasmación singular de la dignidad de la persona y del libre desarrollo de su personalidad, que constituyen el fundamento del orden político y de la paz social (STC n.º 281/2006, de 9 de octubre y STS n.º 766/2008, de 27 de noviembre), por lo que trasciende de mera garantía de la libertad individual, para constituirse en medio necesario para ejercer otros derechos fundamentales. Por ello la protección constitucional del secreto de las comunicaciones abarca todos los medios de comunicación conocidos en el momento de aprobarse la norma fundamental, y también los que han ido apareciendo o puedan aparecer en el futuro, no teniendo limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse (SSTS n.º 367/2001, de 22 de marzo y n.º 137/1999, de 8 de febrero)».

(art. 32)»[57]. Por otra parte, tal y como afirma GIMENO SENDRA cuando se refiere a la naturaleza del derecho al secreto de las comunicaciones, «aun cuando dicho derecho claramente se relacione con el derecho fundamental a la "intimidad" […] no se identifica absolutamente con él, sino que posee un contenido mucho más amplio»[58].

La primera cuestión a destacar, tras el examen del art. 18 CE, radica en la circunstancia de que para que pueda producirse una injerencia en el derecho al secreto de las comunicaciones es necesaria una resolución judicial, lo cual no se produce del mismo modo ante cualquier vulneración del derecho a la intimidad. En este sentido, no todas las intervenciones de las FCSE necesitarán una orden judicial cuando se trate de una actuación que pueda vulnerar la intimidad, mientras que si se trata de una intromisión restrictiva del derecho al secreto de las comunicaciones (a salvo de los supuestos establecidos en el art. 579.3 y 4 LECrim[59] para la intervención de la correspondencia escrita y telegráfica y en el art. 588 ter d.3 LECrim[60] para la interceptación de las comunicaciones telefónicas y telemáticas), exigirá en todo caso la correspondiente autorización judicial.

---

[57] REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*, Madrid, Dykinson, 2000, pp. 58-60. Citado por MEGÍAS QUIRÓS, J. J., «Privacidad e internet: intimidad, comunicaciones y datos personales», *Anuario de Derechos Humanos - Nueva Época*, n.º 3, 2002, p. 546.

[58] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 407.

[59] Establecen los apartados 3 y 4 del art. 579 de la LECrim para la detención y apertura de la correspondencia escrita y telegráfica lo siguiente:

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

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

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

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

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

[60] El art. 588 ter d.3 LECrim reproduce el contenido del art. 579.3 que acabamos de citar.

Efectivamente, tal y como ha declarado el TC en relación con el derecho a la intimidad, y a diferencia de otras medidas restrictivas de derechos fundamentales como la intervención de las comunicaciones, «no existe en la Constitución reserva absoluta de previa resolución judicial» señalando asimismo que aun cuando previamente se había declarado que la limitación del ámbito constitucionalmente protegido del derecho a la intimidad era solo posible por decisión judicial, ello no descarta la posibilidad de que «en determinados casos y con la conveniente habilitación legislativa […], tales actuaciones pudieran ser dispuestas por la Policía Judicial»[61].

Como segunda diferencia —con la que se delimita más nítidamente el derecho al secreto de las comunicaciones en relación con el derecho a la intimidad—, doctrinalmente se ha señalado que «estriba en el sistema adoptado para hacer efectiva la protección de cada uno de los derechos: un sistema formal (secreto) frente a un sistema material, basado en el contenido»[62]. A diferencia del derecho a la intimidad, en el que debe examinarse el contenido sobre el que ha tenido lugar la injerencia para determinar si pertenece al ámbito de lo privado, en el derecho al secreto de las comunicaciones, su contenido, como su propio nombre indica, se encuentra incluido dentro del concepto de secreto, estableciéndose así un concepto formal que «no necesita en modo alguno analizar el contenido de la comunicación —o de sus circunstancias— para determinar su protección por el derecho fundamental»[63]. Es lo que otros autores denominan «garantía formal de intangibilidad», dado que las comunicaciones son de acceso reservado en cuanto tales, y ello por cuanto lo decisivo no es el contenido, es decir, lo que se

[61] Vid. STC 70/2002, de 3 de abril, FJ 10.º la cual añadió que «la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad».

[62] FRÍGOLS I BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», en Boix Reig, Javier (dir.) Jareño Leal, A. (coord.), *La protección jurídica de la intimidad*, Madrid, Iustel, 2010, p. 42.

[63] FRÍGOLS I BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», cit., p. 42.

transmite en la comunicación, sino el continente, o lo que es lo mismo, poder transmitirlo sin que lo sepan los demás, incluido el Estado[64].

En otras palabras, puede afirmarse que el derecho que nos ocupa se configura en torno al concepto de secreto con la finalidad de poder comunicarse libremente, y ello independientemente de que el contenido del mensaje deba incluirse dentro de la esfera privada del individuo y de que pueda o no tener la cualidad de íntimo.

En efecto, tal y como estableció la STC 114/84, de 29 de noviembre, FJ 7.º la cual sigue siendo un referente en esta materia, «el bien constitucionalmente protegido es así —a través de la imposición a todos del "secreto"— la libertad de las comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje —con conocimiento o no del mismo— o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)», declarando asimismo que «sea cual sea el ámbito objetivo del concepto de "comunicación", la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia erga omnes) ajenos a la comunicación misma»[65].

Posteriormente, se han dado otros pronunciamientos acerca de este aspecto definitorio del derecho, entre los que cabe destacar la STC 34/1996, de 11 de marzo, FJ 4.º, que declaró de forma similar que «en definitiva, se pretende garantizar así la "impenetrabilidad de la comunicación" por terceros con eficacia erga omnes, tanto para los ciudadanos de a pie como para los agentes de los poderes públicos y abstracción hecha de la "dimensión material del secreto", lo que se transmite».

Finalmente, en torno a la delimitación entre el derecho al secreto de las comunicaciones y el derecho a la intimidad, ha tenido lugar una particular polémica al plantearse la cuestión de si las comunicaciones en las que el proceso comunicativo ya ha

[64] DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., pp. 298-299.

[65] La STC 114/1984, de 29 de noviembre, FJ 7.º declaró que «el concepto de "secreto" en el art. 18.3 tiene un carácter "formal", en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado», señalando que esta condición formal del secreto de las comunicaciones constituye una *presunción iuris et de iure* de que lo comunicado es "secreto" en un sentido sustancial.

concluido, se encontrarían protegidas por el derecho al secreto de las comunicaciones o por el derecho la intimidad.

Inicialmente el TC declaró que «la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»[66].

En la misma línea se ha pronunciado el TS, considerando que la garantía dispensada por el derecho al secreto de las comunicaciones termina con la comunicación. En este sentido, ha declarado que «los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya protección constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones»[67].

Sin embargo, en otra de sus resoluciones, el TC estimó que el derecho al secreto de las comunicaciones se extiende más allá de la finalización de la comunicación, al precisar que este derecho comprende también los datos registrados durante el proceso de comunicación, «con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso»[68]. En términos similares se pronunció la STC 230/2007, de 5 de noviembre, que, con cita de la STEDH de 3 de abril de 2007, caso Copland c. Reino Unido, apdo. 43, declaró vulnerado el secreto de las comunicaciones por el acceso policial al registro de llamadas de un terminal móvil[69]. También el TS se ha pronunciado en el mismo sentido en alguna de sus resoluciones[70].

---

[66] Vid. STC 70/2002, de 3 de abril, FJ 9.º

[67] Vid. STS 342/2013, de 17 de abril, FJ 8.º

[68] Vid. STC 123/2002, de 20 de mayo, FJ 6.º

[69] La STC 230/2007, de 5 de noviembre, FJ 2.º, declara que «con los antecedentes expuestos, debe concluirse, conforme también interesa el Ministerio Fiscal, que se ha vulnerado al recurrente el derecho al secreto de las comunicaciones (art. 18.3 CE), en tanto que, acreditado y reconocido por las resoluciones judiciales el presupuesto fáctico del acceso policial al registro de llamadas del terminal móvil intervenido al recurrente sin su consentimiento ni autorización judicial, dicho acceso no resulta conforme a la doctrina constitucional reiteradamente expuesta sobre que la identificación de los intervinientes en la comunicación queda cubierta por el secreto de las comunicaciones garantizado por el art. 18.3 CE y, por

Posteriormente, el TC ha mantenido que los mensajes ya leídos quedan protegidos por el derecho a la intimidad y no por el derecho al secreto de las comunicaciones. Concretamente, en la STC 173/2011, de 7 de noviembre, FJ 3.º ha señalado que «a esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado».

En cualquier caso, y no obstante la aparente discrepancia entre las resoluciones mencionadas, consideramos que de la lectura de las mismas, no se desprende estrictamente la existencia de divergencias jurisprudenciales, teniendo en cuenta que en los casos en los que tanto el TC como el TS se han pronunciado en favor de la protección por el derecho al secreto de las comunicaciones incluso una vez concluido el proceso comunicativo, lo ha sido cuando se ha tratado de determinados datos de tráfico y no así del contenido de la comunicación. En este sentido, la doctrina constitucional mencionada ha mantenido sin vacilaciones que la visualización de un mensaje una vez que el mismo ha sido abierto y leído por su destinatario no vulnera el derecho al secreto de las comunicaciones sino el derecho a la intimidad.

La distinción tiene gran importancia teniendo en cuenta fundamentalmente, que, en atención al derecho vulnerado, será necesario el requisito de la jurisdiccionalidad para la intervención policial, ya que para la injerencia en el secreto de las comunicaciones será siempre necesaria autorización judicial, pero no así en aquellos casos en los que la Policía Judicial pueda llevar a cabo una intervención que no vulnere el secreto de las comunicaciones y sí levemente el derecho a la intimidad.

La conclusión más congruente, tal y como se colige de la doctrina jurisprudencial citada, es aquella conforme a la que, con independencia de que un

---

tanto, que resulta necesario para acceder a dicha información, en defecto de consentimiento del titular del terminal telefónico móvil intervenido, que se recabe la debida autorización judicial. Ello supone la imposibilidad de valoración de dicha prueba al tener que quedar excluida del material probatorio apto para enervar la presunción de inocencia, en tanto que obtenida con vulneración de derechos fundamentales del recurrente».

[70] Vid. STS 156/2008, de 8 de abril, FJ 4.º

mensaje haya sido leído o una llamada haya finalizado, no lleva aparejada una desprotección del derecho al secreto de las comunicaciones en relación con los datos que han quedado almacenados o se han originado como consecuencia del proceso de comunicación, como podría ser el listado de llamadas efectuadas registrado en un teléfono.

No obstante, podemos anticipar, como se verá más adelante, que los datos almacenados una vez concluido el proceso de comunicación no siempre quedarán protegidos por el derecho al secreto de las comunicaciones, pudiendo en determinados supuestos quedar protegidos por el derecho a la protección de datos de carácter personal del art. 18.4 CE.

3.2. Concepto de comunicación

A fin de poder adentrarnos en el contenido del secreto de las comunicaciones, resulta necesario referirnos al concepto de «comunicación», como elemento imprescindible para que el derecho despliegue su eficacia, construyéndose este concepto a partir de los elementos del proceso comunicativo que se encuentran amparados por el secreto.

Es de reseñar que, tal y como señaló la STC 70/2002, de 3 de abril, FJ 9.º, «ciertamente los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE».

De forma parecida, la Circular 1/2013 de la FGE señaló que «los imparables avances tecnológicos ponen en manos no sólo de los poderes públicos sino incluso de los particulares enormes poderes que potencialmente son una amenaza para el secreto de las comunicaciones, lo que exige reinterpretar este derecho y afinar el sistema de garantías para proteger la privacidad humana»[71], añadiendo que «como ha declarado el TC "en una sociedad tecnológicamente avanzada como la actual, el secreto de las

[71] FISCALÍA GENERAL DEL ESTADO, *Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, 2013, Consultado en https://www.fiscal.es/documents/20142/b9b37701-c716-79ab-d1dc-111350113518, el 27 de mayo de 2020.

comunicaciones constituye no solo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo"»[72].

Aceptado este nuevo entendimiento del concepto de comunicación, cabría referirse a una nueva noción que, dejando aparte la comunicación postal, comprendiese todas las comunicaciones electrónicas. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, en su artículo 2.d definió comunicación, a los efectos de la misma, como «cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público»[73].

Autores como RODRÍGUEZ LAÍNZ proponen, sin embargo, una definición más ajustada a todas las posibilidades que demanda el mundo de las nuevas tecnologías, considerando que debe concebirse la comunicación como «la transmisión, compartición o intercambio de información entre dos o más sujetos determinados o determinables, dirigida a través de determinados canales de comunicaciones que son gestionados por terceras personas o entidades, en quienes se confía no solo su buen fin, sino también la confidencialidad en su gestión frente al conocimiento ajeno»[74].

Finalmente, del concepto de comunicaciones, cabe destacar en el contexto que nos ocupa relativo a la protección constitucional del secreto de las mismas, que su vulneración no se producirá cuando la intervención de la comunicación se produzca de modo directo, sin intervención técnica alguna. Como ha señalado el TC para que se produzca la limitación del derecho se requiere la interferencia directa en el proceso de comunicación mediante el empleo de cualquier artificio técnico de captación, sintonización o desvío y recepción de la señal telefónica como forma de acceso a los datos confidenciales de la comunicación[75].

---

[72] STC 123/2002, de 20 de mayo, FJ 5.º

[73] Esta definición se encuentra posteriormente reproducida literalmente en el art. 64.c del Real Decreto (RD) 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

[74] RODRÍGUEZ LAINZ, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, n.º 8143, 2013, p. 2.

[75] Auto del Tribunal Constitucional (ATC) 15/2004, de 20 de enero, FJ 4.º

3.3. Elementos de la comunicación protegidos por el derecho

La definición expuesta anteriormente del término comunicaciones nos muestra los cuatro elementos fundamentales que constituyen el contenido del proceso comunicativo, los que, como dijimos al inicio de este apartado, se encuentran protegidos por el secreto. Estos elementos son: el comunicador o emisor, el interlocutor o receptor, la información compartida y un tercero prestador del servicio de comunicación, quien «se encuentra unido a los interlocutores por vínculos de confidencialidad, lo que caracterizará a la comunicación amparada por el secreto»[76]. A ellos hay que añadir los datos de tráfico o asociados, que son aquellos que se generan como consecuencia del establecimiento de comunicación de forma externa a la misma y que pueden facilitar los elementos que la identifican.

3.3.1. La información compartida

En cuanto a la información compartida o contenido de la comunicación, aunque la información que se transmite o comparte es esencial para la existencia de una comunicación, no es menos cierto tal y como afirma GONZÁLEZ-CUELLAR SERRANO que «el carácter formal del derecho al secreto de las comunicaciones convierte a la integridad del procedimiento de comunicación en el núcleo de la cuestión»[77]. Por tanto, lo que se comunica no es lo más relevante a los efectos de la protección constitucional dispensada por el derecho. Sin embargo, ello no obsta para que el contenido de la comunicación se configure como el núcleo central del proceso en el que la comunicación consiste, encontrándose protegidas por el derecho todas las formas que puede tener el mismo, tales como voz, mensajes escritos electrónicos o archivos de audio o video.

3.3.2. Los intervinientes en el proceso de comunicación

Respecto del comunicador o emisor y el interlocutor o receptor, esto es, las personas que intervienen en el proceso, la jurisprudencia del TC ya declaró en la meritada STC 114/1984, de 29 de noviembre, que el término «secreto» cubre además del

[76] RODRÍGUEZ LAINZ, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», cit., p. 2.

[77] GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», en Díaz Maroto y Villarejo, J. y otros, *Derecho y Justicia Penal en el Siglo XXI*, Madrid, Colex, 2006, p. 903.

contenido de la comunicación otros aspectos de la misma como por ejemplo, la identidad subjetiva de los interlocutores o corresponsales[78]. Ha de señalarse que debe tratarse de una comunicación entre personas físicas, habiendo declarado la STC 281/2006, de 9 de octubre, FJ 3.º que «las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana».

No obstante estas menciones referentes a la necesidad de que sean personas humanas las que intervienen en el proceso, no es posible negar la titularidad del derecho a las personas jurídicas, lo que ha sido afirmado por la jurisprudencia del TEDH al declarar que el domicilio «incluye también la oficina registrada de una empresa dirigida por un particular, así como la oficina registrada de una persona jurídica, sucursales y otros locales comerciales»[79].

Se trata de una cuestión que del mismo modo ha sido reiteradamente declarada por la jurisprudencia del TS, que, en muchas de sus sentencias, ha puesto de manifiesto que son titulares del derecho «las personas físicas y las jurídicas tanto nacionales como extranjeras, mayores y menores de edad, porque el secreto de las comunicaciones presupone la libertad, y su restricción se produce en un sentido de control y observación y no propiamente de impedimento a las comunicaciones y se extiende tanto al conocimiento del contenido de las mismas, como a la identidad de los interlocutores»[80].

Sin embargo, no se encuentran protegidos por el derecho los diálogos entre dispositivos electrónicos o informáticos que se generan de forma automática, respecto de lo que tanto el TC como el TS han declarado que «las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana»[81], tratándose de un criterio compartido por la FGE, que se ha pronunciado en idéntico sentido[82].

---

[78] Posteriormente otras SSTC lo han declarado igualmente. Así, por ejemplo, la STC 70/2002, de 3 de abril, FJ 9.º o la STC 142/2012, de 2 de julio, FJ 3.º

[79] Vid. SSTEDH de 27 de septiembre de 2005, caso Petri Sallinen y otros c. Finlandia, apdo. 70; y de 14 de marzo de 2013, caso Bernh Larsen Holding AS y otros c. Noruega, apdo. 104.

[80] Vid. SSTS 1295/1999, de 21 de septiembre, FJ 2.º; 132/1997, de 8 de febrero FJ 2.º; y 276/1996, de 2 de abril, FJ 6.º

[81] Vid. STC 281/2006, de 9 de octubre, FJ 3.º y STS 766/2008, de 27 de noviembre, FJ 3.º

[82] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., p. 11.

Finalmente, en relación con los intervinientes en el proceso de comunicación, cabe referirse a las comunicaciones que tienen lugar a través de las redes sociales (Facebook, Twitter, Youtube, Redes P2P, etc.), en las cuales no puede hablarse de privacidad, dado que la información transmitida a través de ellas es de acceso público, por lo que las mismas no se encuentran protegidas por el derecho fundamental, habiendo señalado el TS que «no se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma»[83].

3.3.3. El tercero prestador del servicio

En cuanto al tercero prestador del servicio de comunicación unido a los interlocutores por vínculos de confidencialidad, se trata de una intervención necesaria para la consecución de la comunicación, la cual no sería posible sin que por el mismo se facilitasen los medios para que se llevase a efecto.

Respecto al vínculo de confidencialidad, es indispensable para la completa realización del derecho, encontrándose lógicamente enlazado con el secreto de la comunicación. Como señala RODRÍGUEZ LAINZ, «la confidencialidad da contenido a lo que podríamos entender como dimensión interna del secreto de las comunicaciones»[84]. El TC se ha referido al citado vínculo declarando que «el fundamento del carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación»[85].

Con base en lo anterior, y siendo necesaria la existencia de algún medio con el que se produzca la comunicación y la de un tercero que de soporte al mismo, para que pueda desplegar efectos el amparo constitucional ofrecido por el art. 18.3 CE, será preciso que el medio permita una comunicación secreta entre dos o más personas, por lo que están excluidas de la protección las conversaciones que tengan lugar en medios de comunicación en los que intervienen multitud de personas como la radio o televisión.

---

[83] Vid. STS 236/2008, de 9 de mayo, FJ 2.º

[84] RODRÍGUEZ LAINZ, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», cit., p. 6.

[85] Vid. STC 281/2006, de 9 de octubre, FJ 3.º

Estarán, por tanto, afectadas por la garantía del derecho al secreto de las comunicaciones, debiendo respetar el mismo, todas las personas ajenas al proceso comunicativo, independientemente de que sean particulares o los agentes de la Policía Judicial en el curso de una investigación, no afectando la garantía del derecho a los intervinientes en la comunicación, y ello sin perjuicio de que pudiera quedar vulnerado el derecho a la intimidad de alguno de ellos[86].

3.3.4. Los datos de tráfico o asociados

A los elementos anteriores, deben añadirse los datos de tráfico o asociados, los cuales se encuentran protegidos por la obligación de confidencialidad de un tercero prestador de servicios de comunicación, y cuya interceptación o entrega a la Policía Judicial por parte del citado tercero prestador de servicios sin el consentimiento del afectado o en su defecto con el soporte de la correspondiente resolución judicial, supondría una vulneración del secreto de los referidos datos, lo que a su vez produciría una limitación del derecho al secreto de las comunicaciones.

El Convenio de Budapest facilitó una definición de los datos de tráfico en su art. 1.d), el cual establece que «por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente».

Por su parte, la LECrim, tras la reforma operada por la LO 13/2015, se ha ocupado de los que ha denominado «datos electrónicos de tráfico o asociados al proceso de comunicación», concretamente en el art. 588 ter b.2, cuyo último párrafo ofrece igualmente una definición de los mismos, al disponer que se entenderá por tales datos «todos aquellos que se generan como consecuencia de la conducción de la comunicación

[86] El no quedar afectadas las personas intervinientes en la comunicación por la garantía del derecho ya quedo sentado tras la emblemática STC 114/1984, de 29 de noviembre, FJ 7.º que declaró que «no hay "secreto" para aquel a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje». Declaró asimismo que «quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera "íntima" del interlocutor, pudiesen constituir atentados al derecho garantizado en el artículo 18.1 de la Constitución».

a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga».

Se trata por tanto de datos no coincidentes con el contenido de la comunicación, aunque pueden facilitar todos los elementos que la identifican, tales como los datos necesarios para para rastrear e identificar el origen de una comunicación; los necesarios para identificar su destino; los necesarios para determinar la fecha, hora y duración; los que sirven para identificar el tipo de comunicación, ya sea de voz, datos, mensajería o servicios multimedia; y finalmente los datos necesarios para identificar el equipo de comunicación de los usuarios.

La protección de los datos de tráfico por el derecho al secreto de las comunicaciones tiene su inicio con la STEDH de 2 de agosto de 1984, caso Malone c. Reino Unido, en la cual se determinó que los números de destino de las llamadas, recopilados por un sistema automático de recuento —denominado *comptage*—, aun cuando no suponen la interceptación del contenido de las conversaciones, son parte integrante de las comunicaciones telefónicas, y por tanto se encuentran protegidos por el derecho fundamental, por lo que no se puede disponer de los mismos sin el consentimiento de su titular[87].

En nuestro país, puede afirmarse que el *leading case* en relación a la protección de los datos de tráfico, lo constituye la STC 123/2002, de 20 de mayo, FJ 6.º, que siguiendo la referida doctrina del TEDH, estableció que los datos de tráfico «configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de

[87] Posteriormente el TEDH en la Sentencia de 3 de abril de 2007, caso Copland c. Reino Unido, declaró en su apdo. 43 «el Tribunal recuerda que la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el artículo 8, ya que dicha información es "parte de las comunicaciones telefónicas"». Y en el apdo. 44 señaló del mismo modo que «en consecuencia, el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, sin su conocimiento, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio».

carácter privado, puede asimismo poseer un carácter íntimo», declarando al mismo tiempo la necesidad de resolución judicial, en defecto del consentimiento del titular, para la cesión de los datos a la Policía Judicial en el marco de una investigación[88].

3.4. Secreto de las comunicaciones e investigación tecnológica

El derecho al secreto de las comunicaciones, como los demás derechos fundamentales no es absoluto, sino que se encuentra sujeto a unas limitaciones, como así ha sido señalado por la jurisprudencia, que ha declarado en numerosas resoluciones que en toda sociedad democrática existen determinados valores que pueden justificar, con las debidas garantías, su limitación, valores entre los que se incluye la prevención de las infracciones penales, como así lo dispone el apartado 2 del art. 8 del CEDH y lo ha declarado la jurisprudencia[89].

En este sentido, para una adecuada investigación del delito, la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, introdujo en nuestra legislación procesal penal, una nueva diligencia de investigación de carácter tecnológico limitativa del derecho al secreto de las comunicaciones, consistente en la intervención de las comunicaciones telefónicas en el ámbito de la instrucción de las causas penales[90], que se articuló mediante una nueva redacción del art. 579 de la LECrim.

---

[88] En relación con la necesidad de resolución judicial, la STC 123/2002, de 20 de mayo, FJ 6.º, declaró que «la aplicación de la doctrina expuesta conduce a concluir que la entrega de los listados por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. En efecto, los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión».

[89] Vid. por todas la STS 720/2017, de 6 de noviembre, FJ 6.º que declaró que «en toda sociedad democrática existen determinados valores que pueden justificar, con las debidas garantías, su limitación (art. 8º del Convenio Europeo). Entre estos valores se encuentra la prevención del delito, que constituye un interés constitucionalmente legítimo y que incluye la investigación y el castigo de los hechos delictivos cometidos, orientándose su punición por fines de prevención general y especial. El propio art 18.3 CE prevé la limitación del derecho al secreto de las comunicaciones mediante resolución judicial (STS n.º 246/1995, de 20 de febrero, entre otras muchas)».

[90] Con anterioridad a la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, únicamente se encontraba prevista en nuestra legislación la posibilidad de intervención de las comunicaciones telefónicas en la Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio, que en su art. 18, apartado 1.º dispone que «cuando la autorización del Congreso comprenda la

Actualmente, las vigentes diligencias de investigación tecnológica, y muy especialmente los registros informáticos pueden suponer una injerencia en el derecho, aunque no de una forma tan directa como con la interceptación de las comunicaciones telefónicas y telemáticas, por cuanto en determinados casos se plantearán dudas sobre el derecho fundamental afectado por la concreta intervención.

Como dijimos al ocuparnos de la delimitación entre el derecho al secreto de las comunicaciones y el derecho a la intimidad, la obtención de datos protegidos por el derecho al secreto de las comunicaciones, requiere en todo caso, a diferencia del derecho a la intimidad y por imposición del art. 18.3 CE, una expresa autorización judicial[91], pudiendo incurrir, en caso de realizar la diligencia sin la debida autorización, en la ilicitud prevista en el art. 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ).

El derecho al secreto de las comunicaciones es susceptible de ser vulnerado principalmente y de forma evidente con la intervención de las comunicaciones telefónicas y telemáticas, pero también con otras diligencias de investigación tecnológica en las que pueden ser captadas conversaciones orales o telemáticas, como así sucede con la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos[92], y de forma muy singular mediante los registros

---

suspensión del artículo dieciocho, tres, de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público», disponiendo asimismo en su apartado 2.º que «la intervención decretada será comunicada inmediatamente por escrito motivado al juez competente».

[91] La STC 145/2014, de 22 de septiembre, FJ 2.º declaró que «en relación con el derecho al secreto de las comunicaciones telefónicas, nuestra doctrina ha venido reiterando que las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga forman parte del contenido esencial del art. 18.3 CE. Dicho sintéticamente, éstas deben explicitar, en el momento de la adopción de la medida, todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Por ello, el órgano judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo».

[92] LÓPEZ ORTEGA, J. J., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (II): Captación y grabación de comunicaciones orales mediante dispositivos electrónicos. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización», *Formación a distancia-Consejo General del Poder Judicial*, n.º 3, 2016, p. 21. En relación con las diligencias de captación y grabación de comunicaciones orales, señala este autor que «la tercera modalidad de injerencia regulada en la LECRIM, a todas luces la más invasiva, es la captación y grabación de las conversaciones privadas (comunicaciones orales directas) del investigado en su domicilio o fuera de él (en la vía pública, en otro espacio abierto o en cualquier otro lugar cerrado). Aunque el

de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos, cuyas especiales particularidades, tal y como se dijo al inicio de este epígrafe, serán objeto de estudio en el capítulo dedicado a los registros informáticos.

4. Derecho a la protección de datos de carácter personal o autodeterminación informativa

4.1. Evolución y desarrollo del derecho

Dijimos, al estudiar con anterioridad el derecho a la intimidad, que, como consecuencia de la irrupción de las TIC, se ha producido una revisión del concepto de intimidad acorde a la nueva realidad, que ha propiciado una ampliación en su contenido, al haber sido superada la anterior concepción por las posibilidades que las TIC ofrecen para captar, conservar, procesar o difundir datos que afectan a cualquier ciudadano en su actividad diaria.

En la actualidad, son numerosos los datos de cualquier persona que circulan por la red ubicándose en registros de organismos o entidades con fines lícitos, tales como el domicilio, documento de identidad, correo electrónico, datos de su tarjeta de crédito, numerosas contraseñas utilizadas para el acceso a portales de proveedores de cualquier servicio o redes sociales, e incluso documentos confidenciales como puede ser

---

legislador, acertadamente, ha diferenciado el régimen de las diversas medidas de observación y vigilancia en función de su gravedad, pues no todas afectan del mismo modo y con la misma intensidad al derecho a la intimidad, al regular las vigilancias acústicas las ha equiparado a la interceptación de las comunicaciones telefónicas. La opción del legislador es lógica, no solo porque las conversaciones telefónicas son las que gozan del más alto nivel de protección, sino también porque tras la STC 145/2014 se ha puesto fin a un amplio debate doctrinal sobre el derecho constitucional afectado por la escucha y grabación de las conversaciones entre presentes (comunicaciones orales directas), situando el núcleo de la tutela constitucional en el ámbito del derecho al secreto de las comunicaciones (art. 18.3 CE), a cuyo régimen legal ahora se asimilan». Efectivamente la STC 145/2014, de 22 de septiembre, al resolver un caso relativo a las grabaciones realizadas al acusado en dependencias policiales, declaró en su FJ 7.º *in fine*, que "de todo lo expuesto se deduce que las grabaciones en dependencias policiales resultaron contrarias al art. 18.3 CE, deviniendo nula la prueba obtenida por ese cauce para todos aquellos que resultaron perjudicados penalmente por ella». No obstante, existe alguna opinión doctrinal que considera que, si el fundamento de la protección del secreto de las comunicaciones se encuentra en la especial vulnerabilidad que se deriva de un tercero intermediario, resultaría difícil entender que este derecho puede resultar afectado por la instalación de un micrófono o mecanismos de grabación de las conversaciones orales directas, quedando afectado en todo caso con esta concreta medida de investigación, el derecho a la intimidad. Vid. DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 458.

sencillamente el resultado de una analítica médica, un extracto bancario o la factura del proveedor de servicios de telefonía e internet, por citar algunos del amplio y heterogéneo elenco de los que podrían ser mencionados.

El uso indebido de tales datos, efectivamente, podría constituir una injerencia en el derecho a la intimidad, pero pronto se planteó, y ya nuestro constituyente de 1978 lo apreció así al redactar el art. 18.4 CE, el establecimiento de un derecho con nombre propio que protegiese a los ciudadanos del tráfico indebido de cualquier dato o conjunto de ellos de los que fuesen titulares, otorgando a cada individuo el poder de disponer sobre el destino a dar a los mismos.

Como acabamos de decir, y conforme afirma GALÁN MUÑOZ, el obligado punto de partida nos viene dado por nuestra Constitución, resultando ciertamente sorprendente que encontrándonos en el momento de su elaboración y promulgación en una época en la que la informática se encontraba en los inicios de su desarrollo e implantación, el constituyente español tuviese en cuenta la importancia y peligrosidad que el fenómeno podía representar para los ciudadanos, recogiendo una previsión y un mandato expreso dirigido al legislador para que adoptase las oportunas medidas legales protectoras ante los posibles abusos que se pudiesen llevar a cabo con las tecnologías de la información[93].

Efectivamente, el art. 18 CE, después de garantizar los derechos a la intimidad, personal y familiar, el honor y la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones, dispone en su cuarto y último apartado que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», estableciendo así una norma que no es posible encontrar, con la salvedad de una previsión similar en la Constitución portuguesa[94], en otros textos constitucionales anteriores ni tampoco en las normas internacionales relativas a los derechos fundamentales.

[93] GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2014, p. 206.

[94] Tal como apunta GALAN MUÑOZ, la Constitución portuguesa de 2 de abril de 1976, dispone en su art. 35 bajo la rúbrica «Utilización de la informática» lo siguiente: «1. Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones

Sin embargo, se necesitaba de una legislación de desarrollo, respecto de la cual el legislador no fue especialmente presto, regulándose inicialmente de manera insuficiente con la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que, en su redacción originaria, estableció en la posteriormente derogada disposición transitoria primera, que «en tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley».

En cualquier caso, y aunque el nuestro y el portugués fuesen los primeros textos constitucionales que se ocuparon de la materia, no puede decirse que en Europa no se tuviese en cuenta este importante asunto del tratamiento de los datos de carácter personal, dado que, con fecha 28 de enero de 1981 se aprobó el Convenio n.º 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, ratificado por España por instrumento de 27 de enero de 1984, que reguló de una forma amplia el tratamiento de los datos de carácter personal, estableciendo claramente su objeto en su art. 1, que bajo la rúbrica «Objeto y fin» dispuso que «el fin del presente Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")».

Como consecuencia del referido Convenio 108 del Consejo de Europa, en España se promulgó, como primera disposición que desarrolló con autonomía el art. 18.4 CE, la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que, aunque cumplía los requisitos para hacer efectivo el derecho[95], tuvo que ser adaptada a la normativa de la UE, que, el 24 de octubre de 1995,

---

políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos». Vid. GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», cit., nota al pie n.º 2.

[95] La derogada LO 5/1992, de 29 de octubre regulaba todos los aspectos de la protección del derecho a la protección de datos, siendo relevante destacar la creación, a través de la misma, de la actual Agencia Española de Protección de Datos, que regulaba en su título VI, promulgándose bajo su vigencia el RD 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, que se

aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, origen de la LO 15/1999, de 13 de diciembre de protección de datos de carácter personal (LOPD 1999).

Por otra parte, la normativa española ha sido indudablemente influida por la jurisprudencia del TEDH y del TC.

La STEDH de 26 de marzo de 1987 determinó, en relación con un registro secreto de la policía, que el mismo contenía datos relativos a la vida privada, y que tanto el almacenamiento como su comunicación suponían una violación del derecho al respeto de su vida privada garantizado por el artículo 8.1[96]. Por su parte, la STEDH de 7 de julio de 1989, declaró la violación del respeto a la vida privada y familiar al no facilitarse al recurrente los datos obrantes en un Ayuntamiento en relación con su infancia[97]. Asimismo, la STEDH de 25 de febrero de 1997, determinó que se había producido la violación del derecho a la vida privada por la difusión de la identidad y enfermedad de una persona, circunstancias que constaban en una sentencia y fueron comunicadas a la prensa[98].

En cuanto a la jurisprudencia de nuestro TC, fue especialmente relevante, del mismo modo que la del TEDH, por el apoyo que otorgaron al legislador para la configuración constitucional del derecho. Como primeros pronunciamientos que otorgaron el amparo por la infracción del art. 18.4 CE, cabe destacar la STC 254/1993,

---

mantuvo vigente con la LO 15/1999, de conformidad con su Disposición Transitoria 3.ª Por otra parte, la exposición de motivos de la LO 5/1992 llevó a cabo una minuciosa exposición en relación con la protección del derecho. Entre otros muchos aspectos señaló que «Los más diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado "dinero plástico", sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner solo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos».

[96] Vid. STEDH, de 26 de marzo de 1987, caso Leander c. Suecia, apdo. 48.

[97] Vid. STEDH, de 7 de julio de 1989, caso Gaskin c. Reino Unido, apdo. 49.

[98] Vid. STEDH, de 25 de febrero de 1997, caso Z c. Finlandia, apdo. 113.

de 20 de julio, en relación con la denegación a un ciudadano de una solicitud de información acerca de sus datos de carácter personal que obraban en ficheros automatizados de la Administración del Estado, o la STC 11/1998, de 13 de enero, en relación con un uso indebido por parte de una empresa del dato relativo a la afiliación sindical de un trabajador de la misma[99].

El siguiente paso de la UE, tras la Directiva 95/46CE, fue el de la incorporación del derecho a la protección de datos en la Carta de derechos fundamentales de la UE, cuya vigente redacción es la que se dio a la misma como consecuencia de su revisión en 2007 en Estrasburgo con carácter previo a la firma del Tratado de Lisboa.

La Carta tiene fuerza vinculante para todos los países de la Unión conforme al art. 6 del Tratado de la UE, excepto para Polonia y Reino Unido[100 y 101].

Tal y como se menciona en el sitio web de EUR-Lex, el cual da acceso al derecho y jurisprudencia de la Unión Europea (UE), la Carta reafirma, dentro del respeto de las competencias y misiones de la Unión así como del principio de subsidiariedad, los derechos que emanan, en particular, de las tradiciones constitucionales y las obligaciones internacionales comunes a los países de la UE, del CEDH, las Cartas Sociales adoptadas por la UE y por el Consejo de Europa, así como de la jurisprudencia del Tribunal de Justicia de la UE y del TEDH, añadiendo que,

[99] Cabe señalar que conforme se indica en el antecedente de hecho tercero de la STC 11/1998, de 13 de enero, resulta ilustrativo que la empresa había sido sancionada por los mismos hechos por la Agencia de Protección de Datos en resolución de 18 de diciembre de 1995, con una multa de 50.000.001 de pesetas (actualmente 300.506,06 €), por una infracción tipificada como muy grave en el art. 43.4 c) de la en aquel momento todavía no derogada Ley Orgánica 5/1992, de 29 de octubre.

[100] El Tratado de la UE, firmado en la ciudad neerlandesa de Maastricht el 7 de febrero de 1992, ha sido objeto de tres revisiones, siendo la primera la que tuvo lugar con el Tratado de Amsterdam, firmado el 2 de octubre de 1997, la segunda con el Tratado de Niza de 14 de febrero de 2000 y la tercera con el Tratado de Lisboa, firmado el 13 de diciembre de 2007 y en vigor desde el 1 de diciembre de 2009. Dispone su art. 6.1 que «la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la UE de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados».

[101] Polonia y Reino Unido con carácter previo a la aprobación del Tratado de Lisboa introdujeron el protocolo n.º 30, conforme al cual y tal y como se dispuso en su art. 2 «cuando una disposición de la Carta se refiera a legislaciones y prácticas nacionales, sólo se aplicará en Polonia o en el Reino Unido en la medida en que los derechos y principios que contiene se reconozcan en la legislación o prácticas de Polonia o del Reino Unido».

al dar mayor visibilidad y claridad a los derechos fundamentales, establece una seguridad jurídica dentro de la UE[102].

El derecho a la protección de datos de carácter personal se encuentra proclamado en el art. 8 de la Carta, que bajo la rúbrica «protección de datos de carácter personal», dispone que: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

Posteriormente, la UE ha desarrollado una importante labor legislativa en materia de protección de datos. Así, el 12 de julio de 2002, como complemento a la Directiva 95/46/CE, se aprobó la Directiva 2002/58/CE, de tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas, con la pretensión de armonizar las disposiciones de los estados miembros necesarias para garantizar un nivel equivalente de protección; en particular, en relación con el derecho a la intimidad , en lo que respecta al tratamiento de los datos personales de las comunicaciones electrónicas.

Asimismo, el 15 de marzo de 2006, fue publicada la Directiva 2006/24/CE, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o redes públicas de comunicaciones, por la que se modifica la Directiva 2002/58/CE. Esta directiva fue traspuesta a nuestro ordenamiento con la promulgación 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[103].

Más recientemente, en la UE se ha dictado el vigente Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de

[102] El sitio web de EUR-Lex se encuentra en la dirección https://eur-lex.europa.eu/homepage.html. La cita mencionada en relación con la Carta de derechos fundamentales de la Unión Euiropea, se encuentra en la extensión de la anterior https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al33501. Acceso el 22 de octubre de 2018.

[103] La Directiva 2006/24/CE, de 15 de marzo fue anulada por el Tribunal de Justicia de la UE por Sentencia de 8 de abril de 2014 dictada en los asuntos acumulados C-293/12 y C-594/12, pese a lo cual la Ley 25/2007, de 18 de octubre que la traspuso, sigue vigente.

las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPDUE), que deroga la Directiva 95/46/CE, encontrándose vigente desde el 25 de mayo de 2018. Asimismo se ha aprobado el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

Con la aprobación del RGPDUE, y con la finalidad de adaptar al mismo el ordenamiento jurídico español, se ha promulgado en nuestro país la vigente LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[104] (LOPD 2018), que ha derogado la LOPD 1999 excepto en los supuestos previstos en la disposición adicional decimocuarta (arts. 23 y 24) y la disposición transitoria cuarta, refiriéndose ésta última al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación y detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales[105].

[104] La vigente LOPD 2018, conforme a su preámbulo pretende lograr la adaptación del ordenamiento jurídico español al RGPDUE y completar sus disposiciones, estableciendo en su art. 1.a) que «el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el art. 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica». Es de destacar, asimismo, que conforme se establece en el preámbulo de la LOPD 2018 «el Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa», añadiendo que «procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios».

[105] Dispone la disposición adicional decimocuarta de la LOPD 2018 que «las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas». Por su parte la Disposición transitoria cuarta de la LOPD 2018 dispone que «los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva».

Por tanto, actualmente la norma prevalente en materia de protección de datos viene constituida por el RGPDUE con las adaptaciones del ordenamiento jurídico español llevadas a cabo por la LOPD 2018 y las disposiciones que se mantienen vigentes de la LOPD 1999.

Finalmente debe señalarse que, el 27 de abril de 2016, el Parlamento Europeo y el Consejo aprobaron la Directiva 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. El plazo de transposición finalizó el 6 de mayo de 2018, sin que se haya producido, habiéndose declarado vigente, conforme hemos señalado en el párrafo anterior, la LO 13/1999 hasta que se produzca. En relación a la misma, cabe señalar que, según consta en el Plan Normativo del Gobierno para el año 2018, se encuentra prevista su incorporación al ordenamiento interno a través de una LO sobre el tratamiento de datos personales para fines policiales y judiciales penales[106].

4.2. Régimen jurídico básico del derecho a la protección de datos de carácter personal

La idea fundamental en virtud de la cual puede desplegar sus efectos el derecho fundamental a la protección de datos, radica en la circunstancia de que para la recogida, tratamiento y cesión de los datos de otra persona, se debe disponer del consentimiento de la misma.

El artículo 4.11 RGPDUE establece que se entenderá por consentimiento del interesado «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». En relación con el consentimiento del interesado, el considerando n.º 32 RGPDUE prevé que «el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de

[106] El Plan Normativo del Gobierno para 2018 ha sido obtenido de la página web http://www.lamoncloa.gob.es/consejodeministros/referencias/documents/2017/refc20171207e_4.pdf encontrándose la citada previsión en la página 9 del mismo. Acceso a la página web el 15 de julio de 2020.

aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal».

Por su parte, el art. 9.1 RGPDUE prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física, excepto en los supuestos relativos al interés general que se detallan en el apartado 2 del citado precepto y en aquellos casos en los que el interesado hubiese dado su consentimiento explícito para el tratamiento de dichos datos personales, siempre y cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada no puede ser levantada por el interesado.

Por lo que a la investigación del delito se refiere, no será requisito imprescindible el consentimiento del interesado para la recogida y tratamiento de los datos personales, teniendo en cuenta además, que, por lo que respecta a la comunicación de datos a un tercero, el art. 11.2.a LOPD 1999 —que se encuentra vigente, tal y como hemos dicho en el apartado anterior, para los fines de prevención, investigación y detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales— dispone que no será preciso el consentimiento cuando «la cesión está autorizada en una ley», no siendo tampoco necesario el consentimiento de conformidad con el art. 11.2.d LOPD 1999 cuando «la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas»[107].

[107] Señala PÉREZ GIL, para diferenciar el tratamiento de datos de la recogida y cesión de los mismos, que el tratamiento se refiere a una operación o conjunto de operaciones sobre datos que deben encontrarse estructurados, ser accesibles y estar almacenados en ficheros, cronológicamente intermedio entre la recogida y su eventual conclusión, por lo que «lo relevante es observar que cuando la obtención de datos constituya la recopilación inicial de los mismos, estaremos ante un supuesto de recogida, mientras que será cesión cuando sea posterior en el tiempo al tratamiento». Indica el autor que se trata de una distinción de notable trascendencia, habida cuenta del diferente grado de injerencia en el derecho a la protección de datos de carácter personal, de la recogida y tratamiento en relación con la cesión, la cual constituye una actuación más gravosa para el titular de los datos que la mera recogida, siendo mayor su potencialidad lesiva del derecho a la protección de los datos de carácter personal. Esa diversa intensidad justifica que el art. 11 LOPD establezca precauciones suplementarias en relación con la cesión al marcar una serie de supuestos tasados en los que cabe prescindir del consentimiento del titular de los datos. PÉREZ GIL, J.; GONZÁLEZ LÓPEZ, J. J., «Cesión de datos personales para la investigación penal. Una propuesta para su

Como limitación al ejercicio de las tareas propias de las FCSE, de conformidad con el art. 22.2 LOPD 1999, «la recogida y tratamiento para fines policiales de datos de carácter personal por las FCSE sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad», estableciendo finalmente el art. 22.4 LOPD 1999 que «los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento», debiéndose considerar a estos efectos especialmente «la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad».

En cuanto al tratamiento de datos en el ejercicio de la potestad jurisdiccional, no será necesario el consentimiento del interesado, ya sean facilitados los datos por las partes o recabados a solicitud del propio tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba. Sin embargo, cuando se trate de datos tratados con fines no jurisdiccionales, se estará a lo dispuesto en la LOPD —debiendo entender ahora la remisión al RGPDUE y LOPD 2018— (art. 236 quáter LOPJ).

4.3. Autonomía de la protección de datos frente al derecho a la intimidad

Tal y como afirma DÍEZ-PICAZO GIMÉNEZ, el mandamiento constitucional de limitación del tratamiento de datos, en principio es una garantía para la efectividad de los derechos al honor y a la intimidad, conforme se expresa por el propio art. 18.4 CE, pesando en este sentido sobre el legislador un mandato para que la regulación del tratamiento de datos se realice de forma respetuosa con los derechos fundamentales[108].

Sin embargo, aunque inicialmente se pudo entender este derecho como una variedad del derecho a la intimidad, pronto el TC determinó la autonomía de la

inmediata inclusión en la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Doctrina*, n.º 7401, 2010, p. 10.

[108] DÍEZ-PICAZO GIMÉNEZ, L. M., «*Sistema de Derechos Fundamentales*», cit., p. 308.

protección de datos de carácter personal respecto del derecho a la intimidad, no obstante la estrecha relación mantenida entre ambos.

Aun así, debe destacarse que, a nivel jurisprudencial, tuvo una gran relevancia para la consolidación de la autonomía del derecho, la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983[109], que formuló el concepto de «autodeterminación informativa», el cual, posteriormente, ha sido usado por nuestro TC al ocuparse de la aludida delimitación entre ambos derechos.

Afirma HOFFMANN-RIEM que «este nuevo derecho fundamental se convirtió en la base de la moderna legislación alemana de protección de datos, en particular de las leyes generales de protección de datos, así como de numerosas reglas especiales sobre la protección de datos personales y de la consiguiente jurisprudencia»[110].

La derogada LO 5/1992, de 29 de octubre, estableció el criterio básico diferenciador, reproducido en la LOPD 1999, disponiendo ambas normas orgánicas, en su art. 3.a, que se entenderá por datos de carácter personal «cualquier información concerniente a personas físicas identificadas o identificables».

Por su parte, el RGPDUE establece, en su art. 4.1, que se entenderá por «datos personales», toda información sobre una persona física identificada o identificable («el interesado»), considerando como tal «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Por tanto, el acceso no autorizado a documentos o archivos en los que no consten datos que se refieran a personas identificadas o identificables, ha de entenderse como

[109] La Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 se dictó como consecuencia de la controversia que se produjo en torno a la recolección de datos estadísticos conforme a la Ley del Censo, datos anónimos como el nombre y apellidos, domicilio, situación económica, profesión, etc., respecto de los cuales se declaró la facultad del individuo de decidir por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a su propia vida.

[110] HOFFMANN-RIEM, W., «Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la sociedad de la información», *Revista de Derecho Constitucional Europeo*, vol. 11, n.º 22, 2014, p. 131.

una injerencia en el derecho a la intimidad del art. 18.1 CE, pero no como una vulneración del derecho a la protección de datos de carácter personal del art. 18.4 CE.

En todo caso, ha tenido especial importancia la delimitación de ambos derechos que llevo a cabo la jurisprudencia, siendo de destacar la STC 254/1993, de 20 de julio, FJ 6.º, que declaró que aunque nos encontramos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, estamos igualmente ante «un derecho o libertad fundamental, el derecho a la libertad frente a 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».

Especialmente relevante es, asimismo, la STC 292/2000, de 30 de noviembre, que declaró que, a diferencia del derecho fundamental a la intimidad del art. 18.1 CE, cuya finalidad es la de proteger frente a cualquier invasión que pueda realizarse en el ámbito de la vida privada, «el derecho fundamental a la protección de datos persigue garantizar a esa persona un 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», lo que «impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías», sin que el objeto de este derecho fundamental quede reducido solo a los datos íntimos de la persona «sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal», es decir, «todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo»[111].

De este modo, a partir principalmente de estas resoluciones del TC, se va conformando el derecho a la autodeterminación informativa o *habeas data*, entendido como el derecho de cualquier persona para solicitar y obtener la información que sobre su persona obre en cualquier base de datos, pública o privada, informática o no, con la

[111] STC 292/2000, de 30 de noviembre, FJ 6.º

potestad para que se proceda a su eliminación o actualización[112], teniendo en cuenta que, como afirma BAYO DELGADO, «la protección de datos parte de la idea de que los datos pertenecen al sujeto a quien se refieren, sobre los que debe mantener su control (habeas data), salvo excepciones legalmente previstas»[113].

El control del individuo en todo momento sobre sus datos personales, hace que el derecho presente un contenido con una vertiente positiva y otro con sentido negativo. De forma positiva, el derecho confiere un poder de acceso a los datos relativos a uno mismo, independientemente de la ubicación donde se encuentren, así como a su cancelación o actualización. Por su parte, su contenido negativo comporta una facultad de oponerse a cualquier utilización de los mismos para fines distintos para los que fueron almacenados.

Este doble contenido del derecho a la protección datos constituye otro de los aspectos que muestran su autonomía respecto del derecho a la intimidad, como igualmente lo ha señalado la STC 292/2000, de 30 de noviembre, al declarar que «el derecho a consentir el conocimiento y el tratamiento informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos»[114].

4.4. Datos de tráfico o asociados y protección de datos de carácter personal

4.4.1. La doble naturaleza de los datos de tráfico o asociados

Al ocuparnos del derecho al secreto de las comunicaciones en el apartado 3.3.4, nos referimos a los datos de tráfico o asociados como un elemento de la comunicación protegido por el secreto de las comunicaciones, que puede tener un gran valor para la

[112] Resulta muy ilustrativa la definición que la STC 96/2012, de 7 de mayo, FJ 6.º, realiza del derecho a la protección de datos del art. 18.4 al declarar que «la llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención» y añadió en el FJ 7.º que se refiere a cualquier dato que sea relevante o tenga incidencia en el ejercicio de cualesquiera derechos de la persona «sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado».

[113] BAYO DELGADO, J., «La protección de datos en la investigación policial y en el proceso penal», *Jueces para la Democracia. Información y Debate*, n.º 63, 2008, p. 11.

[114] STC 292/2000, de 30 de noviembre, FJ 7.º

investigación penal. Sin embargo, son muchas las voces, a las que ya podemos adelantar que nos adherimos, que se inclinan por considerar una buena parte de los datos de tráfico o asociados como integrantes del contenido del derecho a la protección de datos de carácter personal.

Así, por ejemplo, MARCHENA GÓMEZ afirma que «es seguro que algunos de esos datos merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Pero todos, desde luego, no son susceptibles de esa etiqueta»[115]. Y es que, efectivamente, el alcance constitucional de los derechos a la intimidad, a la inviolabilidad de las comunicaciones y a la protección de datos no es equivalente, tratándose de derechos «de distinto significado axiológico y, por tanto, sometidos en su restricción a un régimen jurídico no siempre idéntico[116].

En el mismo sentido, la jurisprudencia ya destacó en alguna sentencia que algunos de los datos de tráfico deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18.3 CE), sino en el marco del derecho a la intimidad personal (art. 18.1 CE) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal[117].

Se trata de una distinción de gran relevancia, dado el distinto alcance constitucional de los derechos del art. 18 CE[118], debiéndose tener en consideración

[115] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuellar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, p. 287.

[116] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 287.

[117] Vid. STS 247/2010, de 18 de marzo, FJ 2.º que declaró que «a nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina *(obiter dicta)*, los datos identificativos de un titular o de un terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18.3 CE) sino en el marco del derecho a la intimidad personal (art. 18.1 CE) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal, LO 15/1999 de 13 de diciembre: art. 11.2 d. o su Reglamento, RD 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, R.D. 424 de 15 de abril de 2005, en los que parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal».

[118] Señala a este respecto la Circular 1/2013 de la FGE que «desde luego, no todos los datos digitalizados merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Debe analizarse la funcionalidad de cada dato para ubicarlo bajo el manto protector del

primordialmente, que, para la injerencia en el derecho a la protección de datos, al igual que sucede con el derecho a la intimidad, el art. 18.4 CE no se exige autorización judicial, existiendo un régimen más flexible para la intromisión en la intimidad y protección de datos que cuando se trata del derecho al secreto de las comunicaciones[119].

Además, como ya se dijo anteriormente, la LOPD 1999 exceptúa del consentimiento del titular la cesión de los datos cuando la comunicación deba efectuarse o tenga por destinatarios al Ministerio Fiscal o los jueces o tribunales, estableciendo asimismo que la recogida y tratamiento para fines policiales de datos de carácter personal por las FCSE sin consentimiento de las personas afectadas, quedan limitadas a los supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales (arts. 11.2.d y 22.2 LOPD 1999).

4.4.2. La obligación de conservación y la cesión de datos

Podríamos preguntarnos, tal y como plantea PEDRAZ PENALVA, si realmente es necesaria una previsión normativa en cuanto al deber de cesión de datos personales, cuando los mismos fuesen requeridos en virtud de una investigación penal en virtud de la obligación impuesta por el art. 118 CE[120].

Como acabamos de señalar, los arts. 11.2.d y 22.2 LOPD 1999 permiten la cesión de datos sin consentimiento del titular cuando los destinatarios sean el Ministerio Fiscal o los jueces o tribunales, así como las FCSE en los casos indicados, lo cual

---

derecho a la intimidad (art. 18.1 CE), del derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE) o del derecho a la protección de datos (art. 18.4 CE), cada uno con su propio sustrato axiológico y, correlativamente, cada uno con una protección de intensidad variable». Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., p. 19.

[119] Tal y como se señaló al ocuparnos de la delimitación entre el derecho al secreto de las comunicaciones y el derecho a la intimidad, y conforme declaró la STC 70/2002, de 3 de abril, FJ 10.º, es necesaria la autorización judicial conforme a criterios de proporcionalidad, si bien esa regla se excepciona en aquellos casos en los que existan razones de intervención policial inmediata, lo cual se hace extensivo a la protección de datos de carácter personal pero no así respecto de las injerencias en el derecho al secreto de las comunicaciones.

[120] PEDRAZ PENALVA, E., «La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva», en Pedraz Penalva, E. (coord.), *Protección de datos y proceso penal*, Madrid, Wolters Kluwer, 2010, p. 35.

implica que dichos datos se ceden cuando son solicitados en el marco de una investigación criminal.

Sin embargo, tratándose de un derecho fundamental con la protección reforzada del art. 53.2 CE, de acuerdo con la doctrina del TEDH —que puso de manifiesto la insuficiencia normativa del art. 579 LECrim en relación con el derecho al secreto de las comunicaciones— no era suficiente una previsión tan genérica[121 y 122]. Este criterio lo consideramos aplicable al derecho a la protección de datos de carácter personal, pudiendo afirmarse, tal y como examinaremos más adelante, que con la promulgación de la LO 13/2015 se ha cumplido con tal obligación de previsión normativa.

Por otra parte, ha de tenerse en cuenta que para que los datos de tráfico o asociados generados como consecuencia de las comunicaciones realizadas por telefonía fija, móvil o por internet, a través de correo electrónico o los datos generados por la simple conexión a internet, puedan cederse para los fines de la investigación criminal, estos han de conservarse por las operadoras. Tal obligación de conservación se dispuso con la promulgación de la Ley 25/2007, de 18 de octubre, a la que nos referiremos a continuación.

4.4.3. Breve examen de la Ley 25/2007 de conservación de datos

El legislador —por lo que respecta, ya no a todos los datos o ficheros de carácter personal, sino a los datos que han de ser conservados por las operadoras— promulgó la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la cual tenía como primer objetivo la transposición de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en

[121] Afirma PEDRAZ PENALVA que para fundar este tipo de injerencias no parece suficiente con una mera habilitación normativa, sin que la prevención de un «peligro real» para la seguridad pública o el comienzo de una investigación policial de un pretendido injusto penal, con genérico apoyo en el deber de colaboración con la Justicia, no puede ser bastante para obligar a terceros a ceder los datos personales sin una más precisa prescripción legal que fije los parámetros, requisitos específicos y mecanismos de control. PEDRAZ PENALVA, E., «La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva», cit., p. 51.

[122] Las primeras resoluciones del TEDH que pusieron de manifiesto la insuficiencia de previsión normativa fueron las Sentencias de 24 de abril de 1990, casos Kruslin y Huvig c. Francia, que declararon que «la ley debe ser lo suficientemente clara para señalar a todos las circunstancias y condiciones en que autoriza a los Poderes públicos a recurrir a una injerencia así, secreta y posiblemente peligrosa, en el derecho al respeto de la vida privada y de la correspondencia».

relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[123].

En su preámbulo, la Ley 25/2007 declara que es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional (TC), respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

4.4.3.1. La obligación de conservación y cesión de datos por parte de las operadoras

El propósito de la Ley 25/2007 queda fijado en su primer precepto, el art. 1.1, que dispone que «esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales».

La obligación de conservar los datos se establece en el art. 4.1 de la Ley 25/2007, que dispone que «los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate», mientras

[123] Aun cuando el primer objetivo de la Ley 25/2007 era la transposición de la Directiva 2006/24/CE, no deja de resultar llamativo que el legislador haya regulado una materia que afecta al derecho al secreto de las comunicaciones y a la protección de datos de carácter personal mediante una ley ordinaria. Esta circunstancia ha sido puesta de manifiesto por el TS, que en la STS 249/2008, de 20 de mayo, FJ 4.º, declaró que «en principio, no deja de llamar la atención la clamorosa insuficiencia, desde el punto de vista de su jerarquía normativa, de una ley que, regulando aspectos intrínsecamente ligados al derecho al secreto de las comunicaciones, y a la protección de datos personales, no acata lo previsto en el art. 81.1 de la CE».

que, en cuanto a la cesión de dichos datos, dispone el art. 6.1 que «los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial».

El art. 5.1 fija una obligación de conservación por un plazo de doce meses computados desde la fecha en que se haya producido la comunicación. No obstante, de forma reglamentaria, se podrá ampliar o reducir dicho plazo para conservación de determinados datos, hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.

4.4.3.2. La polémica tras la derogación de la directiva 2006/24/CE

La Ley 25/2007 ha sido objeto de una particular polémica desde el 8 de abril de 2014, fecha en la que, como consecuencia de sendas cuestiones prejudiciales planteadas por los tribunales de Irlanda y Austria, se dictó la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) por la que se decretó la nulidad de la Directiva 2006/24/CE por constituir la misma «una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario»[124], lo cual ha originado la controversia acerca de si la nulidad de la referida directiva debe reflejarse igualmente en la Ley 25/2007 como norma de desarrollo en nuestro país.

[124] Sentencia del TJUE de 8 de abril de 2014, apdo. 65. Cabe señalar, además, que en su apartado 51 la referida sentencia establece que si bien es cierto que la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización de técnicas modernas de investigación, ello no puede justificar por sí solo que una medida de conservación como la establecida por la Directiva 2006/24 se considere necesaria a los efectos de dicha lucha. Y añade en su apdo. 54 que por lo anterior, la normativa de la Unión de que se trate, debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas, de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos.

No es objeto de este trabajo, por exceder de sus pretensiones, el examen de los argumentos a favor y en contra de la nulidad o no de la referida Ley[125], aunque no cabe ninguna duda de que el legislador no ha tenido, por el momento, la intención de reformar la misma para adaptarla a las exigencias de la Sentencia del TJUE de 8 de abril de 2014, sino que, por el contrario, al promulgar con posterioridad a la misma la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se remite en lo que se refiere a la conservación y cesión de datos a lo establecido en la Ley 25/2007[126], manteniendo por tanto su vigencia.

En cualquier caso, no nos parece que pueda invocarse de forma determinante la nulidad de la ley que transpone una directiva por el hecho de que ésta lo haya sido, por lo que nos inclinamos, más bien, por la autonomía de la ley nacional en virtud de la cual se ha transpuesto la directiva. Nos adherimos, en la línea indicada, a opiniones como la de RODRÍGUEZ LAINZ, quien afirma que, aunque se ha de partir de un principio de la primacía de la directiva, «una vez entre en vigor la norma nacional respetuosa de aquélla, adquiere autonomía en cuanto respecta a su vigencia»[127], añadiendo que «haría falta una nueva norma interna o comunitaria que así lo dispusieran, dentro de los ámbitos de sus respectivas competencias y fuerza normativa de los correspondientes instrumentos legales, para que la norma nacional perdiera su vigencia»[128].

Resulta muy ilustrativo, el Informe del Consejo Fiscal de la FGE al Anteproyecto de la LO 13/2015, en el que se declaró la conformidad con el mantenimiento del sistema instaurado por la Ley 25/2007, consistente en exigir en todo

---

[125] En relación con esta cuestión, MARCHENA GÓMEZ realiza un resumen de distintas opiniones que avalarían la nulidad y de otras que propugnarían la autonomía de la Ley 25/2007 sobre la Directiva 2006/24/CE. Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., pp. 294-296.

[126] El art. 42 de la Ley 9/2014, de 9 de mayo General de Telecomunicaciones, dispone que «la conservación y cesión de los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones».

[127] RODRÍGUEZ LAINZ, J. L., «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley - Sección Doctrina*, n.º 8308, 2014, p. 4.

[128] RODRÍGUEZ LAINZ, J. L., «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», cit., p. 4.

caso autorización judicial, al considerar que el mismo se adecúa a la doctrina sentada por la propia Sentencia del TJUE de 8 de abril de 2014, que aboga por el control judicial de dicha cesión a fin de garantizar adecuadamente los derechos fundamentales a la intimidad y a la protección de datos[129].

4.4.3.3. Problemas en relación con la gravedad del delito

De acuerdo con lo indicado anteriormente, de conformidad con el art. 1.1 de la Ley 25/2007, uno de los requisitos para la cesión de datos de tráfico lo constituye la circunstancia de que los datos se recaben para la detección, investigación y enjuiciamiento de delitos graves, lo que ha planteado ciertos problemas en relación con la interpretación que ha de darse a dicha gravedad del delito, postulándose criterios que defienden que esta se ha de fijar según el concepto de delito grave de nuestro CP, frente a otros que abogan por el establecimiento de la gravedad del delito según las circunstancias que rodean el hecho delictivo en cada caso y la mayor o menor injerencia en el derecho fundamental.

La primera posición, tiene su sustento en la literalidad de la propia Ley 25/2007, que en su art. 1.1 determina que se podrán ceder los datos para la detección, investigación y enjuiciamiento de delitos graves «contemplados en el Código Penal o en las leyes penales especiales», existiendo en defensa de este criterio diversos pronunciamientos de la jurisprudencia menor[130] así como algunas opiniones doctrinales[131]. Por tanto, de seguirse esta doctrina, constituirían delitos graves a los

[129] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, *Informe 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 tecnológica*, 2015, p. 90. Consultado en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_CF_MODIFICACIÓN_LECrim_23-01-2015.pdf?idFile=7c2cd525-01bf-4cc0-864a-29dc8ee0dae9, el 7 de marzo de 2018.

[130] Vid. Auto de la Audiencia Provincial (AAP) 909/2012, Sección 3.ª de Barcelona, de 28 de septiembre, FJ 1.º, que señaló que «no existe razón alguna que justifique una interpretación del precepto contrario a su tenor literal»; AAP 508/2011, Sección 4.ª de Pontevedra, de 30 de noviembre, FJ 2.º que declaró que «aun cuando se calificasen los hechos como delito, habría que determinar si nos hallamos ante un delito grave o no, habida cuenta de la graduación que de las infracciones penales realiza el texto punitivo en su art. 13 en relación con el art. 33 del mismo Código»; y AAP 418/2011, Sección 6.ª de Madrid, de 8 de julio, FJ 2.º que declaró que «la referida Ley es muy clara y contundente, y se refiere únicamente a la investigación de delitos graves, remisión que conduce a lo previsto en el artículo 13 y 33 del Código Penal, esto es, a aquellos en que la pena señalada para el delito sea de prisión superior a cinco años».

[131] Tras reconocer que estamos ante una de las cuestiones problemáticas que plantea la regulación contenida en la Ley 25/2007, pues la equiparación entre «delito grave» y la «gravedad de los hechos de

efectos de la cesión de datos, los establecidos de conformidad con los arts. 13 y 33 del CP, entre los que se incluyen los penados con prisión superior a cinco años.

Respecto a la segunda posición, cabe señalar en primer lugar que, con carácter general, el TC se ha pronunciado en relación con la gravedad del delito declarando que «la infracción punible no puede estar determinada únicamente por la calificación de la pena legalmente prevista, aunque indudablemente es un factor que debe de ser considerado, sino que también deben tenerse en cuenta otros factores, como los bienes jurídicos protegidos y la relevancia social de aquélla»[132], existiendo algún pronunciamiento del TS a favor de la determinación de la gravedad del delito según la trascendencia social del delito que se trata de investigar[133].

Asimismo, por lo que se refiere a los delitos relacionados con las nuevas tecnologías, el TC determinó que «más allá de la pena señalada al delito investigado, resultan evidentes la enorme trascendencia y repercusión social de las conductas objeto de investigación, por tratarse de cuestión íntimamente relacionada con la del uso y abuso de las nuevas tecnologías, y el grave perjuicio económico que son susceptibles de generar»[134].

---

que se trate» podría ampliar o restringir el ámbito de aplicación de la norma, dejando «al albur de los juzgados y Tribunales la interpretación de términos difusos susceptibles de ser dilucidados de muy diferentes maneras», GALLEGO SÁNCHEZ señala que «los componentes de nuestro Foro se inclinan por una interpretación que se atenga "al sentido literal de la norma remitiéndonos a la definición que se establece en el artículo 13 del C.P. y su correlativo artículo 33"». Vid. GALLEGO SÁNCHEZ, G. Y OTROS, «El «delito grave» en relación a la obligación de conservación de datos, según la Ley 25/2007 y las reformas penales recientes», *Revista de Jurisprudencia - El Derecho*, n.º 1, Noviembre, 2015.

[132] Vid. STC 299/2000, de 11 de diciembre, FJ 2.º que declaró que «en este sentido no cabe sostener que, cuando el contrabando de tabaco se realiza a gran escala a través de una organización, lo que constituía objeto de la investigación policial en este caso, merece un reproche social muy escaso, dada la incidencia de tal actividad, no sólo sobre los intereses recaudatorios de la Hacienda Pública, sino también sobre la finalidad extrafiscal inherente a la imposición específica sobre consumos, justificada en el caso del tabaco por los costes sociales, sanitarios en concreto, que genera por tratarse de un producto perjudicial para la salud […] a la hora de ponderar la relevancia social de los hechos y su gravedad, el elemento de que sean organizaciones complejas las que se dedican a su comisión es, sin duda, un factor de suma importancia a atender, por la potencial eficacia de dichas organizaciones en su embate contra los intereses sociales y públicos garantizados por la legalidad que atacan».

[133] Vid. Auto del Tribunal Supremo (ATS) 353/2017, de 2 de febrero, FJ 1.º, que declaró que «para valorar la gravedad no solo es preciso atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar».

[134] Vid. STC 104/2006, de 3 de abril, FJ 4.º

Autores como ORTIZ PRADILLO, han interpretado esta declaración del TC en el sentido de que la «incidencia del uso de las tecnologías de la información, tanto para la perpetración del delito como para la obstrucción a su persecución, se considera igualmente un criterio válido a la hora de entender que nos encontramos ante un delito grave a efectos de legitimar el recurso a la limitación del derecho fundamental al secreto de las comunicaciones, al admitirse la idoneidad de determinadas medidas de investigación basadas en las TIC para investigar aquellos delitos perpetrados a través o con ayuda de las telecomunicaciones»[135].

Se pueden mencionar del mismo modo algunos pronunciamientos de la jurisprudencia menor reclamando que algunos delitos, aun cuando no superen la penalidad prevista en el CP para los delitos graves, sean susceptibles de tener tal consideración por su repercusión[136].

Por otro lado, es de destacar igualmente, que, doctrinalmente, se han pronunciado voces que reclamaban que una previsión como la del art. 1.1 de la Ley 25/2007 no es satisfactoria precisamente para el descubrimiento y sanción de delitos cometidos por medios informáticos. Así, por ejemplo, MORENO CATENA afirma que con esta norma no sería posible solicitar la entrega de esos datos para investigar posiblemente uno de los tipos delictivos a los que sería de más directa y relevante aplicación, los delitos de pornografía infantil, pues la pena señalada al tipo básico de los mismos no supera los cinco años (art. 189.1 CP)[137].

---

[135] ORTIZ PRADILLO, J. C., «Comunicaciones, tecnología y proceso penal: Viejos delitos, nuevas necesidades», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, p. 24.

[136] Vid. Sentencia de la Audiencia Provincial (SAP) 13/2014, Sección 2.ª de Cáceres, de 16 de enero, FJ 3.º que declaró que «no ha de quedar extramuros de la posible utilización procesal de la información almacenada sobre datos relativos a las comunicaciones la investigación criminal relativa, por ejemplo, al tráfico de sustancias estupefacientes que no causaran grave daño a la salud, a los delitos contra el patrimonio de cierta trascendencia social, a la protección del patrimonio histórico, a la utilización de menores con fines pornográficos […] o, conforme a la doctrina desarrollada por la STC 104/2006, de 3 de abril, la investigación de modalidades delictivas que se prevalgan de las posibilidades de anonimato que brinda internet para su comisión y difusión, aunque siempre dentro de un contexto de relativa gravedad o relevancia social»; y AAP 572/2013, Sección 30.ª Madrid, de 11 de julio, FJ 1.º, que declaró que «para valorar la gravedad del delito, de acuerdo con una interpretación teleológica y sistemática de la norma, no solo se debe atender a la previsión legal de una pena privativa de libertad grave, sino que además debe valorarse la trascendencia social del delito que se trata de investigar».

[137] MORENO CATENA, V., «Ley de conservación de datos y garantías procesales», en Domínguez Peco, E. (coord.), *La protección de datos en la cooperación policial y judicial*, Cizur Menor (Navarra), Editorial Aranzadi, 2008, p. 169.

En atención a lo expuesto, se ha impuesto la doctrina conforme a la que la gravedad del delito se ha de valorar de una forma independiente a las normas del CP y ello, por cuanto, tal y como señaló el AAP 572/2013, Sección 30.ª Madrid, de 11 de julio, FJ 1.º, «el Código Penal de 1995, al establecer la distinción entre delitos graves y menos graves en función de la pena asignada, con consecuencias, por ejemplo, en relación con la competencia judicial, no pretendió anudar a la misma la posibilidad de practicar diligencias restrictivas de derechos fundamentales. Estas han de adoptarse por los órganos judiciales en función de parámetros de gravedad, proporcionalidad y necesidad de la medida, en los términos que ha ido delimitando la jurisprudencia constitucional».

Por nuestra parte, consideramos que, para de determinar la gravedad del delito a los efectos de la orden de conservación y cesión de datos de tráfico o asociados, los juzgados y tribunales deben atenerse a las circunstancias concretas de cada caso, haciendo nuestras las razones expuestas.

A ellas, podríamos añadir en primer lugar, que el problema se ha de entender resuelto partiendo de una interpretación sistemática de la reforma operada por la LO 13/2015 en este punto, y ello aun cuando su texto en lo que a este tema se refiere no resulta lo claro que cabría esperar de una reforma de tal calado[138].

En efecto, el precepto en virtud del que, para recabar los datos de tráfico o asociados, se exige autorización judicial (art. 588 ter j LECrim), se encuentra ubicado en el capítulo V del título VIII LECrim, dedicado a la interceptación de las comunicaciones telefónicas y telemáticas. En relación con esta medida de investigación, el art. 579 ter a LECrim dispone que la autorización para la intervención de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el art. 579.1 de esta ley —relativo a la correspondencia escrita y telegráfica—, a saber: 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; 2.º Delitos cometidos en el seno de un grupo u organización criminal; y 3.º Delitos de terrorismo. A ellos añade el referido art. 579 ter a, los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

[138] Vid. ORTIZ PRADILLO, J. C., «Comunicaciones, tecnología y proceso penal: Viejos delitos, nuevas necesidades», cit., p. 28.

Con base en tal intepretación, dada la ubicación del art. 588 ter j LECrim dentro del capítulo dedicado a la intervención de las comunicaciones telefónicas y telemáticas, consideramos que los delitos en virtud de los que puede acordarse esta diligencia de investigación son los que han de aplicarse como presupuesto para la incorporación de los datos previstos por la Ley 25/2007 al proceso penal, más aún cuando, tratándose de una materia que incide en el derecho fundamental del art. 18.4 CE, la cuestión ha sido regulada posteriormente por una norma con rango de Ley Orgánica (LO 13/2015) en contraposición al carácter de Ley Ordinaria de la Ley 25/2007, suponiendo aquella una derogación tácita de esta última en lo que a la gravedad del delito se refiere.

Por otra parte, como señala MARCHENA GÓMEZ, resultaría paradójico el hecho de que para la cesión de datos sea necesaria la investigación de un delito castigado con pena grave, mientras que para la interceptación de la comunicación que genera los datos se exija una pena menor[139].

Por otro lado, de estimarse que la gravedad únicamente se ha de determinar conforme a los arts. 13 y 33 del CP, no sería posible recabar datos de tráfico de las operadoras de servicios para delitos con penas inferiores, impidiéndose consecuente de plano la investigación de un buen número de delitos de los que se cometen por medio de las nuevas tecnologías, tales como estafas informáticas, delitos contra el honor, amenazas, etc.

En cualquier caso, ha de tenerse en consideración que el TJUE ha dictado la reciente Sentencia de 2 de octubre de 2018, resolviendo la cuestión prejudicial que fue planteada por la Audiencia Provincial de Tarragona el 6 de abril de 2016, en la que, esencialmente, se solicitaba aclaración sobre si la gravedad de los delitos ha de identificarse únicamente en relación con la pena a imponer o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos[140].

---

[139] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 218.

[140] La cuestión prejudicial fue planteada por la Audiencia Provincial (AP) de Tarragona tras un recurso de apelación interpuesto por el Ministerio Fiscal contra la inadmisión por el Juzgado de instrucción de la incorporación al proceso de los datos conservados por una operadora, tratándose de un delito de robo con violencia, denegación que se acordó por el juez de instrucción por entender que era contrario al art. 1.1 de la Ley 25/2007 al considerar graves los delitos castigados con pena superior a 5 años de prisión conforme a los arts. 13 y 33 CP.

En la resolución de este asunto, el TJUE ha establecido una doctrina que nos parece del todo acertada y que reafirma la nueva regulación de la LECrim tras la reforma operada por la LO 13/2015.

En síntesis, el alto Tribunal ha declarado que, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de grave.

En cambio, cuando la injerencia que implica dicho acceso no es grave, esta puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general, declarando a continuación, en cuanto al asunto concreto por el que se había planteado la cuestión prejudicial, que la cesión de los datos personales o de filiación del titular de una tarjeta SIM, no permiten extraer información sobre la vida privada, por lo que el acceso limitado únicamente a dichos datos no puede calificarse de injerencia grave en los derechos fundamentales de los individuos cuyos datos se ven afectados[141].

4.4.4. La regulación de la cesión de los datos de tráfico o asociados tras la reforma operada por la LO 13/2015

El legislador de 2015, al regular las diligencias de investigación tecnológica, se ocupa de los datos de tráfico o asociados en el capítulo V del título VIII de la LECrim, relativo a la interceptación de las comunicaciones telefónicas y telemáticas, en dos secciones, la segunda bajo la rúbrica «incorporación al proceso de datos electrónicos de tráfico o asociados» y la tercera relativa al «acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad».

4.4.4.1. Incorporación al proceso de los datos de tráfico o asociados

La Ley 25/2007, de 18 de octubre, de conservación de datos, establece en su art. 6 la necesidad de autorización judicial para la cesión de datos conservados por las operadoras.

[141] Apdos. 56, 57, 60 y 61 de la Sentencia del Tribunal de Justicia de la Unión Europea (STJUE) de 2 de octubre de 2018.

Como hemos mencionado en apartados anteriores, la incidencia de dicha obligación puede afectar al derecho al secreto de las comunicaciones o al derecho a la intimidad o protección de datos de carácter personal, que no tienen la misma naturaleza constitucional al existir un régimen distinto en lo que a la obligatoriedad de la autorización judicial se refiere.

El legislador ha tenido en cuenta tal circunstancia con la reforma operada por la LO 13/2015, estableciendo una salvedad que en el proyecto inicial no figuraba[142]. Así, en relación con la incorporación al proceso de los datos de tráfico o asociados, dispone el apartado 1 del art. 588 ter j LECrim, que «los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial».

Con este precepto se establece una distinción en relación con los datos que requieren autorización judicial para su cesión, dado que será necesaria la autorización judicial para la cesión de datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación, siempre que «se encuentren vinculados a un proceso de comunicación».

Puede afirmarse, por tanto, que quedan establecidas dos modalidades de datos de tráfico: los que se encuentran vinculados a un proceso de comunicación y aquellos que no tienen tal atributo, por lo que el régimen previsto en la Ley 25/2007 ha quedado derogado tácitamente por la LO 13/2015 que, igualmente, ha regulado la posibilidad de que determinados datos puedan ser obtenidos directamente por el Ministerio Fiscal o la Policía Judicial sin necesidad de autorización judicial, como veremos a continuación.

Por otra parte, el apartado 2 del art. 588 ter j LECrim, después de disponer la necesidad de autorización judicial para recabar la información que conste en archivos automatizados de los prestadores de servicios, cuando el conocimiento de los datos

[142] El proyecto inicial de 20 de marzo de 2015 de reforma de la LECrim, que dio lugar a la LO 13/2015 no establecía la condición mencionada de que se tratase de datos electrónicos «vinculados a un proceso de comunicación» lo cual fue introducido a través de la enmienda n.º 108 (Boletín de las Cortes Generales-Congreso de los Diputados de 29 de mayo de 2015) con la justificación de «mejora técnica con la finalidad de mejorar la redacción».

vinculados a un proceso de comunicación resulte indispensable para la investigación, establece la posibilidad de que en la solicitud de autorización al juez competente se incluya la petición de «búsqueda entrecruzada o inteligente de datos» siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

La regla general, por tanto, es que el conocimiento de los datos resulte indispensable para la investigación, siendo necesaria la autorización judicial, para cuya emisión será necesario que se especifique en la solicitud los datos que se interesan y las razones por las que se interesa la cesión.

En cuanto a la búsqueda entrecruzada o inteligente de datos, cabe entender por la misma un cruce, comparación y contraste entre datos personales que obren en archivos automatizados[143], que deberá ser realizado por los prestadores de servicios para disociar los concretos datos que sean requeridos de entre todos los que consten en los distintos archivos automatizados en poder de las compañías operadoras[144].

De acuerdo con lo señalado por PÉREZ GIL Y GONZÁLEZ LÓPEZ, la circunstancia de requerir tal contraste implica un mayor grado de injerencia en el derecho fundamental, dado que «esta diligencia entraña una afección añadida a la propia de cualquier cesión, al suponer el contraste de datos personales procedentes de distintos

[143] Así se establece en el art. 354 del Anteproyecto de LECrim de 2013, que paradójicamente no estableció la necesidad de que para tal cruce, comparación y contraste se precisase de autorización judicial, disponiendo que el Fiscal podría autorizar la medida por decreto impugnable ante el Tribunal de Garantías.

[144] El paradigma de búsqueda entrecruzada lo encontramos en los casos en los que resulta necesario localizar el IMEI —International Mobile Station Equipment Identity— el cual es un código numérico que identifica de forma única a cualquier teléfono móvil a nivel mundial, a través del IMSI —International Mobile Subscriber Identity— tratándose este último de un código para cada dispositivo de telefonía móvil integrado en la tarjeta SIM. Es decir, con los datos de un dispositivo de telefonía móvil (tarjeta SIM), tras una comunicación telefónica, queda registrado por la operadora el concreto teléfono móvil desde el que se ha realizado la misma, el cual deberá ser localizado según los términos usados por las propias operadoras a través de una búsqueda entrecruzada o inteligente de datos. VELASCO NÚÑEZ señala como un concreto ejemplo de búsqueda entrecruzada de datos «buscar los números de teléfono activados en una geolocalización concreta donde ocurrió el delito investigado en un tramo horario, que pueden cruzarse con los de otra localización y fecha posterior o anterior donde ocurrió un delito semejante, para tratar de dar con los teléfonos activados en ambas escenas del crimen». VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Las Rozas (Madrid), Editorial Jurídica Sepín, 2016, p. 107.

archivos automatizados de cualquier persona física o jurídica, con lo que multiplica el carácter restrictivo de la cesión de datos»[145].

Por ello, es del todo justificada la necesaria autorización judicial para tal búsqueda entrecruzada o inteligente de datos, atendiendo a los principios de proporcionalidad así como excepcionalidad y necesidad. Además, será necesario un plus en la motivación de la solicitud que, por parte del Ministerio Fiscal o Policía Judicial, se haga al juez, al tener que precisar la naturaleza de los datos y justificar las razones de la petición. Ha de tenerse en cuenta, por otra parte, que, conforme afirma DELGADO MARTÍN, la separación o filtrado de los datos genera un mayor coste personal y económico a las entidades prestadoras de servicios[146].

4.4.4.2. Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

La LECrim, tras la reforma de la LO 13/2015, ha regulado tres supuestos en los que bajo la denominación de datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, permite que el Ministerio Fiscal o la Policía Judicial puedan, sin necesidad de autorización judicial, obtener determinados datos de tráfico, que se concretan, conforme a la rúbrica de cada uno de los preceptos que los regulan, en la «identificación mediante número IP; identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes; e identificación de titulares o terminales o dispositivos de conectividad».

Previamente ha de significarse que estos tres supuestos tienen la condición de «datos de carácter personal» por cuanto, de conformidad con lo dispuesto en el art. 4.1 del RGPDUE, se trata de datos que contienen información concerniente a una persona identificable, independientemente de que pudiesen ser considerados como vinculados o no a un proceso de comunicación, y, por tanto, el hecho de que el Ministerio Fiscal o la Policía Judicial puedan obtener dichos datos supone una excepción a la regla general establecida en el art. 6 de la Ley 25/2007.

---

[145] PÉREZ GIL, J.; GONZÁLEZ LÓPEZ, J. J., «La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal», *Diario La Ley - Sección Doctrina*, n.º 8217, 2013, p. 12.

[146] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 417.

De conformidad con este precepto, es necesaria la autorización judicial para la cesión de los datos a los que se refiere el art. 3 de la misma Ley, por lo que la reforma operada por la LO 13/2015 supone una derogación parcial tácita del art. 6 de la Ley 25/2007. En primer lugar, establece, como dijimos en el apartado anterior, la doble categoría de datos vinculados a un proceso de comunicación, en los que siempre es exigible la reserva jurisdiccional y aquellos que no tienen tal vinculación; por otro lado establece unos supuestos en los que directamente no es necesaria la autorización del juez competente[147].

Dicho esto, no está de más recordar lo que queda aún más reforzado con estas últimas apreciaciones, es decir, el hecho de que, independientemente de la vinculación o no a un proceso de comunicación, habrá de requerirse siempre la autorización judicial conforme al principio de proporcionalidad, cuando la intervención policial suponga una injerencia en cualquier dato de carácter personal conforme a la definición que facilita el art. 4.1 del RGPDUE. Todo ello, con la salvedad de aquellos concretos supuestos de urgencia que en su momento, al ocuparnos de los registros informáticos, estudiaremos desde una perspectiva crítica, dado que, como veremos, con ellos pueden ser limitados todos los derechos a la vida privada que venimos examinando en este capítulo.

Examinaremos a continuación los tres concretos supuestos que quedan excepcionados de la necesidad de autorización judicial.

A) Identificación mediante número IP

Una dirección IP —protocolo de internet o *internet protocol*— es un número único e irrepetible con el que se identifica un dispositivo informático conectado a una red que utilice dicho protocolo, entendiendo este último como un conjunto de reglas que, en el contexto de un lenguaje informático, se establece para el proceso de comunicación entre varios sistemas. La combinación de números que constituye una IP permite un número aproximado de 4.000 millones de números, es decir, identificar a 4.000 millones

[147] El preámbulo de la LO 13/2015, de 5 de octubre, apdo. IV, cataloga estos supuestos, como desvinculados de un proceso de comunicación al establecer que «también se regula el supuesto de la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial».

de equipos informáticos diferentes conectados a internet en un momento dado, no existiendo dos ordenadores conectados a internet con el mismo número identificador[148].

El art. 588 ter k LECrim, dispone que «cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e LECrim, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso».

En una primera lectura podría parecer que el precepto se limita a indicar la necesidad de autorización judicial para obtener los datos que permitan la identificación y localización de un dispositivo y la identificación del sospechoso. Sin embargo, conforme se desprende de la norma, la autorización judicial se hace preceptiva para la identificación del dispositivo y del sospechoso, por lo que, para ello, se hace necesario que previamente la Policía Judicial haya tenido acceso a una dirección IP. Por tanto, el legislador a partir de la reforma de la LO 13/2015 ha permitido que la obtención de cualquier dirección IP no precise de autorización judicial[149].

---

[148] Vid. SALOM CLOTET, J., «Incidencias de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos», en Emaldi Cirion, A. y otros, *La protección de datos en la cooperación policial y judicial*, Cizur Menor (Navarra), Editorial Aranzadi, 2008, p. 136. Explica este autor a continuación (p. 137), que cualquier usuario de internet puede averiguar la localización de un equipo al que corresponde una dirección IP, a través de un servicio conocido como «whois» facilitado por un organismo que ha asumido el papel de regulador de la red denominado ICANN (Internet Corporation for Assigned Numbers and Names), que ha repartido rangos de números IP a las distintas operadoras o empresas encargadas de su distribución, la cual se ha realizado a través de instituciones delegadas divididas geográficamente del siguiente modo: ARIN para Norteamérica, RIPE para Europa, LACNIC para Iatinoamérica y Caribe, AFRINIC para África y APNIC para Asia y Pacífico.

[149] Ha de tenerse en cuenta, tal y como señala MARCHENA GÓMEZ, que «las Fuerzas y Cuerpos de Seguridad del Estado no pueden mantenerse al margen de lo que cada día acontece en Internet. Carecería de sentido que esas labores de prevención, cotidianas e indispensables para la protección de determinados bienes jurídicos, exigieran de forma anticipada autorización judicial. Solo cuando la serie numérica que identifica una dirección IP, respecto de la que existen sospechas de estar siendo utilizada para la comisión de delitos, vaya a ser puesta en relación con otros datos electrónicos en poder de las operadoras, será precisa la autorización judicial». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 306.

Con esta norma, el legislador ha aceptado el criterio jurisprudencial adoptado por la Sala Segunda del TS, que, al referirse a la dirección IP, ha declarado en numerosas sentencias que no se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma, dado que la huella de la entrada queda registrada siempre y ello lo sabe el usuario. Todo ello, bien entendido que una dirección IP no concreta a la persona del usuario, sino sólo el ordenador que se ha usado, lo que hace necesario, para poder llegar al ulterior conocimiento del número de teléfono y titular del contrato, la posterior autorización judicial[150].

B) Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes

De forma similar a lo establecido por el art. 588 ter k LECrim en relación con la dirección IP, el apartado primero del art. 588 ter l LECrim permite que los agentes de la Policía Judicial puedan —en el marco de una investigación en la que resulte indispensable obtener un determinado número de abonado, y a fin de poder acceder a la numeración IMSI o IMEI—[151], valerse de artificios técnicos[152] que permitan acceder a tales códigos, con la finalidad de identificar el equipo de comunicación o la tarjeta utilizada para acceder a la red de telecomunicaciones.

A continuación, y de una forma consecuente con la regulación previa relativa a la interceptación de las comunicaciones telefónicas y telemáticas, se dispone, en el apartado segundo del referido precepto, la necesidad de que la Policía Judicial recabe la correspondiente autorización del juez competente para intervenir las comunicaciones una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, debiendo poner en conocimiento del órgano jurisdiccional si se ha hecho uso de algún artificio técnico.

---

[150] Vid. SSTS 16/2014, de 30 de enero, FJ 2.º; 680/2010, de 14 de julio, FJ 2.º; y 739/2008, de 12 de noviembre, FJ 4.º

[151] Vid. nota al pie n.º 144 en relación con el IMSI e IMEI, p. 73.

[152] Los artificios más significativos utilizado por la Policía Judicial para la identificación de equipos de comunicación o tarjetas utilizadas para acceder a la red de telecomunicaciones son, como señala VELASCO NÚÑEZ, los «IMSI-catchers», programas informáticos que funcionan a modo de antena, en cuya cercanía se prioriza el establecimiento de la conexión, permitiendo acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o alguno de sus componentes, como puedan ser los números IMSI o IMEI. Vid. VELASCO NÚÑEZ, E., «*Delitos tecnológicos: definición, investigación y prueba en el proceso penal*», cit., p. 109.

Si bien el IMSI y el IMEI, son datos de carácter personal, ya que permiten identificar a una persona, no es menos cierto que para que pueda llevarse a cabo tal identificación es necesario que los códigos que constituyen el IMSI e IMEI se pongan en relación con otros datos que obran en poder de la compañía prestadora de servicios. En este sentido, entendemos justificada la excepción legal, quedando la misma incardinada sin ningún problema dentro de los supuestos del art. 22.2 de la LOPD, que permite la recogida y tratamiento para fines policiales de datos de carácter personal por las FCSE sin consentimiento de las personas afectadas, cuando tal obtención sea necesaria para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

Finalmente, cabe señalar que esta regulación ha recogido los criterios establecidos por la jurisprudencia del TS, cuyo primer exponente es la STS 249/2008. Esta resolución, tras señalar que el IMSI por sí solo no puede integrarse dentro del contenido del derecho al secreto de las comunicaciones, declara que, tratándose de un dato de carácter personal, cabe la posibilidad de que dicho dato pueda ser captado por la Policía Judicial sin necesidad de autorización judicial, siempre que con ello se persiga un fin constitucionalmente legítimo, que se dará siempre que se investigue un delito de especial gravedad[153].

C) Identificación de titulares o terminales o dispositivos de conectividad

Como último supuesto que en materia de cesión de datos de tráfico o asociados el legislador excepciona de la reserva jurisdiccional, permitiendo que por parte de los agentes de la Policía Judicial se pueda en este caso solicitar directamente dicho dato de las prestadoras de servicios, el art. 588 ter m LECrim se ocupa de la identificación de

[153] Vid. STS 249/2008, de 20 de mayo, FJ 4.º que declaró que «la Sala no puede aceptar que la captura del IMSI por los agentes de la Guardia civil haya implicado, sin más, como pretende el recurrente, una vulneración del derecho al secreto de las comunicaciones». Asimismo declaró que «esa capacidad de recogida de datos que la LO 15/1999, 13 de diciembre, otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal –nunca con carácter puramente exploratorio—, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional. También parece evidente que esa legitimidad que la ley confiere a las Fuerzas y Cuerpos de Seguridad del Estado nunca debería operar en relación con datos referidos al contenido del derecho al secreto de las comunicaciones (art. 18.3 de la CE) o respecto de datos susceptibles de protección por la vía del art. 18.4 de la CE que afectaran a lo que ha venido en llamarse el núcleo duro de la privacidad o, con la terminología legal, los datos especialmente protegidos».

titulares o terminales o dispositivos de conectividad, disponiendo que «cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia».

Probablemente pueda parecer a primera vista, que el legislador ha ido demasiado lejos al permitir que por parte del Ministerio Fiscal o la Policía Judicial se pueda obtener sin autorización judicial los datos identificativos de una persona partiendo de su número de teléfono o de los datos identificativos de otro medio de comunicación o viceversa, en el entendimiento de que tal cesión sin la oportuna autorización judicial podría suponer una vulneración del derecho al secreto de las comunicaciones.

Aun así, y partiendo de la base de que, como señala HUETE NOGUERAS, el sistema seguido por el legislador es de interpretación restrictiva (es decir, no cabe sobre la base de la existencia de esa excepción, ampliar la no exigencia de autorización judicial previa, respecto de otros datos que no sean la identidad nominal de los titulares de un teléfono o medio de comunicación o la identificación de terminales o dispositivos de conectividad)[154], las dudas que se pudieran haber planteado inicialmente, pronto se disiparán al reflexionar nuevamente acerca de la cesión de datos según se encuentren vinculados o no a un proceso de comunicación.

En efecto, tal y como se expuso con anterioridad en el apartado referente a la incorporación al proceso de los datos de tráfico o asociados[155], el legislador ha excepcionado la regla general establecida en el art. 6 de la Ley 25/2007, estableciendo en el art. 588 ter j LECrim la necesidad de autorización judicial solamente para aquellos datos de tráfico vinculados a un proceso de comunicación.

En ese mismo sentido, hemos de considerar ahora que la identificación de una determinada persona a partir de su número de teléfono o identificación de otro medio de

[154] HUETE NOGUERAS, J. J., «La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados», *Revista del Ministerio Fiscal*, n.º 2, 2016, p. 77.
[155] Vid. supra apdo. 4.4.4.1 de este capítulo, pp. 71-74.

comunicación o viceversa, solo podrá ser obtenida por petición a las operadoras del Ministerio Fiscal o la Policía Judicial sin necesidad de autorización judicial cuando el dato obtenido inicialmente por los agentes y con base al que se dirigen a la prestadora de servicios, hubiera sido obtenido sin estar vinculado a un proceso de comunicación. Por ejemplo, la Policía Judicial podría haber obtenido el nombre de una persona en un buzón de correos de un edificio y a partir de ahí precisar su número de teléfono; o también a la inversa, tras una investigación con un agente infiltrado conocer el número de teléfono de un presunto delincuente del que solo se conoce su alias y del que se precisa conocer su nombre completo.

Cabe señalar que la STS 7/2014, de 22 de enero, ya había establecido una diferenciación, refiriéndose en lugar de a datos que se encuentran vinculados o no a un proceso de comunicación, a datos estáticos —aquellos que se encuentran en poder de las prestadoras de servicios y que se refieren a comunicaciones ya concluidas— y dinámicos —los que se generan durante un proceso de comunicación— declarando que unos y otros no tienen el mismo tratamiento en lo que a la necesidad de autorización judicial se refiere[156].

En estos casos, nos encontramos ante datos que, aunque sin duda tienen la condición de datos de carácter personal a los efectos de la protección constitucional del art. 18.4 CE, no se encuentran vinculados a un proceso de comunicación, por lo que los mismos, no obstante gozar de la referida protección constitucional, no siempre y en todo caso requerirá su obtención autorización judicial, y en este sentido nos parece loable el criterio del legislador, que por otro lado no ha hecho sino concretar unos supuestos que desarrolla el art. 22.2 de la LOPD que, como ya sabemos, permite la recogida y tratamiento por parte de la Policía Judicial de datos de carácter personal cuando resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

[156] Vid. STS 7/2014, de 22 de enero, FJ 2.º, en la que se declara que «los listados de llamadas generados durante la conversación intervenida tienen un significado distinto de aquel que puede predicarse de esos mismos listados cuando aparecen como dato previo a la investigación, en ausencia de toda medida de interceptación ya acordada» y añade que «es evidente que ese listado no puede estimarse desprovisto de protección constitucional. De hecho, en función de su consideración estática —listado de llamadas obrante en los archivos de las operadoras, expresivo de comunicaciones ya concluidas y que no estaban siendo objeto de intervención judicial—, o dinámica —listado de llamadas generado durante conversaciones que ya son objeto de una medida de injerencia—, su régimen jurídico es diverso y el grado de protección también lo es».

Para justificar esta opinión favorable, en relación con este punto concreto de la reforma, cabe señalar que nos encontramos concluyendo la segunda década del siglo XXI, en un contexto de delincuencia informática donde el peligro de delitos tan infames como el terrorismo, la pornografía infantil o tráfico de drogas, se hace más patente cuando la información puede circular por la red dentro de un estricto anonimato. Por ello, consideramos que, para una adecuada prevención del delito se debe facilitar, más que poner trabas, la investigación policial para combatir estos crímenes, aunque siempre con las debidas cautelas y el necesario respeto a los derechos fundamentales.

4.4.5. Necesidad de una adecuada regulación acerca de los datos que se encuentran vinculados a un proceso de comunicación

Probablemente no serán pocos los problemas que surjan para la distinción entre los datos que se encuentran vinculados o no a un proceso de comunicación, habida cuenta de la amplitud de la relación de datos que se establecen en el art. 3.1 de la Ley 25/2007, de 18 de octubre[157].

[157] La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, concreta cuales son los datos de tráfico —antes de disponer en su apartado 3.2 que «ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley»— en su art. 3.1, el cual, bajo la rúbrica «datos objeto de conservación», establece que «1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:
a) Datos necesarios para rastrear e identificar el origen de una comunicación:
1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.
2.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:
i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.
b) Datos necesarios para identificar el destino de una comunicación:
1.º Con respecto a la telefonía de red fija y a la telefonía móvil:
i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.
2.º Con respecto al correo electrónico por Internet y la telefonía por Internet:
i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.

Afirma MARCHENA GÓMEZ que «exigir del juez de instrucción que discierna en el caudal de datos que las operadoras están obligadas a reservar entre aquellos que tienen vinculación a un proceso de comunicación —respecto de los que sería obligada la autorización judicial— y aquellos otros que, por su falta de vinculación con ese proceso estarían exentos de esa exigencia, no es, desde luego un buen criterio»[158].

---

ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.

2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.

ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).

2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.

2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.

ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.

iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.

iv) La IMSI de la parte que recibe la llamada.

v) La IMEI de la parte que recibe la llamada.

vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.

ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.

2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones».

[158] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 300.

Existe, no obstante, algún pronunciamiento del TS acerca de los datos que merecen la protección reforzada del derecho al secreto de las comunicaciones. Concretamente ha declarado que «en principio, ese carácter habría de predicarse, actualizando la pauta interpretativa ofrecida por el TEDH, de los datos identificativos del origen y del destino de la comunicación, del momento y duración de la misma y, por último los referentes al volumen de la información transmitida y el tipo de comunicación entablada»[159].

Doctrinalmente se ha afirmado que el criterio de distinción podría venir de la mano de la diferente naturaleza del dato en cuestión: dinámica o estática, de tal forma que podrían entenderse como datos vinculados aquellos de carácter dinámico que son interceptados durante el proceso de comunicación que los está generando y desvinculados de ese proceso los de naturaleza estática almacenados por las operadoras una vez concluido el proceso de comunicación, con obligación de conservación[160].

Aunque tales criterios pueden resultar orientativos para el juez, no nos parecen suficientes, por la dificultad que puede suponer encajar muchos de los datos del amplio elenco que establece el art. 3 de la Ley 25/2007, en los supuestos que se mencionan jurisprudencial y doctrinalmente. Tampoco consideramos apropiado que en una cuestión de tanta trascendencia, ante la posible vulneración de un derecho fundamental, se deba dejar al albur de los juzgados y tribunales la decisión acerca de la diferenciación de unos términos que pueden admitir distintas interpretaciones, lo que no hará otra cosa que entorpecer una adecuada actividad jurisdiccional.

Por ello, consideramos que, *de lege ferenda* y en aras de una mayor seguridad jurídica, sería necesaria la plasmación de una forma clara de los datos, que de la extensa relación del art. 3 de la Ley 25/2007, quedan vinculados a un proceso de comunicación. El acceso a estos, exigiría en todo caso el requisito de la reserva jurisdiccional, y por tanto, su régimen jurídico quedaría diferenciado del relativo al de los datos que, por no encontrarse vinculados a un proceso de comunicación, tendrían un régimen más flexible, pudiendo en casos de urgencia ser reclamados directamente por el Ministerio Fiscal o la Policía Judicial a las operadoras.

---

[159] Vid. STS 249/2008, de 20 de mayo, FJ 4.º

[160] LANZAROTE MARTÍNEZ, P., «La nueva regulación de las intervenciones telefónicas y telemáticas: Algunas cuestiones claves y otras discutibles», *Revista del Ministerio Fiscal*, n.º 3, 2017, p. 84.

Para finalizar, ha de reseñarse, que dicha regulación debería llevarse a efecto a través de LO, habida cuenta de su incidencia sobre derechos fundamentales, y estableciendo por tanto una clara diferenciación entre aquellos supuestos que exigen inexorablemente la reserva jurisdiccional, de aquellos que no requieren tal ineludible exigencia.

IV. El entorno virtual

1. La existencia del llamado entorno virtual

Como consecuencia del desarrollo de la informática y de las TIC en general, y muy especialmente por la creciente amplitud de espacio virtual a disposición de los ciudadanos (bien en pequeños dispositivos y sin embargo con una enorme capacidad de almacenamiento, o bien mediante el suministro de espacio virtual por parte de las compañías tecnológicas a los particulares —la llamada nube—), se ha venido planteando en los últimos años la problemática en relación con la información que de cada persona podría extraerse como consecuencia del examen en conjunto de toda la información acumulada en los referidos dispositivos.

Aunque el acceso de forma individual a cada uno de los datos almacenados podría suponer —sin perjuicio de valorar cada caso concreto— una injerencia en un concreto derecho fundamental a la vida privada del art. 18 CE, lo cierto es que toda la información examinada de forma global, permitiría en muchos casos extraer conclusiones sobre los hábitos de una persona, sus desplazamientos, relaciones sociales, preferencias sexuales, ideología, religión, etc., facilitando la obtención de perfil sobre su manera de sentir, pensar o comportarse.

Ello dio lugar a que por parte de determinados sectores doctrinales se invocara la existencia del llamado «entorno virtual», como una realidad que se estimaba digna de protección y que ha sido definido como «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»[161].

[161] DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *Diario La Ley - Sección Doctrina*, n.º 8693, 2016, p. 2.

Uno de los primeros antecedentes en cuanto al planteamiento de esta realidad lo podemos encontrar como consecuencia del estudio que se lleva a cabo del derecho a la intimidad frente a las amenazas de la tecnología dentro del desarrollo del art. 18.4 CE. Como consecuencia del mismo surge, además de una concepción objetiva y subjetiva, una nueva perspectiva del concepto del derecho a la intimidad a la que se denominó «teoría del mosaico», en virtud de la que existen datos que, *a priori*, son irrelevantes desde el punto de vista del derecho a la intimidad, pero que, unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo[162].

Posteriormente, ya en época más actual y como consecuencia de la posibilidad de obtener pruebas acreditativas de la comisión de cualquier delito mediante las TIC, se plantea la necesidad de conferir al entorno virtual una adecuada protección a causa de la vulneración que, por el acceso a tal conjunto de información digital, supondría para los derechos fundamentales a la libertad y la intimidad[163], proponiéndose que la ley se enfrente a los complejos retos que plantea la persecución penal en el entorno virtual adoptándose soluciones a los problemas que se suscitan entre investigación tecnológica y los derechos fundamentales a la privacidad en general[164].

Esta realidad innegable de la existencia de un entorno virtual, entendida como tal, y no como derecho independiente, como veremos más adelante, también fue

---

[162] REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», cit., pp. 181-182. El autor afirma que la teoría del mosaico ha sido formulada por MADRID CONESA, quien señala que la idea completa que se puede configurar de cualquier individuo, lo es «al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado» MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, 1984, p. 45.

[163] GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», cit., p. 890, señala que «por la misma razón que los datos digitales constituyen un provechoso filón para la indagación y el esclarecimiento de los delitos son un preciado tesoro para la persona: en espacios minúsculos o en segmentos temporales de gran fugacidad se concentra una extraordinaria cantidad de información sobre las más variadas actividades de la vida, muchas de ellas íntimas o de una naturaleza diversa a la privada, pero también secreta o reservada. A la enorme utilidad del entorno digital como ámbito de desarrollo de la persecución penal se une la tremenda lesividad potencial de la aprehensión de datos para la libertad individual, grave problema que colocará en profunda crisis nuestro ya deficiente sistema de garantías constitucionales, dadas las dificultades que se presentan para la aplicación en el ciberespacio de los mecanismos de protección de los derechos fundamentales ejercidos en el mundo físico».

[164] GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», cit., p. 916.

reconocida por el TC, al declarar que la observación por los demás del cúmulo de información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional, permitiría descubrir aspectos de la esfera más íntima del ser humano[165].

2. La elevación jurisprudencial del entorno virtual a la categoría de derecho independiente

La problemática en relación con las injerencias sobre el entorno virtual se manifiesta de forma notable una vez que, para la investigación del delito, se hace necesario el acceso policial a los dispositivos informáticos de almacenamiento a fin de obtener pruebas en formato digital. Se plantea entonces la cuestión de cuál o cuáles de los derechos del art. 18 CE (intimidad, inviolabilidad de las comunicaciones o protección de datos de carácter personal) podría resultar vulnerado, habida cuenta de que no todos gozan del mismo grado de protección. Esta cuestión se puso de manifiesto una vez que quedó sentado que la orden de entrada y registro no daba cobertura al registro de dispositivos informáticos, lo que dio lugar a ciertas vacilaciones jurisprudenciales —a las que nos referiremos en el capítulo V dedicado a los registros informáticos—, imponiéndose finalmente el criterio de la necesidad de autorización judicial independiente a la de entrada y registro domiciliario, el cual ha quedado finalmente reflejado en el derecho positivo con la LO 13/2015.

El primer exponente jurisprudencial que se refiere a la existencia de un derecho propio lo constituye la STS 342/2013, de 17 de abril, que, partiendo de la necesidad e importancia de que «la garantía de aquellos derechos se haga efectiva siempre y en todo

[165] Vid. STC 173/2011, de 7 de noviembre FJ 3.º *in fine*, la cual declaró que «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. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información».

caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal», declaró 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»[166], doctrina que ha sido reiterada en algunas sentencias posteriores[167].

3. Problemas en cuanto a la efectiva existencia de un derecho. Reconducción a los derechos a la vida privada del art. 18 CE

Partiendo de la realidad indiscutible de la existencia del entorno virtual al que nos hemos referido, que podrá y deberá tener incidencia en todas las ramas del derecho,

---

[166] Vid. STS 342/2013, de 17 de abril, FJ 8.º, que declaró lo siguiente: «El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar —de hecho, normalmente albergará— información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones…

En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal.

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 él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris propio*, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital».

[167] Vid. SSTS 97/2015, de 24 de febrero, FJ 4.º; 786/2015, de 4 de diciembre, FJ 1.º; y 426/2016 de 19 de mayo, FJ 7.º

no puede afirmarse que el mismo constituya un derecho con *nomen iuris* propio, básicamente, al no constar un reconocimiento expreso por parte del legislador, sin que por otra parte, pueda afirmarse la preexistencia de tal derecho, por cuanto, la problemática relativa a sus efectos, es una cuestión novedosa, al nacer como consecuencia de la irrupción de las TIC.

Recientemente, al referirse el TS a los dispositivos de almacenamiento masivo de información, tras señalar que la necesidad de autorización judicial para el acceso a los mismos obedece a la circunstancia de la serie compleja y densa de datos que en ellos pueden ser almacenados (que afectan de modo muy variado a la intimidad del investigado —tales como comunicaciones tuteladas por el art. 18.3 CE; contactos, fotografías, archivos personales, tuteladas por el art. 18.1 CE; o datos personales y de geolocalización, que pueden cobijarse en el derecho a la protección de datos del art. 18.4 CE— y cuya contemplación disgregada de cada una de esas realidades con regímenes de protección diferenciados resultaría ineficaz), ha declarado que «el legislador con buen criterio ha optado por otorgar un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando ese derecho constitucional de nueva generación, el derecho a la protección del propio entorno virtual», lo cual ha sido reiterado en alguna sentencia posterior[168].

Del mismo modo, se ha afirmado doctrinalmente que el derecho al entorno virtual se encuentra comprendido dentro del derecho a la privacidad del art. 8 CEDH y que al aceptar la existencia de un derecho fundamental al entorno virtual pierden relevancia los debates dogmáticos acerca de si el registro remoto de un ordenador afecta a cualquiera de los derechos del art. 18 CE, pues englobaría a todos ellos[169]. Asimismo, se ha señalado que el tratamiento unitario de los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, responde al reconocimiento de un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual[170].

---

[168] Vid. SSTS 204/2016, de 10 de marzo, FJ 11.º; y 489/2018, de 23 de octubre, FJ 5.º

[169] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, n.º 2195, 2017, pp. 21-22.

[170] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 21, consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/PonenciaConde-Pumpido Tourón.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47, el 12 de junio de 2020.

No compartimos las menciones relativas a que el legislador ha configurado un derecho de nueva generación así como la existencia de un derecho propio y menos aún que pueda otorgarse la naturaleza de derecho constitucional al entorno virtual, dicho sea con el máximo respeto a las resoluciones del TS, dado el importante reconocimiento de la figura que examinamos desde la STS 342/2013 anteriormente mencionada, cuya relevancia es incontrovertible. En tal sentido, tampoco podemos compartir opiniones doctrinales que afirman que el art. 588 sexies apartados a y b LECrim, han refrendado absolutamente dicho reconocimiento[171].

Entendemos que el legislador se ha limitado, con la nueva regulación del art. 588 sexies LECrim, a establecer la necesidad de autorización judicial para los registros de dispositivos de almacenamiento masivo, con la salvedad de aquellos casos, en los que por apreciarse un interés constitucional legítimo que haga imprescindible la medida, la Policía Judicial pueda llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, con la obligación de comunicarlo al juez competente en el plazo máximo de veinticuatro horas (art. 588 sexies c.4 LECrim).

Cuestión distinta es el criterio interpretativo, a nuestro juicio totalmente aceptable, que se desprende tanto del espíritu de la norma (art. 588 sexies LECrim) como de la línea jurisprudencial iniciada con la STS 342/2013, conforme al que, tal y como mencionó esta sentencia, la ponderación que el juez competente ha de llevar a cabo de las razones que justifican el registro de un ordenador, ha de realizarlas sin perder de vista la multifuncionalidad de los datos, por lo que su tratamiento jurídico sería más adecuado, si todos los datos reveladores del perfil personal se contemplan de forma unitaria.

Es lo que de otra forma ha expresado DELGADO MARTÍN, al señalar que una de las consecuencias de la existencia del entorno virtual se concreta en que el legislador de la reforma de 2015 ha otorgado un tratamiento unitario a la injerencia en el espacio virtual del afectado mediante el acceso a los datos contenidos en los dispositivos electrónicos, «lo que contribuye a garantizar una protección eficaz de los diferentes

[171] Vid. RODRÍGUEZ LAINZ, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant Lo Blanch, 2019, p. 38.

derechos fundamentales que pueden resultar afectados»[172]. Es decir, se trata de proteger eficazmente los derechos del art. 18 CE otorgándoles un tratamiento unitario al momento de la decisión judicial.

Por ello, con anterioridad a emitir su resolución —que insistimos, a nuestro juicio y de forma muy discutible, como examinaremos en el apartado correspondiente, puede ser obviada por la Policía Judicial por entender que existe un caso de urgencia, aun cuando puede eventualmente ser vulnerado el derecho al secreto de las comunicaciones—, el juez competente deberá, atendiendo a las circunstancias del caso concreto y a criterios de necesidad y proporcionalidad, valorar la incidencia del acceso a todo el cúmulo de datos de la persona investigada, lo cual no hará sino reconducir el pretendido derecho al entorno virtual a los auténticos derechos proclamados en la CE.

Así, de una forma similar a la que autores como FRÍGOLS I BRINES afirman que los derechos fundamentales del art. 18 CE «sirven, en última instancia, a la protección de la intimidad como elemento fundamental, entendida ésta de un modo amplio, como barrera jurídica a la intromisión de terceros, tanto del Estado como de particulares, siendo todos los derechos del art. 18 CE manifestaciones concretas de ese derecho fundamental de libertad, desgajadas del mismo a los meros efectos de una mejor protección de esas parcelas de realidad»[173], podríamos decir ahora que para la información almacenada globalmente en un ordenador o cualquier dispositivo de almacenamiento, los derechos a la intimidad, secreto de las comunicaciones y protección de datos de carácter personal, se agrupan a fin de dar una adecuada protección al entorno virtual que constituye toda la información almacenada.

En definitiva, con el juicio de proporcionalidad del juez en relación al entorno virtual, se está protegiendo finalmente el derecho a la intimidad personal, que es el que resultaría infringido de conocerse de forma indebida las preferencias, ideología o, en definitiva, las formas de sentir, pensar o comportarse de cualquier persona, sin perjuicio de la vulneración del secreto a las comunicaciones y protección de datos, por lo que, tal y como decíamos, se produce una reconducción a los derechos del art. 18 CE.

---

[172] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 365.

[173] FRÍGOLS I BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», cit., p. 43.

4. Proposición de una adecuada regulación

El hecho de que en el apartado anterior se haya puesto de manifiesto nuestra disconformidad con el reconocimiento del entorno virtual como un derecho constitucional, no obsta para que consideremos necesaria una adecuada regulación (que deberá llevarse a cabo por medio de LO, dada la incidencia de la misma sobre derechos fundamentales) con la que quede cubierta la tutela del entorno digital frente a injerencias estatales.

Esta regulación, consideramos que no puede entenderse realizada con la reforma operada por la LO 13/2015, dado que, además de no haber sido planteado de dicho modo por el legislador, no se ha procedido a una definición y concreción de los aspectos esenciales del entorno virtual, no habiéndose efectuado mención alguna en cuanto a las facetas de la vida privada que pueden quedar vulneradas, sin que tampoco se hayan concretado los supuestos de urgencia en los que la Policía Judicial podría intervenir sin autorización judicial y sin que asimismo conste una específica regulación en cuanto a las medidas de seguridad a adoptar en relación con los dispositivos intervenidos.

A mayor abundamiento, queda claro que tal regulación no se ha producido con la LO 13/2015, si se tiene en cuenta que la averiguación de distintos aspectos personales e íntimos del individuo, que llevaría consigo la consecución de una idea de sus preferencias o ideología, podría producirse con otras medidas de investigación tecnológica como la captación y grabación de comunicaciones orales, la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y la geolocalización e incluso la propia intervención de las comunicaciones telefónicas y, ahora, también telemáticas.

Llegados a este punto, nos parece sumamente acertada la propuesta de GONZÁLEZ-CUELLAR SERRANO cuando sitúa el problema en toda su complejidad en el ámbito del art. 18.4 CE, reclamando el desarrollo legal del derecho constitucional que dicho precepto contiene, «no solo frente a la recopilación, tratamiento automatizado y utilización de datos personales, sino también ante el aprovechamiento por los órganos de persecución penal de los sistemas de almacenamiento y comunicación de datos digitales para la investigación y prueba de los delitos»[174].

[174] GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», cit., pp. 890-891. Señala este autor al final de esta obra (p. 916) que «la ley, consecuentemente,

Efectivamente, el art. 18.4 CE ordena al legislador que mediante ley «limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se trata, al igual que en su día se hizo con la protección de datos de carácter personal, de cumplir tal mandato conforme a la realidad de la era digital, entendiendo que la expresión «limitará el uso de la informática» ha de entenderse como una expresión de una gran amplitud, dirigida al uso de la informática que hagamos todos, incluido por supuesto el Estado en el ámbito de la investigación del delito.

Por ello, concluiremos este apartado y también este capítulo, proponiendo, *de lege ferenda*, un desarrollo legislativo del art. 18.4 CE, interpretado de conformidad con la realidad social del tiempo en que ha de ser aplicado atendiendo fundamentalmente a su espíritu y finalidad (art. 3.1 CC) regulando todos los aspectos del denominado entorno digital, en aras de una mayor seguridad jurídica y respeto a los derechos fundamentales.

---

por mandato constitucional específico, debe enfrentarse a los complejos retos que plantea la persecución penal en el entorno digital […] y adoptar soluciones para los problemas que la revolución tecnológica suscita respetuosas con los derechos fundamentales a la privacidad, la inviolabilidad del domicilio y el derecho de las comunicaciones, que eviten la improvisación y la arbitrariedad a las que en demasiadas ocasiones conducen las lagunas y contradicciones de nuestro anquilosado y decrépito Derecho Procesal Penal».

CAPÍTULO II. CONSIDERACIONES ACERCA DE LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA CON ANTERIORIDAD A SU PREVISIÓN LEGAL Y ANÁLISIS DE LA SUFICIENCIA DE LA LO 13/2015

I. Consideraciones previas

Ya hemos indicado que la sociedad actual se vio inmersa, a partir de la última década del siglo XX, en una serie de avances tecnológicos, cuyo uso se fue incrementando de forma paulatina hasta el punto de transformar nuestra vida cotidiana, nuestras relaciones sociales y por supuesto la forma de comunicarnos, dando lugar a la aparición de nuevas formas de delincuencia que hicieron quedar obsoletos los textos legales, especialmente en lo concerniente a las medidas tecnológicas de investigación del delito.

Como consecuencia de tal avance, y el incremento de la cibercriminalidad, sin la paralela y necesaria reforma legal, se ocasionaron numerosos problemas a los tribunales, que se vieron necesariamente obligados a crear una doctrina jurisprudencial que permitiese la incorporación en la investigación de los medios tecnológicos para evitar la impunidad de las referidas novedosas formas delictivas.

Son numerosas las cuestiones que previamente a la reforma operada por la LO 13/2015, de 5 de octubre, se fueron perfilando por la jurisprudencia, tanto por parte del TEDH como del TC y TS, a fin de revestir de las correspondientes garantías constitucionales a las medidas de investigación tecnológica. En este sentido, el preámbulo de la LO 13/2015, tras referirse al déficit en la calidad democrática de nuestro sistema procesal originado por el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa, reconoció la tarea jurisprudencial declarando en su apartado IV que «se ha estimado oportuna la proclamación normativa de los principios que el Tribunal Constitucional ha definido como determinantes de la validez del acto de injerencia»[175].

[175] Cabe señalar que el preámbulo de la Ley 13/2015, de 5 de octubre, inició el citado apartado IV declarando que «La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos. Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias

II. Requisitos para la validez de las diligencias de investigación tecnológica conforme a la jurisprudencia anterior a la LO 13/2015

A lo largo de este trabajo, en el examen de sus distintos apartados, se hará referencia a los criterios jurisprudenciales anteriores a la LO 13/2015 que han sido tenidos en cuenta por el legislador para la nueva regulación y que, sin duda alguna, sirvieron para evitar las indeseables nulidades de actuaciones, tanto para las víctimas del delito como para la propia sociedad, decretadas como consecuencia de la obtención de prueba ilícita, es decir, la que, conforme al art. 11.1 LOPJ se hubiese obtenido, directa o indirectamente, violentando los derechos o libertades fundamentales. No obstante, con la finalidad de conseguir una adecuada sistemática, resulta conveniente realizar un examen previo de los aspectos principales que conformaron el fundamento de la validez constitucional de las medidas de investigación tecnológica limitativas de derechos fundamentales.

Ha de señalarse que los principales pronunciamientos que pusieron de manifiesto las carencias en relación con este tipo de diligencias de investigación, lo fueron en relación con la intervención de las comunicaciones telefónicas, si bien se trata de consideraciones aplicables a cualquier medida de investigación tecnológica y muy especialmente a los registros informáticos por su elevado grado de intromisión en los derechos fundamentales.

Existen diversos enfoques que pueden ser destacados como consecuencia, en palabras de MARTÍNEZ JIMÉNEZ, del cuerpo de doctrina alumbrado por el TC y el TS ante la insuficiencia de regulación legal[176], los cuales se erigieron en presupuestos necesarios para la validez del acto de injerencia y que afortunadamente han adquirido carta de legalidad en nuestra LECrim.

Es numerosa la jurisprudencia anterior a la LO 13/2015 que hizo referencia a los presupuestos para la validez de las diligencias limitativas de derechos fundamentales,

---

supranacionales han recordado. 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».

[176] MARTÍNEZ JIMÉNEZ, J., *Derecho Procesal Penal*, Madrid, Tecnos, 2015, p. 168.

pudiendo destacar la STS 9/2010, de 22 de enero, la cual recopiló los requisitos que, conforme a la doctrina de la Sala de lo Penal del TS, debían concurrir además de la previsión normativa suficiente, tales como la exclusividad jurisdiccional, la finalidad exclusivamente investigadora, la excepcionalidad de la medida, la proporcionalidad, la limitación temporal de la investigación[177], la especialidad del hecho delictivo, la necesidad de que la medida recaiga sobre los dispositivos de las personas indiciariamente implicadas, la existencia previa de indicios de la comisión del delito, así como la de un proceso judicial de investigación penal, la motivación en la resolución que acuerde la medida y el control judicial además de en la autorización de la medida, en su desarrollo y cese[178].

[177] El registro de dispositivos de almacenamiento masivo se agota en sí mismo no siendo por tanto necesaria una duración concreta. No ocurre lo mismo por el contrario con el registro remoto de equipos informáticos en el que se hace necesaria una limitación temporal.

[178] La STS 9/2010, de 22 de enero, FJ 2.º, declaró que «Los requisitos que según doctrina de esta Sala han de concurrir para la legitimidad y validez de las intervenciones telefónicas son: 1') La exclusividad jurisdiccional en el sentido de que únicamente por la autoridad judicial se pueden establecer restricciones y derogaciones al derecho al secreto de las comunicaciones telefónicas. 2') La finalidad exclusivamente investigadora, en su caso, probatoria, de las interceptaciones para establecer la existencia de delito y descubrimiento de las personas responsables del mismo. 3') La excepcionalidad de la medida, que sólo habrá de adoptarse cuando no exista otro medio de investigación del delito, que sea de menor incidencia sobre los derechos y libertades fundamentales del individuo. 4') La proporcionalidad de la medida que sólo habrá de adoptarse en el caso de delitos graves en los que las circunstancias que concurran y la importancia de la trascendencia social del hecho delictivo aconsejen la adopción de la misma, de tal manera que la derogación en el caso concreto del principio garantizador sea proporcionada a la finalidad legítima perseguida. 5') La limitación temporal de la interceptación de las comunicaciones telefónicas. La Ley de Enjuiciamiento Criminal autoriza (artículo 579.3º) períodos trimestrales individuales, pero no podrá prorrogarse la intervención de manera indefinida o excesiva porque ello la convertiría en desproporcionada e ilegal. 6') La especialidad del hecho delictivo que se investigue pues no cabe decretar una intervención telefónica para tratar de descubrir de manera general e indiscriminada actos delictivos. 7') La medida además, recaerá únicamente sobre los teléfonos de las personas indiciariamente implicadas, ya sean los titulares de los teléfonos o sus usuarios habituales. 8') La existencia previa de indicios de la comisión de delito y no meras conjeturas, de tal modo que se cuente con noticia racional del hecho delictivo que se quiera comprobar y de la probabilidad de su existencia, así como de llegar por medio de las intervenciones al conocimiento de los autores del ilícito, pudiendo ser esos indicios los que facilita la Policía, con la pertinente ampliación de los motivos que el juez estimase conveniente. 9') La existencia previa de un procedimiento de investigación penal, aunque cabe sea la intervención de las telecomunicaciones la que ponga en marcha un verdadero procedimiento criminal, pero sin que puedan autorizarse intervenciones telefónicas de carácter previo a la iniciación de éste. 10') Que la resolución judicial acordando la intervención telefónica se halle suficientemente motivada; riguroso requisito para el sacrificio y derogación en casos concretos de derechos fundamentales reconocidos en la Constitución, y cuya importancia exige del juez una explicación razonada y razonable de acuerdo con la Ley y los principios constitucionales y en la cual encontrarán lugar la explicitación de los indicios sobre cuya base la medida se adopte. 11') La exigencia de control judicial en la ordenación, desarrollo y cese de la medida de intervención».

Todos estos aspectos exigen ser analizados de forma más detallada en siguiente capítulo dedicado a las disposiciones comunes a las disposiciones de investigación tecnológica en la LECrim. Sin embargo, en este capítulo estudiaremos tres de las exigencias de legalidad constitucional que, examinadas desde una visión de sus aspectos esenciales, fueron objeto de cierta controversia con anterioridad a la incorporación a la ley de las medidas de investigación tecnológica en nuestro derecho positivo, la cual se produjo, fundamentalmente, por el tan notable como incomprensible esfuerzo del legislador para que finalmente vieran la luz en nuestra ley procesal penal. Estos presupuestos que podemos considerar primarios, se concretan en la necesidad de una suficiente previsión normativa, en la reserva jurisdiccional para la adopción de las medidas y en el respeto del principio de proporcionalidad[179].

1. La necesidad de previsión normativa

La primera y, sin duda, más relevante de las denuncias llevadas a cabo por la jurisprudencia anterior a la LO 13/2015 es la que se refiere a la necesidad de una previsión legal. Una previsión normativa suficiente constituye un presupuesto insoslayable para que pueda llevarse a cabo una injerencia en cualquiera de los derechos fundamentales a la vida privada de los ciudadanos, lo cual se establece de forma directa en el art. 8 CEDH que, refiriéndose al «derecho al respeto a la vida privada y familiar», dispone en su apartado 2.º que «no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley…».

Nuestro TC ha afirmado en diversas resoluciones de forma expresa la exigencia de que las injerencias estatales en los derechos fundamentales se encuentren presididas por el principio de legalidad, pudiéndose mencionar, por todas, la relevante —a los efectos que nos ocupan— STC 49/1999, de 5 de abril, que declaró que «por mandato

---

[179] En relación con la concurrencia de estos requisitos o exigencias de legalidad constitucional, autores como ARMENTA DEU han señalado que «la concurrencia de estos presupuestos tiene carácter genérico y, por ende, resulta aplicable a todas las medidas limitativas de derechos fundamentales» añadiendo que «tal configuración cumple, además, una importante función hermenéutica de la compleja regulación legal, de su ausencia o de las diferentes interpretaciones de los Tribunales en torno a ambas. Con idéntico objetivo, resulta importante también la jurisprudencia de los Tribunales Constitucional y Supremo, pese a su interpretación no siempre coincidente, y como no, la del Tribunal Europeo de Derechos Humanos». Vid. ARMENTA DEU, T., *Lecciones de Derecho Procesal Penal*, Madrid, Marcial Pons, 2017, p. 184.

expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal»[180].

El TC, desde sus primeras sentencias —tal y como señaló en la referida STC 49/1999—, había declarado que la reserva de ley no es una mera forma, sino que implica exigencias respecto al contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate, refiriéndose asimismo al «máximo esfuerzo» que ha de hacer el legislador para garantizar la seguridad jurídica entendida como la expectativa razonable fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del derecho.

Sin embargo, lo cierto es que la intervención de las comunicaciones como primera diligencia tecnológica relevante, fue regulada legalmente con diez años de retraso desde la aprobación de la CE[181], lo cual permitió que, en algunas resoluciones, se estimase suficiente la regulación del art. 18.3 CE para las intervenciones telefónicas[182]. Se trata de un criterio, en nuestra opinión, inadmisible, dado que, como dice MONTES

[180] Vid. STC 49/1999, de 5 de abril, FJ 4.º, la cual añadió que «esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su título I, 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 (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)».

[181] Con la salvedad de las intervenciones telefónicas en la investigación de delitos de terrorismo que se reguló en el art. 17 de la Ley Orgánica 9/1984, de 26 de diciembre, contra la actuación de bandas armadas y elementos terroristas y de desarrollo del art. 55.2 de la Constitución.

[182] Así, por ejemplo, la STS de 16 de enero de 1992 - ROJ: STS 158/1992, declaró que «el art. 18.3 de la CE garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas o telefónicas, salvo resolución judicial, y en base a ello se permite que la Policía acuda al Juzgado en solicitud de autorización cuando tenga necesidad de intervenir algún teléfono en su labor de averiguación del delito y descubrimiento del delincuente (art. 126 de dicha Ley fundamental). Así lo hizo en el caso presente, cuando aún no se había promulgado la L.O. 4/1.988, de 25 de mayo, que, entre otros, modificó el art. 579 de la LECr añadiendo unos nuevos párrafos relativos a la intervención u observación de las comunicaciones telefónicas, y, por tanto, no había otra regulación positiva que la que genéricamente aparecía en dicho art. 18.3, pues lo dispuesto en el art. 17 de la L.O. 9/1.984, de 24 de diciembre, sólo era aplicable a ciertos delitos cometidos por bandas armadas o elementos terroristas o rebeldes».

ÁLVARO, es necesaria una regulación legal además de la previsión constitucional del art. 18.3 CE, por no hacer este precepto referencia alguna a los presupuestos y condiciones de la injerencia[183].

Fue con la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, con la que el legislador introdujo una previsión legal para la intervención de las comunicaciones telefónicas, mediante la modificación del art. 579 LECrim, que hasta ese momento, regulaba la intervención de las comunicaciones postales y telegráficas, resultando cuando menos sorprendente, por decirlo de una forma eufemística, que el legislador tardase otros veinticinco años hasta que en el año 2015 llevase a cabo una adecuación de la legislación conforme se exigió en las SSTEDH dictadas en los casos Kruslin y Huvig c. Francia, ambas de 24 de abril de 1990[184]. Desde entonces ha sido copiosa la jurisprudencia constitucional y del TS que ha reclamado una adecuada regulación. Nos referiremos, por evidentes razones de extensión, a la más representativa.

En cuanto a las SSTEDH de 24 de abril de 1990, casos Kruslin y Huvig c. Francia, estas son consideradas —por la mención que de las mismas se ha realizado posteriormente por el propio TEDH— el primer precedente del alto Tribunal garante del CEDH en lo que respecta a una previsión legal para la injerencia en los derechos fundamentales, ya que establecían los presupuestos que debían cumplirse, para el respeto de tal requisito de previsión legal suficiente[185].

---

[183] Señala MONTES ÁLVARO que «parece difícil negar que la propia Constitución contiene tal habilitación, y desde esta perspectiva, los Jueces y Tribunales pueden, pues, acordarla, cuando concurran, además, los presupuestos materiales pertinentes (motivación, necesidad, proporcionalidad), sin embargo desde las exigencias de certeza que debe presidir cualquier injerencia en un derecho fundamental, es también patente que el art. 18.3 CE, al no hacer referencia alguna a los presupuestos y condiciones de la intervención telefónica, resulta insuficiente para determinar si la decisión judicial es o no el fruto previsible de la razonable aplicación de lo decidido por el legislador». Vid. MONTES ÁLVARO, M. A., «La regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el art. 18 CE», *Revista del Ministerio Fiscal*, n.º 3, 2017, p. 89.

[184] Dicen JIMÉNEZ SEGADO Y PUCHOL AIGUABELLA que «casi merece el aprobado el simple hecho de que se haya sacado adelante la regulación de estas medidas de investigación, muchas de las cuales, hasta que no entró en vigor la norma, permanecían sumidas en la más absoluta indigencia jurídica, lo que repercutía muy negativamente en la investigación y represión de las nuevas formas de criminalidad». Vid. JIMÉNEZ SEGADO, C.; PUCHOL AIGUABELLA, M., «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos», *Diario La Ley - Sección Doctrina*, n.º 8676, 2016, p. 2.

[185] Debe mencionarse no obstante, que previamente, la STEDH de 2 de agosto de 1984, caso Malone c. Reino Unido, ya había declarado en su apdo. 67, que la frase «prevista por la ley» no se limita a remitirse

En ellas, se estableció que, para que se entendiese cumplido este requisito, además de que la medida tenga fundamento en el ordenamiento jurídico interno, debe estar regulada por una ley de «calidad», lo cual se producirá cuando la dicha ley sea accesible a la persona afectada, quien ha de poder prever las consecuencias, debiéndose tratar por tanto de una norma «previsible». Asimismo, la norma ha de ser «compatible con la preeminencia del Derecho», lo que supone que el derecho interno debe ofrecer alguna protección contra las injerencias arbitrarias de los poderes públicos en los derechos fundamentales. Además, señaló que las escuchas y los demás procedimientos para interceptar las conversaciones telefónicas son un grave ataque a la vida privada y a la correspondencia, por lo que deben fundarse en una ley de singular precisión. Es indispensable que las normas que las regulan sean claras y detalladas, tanto más cuanto que los procedimientos técnicos utilizables se perfeccionan continuamente[186].

Por su parte, el primer precedente del TEDH en el que se puso de manifiesto que la legislación española era insuficiente para la injerencia en el derecho a la vida privada del art. 8 CEDH, fue la STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España, que condena al Estado español[187]. La investigación judicial llevada a cabo por la jurisdicción española, enjuiciada por el TEDH en la citada resolución, tuvo lugar entre los años 1984 —interposición de la denuncia— y 1986 —dictado del auto de procesamiento por el juez de instrucción—, por lo que no todavía no se había promulgado la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, no existiendo por tanto previsión legal (suficiente o no) que regulase la intervención de las comunicaciones telefónicas. En la misma se declaró, siguiendo la doctrina de las sentencias de los casos Kruslin y Huvig c. Francia, que la expresión «prevista por la ley» no se limita únicamente a remitir al Derecho interno, sino que, con

---

al Derecho interno, sino que también se refiere a la calidad de la «ley» y en consecuencia el Derecho interno tiene que ofrecer una determinada protección contra las vulneraciones arbitrarias por el Poder público de los derechos que garantiza el apartado 1 (del art. 8 CEDH), y ello dado que el peligro de la arbitrariedad aparece especialmente cuando las facultades de la Administración se utilizan secretamente, por lo que la ley debe emplear términos lo suficientemente claros para que puedan conocer todos en qué circunstancias y mediante qué requisitos permiten los poderes públicos hacer uso de esta medida secreta y posiblemente peligrosa, que afecta al derecho al respeto a la vida privada y a la correspondencia.

[186] Vid. SSTEDH, de 24 de abril de 1990, casos Kruslin y Huvig c. Francia, apdos. 27, 30 y 33.

[187] Concretamente la STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España, dictó el siguiente pronunciamiento de condena al Estado español: «*a)* que el Estado demandado debe pagar al demandante, en el plazo de tres meses, 1.500.000 (un millón quinientas mil) pesetas en concepto de costas y gastos; *b)* que este importe se incrementará aplicando un tipo de interés simple del 7,5 por 100 anual a partir del vencimiento de dicho plazo y hasta su abono efectivo». Actualmente 1.500.000 pesetas equivalen a 9.015,18 euros.

base a los principios mencionados de «calidad y previsibilidad de la ley», el Derecho interno debe ofrecer una cierta protección contra los atentados arbitrarios de los poderes públicos a los derechos garantizados por el art. 8 CEDH, con lo cual se daría además cumplimiento a la necesidad de que la persona afectada pueda prever las consecuencias de la meritada ley[188].

Puede afirmarse que la citada STEDH de 30 de julio de 1998, además de constituir el primer precedente en el que el TEDH declaró la insuficiencia normativa en relación con la injerencia en los derechos fundamentales, se erigió en el punto de partida de una jurisprudencia constitucional, dado que, tal y como señala LÓPEZ ORTEGA, la meritada sentencia del TEDH «colocó al Tribunal Constitucional español en el dilema de abordar directamente la cuestión relativa a la suficiencia de la cobertura legal que autoriza la injerencia…»[189]. En este sentido desde dicha resolución han sido numerosas las sentencias del TC que han venido reclamando una regulación legislativa que finalmente ha tenido lugar tras un cuarto de siglo desde que aquel inicial precedente tuvo publicidad.

El primer pronunciamiento por parte de nuestro TC acogiendo la doctrina del TEDH se refleja en la STC 49/1999, de 5 de abril, que ya citamos al iniciar este apartado. No obstante ser posterior a la modificación del art. 579 LECrim por la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, enjuició hechos en relación con una investigación judicial llevada a cabo con anterioridad a la misma, y en la que tras referirse al incumplimiento de previsión legal para la injerencia conforme a los principios proclamados en las SSTEDH de los casos Kruslin y Huvig c. Francia, declaró que «ha de subrayarse que estamos en presencia de una vulneración del art. 18.3 CE, autónoma e independiente de cualquier otra: la insuficiencia de la ley, que sólo el legislador puede remediar y que constituye, por sí sola, una vulneración del derecho fundamental. Eso es así porque la insuficiente adecuación del Ordenamiento a los requerimientos de certeza crea, para todos aquellos a los que las medidas de intervención telefónica pudieran aplicarse, un peligro, en el que reside precisamente dicha vulneración».

---

[188] Apdo. 46 de la STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España.

[189] LÓPEZ ORTEGA, J. J., «La utilización de medios técnicos de observación y vigilancia en el proceso penal», en Boix Reig, J. (dir.), Jareño Leal, Á. (coord.), *La protección jurídica de la intimidad*, Madrid, Iustel, 2010, p. 299.

Constituye igualmente una cita de obligada mención la STEDH de 18 de febrero de 2003, caso Prado Bugallo c. España, dado que la misma se ocupa de unos hechos acaecidos con posterioridad a la entrada en vigor de la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal. Esta resolución del tribunal garante del CEDH, se refirió a la mencionada reforma legal declarando, en su apdo. 30, que «las garantías introducidas por la Ley de 1988 no responden a todas las condiciones exigidas por la jurisprudencia del Tribunal, especialmente en las sentencias Kruslin contra Francia y Huvig contra Francia, para evitar abusos».

Efectivamente, la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal no satisfizo la carencia que venía siendo denunciada, fundamentalmente por adolecer de la precisión a la que había referido el TEDH. Por ello, con posterioridad a la referida LO, el art. 579 LECrim[190] ha precisado un constante desarrollo por la jurisprudencia constitucional y del TS[191], que hemos de considerar digno de elogio, habida cuenta de que sin este laborioso trabajo jurisprudencial y dada la inexplicable inactividad del legislador, hubieran quedado impunes numerosos delitos graves. Como señaló el CONSEJO DE ESTADO, la insuficiencia del artículo 579 LECrim «ha sido suplida a través de una ardua e intensa labor jurisprudencial de determinación de las condiciones para una legítima intervención en las comunicaciones a los fines de una investigación penal»[192].

---

[190] Resulta conveniente señalar que los apartados 2 y 3 del art. 579 LECrim, conforme a la redacción dada por la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, tenían el escueto tenor literal siguiente:
«2. Asimismo, el juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.
3. De igual forma, el juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos».

[191] Resulta muy ilustrativo el importante ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992, que tras referirse a la excesiva indeterminación y amplitud de los apartados 2 y 3 de entonces vigente art. 579 LECrim, declaró que «sin llegar a mantener la carencia de cobertura, en sede de legalidad ordinaria, atendida la insuficiencia del artículo 579 de la Ley de Enjuiciamiento Criminal […] hay que manifestar que dada la citada y grave insuficiencia de la regulación actualmente vigente, es obligado llevar a cabo una especie de construcción por vía jurisprudencial de la forma correcta de realización de tal medida…».

[192] CONSEJO DE ESTADO, *Dictamen 97/2015, 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 tecnológica*, 2015, p. 16, Consultado en http://www.boe.es/buscar/doc.php?id=CE-D-2015-97, el 8 de marzo de 2018.

El propio TEDH reconoció, en la meritada Sentencia de 18 de febrero de 2003, esta intrincada tarea de la jurisprudencia española[193]. Este reconocimiento llegó hasta el punto de inadmitir una demanda en la que se invocaba la vulneración del art. 8 CEDH, declarando que «aunque es deseable una enmienda legislativa que incorpore a la ley los principios de la jurisprudencia del Tribunal, como ha indicado sistemáticamente el Tribunal Constitucional, el Tribunal considera que el artículo 579 del Código de Procedimiento Penal, modificada por la Ley 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, y complementada por la jurisprudencia del Tribunal Supremo y el Tribunal Constitucional, establece normas claras y detalladas, y especifica de antemano, con suficiente claridad, el alcance y las modalidades de ejercicio de la discreción de las autoridades en el campo en cuestión»[194].

Por su parte, nuestra jurisprudencia constitucional acoge la citada doctrina del TEDH con la STC 184/2003, de 23 de octubre, en la que en su FJ 7.º se instaba al legislador a que acabase cuanto antes con esta anomia, declarando expresamente que es «función de la tarea legislativa de las Cortes ponerle término en el plazo más breve posible». Previamente, en su FJ 5.º, ponía de manifiesto que «el art. 579 LECrim adolece de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el art. 18.3 CE para la protección del derecho al secreto de las comunicaciones, interpretado, como establece el art. 10.2 CE, de acuerdo con el art. 8.1 y 2 CEDH».

En cuanto a los aspectos que necesariamente deberían ser regulados legalmente, precisaba, en el mismo FJ 5.º, que los mismos se concretaban en «la definición de las categorías de personas susceptibles de ser sometidas a escucha judicial; la naturaleza de las infracciones susceptibles de poder dar lugar a ella; la fijación de un límite a la duración de la ejecución de la medida; el procedimiento de transcripción de las conversaciones interceptadas; las precauciones a observar, para comunicar, intactas y

[193] La STEDH de 18 de febrero de 2003, caso Prado Bugallo c. España, declaró en su apdo. 31 que «estas lagunas han sido señaladas por las jurisdicciones superiores españolas que han entendido que las modificaciones realizadas por esta Ley eran insuficientes para responder a las garantías que deben rodear las intervenciones telefónicas. Por esto, además de las disposiciones legislativas, el Tribunal Supremo, principalmente en su Resolución de 18 de junio de 1992 […] así como el Tribunal Constitucional, consideraron necesario definir toda una serie de garantías complementarias que precisaran el alcance y las modalidades del poder de apreciación de los jueces, así como las condiciones de establecimiento de las actas que consignan las conversaciones interceptadas y su uso por el juez instructor».

[194] Vid. Decisión Sección 5.ª TEDH de 25 de septiembre de 2006, caso Abdulkadir Coban c. España.

completas, las grabaciones realizadas a los fines de control eventual por el juez y por la defensa; las circunstancias en las cuales puede o debe procederse a borrar o destruir las cintas, especialmente en caso de sobreseimiento o puesta en libertad».

Señalaba, asimismo, en el FJ 5.º, que el art. 579 LECrim «tampoco regula expresamente y, por tanto, con la precisión requerida por las exigencias de previsibilidad de la injerencia en un derecho fundamental las condiciones de grabación, custodia y utilización frente a ellos en el proceso penal como prueba de las conversaciones grabadas de los destinatarios de la comunicación intervenida, pues el art. 579 LECrim sólo habilita específicamente para afectar el derecho al secreto de las comunicaciones de las personas sobre las que existan indicios de responsabilidad criminal en el momento de acordar la intervención de las comunicaciones telefónicas de las que sean titulares o de las que se sirvan para realizar sus fines delictivos, pero no habilita expresamente la afectación del derecho al secreto de las comunicaciones de los terceros con quienes aquéllos se comunican».

Por ello, concluía el FJ 5.º conviniendo que el art. 579 LECrim no es por sí mismo norma de cobertura adecuada, atendiendo a las garantías de certeza y seguridad jurídica, para la restricción del derecho fundamental al secreto de las comunicaciones telefónicas (art. 18.3 CE)»[195].

[195] Ha de subrayarse que la STC 184/2003, de 5 de abril, FJ 6.º declaró de una forma similar al criterio mantenido en la Decisión Sección 5.ª TEDH de 25 de septiembre de 2006, caso Abdulkadir Coban c. España, a la que anteriormente nos hemos referido, que la declaración de insuficiencia del art. 579 LECrim, no era, sin embargo, suficiente para resolver la cuestión controvertida de si las deficiencias de dicho precepto implicaban la vulneración del derecho al secreto de las comunicaciones, y aunque en el caso concreto que se enjuiciaba en amparo se determinó finalmente que se había vulnerado el derecho al secreto de las comunicaciones, esta vulneración se produjo por ausencia de datos objetivos que pudieran servir de soporte a la sospecha de comisión de los hechos delictivos y a la implicación en ellos de las personas en cuyas comunicaciones telefónicas se solicitó la intervención, y no así por la ausencia de regulación legal, aduciendo el TC que «si, pese a la inexistencia de una ley que satisficiera las genéricas exigencias constitucionales de seguridad jurídica, los órganos judiciales, a los que el art. 18.3 de la Constitución se remite, hubieran actuado en el marco de la investigación de una infracción grave, para la que de modo patente hubiera sido necesaria, adecuada y proporcionada la intervención telefónica y la hubiesen acordado respecto de personas presuntamente implicadas en el mismo, respetando, además, las exigencias constitucionales dimanantes del principio de proporcionalidad, no cabría entender que el juez hubiese vulnerado, por la sola ausencia de dicha ley, el derecho al secreto de las comunicaciones telefónicas». Asimismo, resulta relevante mencionar que en el FJ 7.º de la referida sentencia, el TC rechazó elevar la cuestión al pleno de conformidad con el art. 55.2 de la Ley Orgánica del Tribunal Constitucional, para ejercer el control de la posible inconstitucionalidad del art. 579 LECrim, argumentando que este control de constitucionalidad «versa sobre un precepto con un núcleo o contenido constitucionalmente válido, pero insuficiente, esto es, sobre un defecto de ley. El ejercicio por este

Cabe señalar que también el TS también se refirió a la insuficiencia del art. 579 LECrim señalando como motivo de la misma «el considerable número de espacios en blanco que contiene», y declaró, en la misma línea a la que nos hemos referido anteriormente, «que tal insuficiencia no implica por sí misma necesariamente la ilegitimidad constitucional de la actuación de los órganos jurisdiccionales que autorizan la intervención, siempre que se hayan respetado las garantías jurisprudencialmente establecidas con respecto a dicha medida que demandan el Convenio Europeo el TEDH y la propia doctrina de nuestro Tribunal Constitucional».[196] Esta denuncia la ha mantenido el TS hasta poco antes de la promulgación de la LO 13/2015, concretamente en la STS 250/2014, de 14 de marzo, FJ 8.º, en la que señaló que «es cierto que la pereza que ha envuelto históricamente al legislador español para abordar una regulación normativa acorde con la revolución tecnológica y el desarrollo de las comunicaciones telemáticas, han convertido el art. 579 de la LECrim en un precepto manifiestamente

Tribunal de su tarea depuradora de normas contrarias a la Constitución culminaría, en su caso, con una declaración de inconstitucionalidad por defecto de la disposición legal —art. 579 LECrim— que agravaría el defecto mismo —la falta de certeza y seguridad jurídicas— al producir un vacío mayor. Los intereses constitucionalmente relevantes que con el art. 579.3 LECrim se tutelan se verían absolutamente desprotegidos por cuanto aquella declaración podría comportar, cuando menos, la obligación de los poderes públicos de inaplicar la norma viciada de inconstitucionalidad. De esta suerte, y en el contexto de un proceso de amparo en el que ya se ha satisfecho la pretensión principal de los recurrentes, no podemos dejar de advertir que el resultado de inconstitucionalidad al que se llegase entraría en conflicto con las exigencias mismas del art. 18.3 CE, pues dejaríamos el ordenamiento desprovisto de cualquier habilitación legal de injerencia en las comunicaciones telefónicas, agravando la falta de certeza y seguridad jurídicas de las situaciones ordenadas por el art. 579 LECrim hasta tanto el legislador no completase el precepto reparando sus deficiencias a través de una norma expresa y cierta».

[196] Vid. SSTS 1335/2001, de 19 de julio, FJ 19.º; y 861/2007, de 24 de octubre, FJ 2.º en la que se indicó que «no es la primera vez que esta cuestión se suscita en un recurso de casación, debiendo significarse que en las numerosas ocasiones en las que esta Sala ha tenido que pronunciarse al respecto, hemos dejado constancia de que, ciertamente, la regulación que el art. 579 efectúa de este acto instructorio resulta ser muy insuficiente por el considerable número de espacios en blanco que contiene en materias tales como los supuestos que justifican la intervención, el objeto y procedimiento de ejecución de la medida, así como de la transcripción en acta del contenido de los soportes magnéticos, la custodia y destrucción de las cintas, etc. Pero también la jurisprudencia de esta Sala, inspirada en la del Tribunal Constitucional, ha sostenido reiterada y pacíficamente que esta situación de práctica "anomia" legislativa ha sido suficientemente colmada por la doctrina jurisprudencial de nuestros Tribunales, que han interpretado el art. 18.3 CE, al igual del resto de las normas que tutelan los derechos fundamentales, de conformidad con el art. 8 del Convenio y de su órgano jurisdiccional de aplicación que es el Tribunal Europeo de Derechos Humanos, subrayándose la necesidad de una "cuidada interpretación constitucional" del art. 579, respetuosa con el principio de proporcionalidad y las restantes garantías que protegen los derechos fundamentales y libertades básicas».

insuficiente para abarcar en sus lacónicos enunciados todos y cada uno de los variados problemas que pueden suscitarse»[197].

En cualquier caso, puede afirmarse que con la LO 13/2015 ha quedado cumplido el requisito de una previsión normativa suficiente, siquiera sea de forma temporal, habida cuenta de las numerosas voces que vienen reclamando la promulgación de una nueva LECrim, conforme detallaremos en el último apartado de este capítulo.

2. La reserva jurisdiccional

2.1. El requisito de la jurisdiccionalidad para la ejecución de medidas limitativas de derechos fundamentales

La exclusividad jurisdiccional es y ha sido durante toda la vigencia de la CE de 1978 un requisito insoslayable en lo que respecta a la ejecución de medidas limitativas de derechos fundamentales. En este sentido, la utilización de diligencias de investigación que limitan derechos fundamentales, a diferencia de las que no restringen los mismos[198], quedan vedadas a la Policía Judicial o el Ministerio Fiscal sin la previa autorización judicial.

---

[197] En esta resolución el TS invocó sus anteriores SSTS 487/2007, de 29 de mayo, FJ 1.º y 363/2008, de 23 de junio, FJ 2.º, en las que llamando la atención sobre la urgencia de la reforma de la LECrim, denunció la situación existente como un «clamoroso ejemplo de mora legislatoris en que vienen incurriendo los poderes públicos encargados de promover los procesos legislativos. Ni las condenas del Tribunal Europeo de Derechos Humanos, ni las reiteradas admoniciones del Tribunal Constitucional llamando a poner término a esta singular forma de anomia, ni los esfuerzos de la Sala Segunda por integrar las insuficiencias del actual art. 579 de la LECrim, han sido suficientes para superar el actual estado de cosas. También la Fiscalía General del Estado, en las Memorias correspondientes a los últimos años, ha incluido entre sus propuestas de reforma legislativa, la solicitud de una regulación más detallada del incompleto art. 579 de la LECrim, insistiendo en la inaplazable necesidad de abordar una reforma del vigente marco jurídico en materia de interceptación de las comunicaciones telefónicas».

[198] Como así ocurre con las diligencias policiales de prevención, entre las que pueden señalarse aquellas que tienen por objeto obtener una prueba preconstituida, por tratarse hechos irrepetibles, que no pueden ser trasladados al momento de la celebración del juicio oral. Entre tales diligencias pueden citarse los métodos alcoholimétricos, las grabaciones de videovigilancia, el análisis sobre estupefacientes, las inspecciones corporales o la geolocalización. Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 363. Aun así, debe recordarse que el art. 295 LECrim exige la puesta en conocimiento de la autoridad judicial de tales diligencias en el plazo máximo de veinticuatro horas, al disponer lo siguiente: «En ningún caso los funcionarios de Policía Judicial podrán dejar transcurrir más de veinticuatro horas sin dar conocimiento a la autoridad judicial o al Ministerio Fiscal de las diligencias que hubieran practicado salvo en los supuestos de fuerza mayor y en el previsto en el apartado 2 del art. 284».

Cabe señalar que la atribución de esta facultad a jueces y tribunales es beneficiosa, en primer lugar, para la propia sociedad, por cuanto las pruebas obtenidas, directa o indirectamente, violentando los derechos y libertades fundamentales, no podrán surtir efecto (art. 11.1 LOPJ). Se puede afirmar, por ello, que serían los propios delincuentes los principales beneficiados en caso de no existir un control jurisdiccional a la actividad investigadora del delito cuando sean utilizadas medidas de investigación que puedan restringir derechos fundamentales.

En cuanto a la justificación o fundamento de este requisito, autores como DELGADO MARTÍN afirman que la autorización de la concreta medida debe ser otorgada por un órgano estatal ajeno a la propia organización policial «como única forma de garantizar la adecuación del juicio de proporcionalidad: solo puede admitirse con la autorización previa y bajo el estricto control de una autoridad pública independiente (la Autoridad judicial)»[199]. Otros autores, como GONZÁLEZ-CUELLAR SERRANO, consideran que su fundamento se encuentra en la circunstancia de que son los órganos judiciales los constitucionalmente previstos para garantizar de forma inmediata la eficacia de los referidos derechos[200]. Puede destacarse asimismo la opinión de ASENCIO MELLADO, quien afirma que la exigencia de jurisdiccionalidad tiene su base «en el principio de exclusividad jurisdiccional (art. 117 CE) y su manifestación negativa que prohíbe a la Administración la restricción, en línea de principios, de derechos fundamentales»[201].

---

[199] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., pp. 346-347. Cita este autor a MIRELLE DELMAS-MARTY, dirigiendo la Asociación de Recherches pénales européennes (ARPE), Procesos penales de Europa, editorial Edijus, Zaragoza, 2000, p. 545, quien afirma lo siguiente: «Se trata del papel del juez como garante de las libertades. Cada vez más, la función del juez no es tanto la búsqueda de equilibrio entre la eficacia de la investigación y la protección de la persona, como la justificación de una excepción a la libertad individual».

[200] Cabe señalar que GONZÁLEZ-CUELLAR SERRANO considera la jurisdiccionalidad como un requisito de la proporcionalidad en los casos en los que la CE impone la decisiva intervención del órgano judicial para la limitación de derechos fundamentales y señala que «son precisamente los órganos judiciales los constitucionalmente previstos para garantizar de forma inmediata la eficacia de dichos derechos y, por ello, queda sometida en todo caso a su juicio la decisión sobre la proporcionalidad de las medidas limitativas, desde la perspectiva del caso concreto, sin que el legislador se encuentre autorizado para privar a los jueces de un margen de apreciación en esta materia, que les permita calibrar el peso de los intereses en conflicto, estableciendo normas de efectos automáticos». Y añade que, «como advierte la doctrina alemana, las disposiciones limitativas de derechos constitucionalmente garantizados sólo son admisibles como "disposiciones de poder" (*Kann-Bestimmungen*), nunca "de deber" (*Muss-Bestimmungen*), en tanto la Constitución haya previsto determinados órganos justamente para controlar la admisibilidad de las medidas en el caso concreto. Vid. GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», *Cuadernos de Derecho Público*, n.º 5, 1998, p. 197.

[201] ASENCIO MELLADO, J. M., *Derecho Procesal Penal*, Valencia, Tirant Lo Blanch, 2010, p. 122.

Finalmente, tal y como se venía reclamando doctrinal y jurisprudencialmente, esta necesidad ha quedado plasmada en el art. 588 bis a.1 LECrim, tras la reforma operada por la LO 13/2015 de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

2.2. Aspectos esenciales de la jurisdiccionalidad

Aun cuando del requisito de la jurisdiccionalidad derivan diversos aspectos que conforman la misma, los cuales desarrollaremos en el primer epígrafe del capítulo IV, dedicado a la «autorización judicial», podemos afirmar que son dos las cuestiones esenciales en virtud de las que cobra sentido este requisito, como son: la exclusividad judicial propiamente dicha y la motivación.

2.2.1. La exclusividad judicial propiamente dicha

Este aspecto acaba de ser examinado en el apartado anterior al estudiar con carácter general «el requisito de la jurisdiccionalidad para la ejecución de medidas limitativas de derechos fundamentales». Baste sencillamente reiterar —recopilando los tres criterios doctrinales que hemos mencionado como justificadores del principio—, que toda aquella resolución que lleve implícita una restricción del derecho fundamental de un ciudadano, deberá ser examinada por una autoridad independiente de la administración investigadora, la cual, teniendo en cuenta el principio de exclusividad jurisdiccional que la CE atribuye a jueces y tribunales para la garantía inmediata de los derechos fundamentales, no podrá ser otra que la autoridad judicial competente en cada caso.

2.2.2. La motivación

Una resolución que, como consecuencia de la necesidad de su dictado en el marco de la investigación de un delito, lleve aparejada la restricción de un derecho o libertad fundamental, precisa una fundamentación acerca de las razones por las que es necesaria tal restricción, habida cuenta que, teniendo en cuenta el canon de protección reforzada que impone el art. 53.2 CE[202], se hace necesario que se justifique la exigencia

[202] Dispone el art. 53.2 CE: «Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección 1.ª del capítulo segundo ante los Tribunales ordinarios por un

de la injerencia en los mismos, sin perjuicio de los supuestos constitucionales de suspensión de los derechos y libertades[203].

Señala a este respecto DE URBANO CASTRILLO, en relación con la intervención de las comunicaciones electrónicas, que «la motivación de la decisión autorizante, dado que debe ser una medida extraordinaria, en absoluto rutinaria o habitual, habrá de ser especialmente exigente, debiendo contener los autos en que se acuerde una intervención de las comunicaciones electrónicas, unos razonamientos detallados respecto a los aspectos fácticos y técnicos así como tener en cuenta cómo se practicará la intervención, a los efectos ele determinar cuestiones como duración de la medida, posibles prórrogas, entrega del material intervenido…»[204].

En este sentido, y conforme veremos más adelante, aunque la motivación así entendida es una manifestación del principio de proporcionalidad, la misma ha de considerarse como un aspecto esencial del principio de reserva jurisdiccional, y ello porque sin una adecuada motivación de la resolución que acuerde la medida, se desnaturalizaría el requisito de la jurisdiccionalidad[205].

El TC, desde sus inicios, dejó sentada la obligatoriedad de la motivación, que, en los casos de limitación de derechos fundamentales, se convierte en un riguroso

---

procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional…»

[203] A este respecto dispone el art. 55 CE: 1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción. 2. Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. La utilización injustificada o abusiva de las facultades reconocidas en dicha ley orgánica producirá responsabilidad penal, como violación de los derechos y libertades reconocidos por las leyes.

[204] DE URBANO CASTRILLO, E., «La investigación tecnológica del delito», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 2, 2007, p. 69, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[205] Señala a este respecto al STS 746/2014, de 13 de noviembre, FJ 11.º que «al ser medida de exclusiva concesión judicial, esta debe ser fundada, es decir, motivada y ello supone exponer sistemáticamente las razones que apoyan una decisión».

requisito[206], declarando asimismo que, en estos casos, se trata de una «motivación más intensa, cuya fundamentación […] radica en la interdicción de la arbitrariedad de los poderes públicos (art. 9.3 CE)» [207].

Con base en lo anterior y siguiendo el trascendental —en lo que a las medidas restrictivas de derechos fundamentales se refiere— ATS de 18 de junio de 1992, la motivación «significa la exteriorización razonada de los criterios en los que se apoya la decisión judicial. Es decir, la exigencia de motivación se satisface cuando, implícita o explícitamente, se puede conocer el razonamiento, esto es, el conjunto de reflexiones que condujeron al juez a tomar la decisión que tomó»[208].

Al mismo tiempo, la motivación se hace necesaria a fin de que el afectado por la medida pueda conocer la razón por la que se adoptó, ya que de no ser así, no podría ejercitar su derecho a interponer los recursos que procediesen, con total conocimiento de las circunstancias[209].

3. La proporcionalidad

Poco podemos aportar en cuanto a la teoría del principio de proporcionalidad, habida cuenta de los ríos de tinta que sobre el mismo han circulado doctrinal y jurisprudencialmente. Ello no obstante, resulta necesaria, al menos una exposición

[206] Vid. STC 26/1981, de 17 de julio, FJ 14.º, que declaró que «sin embargo, cuando se coarta, como en este caso, el libre ejercicio de los derechos reconocidos por la Constitución, el acto es tan grave que necesita encontrar una especial causalización y el hecho o el conjunto de hechos que lo justifican deben explicarse con el fin de que los destinatarios conozcan las razones por las cuales su derecho se sacrificó y los intereses a los que se sacrificó. De este modo, la motivación es no sólo una elemental cortesía, sino un riguroso requisito del acto de sacrificio de los derechos».

[207] Vid. STC 239/1999, de 20 de diciembre, FJ 5.º, que añade que la arbitrariedad «ha de conjurarse por el órgano judicial mediante la rigurosa y precisa exposición del insoslayable juicio de proporcionalidad entre la medida restrictiva adoptada y el derecho fundamental limitado, en atención a las circunstancias de cada caso».

[208] Vid. ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992, FJ 4.º en el que tras señalar que «es preciso que este tipo de injerencias se constituyan en práctica excepcional, sometida de manera efectiva a control judicial, sin que sea por tanto, correcto extender autorizaciones prácticamente en blanco, siendo preciso, por el contrario, una motivación razonable, lo que no quiere decir, desde luego, exhaustiva, que habrá de mantenerse en secreto mientras la investigación se realiza» concluyó que «la motivación de la resolución es, pues, decisivamente importante. No cabe, obviamente, decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos porque en tales circunstancias el principio de proporcionalidad, que afecta al derecho procesal y al sustantivo, jamás podría ser exteriorizado y, por consiguiente, tenido en cuenta por el juez».

[209] Vid. STC 62/1982, de 15 de octubre, FJ 2.º

resumida —nunca mejor dicho, dado que sobre este tema hay diversas tesis doctorales publicadas—[210] de las ideas fundamentales en virtud de las que se conformó la teoría de este trascendental principio, examinado desde el punto de vista del derecho procesal, con anterioridad a su incorporación a la ley mediante la LO 13/2015, en lo que a las medidas restrictivas de derechos fundamentales se refiere[211], y ello por la imprescindible aplicación de este principio cuando deba acordarse la práctica de un registro informático para investigar un delito.

En cuanto al fundamento del principio de proporcionalidad, podemos situar el mismo en el respeto de la dignidad humana, como así se encargó de señalarlo la primera resolución en la que —desde el punto de vista de la injerencia en los derechos fundamentales como consecuencia de las diligencias de investigación del delito— el TS exigió el reconocimiento del principio. Se trata del importante ATS de 18 de junio de 1992, que declaró que «uno de los presupuestos fundamentales de nuestro Estado de Derecho, democrático y social, establecido en la Constitución, es el del respeto a la dignidad e intimidad de la persona humana, esencialmente libre, como base de la convivencia. Por ello existe o debe existir un obligado correlato, una proporcionalidad, entre el reconocimiento de la plenitud de estos derechos y las intromisiones en la vida privada de la persona que, en principio, son ilegitimas»[212]. Cabe señalar que el TC, con anterioridad, en una de las primeras resoluciones en las que sentó doctrina acerca de la proporcionalidad en relación con la injerencia de los actos procesales en los derechos fundamentales, se refirió igualmente a la dignidad de la persona como fundamento del principio, al declarar que la afectación del derecho a la intimidad «es posible sólo por decisión judicial que habrá de prever que su ejecución sea respetuosa de la dignidad de

[210] Conforme ha sido verificado en la base de datos TESEO del Ministerio de Educación, Cultura y Deporte, en la página web https://www.educacion.gob.es/teseo/irGestionarConsulta.do

[211] Para ser estrictos, debe señalarse que la primera incorporación del principio de proporcionalidad en la LECrim se produce en relación con las intervenciones corporales, con la LO 15/2003, de 25 de noviembre, modificadora del CP, que en su Disposición Final 1.1.c) añadió un párrafo segundo al art. 363 LECrim, el cual dispone que «siempre que concurran acreditadas razones que lo justifiquen, el juez de instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad».

[212] Vid. Auto de 18 de junio de 1992, ROJ: ATS 3773/1992, FJ 1.º

la persona y no constitutiva, atendidas las circunstancias del caso, de trato degradante alguno (arts. 10.1 y 15 de la Constitución)»[213].

Doctrinalmente, autores como BARNES, han señalado que la cláusula del Estado de Derecho y los propios derechos fundamentales, representan el fundamento último en el que descansa la proporcionalidad de la injerencia en el derecho fundamental, lo cual expresa de forma abreviada que el principio de proporcionalidad «encarna una idea elemental de justicia material: la proscripción de todo sacrificio de la libertad inútil, innecesario o desproporcionado»[214].

Por nuestra parte, podemos añadir que el principio de proporcionalidad constituye una garantía para el efectivo cumplimiento del principio constitucional de la «interdicción de la arbitrariedad de los poderes públicos (art. 9.3 CE).

Este principio, también denominado «prohibición de exceso», nace en el seno del Derecho Penal y, aunque los orígenes más remotos del mismo se pueden encontrar en el Derecho romano y en las reflexiones sobre la justicia de la filosofía práctica griega, sus primeras formulaciones se remontan al siglo XVIII, en el que autores como Beccaría se refirieron a la pena proporcional a la culpabilidad, siendo destacable que ya en la Declaración de los Derechos del Hombre y del Ciudadano de 1789 se disponía en su art. 8 que «la Ley solo debe establecer penas estricta y evidentemente necesarias…»[215].

En nuestro país, al no tener reconocimiento expreso en la CE de 1978[216], la proporcionalidad se erigió en el ámbito del Derecho Penal, en un principio general del derecho íntimamente relacionado con el principio de intervención mínima, y que, con

---

[213] Vid. STC 37/1989, de 15 de febrero, FJ 7.º

[214] BARNES, J., «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, vol. 5, 1998, p. 19.

[215] En cuanto a las referidas menciones de los orígenes históricos del principio de proporcionalidad, vid. PERELLÓ DOMENECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *Jueces para la Democracia. Información y Debate*, n.º 28, 1997, p. 69; RUIZ RUIZ, R.; DE LA TORRE MARTÍNEZ, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, pp. 30-31; y KLUTH, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 220-221.

[216] Aun cuando lo se menciona expresamente en la CE, GIMENO SENDRA considera que el principio de proporcionalidad «se encuentra implícitamente contenido en el art. 25 (que, al consagrar el principio de "legalidad", no sólo establece el de "tipicidad", sino también el de "proporcionalidad" entre la medida y la sanción) y más concretamente en cada uno de los preceptos que establecen los límites del ejercicio de los derechos fundamentales». Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 57.

base en el valor superior de la libertad proclamado en el art. 1 CE, persigue como objetivo principal evitar una aplicación desmesurada de las penas privativas de libertad y posteriormente de todas las penas en general. Conforme al mismo, la pena a imponer por la comisión de un delito deberá guardar una correlación con el ilícito cometido, sin que quepa imponer una pena que no sea estrictamente necesaria para alcanzar los fines que la justifican.

En cualquier caso, y sin perjuicio de lo anterior, ha de señalarse que, con carácter general para todas las ramas del derecho, la construcción moderna del principio de proporcionalidad tiene su origen en la jurisprudencia alemana[217], país en el que, como señala KLUTH, se alude normalmente, tanto por la doctrina como por la jurisprudencia, al «principio de prohibición de exceso» y no al «principio de proporcionalidad», al entenderse que la prohibición de exceso tiene un contenido más amplio del que formaría parte la proporcionalidad, afirmando este autor que con su reconocimiento por el TC alemán «se ponía fin a una discusión desarrollada en Alemania durante más de cien años».

Situándonos ya en nuestra disciplina, el principio proporcionalidad surge en el Derecho Procesal como un criterio necesario para una adecuada protección de los derechos fundamentales frente a las injerencias en los mismos como consecuencia de cualquier acto procesal, adquiriendo especial relevancia dentro de los actos procesales, los actos procesales de investigación.

El principio cobró especial fuerza en nuestro país en los años 80 del siglo pasado, señalando GONZÁLEZ-CUELLAR SERRANO que en el Derecho procesal español el

[217] Así lo señalan RUIZ RUIZ y DE LA TORRE MARTÍNEZ, indicando que «la construcción de este principio, tal y como se entiende en la actualidad, es obra fundamentalmente de la doctrina y la jurisprudencia constitucionales y administrativas alemanas, a quienes se debe la elaboración técnica del mismo. Así, el Tribunal Constitucional alemán reconoció expresamente en 1968 que la "prohibición de exceso" (Übermaβverbot) y el "principio de proporcionalidad" (Verhältnismäβigkeitsprinzip) eran reglas generales aplicables en todos los ámbitos de la actividad estatal, cuyo rango constitucional deriva del principio constitucional del Estado de Derecho del que aquéllas reglas se deducen. Y, desde entonces, el alto Tribunal alemán ha realizado mediante sus sentencias aportaciones importantes en el reconocimiento del principio, las cuales han ayudado a asentar el concepto de que "en la República Federal de Alemania el principio de proporcionalidad tiene rango jurídico constitucional. Ese reconocimiento deriva del principio de Estado de Derecho, teniendo como sustrato esencial los derechos fundamentales". Esta concepción se ha mantenido hasta la actualidad por la jurisprudencia y la doctrina alemana». Vid. RUIZ RUIZ, R.; DE LA TORRE MARTÍNEZ, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», cit., p. 31.

principio de prohibición de exceso[218] o proporcionalidad en sentido amplio comenzó a ser objeto de estudio doctrinal a finales de la década de los ochenta, sin que con anterioridad hubiese merecido con carácter general y salvo algunas excepciones la atención de los estudiosos del derecho procesal[219].

Con anterioridad, la proporcionalidad había sido proclamada en el CEDH que, en el apartado segundo de los arts. 8, 9, 10 y 11 —en los que consagra respectivamente los derechos a la vida privada y familiar; a la libertad de pensamiento, de conciencia y de religión; a la libertad de expresión; y a la libertad de reunión y asociación—, dispone de una forma similar en todos ellos que las restricciones a dichos derechos solo podrán tener lugar cuando la injerencia constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Estos postulados fueron aplicados en distintos supuestos por la jurisprudencia del TEDH, la cual tuvo indudable influencia para el desarrollo del principio en nuestro país.

---

[218] Cabe señalar que con este nombre se definió al principio en el Anteproyecto de LECrim de 2013. Concretamente, su art. 12 disponía lo siguiente:
«Artículo 12. Principio de prohibición de exceso
1. La adopción y práctica de medidas restrictivas de derechos individuales sólo es admisible cuando no resulten excesivas y concurran la totalidad de los requisitos de legalidad, idoneidad, necesidad y proporcionalidad establecidos en este artículo.
2. Sólo podrán autorizarse y ejecutarse las medidas de investigación o cautelares restrictivas de derechos previstas por la Ley. Las medidas no previstas por la Ley están prohibidas.
3. Las medidas han de acordarse exclusivamente para la consecución de las finalidades para las que se encuentran legalmente previstas.
4. Las medidas deben ser idóneas para alcanzar sus fines y adecuadas a los mismos en las circunstancias del caso en su contenido, medida, duración y en su ámbito subjetivo de aplicación.
5. Será preferida la medida menos gravosa que sea suficientemente eficaz.
6. Las medidas serán proporcionadas, de forma que, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la realización de la ponderación de los intereses en conflicto la valoración del interés público se basará en la gravedad del hecho, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».

[219] Señala GONZÁLEZ-CUELLAR SERRANO que entre las excepciones relativas a los autores que si trataron el principio de proporcionalidad con anterioridad a los años finales de la década de los 80 del siglo pasado, en los que comenzó a ser objeto de estudio este principio, cabe destacar a GIMENO SENDRA, que incluía la proporcionalidad entre los principios del proceso penal en sus manuales. Vid. GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», cit., p. 191.

El primer referente lo constituye la STEDH de 7 de diciembre de 1976, caso Handyside c. Reino Unido, en la que se determinó que, si bien corresponde a cada Estado adoptar, conforme a sus leyes, los casos en los que resulta posible la restricción de los derechos y libertades, el ejercicio de tal margen de apreciación habrá de ser proporcionado a la finalidad perseguida[220], situando el criterio fundamental para estimar que la medida ha sido proporcionada, en la circunstancia de que la misma fuese «necesaria para obtener el fin perseguido»[221].

Por su parte, la STEDH de 22 de octubre de 1981, caso Dudgeon c. Reino Unido declaró en su apdo. 53 que «finalmente, en el artículo 8, al igual que en otros varios artículos del Convenio, el concepto de "necesidad" está vinculado al de "sociedad democrática"» y añadió que «de acuerdo con el derecho emanado de los fallos del Tribunal una restricción de un derecho amparado por el Convenio puede no considerarse como "necesaria en una sociedad democrática" —de lo cual son dos puntos de referencia la tolerancia y la liberalidad—, a menos que, entre otras cosas, sea proporcional al legítimo fin perseguido».

Por lo que respecta a nuestro TC, este inició la afirmación del principio de una forma fragmentaria al referirse al mismo, no de una manera unitaria, sino en relación a diversos derechos constitucionales, como por ejemplo a los derechos a la igualdad[222], a la intimidad[223], a la libertad de expresión[224] o a la tutela judicial efectiva[225], llegándose a

[220] En el apdo. 49 de la citada sentencia, el Alto Tribunal Europeo enjuiciaba unos hechos en relación con el derecho a la «libertad de expresión» y destacó que «... toda formalidad, condición, restricción o sanción impuesta en la materia debe ser proporcionada al fin legítimo que se persigue».

[221] En el apdo. 58, la misma STEDH declaró que el Reino Unido habría violado «el principio de proporcionalidad inherente al adjetivo "necesario"».

[222] Vid. STC 22/1981, de 2 de julio, FJ 3.º que declaró que «la igualdad es sólo violada si la desigualdad está desprovista de una justificación objetiva y razonable, y la existencia de dicha justificación debe apreciarse en relación a la finalidad y efectos de la medida considerada, debiendo darse una relación razonable de proporcionalidad entre los medios empleados y la finalidad perseguida».

[223] Vid. STC 37/1989, de 15 de febrero, FJ 7.º, que declaró que «la protección de la intimidad reclama […] la razonable apreciación, por la autoridad actuante, de la situación en que se halle el sujeto […] pues no se acomodaría, ciertamente, al derecho fundamental la resolución que constriñese el ámbito de intimidad de quienes no se hallan en una posición o situación específica respecto de aquella actuación, como tampoco respetaría la garantía que consideramos, la medida desatenta a toda estimación de proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquel a quien se le impone».

[224] Vid. STC 62/1982, de 15 de octubre, FJ 5.º, que al enjuiciar si se había infringido el principio de proporcionalidad en relación con el derecho a la libertad de expresión, declaró que «el Tribunal Constitucional ha de circunscribirse a determinar si el principio de proporcionalidad ha quedado infringido, desde la perspectiva del derecho fundamental y del bien jurídico que ha venido a limitar su

una definitiva construcción de la teoría del principio y su paralela consolidación jurisprudencial, con la STC 207/1996, de 16 de diciembre[226], la cual, no obstante resolver acerca de una intervención corporal, establece una doctrina del principio totalmente válida para las diligencias de investigación tecnológica, y que, en palabras de GONZÁLEZ-CUELLAR SERRANO, «constituye un magnífico ejemplo de rigor conceptual en el tratamiento del principio que nos ocupa»[227].

En definitiva, como señaló BARNES con anterioridad a la promulgación de la LO 13/2015, «se trata, pues, de un principio general que, aunque no escrito, está reconocido al máximo nivel, y, por tanto, vincula a todos los poderes públicos»[228], añadiendo en relación con los numerosos pronunciamientos del TC reafirmando el principio, que «siendo reconducibles a una concepción sistemática y unitaria de la acción del Estado y de la dignidad de la persona a la que aquélla se dirige, se resuelven en afirmar que el principio de proporcionalidad es inherente al Estado de Derecho y al valor justicia proclamado en el art. 1.1 CE»[229].

En todo caso, y sin perjuicio de todo lo expuesto anteriormente, ha de tenerse en cuenta que, con anterioridad a su incorporación a la LECrim por la LO 13/2015, el principio de proporcionalidad tuvo aplicación directa por imperativo del art. 10.2 CE.

De conformidad con este precepto, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán no solo de

---

ejercicio, por ser las medidas adoptadas desproporcionadas para la defensa del bien que da origen a la restricción».

[225] Vid. STC 36/1986, de 12 de marzo, FJ 2.º que, al examinar la proporcionalidad que ha de existir entre un defecto procesal en el que incurra una de las partes en el proceso y la sanción que se establezca legalmente por dicho defecto, declaró que «debe procederse a la subsanación del defecto, más que a eliminar los derechos o facultades que se vinculan a su cauce formal, lo que, con mayor razón, debe sostenerse cuando el efecto que pueda producir la inobservancia de un requisito formal sea precisamente el cierre de la vía de recurso. Esta interpretación finalista y su corolario, la proporcionalidad entre la sanción jurídica y la entidad real del defecto, no es sino una consecuencia más de la necesaria interpretación de la legalidad ordinaria en el sentido más favorable a la efectividad de un derecho fundamental».

[226] La construcción doctrinal que la STC 207/1996 realiza acerca de la proporcionalidad se lleva a cabo en el FJ 4.º al cual nos remitimos en las sucesivas menciones que hagamos de esta resolución en este apartado.

[227] GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», cit., p. 192.

[228] BARNES, J., «El principio de proporcionalidad. Estudio preliminar», cit., p. 19.

[229] BARNES, J., «El principio de proporcionalidad. Estudio preliminar», cit., p. 19.

conformidad con la Declaración Universal de Derechos Humanos sino también de acuerdo con «los tratados y acuerdos internacionales sobre las mismas materias ratificados por España».

En este sentido, el principio de proporcionalidad se encuentra proclamado en la Carta de los Derechos Fundamentales de la Unión Europea, que dispone en su art. 52.1 que «cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el "principio de proporcionalidad", cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás»[230].

En cuanto al contenido del principio, la STC 207/1996 —que conforme a lo expuesto anteriormente puede ser considerada el *leading case* en lo que respecta a la doctrina constitucional respecto del principio de proporcionalidad en el derecho procesal—, declara que el principio de proporcionalidad será respetado, cuando en relación con la medida, se cumplan los requisitos de idoneidad, necesidad y proporcionalidad en relación con un fin constitucionalmente legítimo[231].

Con base en ello, el estudio del principio que nos ocupa ha sido sistematizado en un doble sentido: amplio y estricto, aspectos que trataremos a continuación.

---

[230] Por otra parte, ha de tenerse en cuenta que el art. 2 de la LO 1/2008, de 30 de julio, por la que se autoriza la ratificación por España del Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, firmado el 13 de diciembre de 2007, ya establecía que «a tenor de lo dispuesto en el párrafo segundo del artículo 10 de la Constitución española y en el apartado 8 del artículo 1 del Tratado de Lisboa, las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán también de conformidad con lo dispuesto en la Carta de los Derechos Fundamentales publicada en el "Diario Oficial de la Unión Europea" de 14 de diciembre de 2007».

[231] En relación con el «fin constitucionalmente legítimo, cabe señalar, como así lo ha hecho GIMENO SENDRA, que «el ius puniendi del Estado y la tutela judicial de la víctima integran bienes constitucionales que posibilitan la lícita instauración de correlativas obligaciones del inculpado a fin de garantizar el cumplimiento de los fines del proceso penal». Vid. GIMENO SENDRA, J. V., «Medidas limitadoras de derechos fundamentales en el proceso penal», en Perez-Cruz Martín, A.J., Ferreiro Baamonde, X. (dirs.), Neira Pena, A. (coord.), *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011*, A Coruña, Universidade da Coruña, 2012, p. 82.

3.1. El principio de proporcionalidad en sentido amplio

El principio de proporcionalidad es considerado, en primer lugar, en un sentido amplio al estar comprendidos dentro del mismo tres subprincipios como son: el principio de idoneidad, el de necesidad y el de proporcionalidad en sentido estricto.

Así lo estableció la STC 207/1996, que declaró que «para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"».

3.1.1. El juicio de idoneidad

Al ocuparnos del subprincipio de la idoneidad, o quizás mejor dicho «juicio de idoneidad», este puede ser definido como aquella valoración que ha de realizarse por el juez a fin de determinar si el objeto de la medida de investigación es apropiado para la obtención de evidencias que sirvan para la averiguación de un hecho aparentemente delictivo. Dicho de otro modo, como señala PERELLÓ DOMENECH, «es preciso, por tanto, que la restricción que sufre el derecho resulte realmente útil para justificar el fin perseguido, o, dicho en negativo, que la medida restrictiva no sea desde todo punto de vista, y en principio, absolutamente inútil para alcanzar el fin»[232].

El CEDH proclama la exigencia del juicio de idoneidad en su art. 18, que bajo la rúbrica «limitación de la aplicación de las restricciones de derechos», establece que «las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual hayan sido previstas». Cabe señalar que este precepto fue mencionado por la STC 207/1996, que declaró que la medida ha de ser «idónea (apta, adecuada) para alcanzar el

[232] PERELLÓ DOMENECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», cit., p. 70.

fin constitucionalmente legítimo perseguido con ella (art. 18 CEDH), esto es, que sirva objetivamente para determinar los hechos que constituyen el objeto del proceso penal».

Para un correcto juicio de idoneidad, GONZÁLEZ-CUELLAR SERRANO, partiendo de la base de que este criterio hace referencia, tanto desde una perspectiva objetiva como subjetiva, a la causalidad de las medidas en relación con sus fines y exige que las injerencias faciliten el éxito perseguido en virtud de su adecuación cualitativa, cuantitativa y de su ámbito subjetivo de aplicación considera en tal sentido que la idoneidad se encuentra compuesta por tres elementos como son: «la adecuación cualitativa y cuantitativa, la adecuación de su ámbito subjetivo de aplicación y la prohibición de la desviación de poder»[233].

a) En cuanto a la adecuación cualitativa y cuantitativa, una medida será adecuada cualitativamente cuando sea apta por su propia naturaleza y no de una forma abstracta. Así, por ejemplo, un registro informático es adecuado para encontrar archivos que acrediten la comisión de un delito de pornografía infantil.

Por su parte, el aspecto cuantitativo se refiere a la duración o intensidad de la medida. De este modo, un registro remoto de un equipo informático no sería adecuado cuantitativamente, una vez que haya transcurrido cierto tiempo desde que se inició la intervención y los resultados hubiesen resultado infructuosos.

b) Respecto a la adecuación del ámbito subjetivo de aplicación, será estrictamente necesaria la individualización de los sujetos pasivos de las medidas a adoptar, sin que sea posible someter a un conjunto indeterminado de ciudadanos. Para la individualización de las personas, las circunstancias que permiten llevar a cabo la misma son las mismas que fundamentan la sospecha acerca de la participación del imputado en la comisión del hecho punible.

c) Y, finalmente, por lo que se refiere a la prohibición de la desviación de poder, esta se traduce en la particularidad de que el órgano de persecución penal no podrá pretender una finalidad distinta de la prevista por la ley, por lo que será inconstitucional toda medida dirigida a la consecución de fines no previstos legalmente.

[233] GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», cit., pp. 199-206.

3.1.2. La necesidad

El requisito de la necesidad, como su propio nombre indica, se centra en la circunstancia de que la medida ha de ser indispensable para conseguir el objetivo propuesto. Ello se producirá cuando no exista otra medida menos gravosa, entendiéndose por tanto que, en general, para cualquier acto de investigación limitativo de un derecho fundamental, el juzgador deberá llevar a cabo un «juicio de necesidad», en virtud del cual determine cuál es la medida que siendo la menos restrictiva del derecho fundamental de que se trate, resulta suficiente para alcanzar el fin perseguido.

Como declaró la STC 207/1996, de 16 de diciembre, para que la medida limitativa del derecho fundamental satisfaga las exigencias del principio de proporcionalidad, es preciso que la misma «sea necesaria o imprescindible para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de los derechos fundamentales a la integridad física y a la intimidad, o con un menor grado de sacrificio, sean igualmente aptas para conseguir dicho fin». La necesidad, por tanto, supone la aplicación de una regla de subsidiariedad, en virtud de la cual, se aplicará una medida limitativa de derechos fundamentales, en defecto de otra medida con menor grado de lesividad de un derecho fundamental.

Ante la dificultad que en algunos casos puede suponer la elección de la medida menos gravosa[234], tal y como puso de manifiesto GONZÁLEZ-CUELLAR SERRANO con anterioridad a la LO 13/2015, refiriéndose a aquellos supuestos en los que se localizasen dispositivos de almacenamiento en un registro domiciliario, debería otorgarse preferencia a las medidas de colaboración del imputado que evitasen búsquedas coactivas de las que pudiera prescindirse, concediendo prioridad a la inspección y copia in situ de los datos, de tal forma que no fuese necesaria la recogida de los dispositivos o soportes que los contengan. De todos modos, de acuedo con lo expresado por el referido autor, serían las circunstancias del caso concreto las que condujesen a la elección de un modo de actuar u otro, siendo posiblemente la mejor opción en la mayoría de las ocasiones, la recogida para el posterior análisis del equipo informático; por ejemplo en aquellos casos en los que el interesado se negase a proporcionar la clave de acceso al disco duro del ordenador o ante el riesgo de que un intento de acceso y copia de los

[234] Afirma KLUTH que «pese a que, en abstracto, los criterios señalados pueden parecer claros, lo cierto es que su aplicación práctica resulta con frecuencia muy complicada». Vid. KLUTH, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», cit., p. 228.

datos sin introducción de un determinado código provoque la destrucción de la información[235].

3.2. El principio de proporcionalidad en sentido estricto

3.2.1. Concepto

La STC 207/1996, de 16 de diciembre, declara que para que la medida restrictiva del derecho fundamental cumpla con las exigencias del principio de proporcionalidad, es necesario que, «aun siendo idónea y necesaria, el sacrificio que imponga de tales derechos no resulte desmedido en comparación con la gravedad de los hechos y de las sospechas existentes».

En dicha afirmación, queda perfectamente condensado el subprincipio de la «proporcionalidad en sentido estricto» desprendiéndose de la misma una obligada comparación, o como dice ALEXY, ponderación[236] entre el derecho sacrificado y el beneficio obtenido para el conjunto de la ciudadanía, en el entendimiento de que la adopción de la medida respetará el principio de proporcionalidad si el citado beneficio social supera desde una perspectiva axiológica al perjuicio sufrido por la persona investigada. Por tanto, y conforme señaló la STC 49/1999, de 5 de abril, «la desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a un enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que la Constitución garantiza»[237].

3.2.2. Criterios para la ponderación

Por lo que se refiere a los criterios para llevar a cabo la ponderación, conforme declara el inciso anteriormente citado de la meritada STC 207/1996, de 16 de diciembre, estos se concretan en la entidad de las sospechas existentes y en la gravedad de los hechos.

---

[235] GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», cit., p. 898.

[236] Afirma ALEXY que la ponderación «es el tema del tercer subprincipio del principio de proporcionalidad, esto es, el principio de proporcionalidad en sentido estricto». Vid. ALEXY, R., «Los derechos fundamentales y el principio de proporcionalidad», *Revista Española de Derecho Constitucional*, n.º 91, 2011, p. 15.

[237] Vid. STC 49/1999, de 5 de abril, FJ 7.º, que cita diversas sentencias anteriores.

3.2.2.1. Entidad de las sospechas existentes

La entidad de las sospechas se identifica con la existencia de indicios suficientes, siendo de destacar lo mencionado por la Circular 1/2013 de la FGE cuando señala que «los indicios suficientes para acordar la intervención son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento», así como que «las sospechas no han de ser tan solo circunstancias meramente anímicas, sino que precisan hallarse apoyadas en datos objetivos»[238].

En el mismo sentido se había pronunciado con anterioridad la jurisprudencia del TC, declarando que la exteriorización en la resolución judicial de los indicios que permiten la intervención es indispensable, habida cuenta que «el juicio sobre la legitimidad constitucional de la medida exige verificar si la decisión judicial apreció razonadamente la conexión entre el sujeto o sujetos que iban a verse afectados por la medida y el delito investigado», así como que «la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas hallarse apoyadas en datos objetivos, que han de serlo en un doble sentido; en primer lugar, en el de ser accesibles a terceros, sin lo que no serían susceptibles de control; y en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona»[239].

También el TS ha tenido la oportunidad de pronunciarse en relación con la entidad de las sospechas como criterio para la resolución de la proporcionalidad en sentido estricto, al señalar que «la sospecha acerca de la comisión del delito o de la participación del sospechoso no puede ser considerada un indicio, por más contundente que sea su expresión, ni tampoco, consecuentemente, puede serlo la afirmación de la existencia del delito y de la participación; o de su posibilidad o probabilidad», así como que «el juez, en el cumplimiento de su función de protección del derecho fundamental, no puede operar sobre el valor que otorgue o la confianza que le proporcione la sospecha policial en sí misma considerada, sino sobre el significado razonable de los datos

[238] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., p. 134.
[239] Vid. STC 167/2002, de 18 de septiembre, FJ 2.º

objetivos que se le aportan, valorados como indicios, obtenidos por la policía en el intento inicial de verificación de la consistencia de sus sospechas»[240].

Por tanto, puede concluirse que en nuestro derecho se impone la necesidad de que la convicción del juez se manifieste en la resolución judicial, haciendo constar los factores que permitieron llegar a la misma, sin que estos factores constituyan meras suposiciones o conjeturas de la existencia del delito.

3.2.2.2. Gravedad de los hechos

Una vez determinada la suficiencia de los indicios, habrá que estar a que los presuntos hechos delictivos sobre los que se tienen sospechas fundadas, tengan una gravedad que permita la injerencia en los derechos fundamentales. Cabe señalar que el TS declaró que «el interés del Estado y de la Sociedad en la persecución y descubrimiento de los hechos delictivos es directamente proporcional a la gravedad de estos», por lo que «solo en relación a la investigación de delitos graves, que son los que mayor interés despiertan su persecución y castigo, será adecuado el sacrificio de la vulneración de derechos fundamentales para facilitar su descubrimiento, pues en otro caso, el juicio de ponderación de los intereses en conflicto desaparecería si por delitos menores, incluso faltas se generalizase este medio excepcional de investigación, que desembocaría en el generalizado quebranto de derechos fundamentales de la persona sin justificación posible»[241].

---

[240] Vid. STS 775/2014, de 20 de noviembre, FJ 1.º, la cual también señaló que «en consecuencia no es suficiente que quien solicita la medida comunique, sobre la base de sus noticias o informaciones, que sabe o cree saber que el sospechoso ha cometido, está cometiendo, o va a cometer un delito; o que ha practicado una investigación y que exponga a continuación sus conclusiones. Por el contrario, es preciso que traslade al juez las razones de tal afirmación, o el contenido de aquella indagación en su integridad, identificando las diligencias practicadas y los datos objetivos relevantes alcanzados como su resultado, pues precisamente esos elementos son los que deben ser valorados por el juez para decidir acerca de la consistencia de los indicios y, en consecuencia, de la necesidad y proporcionalidad de la restricción del derecho fundamental que le es solicitada».

[241] Vid. STS 297/2006, de 6 de marzo, FJ 2.º que al referirse a la intervención de las comunicaciones telefónicas como un medio de investigación excepcional, declaró asimismo que «frente a otras legislaciones que establecen un catálogo de delitos para cuya investigación está previsto este medio excepcional, la legislación española guarda un silencio que ha sido interpretado por la jurisprudencia en el sentido de exigir la investigación de hechos delictivos graves, y desde luego, aquellos que revisten la forma de delincuencia organizada; de alguna manera, puede decirse que en un riguroso juicio de ponderación concretado a cada caso, la derogación del principio de intangibilidad de los derechos fundamentales, debe ser proporcionado a la legítima finalidad perseguida».

Por otra parte, autores como SUBIJANA ZUNZUNEGUI afirman que «el enorme sacrificio que para la plenitud de los derechos fundamentales supone su limitación conlleva que la misma sólo encuentre justificación cuando el interés estatal en la investigación penal tenga una especial relevancia, en atención a la gravedad del delito investigado, utilizando para determinar la gravedad tanto un criterio cuantitativo (importancia de la pena asignada al delito) como cualitativo (transcendencia social de los hechos investigados)»[242].

Por tanto, de acuerdo con lo indicado por este autor, atendiendo a los aspectos cuantitativo y cualitativo que han de tenerse en cuenta para fijar la mayor o menor gravedad de los hechos, las medidas limitativas de derechos fundamentales podrán acordarse para la investigación de los delitos graves contemplados en el CP según los arts. 13 y 33 del mismo en función de la pena a imponer. Pero además, podrán acordarse para la investigación de delitos, que aun sin alcanzar la pena prevista para los delitos graves previstos por el CP, estén ocasionados por unos hechos cuya gravedad tenga una trascendencia social que exija la intervención.

Tal y como apuntó VELASCO NUÑEZ con anterioridad a la promulgación de la reforma operada por la LO 13/2015, «a diferencia de los países que señalan el tipo de delitos concretos que permiten la investigación a través de intervenciones telecomunicativas (Alemania, Bélgica) y de aquellos otros que la modulan en función de la pena (Reino Unido, Francia)», España mantenía un esquema abierto en que la ponderación se hacía «en función no sólo del tipo de delito sino sobre todo de las circunstancias que en el caso concreto explican la afección a la relevancia jurídico penal de los hechos, su bien jurídico protegido y la trascendencia social del mismo (SSTC 166/99, de 27 de septiembre, 299/2000, de 11 de diciembre, 104/2006, de 3 de abril)»[243], criterio que se ha mantenido por la jurisprudencia hasta fechas más recientes[244].

---

[242] SUBIJANA ZUNZUNEGUI, I. J., «Policía judicial y derecho a la intimidad en el seno de la investigación criminal», *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n.º 10, 1997, p. 148.

[243] Menciona este autor algunos casos en los que la jurisprudencia del TC y TS, permitieron la injerencia en la investigación de delitos que no siendo graves conforme a los arts. 13 y 33 del CP, así fueron considerados por su repercusión social, señalando resoluciones de los altos tribunales en los que se admitió la injerencia al tratarse de delitos cometidos por funcionarios (STS 14/06/1993); contrabando, por afectar a intereses fiscales y a la vez a costes sociales sanitarios; contra la propiedad intelectual, por la potencialidad lesiva y rápida difusión del uso de instrumentos como los informáticos que facilitan su comisión en masa (STC 104/2006, de 3 de abril); o porque versen sobre organizaciones criminales complejas con posibilidad de atacar intereses sociales y públicos (SSTC 299/2000, de 11 de diciembre, 14/2001, de 29 de enero, 202/2001, de 15 de octubre, 82/2002, de 22 de abril). Vid. VELASCO NÚÑEZ, E.,

Esta cuestión, dio lugar a cierta polémica doctrinal, existiendo, en línea con lo señalado anteriormente, posiciones que defendían que únicamente debían ser considerados graves los delitos señalados como tales por el CP, mientras que por otro lado se sostenía que para la adopción de medidas limitativas de derechos fundamentales, debían incluirse aquellos delitos que aunque no superaran los límites penológicos previstos en el CP para ser considerados graves, su repercusión o trascendencia social así lo exigiese. A estas opiniones se unieron las que propugnaban que debía admitirse la la práctica de estas medidas cuando se investigasen delitos informáticos (tales como fraudes informáticos, accesos no autorizados, contra la propiedad intelectual, etc.), aun cuando no superasen las penas previstas para los delitos graves.

A esta polémica nos referimos en el capítulo I, donde hicimos constar con distintas menciones doctrinales y jurisprudenciales, que se había impuesto la doctrina conforme a la que la gravedad del delito se ha de valorar de una forma independiente a las normas del CP, doctrina a la que nos acogimos argumentando nuestra posición, a todo lo cual nos remitimos[245].

Señalaremos, por último, que el TS, en una de las últimas sentencias en la que se refirió a este tema atendiendo a la regulación anterior a la LO 13/2015, declaró que las medidas de investigación tecnológica de derechos fundamentales, en la investigación de delitos cometidos por medios informáticos, han de considerarse proporcionadas «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»[246].

«Correo electrónico, SMS y virus troyanos: aspectos procesales penales», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009, p. 15, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[244] Vid. STS 513/2014, de 24 de junio, FJ 1.º que declaró que «en el momento de adoptar su decisión, el juez ha de atender, necesariamente a varios aspectos. En primer lugar, a la proporcionalidad, en el sentido de que ha de tratarse de la investigación de un delito grave. Para valorar la gravedad no solo es preciso atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar».

[245] Concretamente nos ocupamos de ello en el subepígrafe 4.4.3.3 del capítulo I «Problemas en relación con la gravedad del delito» dentro del apartado 4.4.3 dedicado al examen de la Ley 25/2007 de conservación de datos. Vid. supra, pp. 66-71.

[246] Vid. STS 811/2015, de 9 de diciembre, FJ 1.º, la cual, aun cuando es de fecha un poco posterior a la entrada en vigor de la LO 13/2015, que mencionó, justifica la proporcionalidad de las diligencias de investigación tecnológica cuando se trate de a investigación de los delitos cometidos por medios informáticos de forma independiente a la nueva regulación. Además, en la misma se declaró que «en esta

III. Análisis de la suficiencia de la LO 13/2015 en atención a la jurisprudencia anterior a su promulgación relacionada con las diligencias de investigación tecnológica.

Son muchos, como ya hemos visto, y como se verá a lo largo de esta tesis, los problemas interpretativos de la nueva LO 13/2015, en lo que respecta a la regulación de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 CE que ha tenido lugar en el nuevo título VIII del libro II de la LECrim.

Sin embargo, nuestra valoración sobre la regulación en general llevada a cabo por la misma de los principales elementos que, o no estaban regulados, o lo estaban deficientemente, en relación con las medidas de investigación limitativas de los derechos a la intimidad, al secreto de las comunicaciones o a la protección de datos de carácter personal, ha de tener, a nuestro criterio, no obstante alguna opinión desfavorable[247], una valoración positiva[248], como también así se ha estimado doctrinalmente[249], principalmente por la no poco relevante circunstancia de haber

---

clase de delitos, la posible volatilidad de las pruebas documentales puede aconsejar claramente en numerosos supuestos una rápida intervención tendente a su más pronta ocupación, sin las demoras que produciría una investigación más amplia».

[247] Así, por ejemplo, SÁNCHEZ YLLERA afirma que «la LO 13/2015 ha sido criticada por su deficiente técnica legislativa, caracterizada por una minuciosidad que pretende ser exhaustiva. Algunos autores la han calificado como "propia de un formulario"». Vid. SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», *Formación a distancia-Consejo General del Poder Judicial*, n.º 3, 2016, p. 2.

[248] Una visión positiva global, que no impedirá un examen crítico, que a lo largo de esta obra se llevará a cabo de diversas cuestiones que se consideran mejorables.

[249] Así, por ejemplo, MONTES ALVARO señala que «debemos valorar positivamente que mediante tal reforma, se dote de certeza y seguridad jurídica al ordenamiento». Vid. MONTES ÁLVARO, M. A., «La regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el art. 18 CE», cit., p. 111. Por su parte, BUENO DE MATA ha señalado que «estamos ante una normativa arriesgada pero muy necesaria en los tiempos que corren. Nos encontramos así un catálogo de diligencias que contemplan desde una interceptación integral de las comunicaciones electrónicas hasta otras más polémicas como el uso de drones en espacios abiertos, que tienen como fin intentar poner freno a conductas delictuales producidas en la Red. Si tuviéramos que hacer una valoración global de la Ley, el resultado sería altamente positivo, a la espera de su entrada en vigor antes de que finalice el año 2015» Vid. BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», *Diario La Ley - Sección Doctrina*, n.º 8627, 2015, p. 6. Asimismo GONZÁLEZ-MONTES SÁNCHEZ indica que «debe valorarse muy positivamente, al menos en abstracto, la loable voluntad del legislador de acometer reformas que respondan a la nueva criminalidad

llenado el vacío normativo de más de veinticinco años, así como por haber sido ordenadas las cuestiones relevantes que venían siendo reclamadas por la doctrina y la jurisprudencia, las cuales se han recogido, principalmente, en el nuevo capítulo IV del título VIII del libro II de la LECrim, dedicado a las disposiciones comunes a todas las diligencias de investigación tecnológica[250 y 251].

Asimismo, hemos de mostrar una inicial y favorable apreciación, dado que, conforme afirma CABEZUDO RODRÍGUEZ, «la nueva normativa supera el enfoque marcadamente casuístico que hasta ahora regía en estas materias y traslada definitivamente el foco de atención desde el modo en que tales medidas de investigación han de llevarse a cabo para que puedan ser lícitamente valoradas como fuentes de

---

organizada, a la nueva realidad social, a la implantación en el ámbito de la investigación de los delitos de todas aquellas nuevas tecnologías que por razones obvias no pudo recoger en su momento una Ley del siglo XIX».Vid. GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», *Revista Electrónica de Ciencia Penal y Criminología*, vol. 17, n.º 06, 2015, p. 5. Consultado en http://criminet.ugr.es/recpc/17/recpc17.html el 26 de febrero de 2019.

[250] Sin perjuicio de las particularidades propias de cada una de las diligencias de investigación tecnológica reguladas en capítulos independientes. Afirma RICHARD GONZÁLEZ, que no obstante afectar las distintas diligencias de investigación tecnológica a actividades y derechos distintos, estas pueden ser clasificadas según su fin y los derechos fundamentales afectados, en los siguientes cuatro grupos:

«1º La intervención de las comunicaciones que afecta al derecho reconocido en el art. 18.3 CE. Esta es la medida más común y podríamos decir tradicional. Sin embargo, debe señalarse el extraordinario ámbito que adquiere en la regulación legal, ya que la intervención no sólo se refiere al tradicional teléfono, sino que se amplía a toda clase de formas de comunicación no orales que pueden tener lugar mediante los modernos dispositivos electrónicos. También se prevé el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos (588 ter a-m LECrim).

2º La grabación de imagen y sonido tanto en la vía pública como en el domicilio, que afecta al derecho a la intimidad personal y familiar (art. 18.1 CE) (art. 588 quater a-e y quinquies a. LECrim).

3º La instalación y utilización de dispositivos técnicos de seguimiento y localización, que afectan tanto al derecho a la intimidad (art. 18.1 CE) como al derecho a la libertad de circulación (art. 19 CE) (arts. 588 quinquies b-c LECrim).

4º El registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies a - c LECrim) y los registros remotos sobre equipos informáticos (arts. 588 septies a - c LECrim). En este caso, se afecta tanto el derecho a la intimidad (art. 18.1 CE) como el derecho al secreto de las comunicaciones (art. 18.3 CE)».

Vid. RICHARD GONZÁLEZ, M., «La Investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, 2017, p. 17.

[251] De las disposiciones comunes a todas las diligencias de investigación tecnológica, nos ocuparemos en los dos capítulos de esta tesis, en los que se realizarán distintas reflexiones en cuanto la legalización de los aspectos esenciales de estas medidas, sin perjuicio de las que se efectúen en el capítulo especialmente dedicado a los registros informáticos.

prueba al plano de la apreciación judicial de los resultados obtenidos»[252], lo cual ha reforzado la seguridad jurídica, al tiempo que nuestra legislación ha quedado actualizada en relación con una incontrovertible realidad a la que, de una forma apremiante, no se podía hacer caso omiso[253].

Realizaremos ahora unas consideraciones acerca de la suficiencia de la nueva regulación en relación con los principales aspectos que han sido objeto de estudio en el presente capítulo, sin perjuicio de que sobre otras cuestiones más específicas relacionadas con las particularidades de los registros informáticos y su valor probatorio, se realicen las correspondientes valoraciones en los capítulos V y VI.

1. La previsión legal suficiente

La primera de las cuestiones a examinar es la referente a si las exigencias de previsión normativa suficiente para la práctica de diligencias de investigación tecnológica han quedado colmadas.

Para que el requisito de una previsión legal suficiente quedase cumplido, de acuerdo con lo ya indicado, se precisaba, además de la positivización de las medidas de injerencia en los derechos fundamentales, que la ley que las regulase fuese una ley de «calidad», en el sentido de que se tratase de una norma previsible para las personas afectadas, quienes han de poder prever las consecuencias. Asimismo, era necesaria una

---

[252] CABEZUDO RODRÍGUEZ, N., «Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim», en Jimeno Bulnes, M., Perez Gil, J. (coords.), *Nuevos horizontes del derecho procesal*, Barcelona, Bosch Editor, 2016, p. 558.

[253] No obstante lo anterior; debemos recordar que nuestro trabajo se centra en el examen de todo lo atinente a los registros informáticos, lo cual exige un estudio de las disposiciones comunes a todas las medidas tecnológicas así como de todo su contorno jurídico-procesal, y es en este aspecto en el que valoramos positivamente la reforma. En este sentido, no someteremos a examen, por no ser objeto de este trabajo, consideraciones en relación con la mayor o menor oportunidad de otras diligencias de investigación tecnológica, como son la captación y grabación de comunicaciones orales e imágenes mediante la utilización dispositivos electrónicos o la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, respecto de las que autores como GONZÁLEZ-MONTES SÁNCHEZ han afirmado que posiblemente «su plasmación normativa ha ido más allá de donde debiera, incluyendo posibilidades de investigación hasta ahora desconocidas por nuestra norma procesal que son factibles desde el punto de vista técnico pero que nos plantean supuestos de dudosa constitucionalidad». Vid. GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», cit., p. 22.

norma compatible con la preeminencia del derecho, a fin de evitar injerencias arbitrarias de los poderes públicos, lo que exigía que se tratase de prescripciones legales claras y detalladas.

Nos ocuparemos a continuación de estos dos elementos necesarios para una previsión legal suficiente, sin dejar de mencionar que un primer presupuesto ya ha sido cumplido, al haberse legislado mediante LO, al disponerse acerca de una materia —las medidas de investigación tecnológica—, que afecta a derechos fundamentales (art. 81.1 CE).

1.1. Previsibilidad de la norma

Consideramos que en lo que respecta a una idónea previsibilidad de la norma, de tal forma que la persona afectada pueda conocer las consecuencias de su incumplimiento, como un elemento necesario para el respeto al principio constitucional de seguridad jurídica, esta ha quedado, en lo más fundamental, satisfecha con la LO 13/2015, al haberse regulado las particularidades de cada tipo de diligencia en un capítulo independiente para cada una de ellas, y, sobre todo, con el capítulo dedicado a las disposiciones comunes a todas las medidas de investigación tecnológica, en el cual han quedado reglados los principales aspectos cuya ausencia podía comprometer la seguridad jurídica y que habían sido reclamados por la jurisprudencia del TEHD y del TC, tales como la duración de la medida, su control judicial, afectación de terceras personas, la regulación de los supuestos en los que sea necesaria la utilización de la información obtenida en un procedimiento distinto, la de los hallazgos casuales o las circunstancias en las que se debe proceder a la destrucción de los registros obtenidos tras las intervenciones.

Uno de los temas, cuya incorporación a la ley ha reforzado especialmente la seguridad jurídica, ha sido el referente a la gravedad de los delitos, que tanta relevancia tiene para el cumplimiento del principio de proporcionalidad en sentido estricto, y respecto del que, además de la jurisprudencia del TEDH y TC, también el TS había abogado por que se llevase a cabo una concreción legal de los delitos en virtud de cuya investigación se pudieran acordar medidas limitativas de derechos fundamentales[254].

[254] Vid. STS 746/2014, de 13 de noviembre, FJ 11.º, en la que declaró que «en repetidas ocasiones esta Sala ha manifestado la conveniencia de que la Ley prevea con claridad el protocolo a seguir para este medio de investigación y la clase de delitos que pudieran justificar este medio excepcional de

De este modo, la reforma operada por la LO 13/2015, ha incluido un catálogo de delitos, en cuya investigación se podrán acordar determinadas medidas de investigación. Así, por su especial grado de injerencia, se ha establecido tal catálogo, en los registros remotos sobre equipos informáticos. Sin embargo, nada se ha acordado en relación con el registro de dispositivos de almacenamiento masivo de información, lo cual implica que, para esta medida de investigación, habrá que atender a las reglas generales del principio de proporcionalidad que fueron examinadas anteriormente[255].

Aun así, existen algunas cuestiones en las que, aunque sin la trascendencia de las que hemos mencionado, entendemos que no se ha colmado debidamente la seguridad jurídica. Así, por ejemplo, consideramos que, como examinaremos en el capítulo siguiente, sería aconsejable establecer la obligación de fijar en la resolución judicial (art. 588 bis c LECrim) el día y hora en el que se iniciará la medida así como el día y hora de su finalización. Asimismo, entendemos que al disponer el art. 588 bis k.2 LECrim, que el tribunal acordará la destrucción de los registros obtenidos tras la investigación, siempre que, a su juicio, no fuera precisa su conservación, deberían concretarse los supuestos en los que las copias podría conservarse sin dejarlo al arbitrio del tribunal.

1.2. Norma compatible con la preeminencia del derecho

Para que una norma sea compatible con la preeminencia del derecho, esta debe asegurar la eliminación de cualquier riesgo de arbitrariedad en la actuación de los poderes públicos, que, por otra parte, también se configura como un principio constitucional, al garantizar el art. 9.3 CE la interdicción de tal arbitrariedad. Para ello, la ley ha de establecer unas reglas claras y detalladas, exigencia que se acentúa aún más cuando nos encontramos ante las TIC[256] por su especial y compleja naturaleza. Por tanto, el legislador habrá de ser muy cauteloso a la hora de incluir las correspondientes reglas en abstracto, ante la posibilidad de lagunas que puedan vulnerar el principio de la

---

investigación, bien estableciendo un catálogo seriado de delitos, bien atendiendo a la pena a imponer a los delitos susceptibles de ser investigados con este medio».

[255] Vid. supra apdo. II.3 de este mismo capítulo, pp. 111-122.

[256] Afirma LÓPEZ-BARAJAS PEREA, que «el peligro de la arbitrariedad es mayor cuando el poder de apreciación es ejercido en secreto. En un contexto cada vez más digital, las normas que regulen las medidas secretas de vigilancia o de interceptación de las comunicaciones por las autoridades públicas deben sean muy claras y detalladas». Vid. LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley», *Revista de Derecho Político*, n.º 98, 2017, p. 100.

preeminencia del derecho, impidiendo de este modo que por los poderes públicos se puedan llevar a cabo actuaciones arbitrarias.

En este sentido, de acuerdo con lo apuntado por LÓPEZ-BARAJAS PEREA, «la ley debe habilitar y definir en abstracto los supuestos en que cabe el sacrificio del derecho fundamental en pro del mayor interés social en la persecución de una determinada actuación delictiva, y debe regular también las garantías concretas que permitan a la persona investigada ejercer una efectiva defensa, debiendo precisar todos y cada uno de los presupuestos y condiciones de la intervención, no pudiendo la limitación de un derecho crear el riesgo de abusar de dicha limitación»[257]. Esta, por tanto, es la forma de asegurar que la norma respete la primacía del derecho y de los derechos.

Entendemos que, en general, la LO 13/2015 cumple el requisito de una regulación en la que se comprendan todas las cuestiones que venían siendo reclamadas jurisprudencialmente, para poder contar con una legislación en la que se respete la preeminencia del derecho. No obstante, existen algunos aspectos criticables que, en nuestra opinión y también en la de otros autores, conceden una discrecionalidad excesivamente extensa a las FCSE, en algunas actuaciones que no precisan de autorización judicial.

Así, por ejemplo, BUENO DE MATA critica el apartado 5 del art. 588 sexies c LECrim, señalando que «tras distintas cuestiones más o menos cuestionables, la regulación establece un precepto en el que hace suya la frase de "el fin justifica los medios"» por cuanto al disponer que «las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia», se está haciendo uso de un término muy amplio, que podría permitir determinados excesos en la actividad investigadora[258].

[257] LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley», cit., p. 101.

[258] Apunta BUENO DE MATA que «con la denominación "cualquier persona" se desprenden dos efectos negativos inmediatos. En primer lugar, se desvalora o se reconoce como insuficiente la capacitación técnica de la Policía Judicial en términos de investigación policial, cuando existen unidades concretas con miembros con años de especialización que han sido formados para tal fin y están en constante reciclaje y capacitación, por lo que a nivel publicitario y de imagen exterior no creemos que nos haga ningún bien y,

Asimismo, otro tema de especial importancia que, a nuestro juicio, ha sido regulado de una forma insatisfactoria, es el relativo a la intervención policial sin autorización judicial en los supuestos de urgencia. Se trata de una cuestión que adquiere especial relevancia en el escenario de los registros de dispositivos de almacenamiento masivo de información[259], los cuales pueden ser receptores de información de distinta naturaleza, pudiendo lesionarse, con el acceso a dicha información, como ya hemos tenido la oportunidad de analizar, tanto los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos de carácter personal. Como nota favorable, ha de señalarse que no se ha permitido la intervención sin autorización judicial, cuando se pretenda ejecutar un registro remoto de equipos informáticos, sea o no urgente.

Ya hemos comentado, que el derecho a la intimidad no goza del mismo grado de protección que el derecho al secreto de las comunicaciones, permitiéndose determinadas injerencias por parte de la Policía Judicial sin autorización judicial, en casos de urgencia, tanto en el derecho a la intimidad como en el derecho a la protección de datos de carácter personal.

Pero insistimos, tales injerencias no están permitidas en lo que respecta al secreto de las comunicaciones. No pretendemos con ello afirmar, que por parte de las FCSE o el Ministerio Fiscal se practiquen actuaciones discrecionales —cuando la ley lo permita— sin respeto al principio de proporcionalidad. No obstante, se trata de asegurar la preeminencia del derecho y, consecuentemente, vedar cualquier posibilidad de actuación arbitraria. En tal sentido, entendemos que la ordenación de esta fundamental cuestión, debería precisar, especialmente para una diligencia de investigación tan invasiva como es un registro informático, los supuestos en los que concurriría una especial urgencia.

---

en segundo lugar, ¿qué perfil tiene esa persona? Al hablarse de un cualquier no se acota la identidad de ese sujeto, ¿se está hablando de un ingeniero informático profesional? O por el contrario ¿se abre la puerta al fichaje de hackers que actúen sin fines éticos e incluso criminales?». Vid. BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», cit., pp. 5-6.

[259] Cabe reseñar que la intervención policial en supuestos de urgencia, además de ser desarrollada para las diligencias de detención y apertura de la correspondencia escrita y telegráfica y para la intervención de las comunicaciones telefónicas y telemáticas —cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas—, ha sido establecida solamente para dos diligencias concretas, como son: la utilización de dispositivos o medios técnicos de seguimiento y localización (art. 588 quinquies b.4) y el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies c, 3 y 4).

Nos ocuparemos con detalle de este asunto en un epígrafe dedicado al mismo, en el capítulo V de esta obra. Baste ahora señalar que el TC, en la STC 115/2013, de 9 de mayo, FJ 3.º, admitió la legitimidad constitucional de una injerencia leve en el derecho a la intimidad por razones de urgencia, ahora bien, «con la suficiente y precisa habilitación legal», entendiendo que dos adjetivos como «suficiente y precisa» no son aptos para considerar que hay que dejar a criterio, dicho sea con el debido respeto, de los agentes investigadores actuantes, de la determinación de la urgencia. Por otra parte, no debe olvidarse que podría verse vulnerado el principio de reserva jurisdiccional proclamado en los arts. 24.1 y 117.3 CE, principio del que pasamos a ocuparnos dentro de la valoración que estamos efectuando sobre la suficiencia de la legalización de las diligencias de investigación tecnológica.

2. La jurisdiccionalidad de la medida

Consideramos satisfactoria la inclusión del requisito de la jurisdiccionalidad de las medidas de investigación tecnológica en nuestra LECrim, dado que, han quedado debidamente cubiertos los dos aspectos esenciales de este requisito, como son: la exigencia de resolución judicial y su motivación.

Debe señalarse además, que tras dejar sentado en el primer precepto del capítulo dedicado a las disposiciones comunes a todas las medidas (art. 588 bis a.1 LECrim), que se podrá acordar alguna de las medidas «siempre que medie autorización judicial», se ha incluido una regulación específica para cada una de ellas además de una detallada relación, en el referido capítulo dedicado a las disposiciones comunes, de todos los aspectos que han de constar tanto en la solicitud de autorización judicial como en la propia resolución.

En efecto, el art. 588 bis b LECrim, se refiere entre otras —por hacer una breve mención, ya que nos ocuparemos de todas ellas en el capítulo siguiente—, a la relevante cuestión referente a que la solicitud habrá de contener «la exposición detallada de las razones que justifiquen la necesidad de la medida, de acuerdo a los principios rectores establecidos en el artículo 588 bis a, 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». Por su parte, el art. 588 bis c LECrim establece, en ocho apartados, una amplia relación de todos los extremos que, «al menos», deberá concretar la resolución judicial, entre los que pueden mencionarse, «el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales, la

identidad de los investigados y de cualquier otro afectado por la medida, la duración o la finalidad perseguida».

En definitiva, el legislador ha llevado a cabo una positivización del requisito de la jurisdiccionalidad de una forma minuciosa y detallada, que, a nuestro juicio, asegura el efectivo cumplimiento del principio proclamado en los arts. 24.1 y 117.3 CE, excepto en aquellos casos, en los que por una indebida interpretación de los supuestos de urgencia, se ejecuten intervenciones inapropiadamente, de acuerdo con lo expuesto en el apartado anterior.

Por otra parte, como dijimos, ha quedado incorporada a la ley la exigencia de autorización judicial para el registro de dispositivos de almacenamiento masivo de información, ya se lleve a cabo de forma simultánea a un registro domiciliario o se realice con independencia de este, regulación que consideramos igualmente satisfactoria, dado que el art. 588 sexies LECrim ha distinguido ambos supuestos en sus apartados a y b.

Precisamente, afirma GARCÍA SAN MARTÍN, lo singular y oportuno del precepto, es la delimitación efectuada entre la aprehensión de los dispositivos y el acceso a la información contenida en ellos, al establecerse expresamente que la aprehensión de los consiguientes dispositivos durante la práctica de la diligencia de entrada y registro domiciliario no legitima el acceso a su contenido, sin perjuicio de que pueda autorizarse judicialmente dicho acceso[260].

Sin perjuicio de lo anterior, existe una cuestión, como es la relativa a la «orden de conservación de datos» prevista como medida de aseguramiento en el art. 588 octies, respecto de la que estimamos que debería llevarse a cabo bajo control judicial, por tratarse de una diligencia de investigación común a todas las medidas de investigación tecnológica. Justificaremos las razones por las que así lo estimamos en el último apartado del capítulo siguiente.

[260] GARCÍA SAN MARTÍN, J., «Consideraciones en torno 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», *Diario La Ley - Sección Doctrina*, n.º 8648, 2015, p. 15.

3. La proporcionalidad

Sin duda, tiene una gran relevancia el hecho de que, finalmente, el principio de proporcionalidad haya tenido reconocimiento expreso en la LECrim. Este reconocimiento lo ha sido, aunque de una forma concisa, conforme a la teoría consolidada jurisprudencial y doctrinalmente, que analizamos ampliamente en el apartado II.3 de este capítulo.

En efecto, el legislador, al ocuparse de los principios rectores que deben regir la práctica de toda medida de investigación, contempla la proporcionalidad tanto desde el punto de vista amplio como estricto.

En sentido amplio, puesto que se han incluido como principios rectores necesarios los de idoneidad y necesidad, los cuales, de acuerdo con lo ya analizado, se consideran subprincipios del principio de proporcionalidad, habiéndose efectuado una conceptuación de los mismos en los apartados 3 y 4 del art. 588 bis a LECrim, de una forma lacónica pero, a nuestro juicio, precisa, tal y como estudiaremos en el primer epígrafe del capítulo siguiente, que dedicaremos a los principios rectores.

Del mismo modo, como también se examinará, se ha plasmado de una forma muy adecuada la proporcionalidad en sentido estricto en el apartado 5 del art. 588 bis a LECrim, en el que, en unas pocas líneas, se realiza una correcta exposición del significado de este principio.

4. Necesidad de una nueva Ley de Enjuiciamiento Criminal

De acuerdo con lo expuesto en los apartados anteriores, hemos realizado, con carácter general y sin perjuicio de las observaciones efectuadas y las que se someterán a examen en los próximos capítulos, una valoración favorable de la nueva regulación de las medidas de investigación tecnológica llevada a cabo mediante la reforma de la LECrim por la LO 13/2015, una materia, respecto de la que, puede decirse que, sin lugar a dudas, existía un menester perentorio de inclusión en nuestro ordenamiento jurídico.

Sin embargo, estimando acertada la reforma desde un punto de vista material, no podemos opinar mismo desde una perspectiva formal. La razón es obvia: nuestro

sistema precisa de una nueva LECrim, como así lo viene reclamando forma unánime la doctrina[261].

Razones políticas[262], impidieron que viese la luz el Anteproyecto de LECrim de 2013, en el que se abordó un cambio radical del sistema procesal penal, en el que destacaban, entre diversos aspectos novedosos, el proceso por aceptación de decreto, las diligencias de investigación tecnológica, una extensa regulación del proceso de ejecución penal, así como la atribución de la fase de instrucción al Ministerio Fiscal, con la paralela instauración de la figura de un Tribunal de Garantías que legitimase las

[261] Por citar algunas de las autorizadas voces que reclaman una nueva LECrim, podemos señalar las siguientes:
- El CONSEJO DE ESTADO en su informe al Anteproyecto de la LO 13/2015, consideró necesario «reiterar la conveniencia de no abandonar, sino de abordar, una reforma integral del proceso penal a través de una norma que venga a sustituir a la vigente LECrim y se adecue a las exigencias últimas del principio acusatorio, haciendo así realidad lo que ya en la exposición de motivos de aquella Ley se consideraba un objetivo deseable por razones que hoy siguen siendo válidas». Vid. CONSEJO DE ESTADO, «*Dictamen 97/2015, 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 tecnológica*», cit., p. 28.
- GIMENO SENDRA se refiere a «la conveniencia de promulgar un nuevo Código Procesal Penal de la democracia que simplifique y reduzca a dos el número de procesos ordinarios: el proceso ordinario por delito y el juicio por delitos menos graves». Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 667.
- MARCHENA GÓMEZ afirma que un nuevo Código Procesal Penal «permitiría contar con una regulación procesal más coherente y racional y haría posible adoptar mecanismo de agilización de mayor eficacia, fundamentalmente con la atribución de la investigación al Ministerio Fiscal y una regulación apropiada del principio de oportunidad en el ejercicio de la acción penal». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 40.
- GONZÁLEZ-MONTES SÁNCHEZ ha señalado que «…hemos escuchado en numerosas ocasiones críticas, de las cuales participamos, acerca de la imperiosa necesidad de implantar una nueva Ley de Enjuiciamiento Criminal en nuestro ordenamiento habida cuenta de la evidente falta de adaptación del actual texto normativo a la realidad social y penológica que rige nuestros días, tratándose como es sabido de una ley que data ya de 1882». Vid. GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», cit., p. 4.

[262] Comienza el preámbulo de la LO 13/2015 indicando que «la propuesta de Código Procesal Penal presentada por la Comisión Institucional para la elaboración de un texto articulado de Ley de Enjuiciamiento Criminal, constituida por Acuerdo del Consejo de Ministros de 2 de marzo de 2012, actualmente sometida a información pública y debate, plantea un cambio radical del sistema de justicia penal cuya implantación requiere un amplio consenso. En tanto dicho debate se mantiene, en la confianza de encontrar el máximo concierto posible sobre el nuevo modelo procesal penal, resulta preciso afrontar de inmediato ciertas cuestiones que no pueden aguardar a ser resueltas con la promulgación del nuevo texto normativo que sustituya a la más que centenaria Ley de Enjuiciamiento Criminal».

injerencias en los derechos fundamentales, siendo este último aspecto el que, mayormente, no permitió el necesario consenso para la promulgación de la nueva LECrim, tan necesaria para una regulación con una mayor calidad técnica y coherencia en su sistemática, renovando así una magnífica LECrim, pero, en la que, sin embargo, tanto su técnica como sistemática no se ajustan a la época actual[263]. Todo ello, sin dejar de mencionar que, de acuerdo con lo señalado por algunos autores, en algunos aspectos, tampoco la reforma ha sido redactada con la mejor sistemática[264].

Por tanto, y aunque no deben restarse méritos a la encomiable Ley de 1882[265], es notable la desidia que la clase política ha demostrado en los últimos años para conseguir unos acuerdos tan necesarios que doten de una mayor seguridad jurídica a nuestro sistema procesal penal, que beneficiaría no solo al justiciable, sino, en general, a todos los operadores de la justicia.

---

[263] Se inicia la exposición de motivos del Anteproyecto de LECrim de 2013 señalando que «tan obvia resulta la obsolescencia de la Ley de Enjuiciamiento Criminal de 1882 que el clamor unánime en favor de su sustitución por un nuevo texto legal haría vana una detallada exposición de los argumentos justificativos de la decisión de emprender la reforma. Sólo por la necesidad de la superación de las incoherencias normativas que las numerosas modificaciones de la Ley han provocado, la redacción de un Código de Proceso Penal es hoy ineludible. Pero no es la calidad técnica el objetivo de la norma procesal, sino presupuesto para su eficacia al servicio de los fines que le son propios: la aplicación de la ley penal y la salvaguarda de los derechos de los justiciables. Para la consecución de dichos objetivos, en muchas ocasiones en conflicto, el nuevo Código de Proceso Penal configura un sistema de investigación y enjuiciamiento moderno, ágil y equilibrado, que se atreve a romper con la perniciosa tradición inquisitorial y atribuye la dirección de la investigación al Ministerio Fiscal, sin duda una de las novedades más sobresalientes».

[264] Según MARCHENA GÓMEZ, «el criterio de ordenación sistemática asumido por la reforma pierde su lógica en algunos aspectos. Por ejemplo, avala el erróneo entendimiento de que las disposiciones comunes en las que se enumeran los principios constitucionales que legitiman la interceptación de las comunicaciones telefónicas y telemáticas, así como el resto de las diligencias de investigación a que se refiere el enunciado del capítulo IV del mismo título VIII, no afectarían a diligencias como la apertura de correspondencia, la entrada y registro en lugar cerrado o el registro de libros y papeles», añadiendo que esta interpretación carece de sentido y que hubiera sido deseable que las disposiciones comunes abriesen el título VIII. Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., pp. 173-174.

[265] Afirma MARCHENA GÓMEZ que, aun cuando la LECrim desde su elaboración decimonónica ha demostrado algunas carencias o limitaciones, «se trata de insuficiencias que nada tiene que ver con su perfecta hechura, con la precisión de su lenguaje y con el revolucionario mensaje histórico que abanderaba su articulado». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., pp. 177.

En tal sentido, compartimos la opinión de GONZÁLEZ-MONTES SÁNCHEZ cuando señala que «a nuestro juicio, se ha perdido una oportunidad inmejorable para abordar en este tiempo la reforma integral de nuestro proceso penal. Este tipo de modificaciones, por su importancia y tramitación, requieren de actuaciones que conllevan prácticamente una legislatura completa, y esto se había conseguido iniciando como se ha dicho los trabajos los trabajos respectivos con la creación de la Comisión Institucional en torno a marzo de 2012, pero la aludida falta de consenso lo ha impedido»[266].

Por todo ello, no podemos sino proponer una vez más la promulgación de una nueva LECrim, con la finalidad de suplir las carencias de una norma que sigue presentando una estructura decimonónica y que, por tanto, exige una completa y nueva regulación que permita una justicia penal más eficaz, acorde con las necesidades de nuestra sociedad, en especial de todos los justiciables y operadores de la Administración de Justicia, todo ello conforme a las exigencias de una inexorable realidad del siglo XXI, muy alejada de la que, de una forma sobresaliente, fue recogida por el legislador del siglo XIX.

[266] GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», *Revista Electrónica de Ciencia Penal y Criminología*, vol. 17, n.º 06, 2015, p. 5. Consultado en http://criminet.ugr.es/recpc/17/recpc17.html el 26 de febrero de 2019.

CAPÍTULO III. DISPOSICIONES COMUNES A LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA EN LA LECRIM (I): PRINCIPIOS RECTORES Y CUESTIONES GENERALES

El capítulo IV del título VIII del libro II de la LECrim, que la reforma operada por la LO 13/2015 ha dedicado a las disposiciones comunes a todas las medidas de investigación tecnológica, debe ser analizado a fin de realizar un oportuno examen de todos los aspectos que, con carácter universal, afectan a las diligencias de investigación tecnológica y que, evidentemente, también inciden en los registros informáticos.

Cabe reseñar, que muchas de las consideraciones así como citas doctrinales y jurisprudenciales, tienen como referencia el análisis de casos en los que fue acordada la intervención de comunicaciones telefónicas, al encontrarse regulada esta medida desde mucho antes. En cualquier caso, tales referencias son aplicables a las medidas de investigación tecnológica en general, especialmente a los registros informáticos, habida cuenta, como ya hemos tenido la oportunidad de advertir en los capítulos anteriores, de la posible injerencia con la ejecución de los mismos, no solo en el derecho a la intimidad y a la protección de datos, sino también en el derecho al secreto de las comunicaciones.

Con la finalidad de obtener una mejor sistemática en el examen de estas disposiciones, dividiremos su estudio en dos capítulos, dedicando el primero de ellos a los principios rectores y cuestiones generales, ocupándonos en una segunda parte a los demás aspectos procesales comunes.

I. Principios rectores de las medidas de investigación tecnológica

De una forma concisa, la LECrim determina, al iniciar el capítulo IV del título VIII del libro II, que «durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida» (art. 588 bis a.1 LECrim).

Se establecen así, conforme a la rúbrica del citado precepto, unos principios rectores, cuyo fundamento reside en asegurar el respeto a los derechos fundamentales que pudieran verse afectados como consecuencia de la ejecución de las medidas de investigación. Dedicaremos este apartado al estudio de estos principios, si bien el principio de reserva jurisdiccional, cuyo examen comprenderá tanto los aspectos relevantes de la solicitud de autorización judicial como los de la propia resolución judicial, será examinado en el capítulo siguiente.

Debe dejarse constancia previamente, sin perjuicio de los puntuales incisos que se efectúen en este apartado, que el legislador no ha positivizado el principio de proporcionalidad en sentido amplio o principio de prohibición de exceso, como sí lo hizo en el Anteproyecto de LECrim de 2013[267], sino que ha incluido los principios que la doctrina y la jurisprudencia venían considerando como subprincipios de aquel; esto es, los de idoneidad, necesidad (desglosado en los de excepcionalidad y necesidad) y proporcionalidad en sentido estricto.

1. Principio de especialidad

De conformidad con el principio de especialidad, cualquier acto de investigación tecnológica debe estar relacionado con la averiguación de un delito concreto, sin que puedan autorizarse medidas que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva (art. 588 bis a.2 LECrim).

Por tanto, quedan vedadas aquellas que estuvieran dirigidas a vigilar conductas, sin que existan indicios claros de la posible comisión de un delito, no siendo lícitas, en consecuencia, las observaciones encaminadas a una prospección sobre la conducta de una persona en general[268].

Como señala el preámbulo de la LO 13/2015, el legislador ha estimado oportuna la proclamación normativa de los principios que el TC había definido como determinantes de la validez del acto de injerencia. En este sentido, se exige que toda medida tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose las medidas de investigación tecnológica de naturaleza prospectiva[269].

---

[267] Vid. nota al pie n.º 218, p. 115.

[268] Vid. STS 454/2015, de 10 de julio, que declaró: «En este aspecto debe delimitarse objetivamente la medida mediante la precisión del hecho que se está investigando, y subjetivamente mediante la suficiente identificación del sospechoso, vinculando con él las líneas telefónicas que se pretende intervenir. Para ello es preciso que el juez cuente con indicios suficientes de la comisión del delito y de la participación del investigado».

[269] El preámbulo de la LO 13/2015, a fin de indicar que el legislador ha seguido el criterio establecido por el TC, menciona por todas la STC 253/2006, de 11 de septiembre, que en su FJ 2.º declaró que «se trata, por consiguiente, de determinar si en el momento de pedir y adoptar la medida de intervención se pusieron de manifiesto ante el juez, y se tomaron en consideración por éste elementos de convicción que constituyan algo más que meras suposiciones o conjeturas de la existencia del delito o de su posible comisión, y de que las conversaciones que se mantuvieran a través de la línea telefónica indicada eran medio útil de averiguación del delito. En consecuencia, la mención de los datos objetivos que permitieran precisar que dicha línea era utilizada por las personas sospechosas de su comisión o de quienes con ella se

La STC 26/2010, de 27 de abril, FJ 2.º, con cita de otras[270], estableció como presupuestos materiales habilitantes de la intervención, para el cumplimiento del principio de especialidad, «los datos objetivos que puedan considerarse indicios de la posible comisión de un hecho delictivo grave y de la conexión de las personas afectadas por la intervención con los hechos investigados». De este modo, declaró asimismo la referida resolución, se ha de proporcionar «una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito, sin que puedan consistir en valoraciones acerca de la persona», dado que «si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones, tal y como la CE lo configura, quedaría materialmente vacío de contenido».

Por su parte, el TS se ha pronunciado en diversas ocasiones en relación con este principio. Así, la STS 991/2016, de 12 de enero de 2017, FJ 1.º, declaró que «sólo la autoridad judicial competente puede autorizar el sacrificio del derecho fundamental al secreto de las comunicaciones y a la intimidad, y siempre con la finalidad exclusiva de proceder a la investigación de un delito concreto y a la detención de los responsables, rechazándose las intervenciones predelictuales o de prospección». Para ello, «los datos facilitados por la policía han de tener un grado de objetividad que los diferencie de la mera intuición policial o conjetura»[271].

2. Principio de idoneidad

Para que el principio de idoneidad se cumpla, la adopción de la medida ha de ser adecuada para la consecución del fin pretendido. Por ello, en el ámbito de los registros informáticos deberán existir sospechas fundadas de que en los concretos dispositivos existen contenidos con utilidad para probar la comisión del hecho delictivo.

---

relacionaban, y que, por lo tanto, no se trataba de una investigación meramente prospectiva, pues el secreto de las comunicaciones no puede ser desvelado para satisfacer la necesidad genérica de prevenir o descubrir delitos o para despejar las sospechas sin base objetiva que surjan de los encargados de la investigación, ya que de otro modo se desvanecería la garantía constitucional».

[270] SSTC 49/1999, de 5 de abril, FJ 8.º; 166/1999, de 27 de septiembre, FJ 8.º; 171/1999, de 27 de septiembre, FJ 8.º; 299/2000, de 11 de diciembre, FJ 4.º; 14/2001, de 29 de enero, FJ 5.º; 138/2001, de 18 de junio, FJ 3.º; 202/2001, de 15 de octubre, FJ 4.º; 167/2002, de 18 de septiembre, FJ 2.º; 184/2003, de 23 de octubre, FJ 11.º; 261/2005, de 24 de octubre, FJ 2.º; y 220/2006, de 3 de julio, FJ 3.º

[271] En la citada STS se citan otras que avalan la doctrina mencionada, entre las que se pueden mencionar las SSTS 77/2007, de 7 de febrero; 610/2007, de 28 de mayo; 712/2008, de 4 de noviembre; 778/2008, de 18 de noviembre; y 85/2013, de 4 de febrero.

Tal y como señala AÑÓN CALVETE, el principio de idoneidad «permitirá al juez instructor valorar si los hechos y las personas a quienes se pretende investigar guardan relación con los hechos y personas objeto del procedimiento en el que se pretende la adopción de la medida»[272].

Por otra parte, el TC ha invocado, para referirse al principio de idoneidad, el art. 18 CEDH[273], declarando en sintonía con dicho precepto, que para que la medida sea idónea, esta ha de ser apta o adecuada para alcanzar el fin constitucionalmente legítimo perseguido con ella, declarando asimismo, que las medidas deberán servir objetivamente para determinar los hechos que constituyan el objeto del proceso penal[274].

La LECrim se ocupa de la idoneidad, como principio rector de las medidas de investigación tecnológica, disponiendo que: «El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad» (art. 588 bis a.3 LECrim).

De este modo, el legislador supedita la utilidad de la medida, a los aspectos esenciales que determinarán que la misma es apta y adecuada para conseguir el fin perseguido, como son las cosas y las personas sobre las que habrá de llevarse a cabo la investigación (ámbito objetivo y subjetivo). A estos elementos, el legislador añade la duración de la medida de investigación[275].

La inclusión de la duración de la medida como requisito necesario para que la misma pueda considerarse idónea para la consecución del fin perseguido, nos parece correcta si tenemos en cuenta que, tal y como analizamos en el capítulo anterior[276], el principio de idoneidad es un subprincipio del principio de proporcionalidad en sentido amplio o principio de prohibición de exceso.

---

[272] AÑÓN CALVETE, J., «Diligencias de Investigación Tecnológica y Derechos Fundamentales», *Tirant Online, Documento TOL5.429.306*, 2015.

[273] El art. 18 del CEDH bajo la rúbrica «Limitación de la aplicación de las restricciones de derechos» dispone: «Las restricciones que, en los términos del presente Convenio, se impongan a los citados derechos y libertades no podrán ser aplicadas más que con la finalidad para la cual hayan sido previstas».

[274] SSTC 207/1996, de 16 de diciembre, FJ 4.º y 25/2005, de 14 de febrero, FJ 6.º

[275] Como se tendrá la oportunidad de indicar en otro apartado de este trabajo, la duración de la medida, en el ámbito de los registros informáticos, tiene sentido en relación con los registros remotos, pero no así con los registros de dispositivos de almacenamiento masivo de información, en los cuales la diligencia se agota por su propia naturaleza, sin que sea posible fijar una duración concreta.

[276] Vid. supra apdo. II.3.1 del capítulo II, p. 119.

Efectivamente, establecer una concreta duración de las medidas de investigación que por su naturaleza la requieran, es una premisa necesaria para hacer valer la prohibición de cualquier exceso en la investigación y, por ello, la duración se encuentra íntimamente ligada a la idoneidad de la medida para la obtención del perseguido. Por tanto, consideramos que la duración de la medida se proyecta como un elemento del principio de idoneidad[277], por lo que entendemos acertada la opción del legislador.

3. Principios de excepcionalidad y necesidad

La doctrina y la jurisprudencia venían considerando el principio de necesidad como un subprincipio del principio de proporcionalidad en sentido amplio. El legislador, al establecer este principio, lo ha desglosado, a su vez, en dos: excepcionalidad y necesidad propiamente dicha.

En relación con esta regulación, nos parecen acertadas opiniones de algunos autores como SÁNCHEZ MELGAR quien, en relación con estos principios, afirma que «la ley los trata conjuntamente, pero tienen entidad separada y cada uno ostenta un significado propio»[278], mientras que ÁLVAREZ SUÁREZ ha señalado como punto en común entre ambos, que «la necesidad y la excepcionalidad guardan relación con la posibilidad (o no) de adoptar otras medidas de investigación con similar finalidad», y en tal sentido «la necesidad ha de determinarse en relación a la trascendencia que el previsible resultado de la medida ha de tener para la investigación; la excepcionalidad supone que no es posible (o resulta más gravoso) llegar a ese previsible resultado a través de otras medidas»[279].

El legislador ha desglosado ambos principios en el art. en el art. 588 bis a.4 LECrim, existiendo opiniones tanto a favor como en contra de tal tratamiento

[277] Autores como CABEZUDO RODRÍGUEZ opinan que la exigencia de la fijación de una concreta duración de la medida, es una proyección de los principios de excepcionalidad y necesidad. CABEZUDO RODRÍGUEZ, N., «Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim», cit., p. 545.

[278] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», *Práctica Penal - Cuaderno Jurídico*, n.º 82, 2016, Madrid, Editorial Jurídica Sepín, p. 25.

[279] ÁLVAREZ SUÁREZ, L., «El Ministerio Fiscal y las Diligencias de Investigación Tecnológica», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, pp. 108-109.

separado[280]. Por nuestra parte, nos posicionamos a favor de la opción del legislador, en el entendimiento de que es preferible una mayor concreción, tratándose de la regulación de unos principios que han de regir medidas de investigación que pueden restringir derechos fundamentales.

3.1. Principio de excepcionalidad

De acuerdo con lo declarado por el TS, del principio de excepcionalidad, también denominado principio de subsidiariedad, se infiere que cuando se acuerda la práctica de una diligencia de investigación tecnológica, no nos encontramos ante un medio normal de investigación, sino excepcional «en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado». Por ello, «ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria»[281].

Por ello, el apartado a) del art. 588 bis a.4, exige para que pueda ser acordada una medida de esta clase, que «no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado[282] e igualmente útiles para el esclarecimiento del hecho».

---

[280] A favor de que ambos principios se hubiesen unificado en uno solo, vid. GARCIMARTÍN MONTERO, R., *Los medios de investigación tecnológicos en el proceso penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2018, p. 36. Por su parte, entre los estudios realizados desde una posición favorable a la opción legislativa de desglosar ambos principios, vid. CASTILLEJO MANZANARES, R., «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», *Revista Aranzadi de Derecho y Proceso Penal - Parte Análisis Doctrinal*, n.º 45, 2017, p. 8.

[281] Vid. STS 168/2015, de 25 de marzo, FJ 3.º, que declaró, asimismo, que «en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención telefónica, por ello 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».

[282] Podría plantear dudas que el legislador se refiera al «investigado o encausado», dado que, aun cuando el término «encausado» conforme al DRAE comprende toda persona que se encuentra sometida a un proceso penal en general, en la práctica forense se trata de un término referido a la persona contra la que se produce una acusación formal presentada por el fiscal o por la acusación particular o popular, por lo que, estrictamente, ya ha dejado de ser investigada pasando a ser encausada. Son diversas las menciones de la LECrim al «investigado o encausado» en las que ambas figuras pueden darse y tener sentido en relación con la concreta regulación (por ejemplo en relación con la prisión provisional). Pero en el ámbito que nos ocupa, si se tiene en cuenta que no es posible acordar diligencias de investigación una vez que ha formulado la acusación, consideramos que el legislador podría haber evitado esta alusión al «encausado», siendo suficiente con que se hubiese referido al «investigado».

De este modo, la LECrim proclama el carácter extraordinario de estos actos de instrucción. En tal sentido, resulta convincente la afirmación de DELGADO MARTÍN, al señalar que «probablemente la práctica judicial debería profundizar sobre las consecuencias de la aplicación de este principio en cada uno de los supuestos sometidos a autorización judicial, especialmente cuando se trate de medidas que supongan una injerencia más intensa en derechos fundamentales»[283].

3.2. Principio de necesidad

Una medida es necesaria cuando, de no llevarse a efecto la misma, la investigación pudiera verse frustrada. Como declaró el TS, de conformidad con el principio de necesidad, solo cabe acudir a una concreta diligencia de investigación «si es realmente imprescindible tanto desde la perspectiva de la probable utilidad como de la cualidad de insustituible»[284]. Es decir, como señala LANZAROTE MARTÍNEZ, «se requiere que la intervención sea un medio sin el cual la obtención de las pruebas sería extraordinariamente difícil»[285].

Así se dispone en la LECrim, al establecer en el apartado b) del art. 588 bis 4 que, en aplicación del principio de necesidad, solo podrá acordarse una diligencia de investigación tecnológica «cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida».

4. Principio de proporcionalidad

Al principio de proporcionalidad, desde un punto de vista amplio, nos referimos en el capítulo II al llevar a cabo un estudio sobre los aspectos más relevantes en relación con las diligencias de investigación tecnológica con anterioridad a la LO 13/2015, indicando en dicho apartado que el principio de proporcionalidad se encontraba

[283] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 350.

[284] Vid. STS de 1 de diciembre de 1995 - ROJ: 6105/1995, FJ 9.º

[285] LANZAROTE MARTÍNEZ, P., «Intervención de las comunicaciones», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo II*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, p. 390.

conformado por tres subprincipios, a saber, idoneidad, necesidad y proporcionalidad en sentido estricto.

Una vez examinados, en los apartados anteriores, los principios de idoneidad y necesidad (este último desglosado en los principios de excepcionalidad y necesidad propiamente dicha), ha de señalarse, como así lo hace VEGAS TORRES, que «la referencia al principio de proporcionalidad en el artículo 588 bis a de la LECrim ha de entenderse referida a lo que el TC denomina "juicio de proporcionalidad en sentido estricto"»[286].

En efecto, el art. 588 bis a.5 LECrim contempla el principio rector de la proporcionalidad de una forma estricta, ya que parte de una ponderación entre el interés de la persona que sufre la injerencia en sus derechos fundamentales y el interés público y de terceros. De este modo, dispone el referido precepto que «las medidas de investigación reguladas en este capítulo solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros».

El principio de proporcionalidad exige un enjuiciamiento del juez, que evalúa en cada caso la proporción existente entre el medio empleado y los objetivos que se pretenden alcanzar, evitando así la injerencias en los derechos fundamentales que pudieran resultar excesivas o no estrictamente necesarias, exigiéndose en consecuencia una resolución motivada.

Para ponderar los intereses en conflicto, el referido precepto establece, en su segundo inciso, una serie de criterios en los que se basará la valoración del interés público, como son: «la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho».

Ya nos hemos ocupado, en los capítulos I y II[287], de la gravedad del hecho y la intensidad de los indicios existentes, habiéndonos referido igualmente a los criterios de la trascendencia social del delito y su ámbito tecnológico de producción.

---

[286] VEGAS TORRES, J., «Las medidas de investigación tecnológica», en Cedeño Hernán, M. (coord.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2017, p. 14.

[287] Vid. supra apdo. III. 4.4.3.3 del capítulo I, pp. 66-71; y apdo. II.3.2.2 del capítulo II, pp. 122-126.

Estos elementos han sido incluidos por el legislador de 2015 en la LECrim, si bien ha añadido un último aspecto a tener en cuenta, como es el de la «relevancia del resultado perseguido con la restricción del derecho». Se trata de una novedad, cuya inclusión en el texto legal nos parece del todo pertinente, por cuanto guarda estrecha relación con la «trascendencia social del hecho» y refuerza, por tanto, la posibilidad de que por la magnitud o importancia, que para el interés público y de terceros, pudieran tener tanto los hechos delictivos como el resultado perseguido por la investigación, pueda llevarse a cabo una concreta diligencia de investigación tecnológica sin mayores impedimentos, siempre que, además del principio de proporcionalidad en sentido estricto, se cumplan los demás principios rectores y las exigencias específicas establecidas para cada una de ellas.

II. Control judicial de las medidas de investigación tecnológica

Como ya dijimos en el capítulo II, en el apartado dedicado a la reserva jurisdiccional como requisito necesario para la validez de las diligencias de investigación, con carácter general, para la adopción de cualquier medida limitativa de derechos fundamentales y, consecuentemente, para la ejecución de medidas de investigación tecnológica, se exige autorización judicial, respetándose de este modo el principio de reserva jurisdiccional.

La LO 13/2015 ha incorporado este principio a nuestra legislación, estableciendo en el art. 588 bis a.1 LECrim que «durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial…» y, asimismo, dispone el art. 588 bis b.1 LECrim que «el juez podrá acordar su práctica de oficio o a instancia del Ministerio Fiscal o la Policía Judicial»[288].

[288] A este respecto, autores como MORENO CATENA señalan que aunque el juez no ha perdido su condición de dirigir la investigación, «la verdad es que las últimas reformas normativas tienden a considerar que la iniciativa investigadora ha de situarse en la Policía judicial, que sería el cuerpo de funcionarios públicos con unos específicos conocimientos y preparación profesional en materia de investigación criminal, desplazando el papel del juez a confirmar o rechazar las iniciativas policiales. Concretamente en la regulación de 2015 sobre la utilización de medios tecnológicos de investigación, la ley prevé que las medidas se puedan acordar de oficio o a instancia del Ministerio Fiscal o de la Policía judicial (art. 588 bis b LECrim), si bien en el desarrollo de las diferentes medidas incide muy especialmente en la solicitud de la autorización de cada concreta medida, situando la iniciativa fuera del propio juez, como claramente sucede en la medida prevista en el art. 588 ter k) para identificación de un terminal y de un sospechoso a través de una dirección IP. Parece cada vez más necesario resituar al juez

Se establece por tanto que la medida, también pueda ser acordada de oficio. Ello no obsta, como correctamente indica LÓPEZ CAUSAPÉ, para que, teniendo en cuenta que a la luz del art. 588 bis c LECrim, se exige en todo caso, antes del auto motivado que autorice o deniegue la medida, la audiencia al Ministerio Fiscal —a la que en el capítulo siguiente nos referiremos—, tal audiencia se conceda, sin lugar a dudas, incluso cuando el juez de instrucción inicie de oficio el procedimiento para la adopción de cualquier medida de investigación[289].

El control judicial de las medidas de investigación puede ser dividido en tres niveles. Así lo declaró la jurisprudencia del TEDH al señalar que «la vigilancia puede sufrir un control en tres niveles: cuando se ordena, mientras es desarrollada y después cuando ella cesa», declarando en la misma resolución que en relación con las dos primeras fases «la naturaleza y la lógica misma de la vigilancia secreta exigen que se ejerzan sin el conocimiento del interesado no solamente la vigilancia como tal, sino también el control que le acompaña», para concluir que «puesto que se le impide al interesado presentar un recurso efectivo o de tomar parte directa en cualquier control, se revela indispensable que los procedimientos existentes proporcionen en sí las garantías apropiadas y equivalentes para la salvaguarda de los derechos del individuo»[290].

Realizaremos un examen, con carácter general, del control judicial de las medidas de investigación en la LECrim atendiendo a los referidos tres niveles.

1. Primera fase del control judicial

1.1. Formalidades exigidas

La resolución judicial que autorice la medida de investigación tecnológica, constituye la primera fase o primer nivel del control judicial de la misma.

---

en un diseño más coherente del proceso penal, haciéndole intervenir solamente como garante de los derechos fundamentales y dejando la iniciativa y la responsabilidad de la investigación pública de los delitos a otra instancia, que en todos los países de nuestro entorno es el Ministerio Fiscal y, bajo su dependencia, la Policía judicial». Vid. MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 266.

[289] LÓPEZ CAUSAPÉ, E., «Las medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín Digital Asociación de Jueces y Magistrados Francisco de Vitoria*, n.º 6, 2016, p. 5.

[290] Vid. STEDH de 6 de septiembre de 1978, caso Klass c. Alemania, apdo. 55, primer inciso.

Las formalidades que ha de cumplir este primer nivel del control judicial a través del auto autorizando la intervención policial, que podrá ser dictado, bien de oficio o bien tras la petición del Ministerio Fiscal o Policía Judicial, se encuentran previstas en el art. 588 bis c LECrim.

En relación con las mismas, ha de decirse, como así lo hace RICHARD GONZÁLEZ, que «la Ley no ha escatimado respecto a la exigencia de la constancia de elementos de control que permitan garantizar no sólo la constitucionalidad de la medida de intervención, sino también el buen fin de la misma, para lo que será necesario que se desarrolle de forma correcta y, especialmente, que se produzca un adecuado control de su ejecución»[291].

Sin perjuicio de ello, ha de tenerse en cuenta, conforme señala VELASCO NUÑEZ, que el auto judicial al que le falte alguno de los requisitos establecidos en el citado precepto, «no estará viciado de nulidad, salvo que lo omitido sea fundamental, como puede ser la descripción —aunque sea somera— del hecho o la existencia de indicios, siempre que lleven a indefensión, viciando el resultado de la injerencia por vulnerar la posibilidad de ejercer una defensa efectiva contra el mismo, que se podrá llevar a cabo cuando se alcen las medidas y el secreto, si la parte afectada lo recurre en plazo»[292].

Ante la circunstancia de ser diversos los aspectos que se han de consignar necesariamente en la resolución, en algunos casos coincidentes con los que deben reflejarse en la solicitud; cabe preguntarse si, tras la LO 13/2015, puede aceptarse que el auto autorizando la medida sea motivado por remisión a la solicitud policial.

1.2. Motivación del auto por remisión a la solicitud del Ministerio Fiscal o Policía Judicial

Con anterioridad a la reforma operada por la LO 13/2015, tanto el TC como el TS, venían admitiendo, con abundante jurisprudencia, la motivación de la resolución por

---

[291] RICHARD GONZÁLEZ, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, Las Rozas (Madrid), Wolters Kluwer, 2017, p. 64.

[292] VELASCO NÚÑEZ, E., «Investigación Tecnológica de Delitos: Disposiciones Comunes e Interceptaciones Telefónicas y Telemáticas», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 8, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Velasco Nuñez, Eloy.pdf?idFile=7b2fdf75-4a93-41bd-9adc-fe3042c95cc0, el 9 de junio de 2020.

remisión, considerando, en consecuencia, suficientes los elementos indiciarios consignados en el oficio policial o del Ministerio Fiscal.

Así, por ejemplo, la STC 72/2010, de 18 de octubre, declaró que «aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención se exteriorice directamente en la resolución judicial, ésta, según una consolidada doctrina de este Tribunal, puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial a la que puede remitirse, contiene los elementos necesarios para considerar satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva»[293].

También el TS había aceptado la motivación por remisión, siempre y cuando en el oficio policial se contuviesen una serie de detalles y concreciones que no pudieran contestarse con referencias genéricas a una posible actividad delictiva, debiendo exponerse por los agentes actuantes la metodología de la investigación, aportándose elementos necesarios que llevasen al juez a la convicción de que los hechos justificaban la medida. Siempre que se diesen estos requisitos, «se ha abierto paso una línea jurisprudencial flexible en la que se convalida la decisión judicial [...] por la remisión al contenido del oficio policial»[294].

Actualmente, tras la reforma de la LECrim operada por la LO 13/2015, la cuestión relativa a la motivación por remisión sigue admitiéndose jurisprudencialmente, estimándose que, si bien no es una técnica judicial modélica, es suficiente, sin necesidad de innecesarias repeticiones, si la solicitud, una vez extraídos los indicios especialmente relevantes, contiene todos elementos necesarios para llevar a cabo el juicio de proporcionalidad[295].

---

[293] Vid. STC 72/2010, de 18 de octubre, FJ 2.º, la cual, para referirse a la consolidada doctrina del TC cita las SSTC 167/2002, de 18 de septiembre, FJ 2.º; 184/2003, de 23 de octubre FFJJ 9.º y 11; y 261/2005, de 24 de octubre, FJ 2.º

[294] Vid. STS 239/2008, de 30 de abril, FJ 1.º

[295] Vid. STS 145/2017, de 8 de marzo, que declara que «de otra parte, aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución judicial, ésta puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial, a la que puede remitirse, contiene los elementos necesarios para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva». Por su parte, la STS 180/2018, de 13 de abril, con cita de otras resoluciones del TS y TC declara que «la motivación por remisión no es una técnica jurisdiccional modélica, pues la

Sin embargo, tras la LO 13/2015, desde una perspectiva dogmática, cabe plantearse hasta qué punto es válida una motivación por remisión, cuando el art. 588 bis c.3 LECrim establece en el apartado a) que la resolución deberá reflejar «el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que se funde la medida»[296].

Cabe hacerse esta pregunta, más aun, cuando del preámbulo de la LO 13/2015, parece que la intención del legislador, no es precisamente admitir una motivación por remisión, dado que, tras referirse a los casos que se dan en la práctica forense, de solicitudes policiales y de ulteriores resoluciones judiciales que adolecen de un laconismo argumental susceptible de vulnerar el deber constitucional de motivación, señala que «a evitar ese efecto se orienta la minuciosa regulación del contenido de esa solicitud, así como de la resolución judicial que, en su caso, habilite la medida de injerencia».

Por otra parte, al art. 588 bis c.3 LECrim le resulta perfectamente aplicable el aforismo *in claris non fit interpretatio* (donde está claro no es necesario interpretar) dado que, de una forma explícita, dispone que la resolución judicial que autorice la medida «concretará al menos los siguientes extremos».

Como dijimos en el capítulo anterior, al ocuparnos del requisito de la motivación, como uno de los aspectos esenciales del requisito de la reserva jurisdiccional, el TC, desde sus inicios, dejó sentada su obligatoriedad, y estableció que, en los casos de limitación de derechos fundamentales, se convierte en un riguroso requisito, razonando que cuando se coarta, como en este caso, el libre ejercicio de los derechos reconocidos por la Constitución, el acto es tan grave que necesita encontrar una especial justificación, y el hecho o el conjunto de hechos que lo justifican deben

---

autorización judicial debería ser autosuficiente (STS n.º 636/2012, de 13 de julio). Pero la doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada sí, integrada con la solicitud policial, a la que se remite, o con el informe o dictamen del Ministerio Fiscal en el que solicita la intervención (STS n.º 248/2012, de 12 de abril), contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (doctrina jurisprudencial ya citada, por todas STC 72/2010, de 18 de octubre). Resultando en ocasiones redundante que el Juzgado se dedique a copiar y reproducir literalmente la totalidad de lo narrado extensamente en el oficio o dictamen policial que obra unido a las mismas actuaciones, siendo más coherente que extraiga del mismo los indicios especialmente relevantes (STS n.º 722/2012, de 2 de octubre)».

[296] Este requisito lo examinaremos en el capítulo siguiente en el apartado dedicado a los requisitos que ha de reunir la solicitud de autorización judicial.

explicarse con el fin de que los destinatarios conozcan las razones por las cuales su derecho se sacrificó, de tal modo que la motivación no es solo una elemental cortesía, sino un riguroso requisito del acto de sacrificio de los derechos[297].

Con base en todo lo anterior, estimamos que, con la regulación de las medidas de investigación limitativas de los derechos reconocidos en el art. 18 CE, incorporada a la LECrim por la LO 13/2015, no está permitida la motivación de la resolución judicial por remisión al oficio policial.

No consideramos, que se pueda tachar de reiteraciones innecesarias aquellas cuestiones que, cuando se restringen derechos fundamentales, el juez competente extraiga de los argumentos plasmados por el Ministerio Fiscal o la Policía Judicial en la correspondiente solicitud. Es más, entendemos que el juez, por imperativo del ya mencionado apartado a) del art. 588 bis c.3, debe realizar esa tarea de extraer lo necesario del oficio policial, y motivar la necesidad de la intervención con sus propios argumentos, que deberán ser respetuosos con el principio de proporcionalidad y el resto de los principios rectores de las medidas de investigación tecnológica.

Por tanto, consideramos que la doctrina jurisprudencial, a la que nos hemos referido, que, con anterioridad a la LO 13/2015 —aun señalando que no era una práctica judicial modélica—, se mostraba permisiva con la motivación por remisión a la solicitud policial, no se ajusta a una correcta interpretación de la vigente LECrim.

Señalar por último, que se trata de una opinión compartida por algún sector doctrinal. Así, por ejemplo, SÁNCHEZ MELGAR, de forma terminante afirma que «el hecho de que se tengan que expresar los indicios racionales en los que se funda la medida, juega positivamente postergando el vicio de remisión indiscriminada a los oficios policiales, de manera que ahora deberá justificarse en la propia resolución judicial, y no en el escrito de petición»[298]. Y termina concluyendo este autor que, «hoy por hoy, la posibilidad de motivación por remisión al oficio policial debe mantenerse como algo no autorizado, o rigurosamente excepcional»[299].

---

[297] Vid. apartado II.2.2.2 del capítulo II, pp. 112-114 y, en el mismo, las citas de las SSTC 26/1981, de 17 de julio, FJ 14.º y STC 239/1999, de 20 de diciembre, FJ 5.º

[298] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 27.

[299] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 28.

2. Segunda fase del control judicial

El requisito de la jurisdiccionalidad exigido para la adopción de las medidas restrictivas de derechos fundamentales, se vería gravemente menoscabado en caso de que el juez de instrucción se limitase a ordenar la medida sin un control posterior de su ejecución, en cuyo caso no se garantizaría una debida tutela de los derechos fundamentales restringidos por las diligencias de investigación.

En virtud de este control, que constituye el segundo nivel al que se refirió el TEDH y que tiene lugar «mientras es desarrollada la medida de investigación», se exige que el juez de instrucción tenga cumplido conocimiento de todas las vicisitudes que se produzcan durante la ejecución de la misma medida.

El TEDH justificó principalmente la existencia de tal control jurisdiccional en la circunstancia de que la preeminencia del Derecho, dentro de los principios fundamentales de una sociedad democrática, exige un control eficaz del poder judicial en las injerencias en los derechos fundamentales, dado que él ofrece las mejores garantías de independencia, de imparcialidad y de regularidad en el procedimiento[300].

En este sentido, la LECrim ha dispuesto en el primer inciso de su art. 588 bis g, que «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…». De este modo, el legislador ha señalado como presupuesto para que se dé un adecuado control judicial, la información al tribunal sobre el desarrollo, resultados y finalización de la diligencia, información que se deberá realizar en la forma y con la periodicidad determinada por el juez de instrucción competente.

El control judicial de la medida se configura así, además de como un deber de la Policía Judicial, como un deber de la propia autoridad judicial, quien, al dictar el correspondiente auto, tendrá la obligación de ordenar a la Policía Judicial que le sean

[300] Vid. STEDH de 6 de septiembre de 1978, caso Klass c. Alemania, apdo. 55, que en su segundo inciso declaró que: «Hace falta establecer, para no extralimitar las necesidades en el sentido del artículo 8, § 2, respetar también, tan fielmente como sea posible, en los procedimientos de control los valores de una sociedad democrática. Entre los principios fundamentales de tal sociedad figura la preeminencia del Derecho, a la cual se refiere expresamente el preámbulo del Convenio […]. Ella implica, entre otras, que una injerencia del ejecutivo en los derechos de un individuo sea sometida a un control eficaz que debe normalmente asegurar, al menos como último recurso, el poder judicial, pues él ofrece las mejores garantías de independencia, de imparcialidad y de regularidad en el procedimiento».

comunicadas todas las incidencias que tengan lugar a lo largo de la investigación, así como poner a su disposición cualquier grabación o material informático intervenido, lo cual deberá plasmar en la resolución con la debida claridad, estableciendo los periodos en los que deba facilitar la información[301], todo ello sin perjuicio de que por el juez se solicite los informes que considere necesarios en cualquier momento. En cuanto a la periodicidad en la que se ha de facilitar la información, nos ocuparemos de ello en el capítulo siguiente, al referirnos a los requisitos que ha de cumplir la resolución judicial que acuerde la medida.

También el TS se ha ocupado de los requisitos exigidos para un debido control judicial, declarando que el mismo forma parte del núcleo constitucional de la ejecución de la medida, por tratarse de una actividad judicial precisa para su corrección y proporcionalidad[302].

Por otra parte, el control judicial de la medida de investigación «no debe ser una mera práctica formal de una dación de cuenta, sino un trámite importante en el que el tribunal debe evaluar, con base en los resultados, si la intervención era idónea y necesaria»[303], y ello a los efectos de en su caso prorrogar la misma o darla por concluida. En tal sentido, procede incluir en el estudio de esta segunda fase del control judicial, la posibilidad legal de prórroga.

---

[301] Vid. STC 184/2003, de 23 de octubre, FJ 10.º en la que examinando un proceso relacionado con una diligencia de intervención de las comunicaciones telefónicas —perfectamente trasladable al registro remoto de sistemas informáticos— declaró que para la legitimidad de la medida limitativa del derecho al secreto de las comunicaciones debe determinarse con precisión el número o números de teléfono que deben ser intervenidos, el tiempo de duración de la intervención, quién ha de llevarla a cabo y los períodos en los que deba darse cuenta al juez de sus resultados a los efectos de que éste controle su ejecución (por todas SSTC 49/1999, de 5 de abril, FJ 7 y siguientes; 167/2002, de 18 de septiembre, FJ 2)».

[302] STS 435/2013, de 28 de mayo, FJ 2.º en la que resaltó que «dicho control, según la jurisprudencia constitucional (SSTC 49/99, 166/99, 299/00, 138 y 202/01 y 167/02) puede resultar ausente o deficiente cuando no se han fijado temporalmente los periodos en que deba darse cuenta al juez del resultado de la restricción, cuando la policía los incumpla, pero también si el juez que autorizó la restricción no efectúa un seguimiento de las vicisitudes del desarrollo y cede de la misma y si desconoce el resultado obtenido en la investigación».

[303] RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», *Diario La Ley - Sección Tribuna*, n.º 8808, 2016, p. 17.

2.1. Prórroga de la medida

El art. 588 bis e LECrim, establece en su segundo apartado que «la medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron».

La prórroga de la medida supone una ampliación en el tiempo, por ser necesario para el buen fin de la investigación, de lo ya acordado motivadamente en la resolución inicial que acordó la intervención. Ahora bien, en línea con lo que venimos exponiendo, para que la prórroga sea procedente, se hace necesario que el juez examine si subsisten las razones que dieron lugar a la intervención, justificando la legitimidad de la continuación restrictiva del derecho fundamental y, por tanto, si se siguen cumpliendo los principios rectores que han de presidir toda diligencia de investigación tecnológica limitativa de derechos fundamentales, lo cual no hace sino fortalecer el imperativo control judicial de la medida.

De este modo, conforme ha declarado la jurisprudencia, «el principio de fundamentación de la medida, abarca no solo al acto inicial de la intervención, sino también a las sucesivas prórrogas, ya que el control es un *continuum* que no admite rupturas»[304]. Aun así, ha de tenerse en cuenta, como igualmente ha declarado el TS al referirse a la prórroga, que «en las sucesivas resoluciones la legitimidad constitucional de la medida exigirá que el control judicial siga siendo efectivo, pero no que se expresen renovados presupuestos fácticos que, por definición, pueden ser los mismos que los que motivaron la inicial autorización de la injerencia»[305]. Asimismo, «no es preciso ponderar de forma redundante lo ya ponderado antes, y será únicamente objeto del control la justificación de la prórroga en lo que supone de concesión de un nuevo período temporal para una intervención ya justificada»[306].

2.2. Solicitud de prórroga

La prórroga, dice el art. 588 bis e.2 LECrim, podrá ser acordada de oficio o previa petición razonada del solicitante.

[304] Vid. STS 993/2016, de 12 de enero de 2017, FJ 6.º
[305] Vid. STS 598/2008, de 3 de octubre, FJ 1.º
[306] Vid. STS 497/2016, de 9 de junio, FJ 1.º

En relación con la decisión *motu proprio* por parte del tribunal, esta podrá tener lugar cuando por la Policía Judicial se haya efectuado una regular rendición de cuentas con la periodicidad que hubiese sido acordada, de tal forma que, sin necesidad de una nueva petición, permita al juez de instrucción quedar debidamente instruido y resolver sobre la continuación de la medida.

Por lo que respecta al acuerdo de prórroga a instancia de parte, se ocupa de ello el art. 588 bis f LECrim, que en su apartado 1 dispone que «la solicitud de prórroga se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido». Obviamente, la prórroga ha de resolverse con anterioridad al vencimiento del plazo inicialmente concedido, por lo que es necesaria la presentación de la solicitud dentro de un término prudencial previo a la finalización del plazo inicial, que permita una resolución debidamente reflexionada.

Continúa disponiendo el art. 588 bis f.1 LECrim, que la solicitud deberá incluir en todo caso, un informe detallado del resultado de la medida y las razones que justifiquen la continuación de la misma.

En cuanto al informe detallado del resultado de la medida, como ya hemos visto, se trata de una comunicación preceptiva por imperativo del art. 588 bis g LECrim, para poder llevar a efecto un adecuado control judicial, y que permitirá al juez analizar si subsisten las razones que motivaron la intervención. En este sentido, dice SÁNCHEZ YLLERA, la información a facilitar al juez dentro del control de la medida que establezca «es también soporte de la decisión de prórroga»[307].

Por lo que se refiere a las razones que justifiquen la continuación de la medida, el apartado b) del art. 588 bis f.1 LECrim, exige una labor de motivación al Ministerio Fiscal o a la Policía Judicial, a fin de acreditar adecuadamente la necesidad de continuar con la intervención y consecuentemente con la restricción del derecho fundamental, ilustrando de ello debidamente al juez.

Consideramos muy apropiada una previsión como esta, dado que, conforme señala SÁNCHEZ YLLERA, en el momento de decidir sobre la prórroga el juez no puede ya atender únicamente a las razones iniciales, es decir a las sospechas fundadas, que le

[307] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art . 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 20.

llevaron a adoptarla. Por ello, la decisión de prórroga no puede hacerse implícitamente o por remisión a la inicial resolución autorizadora, porque no puede dejar de analizar y tomar en consideración los resultados obtenidos con la injerencia ya practicada, siendo esta «la única forma de garantizar la necesidad e idoneidad de la continuación de la medida inicialmente adoptada»[308].

La STC 145/2014, de 22 de septiembre, FJ 4.º, lo interpretó del mismo modo, al declarar que «tales exigencias de motivación se reproducen en las prórrogas y en las nuevas escuchas acordadas a partir de datos obtenidos en una primera intervención, debiendo el juez conocer los resultados de ésta con carácter previo al acuerdo de prórroga, explicitando las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión tácita o presunta a la inicial».

Por su parte, de acuerdo con la Circular 1/2019 de la FGE, para cumplir con el requisito de emitir un informe detallado del resultado de la medida expresivo de las razones que justifiquen su continuación, «podrán utilizarse tanto la específica comunicación de los resultados de la medida como cualesquiera otros datos o circunstancias que deriven de la investigación (así, los resultantes de seguimientos, averiguaciones de toda índole o los que aporten otras medidas restrictivas de derechos fundamentales que se pudieran estar empleando)»[309]. En cualquier caso, como también, acertadamente en nuestra opinión, señala SANTOS MARTÍNEZ, «las razones que justifiquen la prórroga deben ser objetivas, quedando fuera de la petición valoraciones que destaquen aspectos subjetivos del investigado o que se basen en sospechas e intuiciones policiales»[310].

[308] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art . 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 20-21.

[309] FISCALÍA GENERAL DEL ESTADO, *Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*, 2019, p. 18, Consultado en https://www.fiscal.es/documents/20142/972fdb98-5e62-2609-f99f-7a6d887b5d03, el 1 de junio de 2020.

[310] SANTOS MARTÍNEZ, A. M., «Examen de las disposiciones comunes de las medidas de investigación tecnológica», *Tirant Online, Documento TOL6.677.116*, 2018, p. 17.

2.3. Plazo para resolver la prórroga y cómputo de la misma

Pasando a ocuparnos del plazo en el que se ha de resolver la solicitud de prórroga, el art 588 bis f LECrim, establece en su apartado 2, que el juez resolverá en el plazo de dos días siguientes a la presentación de la solicitud sobre el fin de la medida o su prórroga.

No obstante la fijación de este breve plazo que, en principio, tratándose de la prórroga, nos parece razonable, ha de tenerse en cuenta, como ha puesto de manifiesto la Circular 1/2019 de la FGE, que «el incumplimiento de este plazo carece de trascendencia invalidante, tratándose de una simple irregularidad procesal que se agota en sí misma», si bien con la salvedad de que, en caso de que la medida se prorrogara después de vencido el plazo de duración inicialmente fijado, «no podrían ser utilizados los resultados obtenidos sin cobertura judicial, es decir, entre el día de vencimiento del plazo y el día de la prórroga, pero sin que la irregularidad producida alcanzara a afectar a los resultados obtenidos después de la prórroga»[311].

Establece asimismo el referido precepto que, antes de dictar la resolución, el juez podrá solicitar aclaraciones o mayor información. A este respecto, afirma MARCHENA GÓMEZ que, «la posibilidad al alcance del juez de solicitar una ampliación de la información obtenida […] forma parte del deseo legislativo de consolidar fórmulas eficaces de control»[312], lo cual ha de conectarse con la circunstancia de que, como igualmente señala el precepto, tras la solicitud de prórroga el juez podrá denegar la misma acordando el fin de la medida.

Finalmente, de conformidad con el art. 588 bis f.3 LECrim, una vez concedida, «su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada». Con ello queda excluida la posibilidad de que la prórroga se inicie en la fecha en la que se dicte el auto admitiéndola, sino que el cómputo se iniciará el día siguiente a la finalización del plazo inicial o en su caso el de la prórroga anterior.

---

[311] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., p. 19. En relación con esta apreciación, la Circular 1/2019 de la FGE cita las SSTS 926/2012, de 27 de noviembre y 55/2013, de 22 de enero.

[312] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 267.

3. Tercera y última fase del control judicial

El acuerdo de cese de la intervención forma parte del control judicial de la misma, encontrándonos ante el que el TEDH denominó el tercer nivel del control judicial de la medida[313].

En este sentido el TC ha recordado que el control judicial efectivo, tanto en el desarrollo como en el cese de la medida, es indispensable para el mantenimiento de la restricción de los derechos fundamentales, dentro de los límites constitucionales[314].

Efectivamente, es fácil llegar a la conclusión de que se está llevando a cabo un adecuado control judicial de la diligencia de investigación, necesario para preservar el requisito de la jurisdiccionalidad exigido para la adopción de las medidas restrictivas de derechos fundamentales, en aquellos casos en los que, por la autoridad judicial, se acuerde de forma motivada que ya no concurren las circunstancias que se tuvieron en cuenta para su adopción o cuando no se estén obteniendo los resultados pretendidos y, consecuentemente, se acuerde el cese.

La no concurrencia de las causas que dieron lugar a la intervención, dando lugar, por tanto, al cese de la medida, se producirán, tal y como dice SÁNCHEZ YLLERA, cuando «se desvanezcan los indicios que la hacían necesaria e idónea para el esclarecimiento de los hechos»[315] y, como señala RICHARD GONZÁLEZ, la valoración de las circunstancias mencionadas, solo se podrá realizar «…cuando se lleve a cabo un control real y efectivo del desarrollo de la medida»[316].

Todo ello queda corroborado, además, por el inciso final del art. 588 bis g LECrim, el cual establece que la Policía Judicial informará al juez del desarrollo y resultados de la medida «…y en todo caso, cuando por cualquier causa se ponga fin a la misma».

---

[313] Vid. texto relacionado con la nota al pie n.º 290 en la que se menciona la STEDH de 6 de septiembre de 1978, caso Klass c. Alemania, apdo. 55, pp. 152.

[314] Vid. STC 49/1996, de 26 de marzo, FJ 3.º

[315] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 21.

[316] RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», cit., p. 17.

En cuanto a los distintos supuestos por los que puede acordarse el cese de la medida, de conformidad con el art. 588 bis j LECrim, el juez ordenará el mismo, si se produce alguna de las tres siguientes situaciones:

1.º Si desaparecen las circunstancias que justificaron su adopción.

2.º Cuando resulte evidente que a través de la misma no se estén obteniendo los resultados pretendidos.

3.º En caso de transcurrir el plazo para el que hubiera sido autorizada.

Por tanto, de concurrir alguno de los supuestos mencionados, deberá el juez dictar la correspondiente resolución ratificando, en su caso, la finalización de la medida, siendo necesaria esta última resolución por las referidas exigencias del requisito de la jurisdiccionalidad necesarias para un adecuado control.

Con todo ello, las causas de cese de la medida pueden sistematizarse en dos apartados, como son: por la no necesidad de la continuación de la medida y por el transcurso del plazo.

3.1. Cese por la no necesidad de la continuación de la medida

Podemos afirmar que tanto en el caso de que desaparezcan las causas que justificaron la adopción de la medida como cuando sea evidente que no se están obteniendo los resultados pretendidos, no resulta necesario continuar con la intervención.

En estos casos, deja de concurrir el principio rector de la necesidad, común a todas las diligencias de investigación tecnológica. Consecuentemente, en atención a lo dispuesto en el art. 588 bis a.4 b) LECrim (referido a los supuestos en los que, únicamente, en aplicación del principio de necesidad, podrá acordarse la medida —para el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito—), la investigación ya no se vería gravemente dificultada sin recurrir a la concreta medida de investigación.

En relación con estos casos, como dice GARCIMARTÍN MONTERO, siendo evidente a la vista de los mismos que no es necesario agotar el tiempo por el que fue concedida la medida «el legislador parece considerar esta forma de cese de la medida como

subsidiaria y como forma ordinaria de terminación la decisión judicial cuando desaparezcan las circunstancias que motivaron su adopción o cuando no se estén obteniendo resultados»[317].

Asimismo, estos supuestos de finalización de la medida anteriores a la expiración del plazo por el que hubiese sido acordada, por falta sobrevenida del elemento de la necesidad, deben ser necesariamente confrontados con el art. 588 bis e.1 LECrim, que dispone que las medidas «…no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos».

Por otra parte, el hecho de que deba acordarse el cese de la medida por las anteriores circunstancias pone de manifiesto que, aunque se haya establecido un plazo máximo de duración de la intervención, el juez no puede mantener la medida más del tiempo necesario para la obtención de los resultados esperados por la investigación, lo cual convertiría a la medida en desproporcionada e ilegal[318].

3.2. Cese por el transcurso del plazo

Respecto al cese de la diligencia de investigación por el transcurso del plazo por el que fue autorizada, sin perjuicio de lo dispuesto en el art. 588 bis j LECrim, que como dijimos, en su último inciso establece que el juez acordará el cese «…en todo caso, cuando haya transcurrido el plazo para el que hubiera sido acordada», ha de tenerse en cuenta que de conformidad con el art. 588 bis e.3 LECrim, una vez transcurrido dicho plazo, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, la medida cesará a todos los efectos. Por ello, el cese se producirá por ministerio de la ley y como se ha señalado doctrinalmente[319], sin necesidad de dictar una resolución judicial que así lo dictamine.

Sin embargo, esta afirmación no ha de entenderse en el sentido de que no será necesaria una resolución judicial, lo cual iría en contra del espíritu de la regulación legal

---

[317] GARCIMARTÍN MONTERO, R., «*Los medios de investigación tecnológicos en el proceso penal*», cit., p. 65.

[318] Vid. STS 622/1998, de 11 de mayo, FJ 2.º

[319] Afirma MARCHENA GÓMEZ que «por supuesto, como expresa el apartado 3 del art. 588 bis e, el cese de la injerencia, una vez transcurrido el término exacto para el que fue concedida, se producirá sin necesidad de dictar una resolución que formalmente así lo exprese». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 265.

en su conjunto. Conforme a una interpretación adecuada, lo que ha de inferirse es que la Policía Judicial no podrá prolongar la intervención más allá del plazo por el que fue acordada, so pena de ilicitud, pero ello no debe obstar a que en el marco de un conveniente y oportuno control jurisdiccional se dicte la correspondiente resolución judicial acordando el cese de la concreta investigación, por lo que entendemos que, en cumplimiento del art. 588 bis j LECrim, el juez deberá dictar en todo caso la correspondiente resolución dando por concluida la medida.

3.3. Comunicación del cese de la medida al investigado

Como quiera que la práctica de la diligencia de investigación tecnológica debe permanecer en secreto para el investigado, lo cual se halla dentro de lo correcto y de la más elemental lógica[320], se plantea la cuestión de si el auto acordando el cese deberá ser notificado al investigado. La jurisprudencia del TS se ha pronunciado en sentido afirmativo en diversas sentencias remarcando la necesidad de que «el cese de la medida se le comunique al afectado y éste disponga de un recurso efectivo en cuyo marco pueda discutir la legalidad de la intervención, sin perjuicio de su posible impugnación en el juicio oral»[321].

Debe distinguirse no obstante, entre aquellos casos en los que tras la investigación se apreciasen indicios delictivos, en los cuales ha de notificarse la resolución acordando el cese al investigado, conforme a lo señalado en el párrafo anterior, de aquellos, en los que por no resultar debidamente justificada la perpetración del delito o no haya motivos suficientes para acusar al investigado o investigados, se acordase el sobreseimiento provisional, dado que tal resolución no implica el fin de la investigación sino la insuficiencia de las diligencias que hasta ese momento hubiesen sido practicadas. Así lo ha declarado el TS, que en una de sus sentencias desestimó la impugnación por la falta de comunicación del cese de la medida, al haberse acordado el sobreseimiento provisional[322].

---

[320] De acuerdo con lo declarado por la STS 387/2016, de 6 de mayo, FJ 1.º, el secreto de las actuaciones debe acordarse imperativamente sin mayores argumentaciones, ya que lo contrario sería un absurdo «que además se hallaría en contradicción, con la finalidad de la medida injerencial, que resultaría arruinada».

[321] Vid. SSTS 938/2013, de 10 de diciembre, FJ 1.º; 64/2011, de 8 de febrero, FJ 1.º; 864/2005, de 22 de junio, FJ 1.º

[322] Vid. STS 960/2008, de 26 de diciembre, FJ 1.º, la cual declaró que no podía prosperar la denunciada falta de comunicación al afectado de la medida una vez que se había ordenado su cese, señalando que «si la alegación se refiere a la no notificación del auto de sobreseimiento provisional no se puede olvidar que

III. Duración de la medida

1. Plazo legal

Cuando se acuerda una medida de investigación que necesariamente limitará un derecho fundamental, no puede plantearse que dicha actuación se establezca de forma indefinida, ya que nos encontraríamos ante una intervención desproporcionada e ilegítima y que, por lo tanto, carecería de validez constitucional, comprometiéndose seriamente el principio de seguridad jurídica.

En este sentido, autores como MARCHENA GÓMEZ afirman que la necesidad de fijar límites temporales deriva de la propia naturaleza del derecho a la inviolabilidad de las comunicaciones (aunque se refiere a la inviolabilidad de las comunicaciones, la necesidad es perfectamente trasladable a cualquier otro de los derechos a la vida privada)[323], añadiendo que «una solicitud que no autolimitara su vigencia en el tiempo sería rechazable por sí sola»[324].

El TEDH, en numerosas sentencias, ya desde hace tiempo, determinó que el hecho de que el juez no estuviese obligado a fijar una duración a una medida de investigación tecnológica, podría ser considerado como un abuso[325]. Asimismo, consideró la fijación de la duración de la medida como una de las condiciones necesarias para asegurar la previsibilidad de la ley y garantizar en consecuencia el respeto de la vida privada[326].

---

tal resolución no implica el fin de la investigación sino la insuficiencia de la hasta entonces practicadas, y ello determina que no haya una persona formalmente imputada y que la investigación judicial haya concluido provisionalmente, lo que no excluye su posterior reapertura, y su posterior comunicación, como aquí sucedió cuando se dejó sin efecto el secreto del sumario, y ese sobreseimiento provisional no impide que continúen las investigaciones policiales, sin que exista un derecho constitucional que exija advertir a una persona que caso de cometer delitos puede ser objeto de investigación, no apreciándose, en consecuencia, vulneración alguna del derecho al secreto de las comunicaciones ni, en modo alguno, la invocada vulneración del derecho a la libertad, que carece en el recurso del más mínimo desarrollo».

[323] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 245.

[324] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 245.

[325] Vid. STEDH de 24 de abril de 1990, caso Kruslin c. Francia, apdo. 35, que declaro: «Sobre todo, el sistema no proporciona hasta el momento la protección adecuada contra los posibles abusos…; el juez no tiene obligación de fijar un límite a la duración de la medida…»

[326] Vid. STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España, apdo. 59, que declaró: «El Tribunal subraya que algunas de las condiciones derivadas del Convenio, necesarias para asegurar la

Por su parte, el TC se ha pronunciado en diversas ocasiones y ha considerado la duración de la medida como un elemento indispensable para realizar el juicio de proporcionalidad[327], mientras que el TS de forma similar ha declarado que «la medida no puede prorrogarse de manera indefinida o excesivamente larga porque ello la convertiría inexorablemente en desproporcionada e ilegal fuese cual fuese la naturaleza y gravedad del delito investigado»[328].

Acorde con estas consideraciones, la LECrim ha dispuesto en el art. 588 bis e.1, tras la reforma operada por la LO 13/2015, que las medidas de investigación tecnológica tendrán la duración que se especifique para cada una de ellas.

De este modo, se ha fijado para la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter g LECrim), y para el uso de dispositivos técnicos de seguimiento y localización (art. 588 quinquies c.1 LECrim) un plazo de 3 meses, prorrogables por iguales períodos hasta 18 meses, mientras que para los registros remotos de sistemas informáticos (art. 588 septies c LECrim), se ha fijado una duración máxima de un mes prorrogable por iguales periodos hasta un máximo de tres meses[329]. Resulta llamativo que para los registros remotos se establece un plazo notablemente inferior al de las otras diligencias de investigación tecnológica mencionadas, aunque de esta problemática nos ocuparemos en el apartado correspondiente dentro del capítulo V, dedicado a los registros informáticos.

---

previsibilidad de la "ley" y garantizar así el respeto de la vida privada y de la correspondencia, no están incluidas ni en el artículo 18.3 de la Constitución ni en las disposiciones de la Ley de Enjuiciamiento Criminal […] en particular, […] la duración máxima de la ejecución de la medida…».

[327] Vid. STC 25/2011, de 14 de marzo, FJ 2.º que declaró que «este Tribunal ha venido reiterando que las exigencias de motivación de las resoluciones judiciales que autorizan la intervención telefónica o su prórroga forman parte del contenido esencial del art. 18.3 CE. Éstas deben explicitar, en el momento de la adopción de la medida, todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Así, la resolución judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito […] así como determinar […] el tiempo de duración de la intervención…».

[328] STS de 9 de mayo de 1994 – ROJ: STS 3386/1994, FJ 2.º

[329] Dice CABEZUDO RODRÍGUEZ que: «El resto de las medidas no tienen previsto un plazo máximo, bien porque se agotan en sí mismas, como es el caso del registro de dispositivos de almacenamiento masivo de información, bien porque su uso viene acotado por la previsibilidad de encuentros concretos del investigado, en la captación y grabación de comunicaciones orales (art. 588 quater b)». Vid. CABEZUDO RODRÍGUEZ, N., «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín del Ministerio de Justicia*, n.º 2186, 2016, nota al pie n.º 53, p. 28.

2. Duración dependiendo del caso concreto

El art. 588 bis e.1 LECrim, no se limita a establecer que la duración de la medida será la que se especifique para cada una de ellas, sino que añade en su segundo inciso que las medidas «no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos». A este respecto, cabe destacar que la Circular 1/2013 de la FGE, se había pronunciado en el sentido de que «no es suficiente con señalar un plazo de duración dentro de los límites permitidos por la LECrim, sino que es necesario que ese plazo no sea abusivo ni desproporcionado»[330].

Se establecen de este modo legalmente unos plazos máximos que no necesariamente han de ser aplicados, sino que, dependiendo de cada caso concreto, el juez deberá establecer el plazo que estrictamente considere necesario para el esclarecimiento de los hechos y así, de este modo, la diligencia cumpla el requisito de la idoneidad, a mayor abundamiento cuando no existe impedimento para que el plazo inicialmente fijado pueda ser prorrogado. Dicho de otro modo, siguiendo a MARCHENA GÓMEZ, el plazo establecido legalmente «no es una duración que, siempre y en todo caso con independencia de naturaleza y de las circunstancias del delito que está siendo investigado, haya de operar como plazo de referencia. Los principios de necesidad y excepcionalidad impiden someter el tiempo de la injerencia del Estado en las comunicaciones del sospechoso a parámetros cuantitativos de duración que actúen como referencia estandarizada»[331].

En parecido sentido se pronuncia la FGE en su reciente Circular 1/2019, en la que señala que la duración concreta de cada medida está afectada por tres límites, como son: en primer lugar, por el plazo máximo de duración que haya previsto el legislador; en segundo lugar, por el límite que ha de imponer el juez competente en la correspondiente resolución, en atención a las exigencias que los principios de idoneidad, necesidad, excepcionalidad y proporcionalidad presenten para el caso concreto; y por último, el límite que se determine por el propio devenir de la intervención, en el caso de

---

[330] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., p. 92. Añade la circular que no obstante el plazo máximo establecido en la Ley, «ello no significa que el juez pueda mantener la medida de forma indiscriminada e ilimitada, sino sólo el tiempo estrictamente indispensable para el buen resultado de la investigación, ya que, en caso contrario, la medida devendría desproporcionada e ilegal».

[331] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 246.

que se hubiera logrado el esclarecimiento de los hechos, o si se constatara que la diligencia no es adecuada para el fin que la justificó[332].

3. Cómputo del plazo

En cuanto al cómputo del plazo, ha sido objeto de cierta controversia jurisprudencial si el plazo por el que se acuerde la medida ha de iniciarse desde la resolución que lo acuerda o a partir del momento en que se haga efectiva la intervención.

El principal exponente que sostiene que el cómputo ha de iniciarse desde la resolución judicial lo constituye la STC 205/2005, de 18 de julio, la cual fue contundente al manifestarse sobre la improcedencia de que la práctica de la diligencia comenzase a desplegar sus efectos a partir del momento en que la misma se realiza, entendiendo que ello supone aceptar que se ha producido una suspensión individualizada del derecho fundamental al secreto de las comunicaciones desde el día en que se acuerda la resolución judicial hasta aquél en el que la intervención telefónica empieza a producirse, concluyendo que la Constitución solamente permite —con excepción de las previsiones del art. 55 CE—, que el secreto de las comunicaciones pueda verse lícitamente restringido mediante resolución judicial, sin que la intervención de terceros pueda alterar el *dies a quo* determinado por aquélla[333].

---

[332] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., pp. 17-18.

[333] STC 205/2005, de 18 de julio, FJ 5.º la cual declaró que aunque el argumento señalado en el texto sería suficiente para considerar lesionado el derecho fundamental, llevan a la misma conclusión otros razonamientos suplementarios. En este sentido señaló que «…debemos recordar que cuando la interpretación y aplicación de un precepto "pueda afectar a un derecho fundamental, será preciso aplicar el criterio […] de que las mismas han de guiarse por el que hemos denominado principio de interpretación de la legalidad en el sentido más favorable a la efectividad de los derechos fundamentales, lo que no es sino consecuencia de la especial relevancia y posición que en nuestro sistema tienen los derechos fundamentales y libertades públicas […]. En definitiva, en estos supuestos el órgano judicial ha de escoger, entre las diversas soluciones que entiende posibles, una vez realizada la interpretación del precepto conforme a los criterios existentes al respecto, y examinadas las específicas circunstancias concurrentes en el caso concreto, aquella solución que contribuya a otorgar la máxima eficacia posible al derecho fundamental afectado"». Asimismo señaló que «debemos afirmar ahora que el entendimiento de que el plazo previsto en una autorización judicial que autoriza la restricción del secreto de las comunicaciones comienza a correr el día en que aquélla efectivamente se realiza compromete la seguridad jurídica y consagra una lesión en el derecho fundamental, que tiene su origen en que sobre el afectado pesa una eventual restricción que, en puridad, no tiene un alcance temporal limitado, ya que todo

Sin embargo, previamente a esta resolución del TC, el TS se había pronunciado en sentido contrario, es decir, entendiendo que el cómputo debería iniciarse con la efectiva ejecución de la diligencia de investigación, matizando que ello podría ser así siempre y cuando no exista una desconexión temporal relevante entre uno y otro momento[334]. Además el TS se ha pronunciado del mismo modo con posterioridad a la doctrina constitucional referida. Así, por ejemplo, en la STS 453/2013, de 29 de mayo, FJ 1.º, declaró que «puede establecerse que en los supuestos del cómputo de los plazos de treinta días, concedidos para las intervenciones en los respectivos autos autorizantes o de concesión de sus prórrogas, el cómputo ha de realizarse desde su realización efectiva»[335].

Tras estos vaivenes jurisprudenciales, el legislador ha establecido legalmente, a nuestro juicio de forma acertada, el criterio fijado por la doctrina constitucional y en este sentido ha dispuesto para la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter g LECrim) y para la utilización de dispositivos técnicos de seguimiento y localización (art. 588 quinquies c LECrim), que el cómputo se iniciará a partir de la fecha de la autorización judicial. Sin embargo resulta sumamente criticable que no se haya efectuado una mención similar para el registro remoto de sistemas informáticos. Ello no debe obstar para que, ante tal laguna jurídica, se pueda recurrir a una autointegración analógica con base a las dos regulaciones referidas en diligencias de la misma naturaleza.

En cualquier caso, y con independencia de las citadas posiciones jurisprudenciales y la regulación legal, teniendo en cuenta la improcedencia del cómputo del plazo a partir de la ejecución de la diligencia llevada cabo en un día y hora

---

dependerá del momento inicial en que la intervención tenga lugar. Es así posible, por ejemplo, que la restricción del derecho se produzca meses después de que fuera autorizada, o que la autorización quede conferida sin que la misma tenga lugar ni sea formalmente cancelada por parte del órgano judicial».

[334] Vid. STS 774/2004, de 16 de junio, FJ 2.º que considera que en el caso que se resuelve no se puede entender que exista tal desconexión temporal, dado que «no solo no había transcurrido el plazo inicial, sino que además el oficio policial contiene nuevos datos sobre los sospechosos que, aunque no sean especialmente relevantes, sirven de complemento a los anteriormente aportados».

[335] Sin perjuicio de que es este un tema que requeriría un trabajo independiente, nos hemos de posicionar en contra de que por el TS se dicte resolución alguna en contra de la doctrina constitucional establecida por el TC en sus sentencias, en materias que afecten a derechos fundamentales. Ha de tenerse presente que el art. 5.1 de la LOPJ dispone que: «La Constitución es la norma suprema del ordenamiento jurídico y vincula a todos los Jueces y Tribunales quienes interpretarán y aplicarán las leyes y los reglamentos según los preceptos y principios constitucionales, conforme a la interpretación de los mismos que resulte de las resoluciones dictadas por el Tribunal Constitucional en todo tipo de procesos».

discrecionalmente fijado por la Policía Judicial —lo cual nos podría llevar a considerar ficticio el plazo máximo fijado legalmente—, consideramos que, una mayor protección de los derechos fundamentales en juego así como las exigencias del principio de seguridad jurídica, aconsejan que el día y hora concreto en el que la medida deberá iniciarse, deba ser fijado en el auto acordando la práctica de la medida, así como, consecuentemente, el día y hora de su finalización.

Cabe señalar que el TC declaró válido el cómputo de un plazo a partir de la intervención, ya que en la resolución judicial así se había establecido[336], lo que abrió la posibilidad mencionada de que en el propio auto se establezca una fecha concreta, aunque en este caso se seguía dejando margen a la Policía Judicial para la práctica de una diligencia limitativa de un derecho fundamental, lo cual, con el debido respeto a la legalidad vigente y doctrina constitucional, no consideramos admisible, entendiendo que se vulneran las exigencias del control judicial de la medida.

En este sentido, no nos parece correcto que se establezca un plazo para intervenir, siendo más acorde con la legalidad constitucional la fijación de día y hora tras la correspondiente petición del Ministerio Fiscal o la Policía Judicial. Ello contribuiría a evitar el transcurso de plazos excesivos entre el acuerdo y la ejecución, impidiendo que en las diligencias en las que puedan verse comprometidos los derechos fundamentales la Policía Judicial tenga un excesivo margen de actuación, que, no obstante ser conveniente en general para la investigación policial, no debe serlo en ningún caso cuando exista la posibilidad de restricción de derechos fundamentales, en cuyo caso ha de exigirse un estricto control judicial de la medida.

IV. Afectación de terceras personas

Podrán acordarse las medidas de investigación tecnológica aun cuando afecten a terceras personas, en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas (art. 588 bis h LECrim).

Previamente, debe recordarse que, para estos casos, los arts. 588 bis b y 588 bis c LECrim, exigen que tanto en la solicitud policial o del Ministerio Fiscal, como en la resolución judicial, se identifique a tales personas, lo cual, conforme indica LÓPEZ-

[336] Vid. STC 148/2009, de 15 de junio, FJ 3.º

BARAJAS PEREA, requerirá una motivación reforzada en atención a la delimitación subjetiva que viene impuesta por los principios de especialidad e idoneidad[337].

Esta afectación a terceras personas, que no son investigadas —aunque pudieran serlo—, no puede soslayarse, dado que sin la misma no podrían investigarse adecuadamente determinados delitos.

En este sentido, de conformidad con lo afirmado por RICHARD GONZÁLEZ esta necesidad de precisar las personas que pueden verse afectadas por la medida y cuales otras están obligadas a colaborar y a guardar secreto respecto a las medidas acordadas, se justifica en las actividades de relación y comunicación social que son objeto de las medidas de investigación tecnológica[338].

No obstante, estableciendo el precepto que habrá que estar a los casos y con las condiciones que se regulan para cada medida de investigación, ha de señalarse que, en lo que respecta a los registros informáticos, no se encuentra prevista esta circunstancia, ni para los registros de dispositivos de almacenamiento masivo, ni para los registros remotos de equipos informáticos, y ello a diferencia de lo establecido para la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter c LECrim) o para la captación de imágenes en lugares públicos (art. 588 quinquies a LECrim).

En todo caso, el análisis de la posibilidad de afectación de terceras personas y las razones por las que no se ha previsto dicha circunstancia para los registros informáticos, serán examinados en el capítulo dedicado a los mismos, en el apartado relativo a las disposiciones comunes a sus dos modalidades.

V. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales

La utilización de la información obtenida en un procedimiento distinto y los descubrimientos casuales, (conocidos ambos supuestos con la denominación común de «hallazgos casuales»), se encuentran regulados en el mismo precepto (art. 579 bis LECrim), al que se remite, para las diligencias de investigación tecnológica, el art. 588

[337] LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley», cit., p. 112.
[338] RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», cit., p. 15.

bis i LECrim, justificándose tal regulación conjunta en la circunstancia de que ambas incidencias tienen el mismo origen, que se encuentra en la práctica de una diligencia de investigación; es decir, en ambos casos debe haberse iniciado previamente una investigación acordada en un proceso instructor con una finalidad distinta.

Sin embargo, debe señalarse que, no obstante su estrecha relación, se trata de figuras distintas que merecen un estudio separado, y ello por cuanto la utilización de la información obtenida en una concreta investigación en un procedimiento distinto, se refiere al uso de la propia medida de investigación o la utilización de una prueba obtenida en la misma en otra causa ya iniciada o que se iniciase posteriormente, mientras que los descubrimientos casuales, tal y como expone ARMENTA DEU, son «aquellas conductas constitutivas de delito que se descubren a raíz de la injerencia, pero cuya investigación no estaba prevista en el auto habilitador de la misma»[339] y en las que por tanto se requiere la apertura de un nuevo procedimiento o bien el enjuiciamiento, por tratarse de delito conexo, en el mismo procedimiento donde se produjo el descubrimiento casual o en otro ya iniciado en el que se pudiese apreciar tal conexidad[340].

Habida cuenta de la complejidad que puede presentar el estudio de los hallazgos casuales, realizaremos por un lado un examen de la utilización de la información obtenida como medio de investigación o prueba en un proceso penal ya iniciado o que se iniciase posteriormente, y por otro analizaremos el descubrimiento casual propiamente dicho, entendiendo por tal el delito casualmente descubierto, para el que, o bien se debería iniciar un nuevo proceso o bien enjuiciarlo como delito conexo.

Dicho de otro modo, distinguiremos entre la problemática de la prueba, y la referente a la investigación de un nuevo delito. Como afirma NADAL GÓMEZ, «aunque son dos cuestiones relacionadas, con un valor eventualmente idéntico y con un régimen

[339] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 195.

[340] Así, por ejemplo, nos encontraríamos ante un supuesto de uso de medio de investigación o prueba a usar en un procedimiento distinto en el caso de que se esté investigando un presunto delito de tráfico de drogas, y se acuerde para su investigación un registro informático, apareciendo durante el mismo unos documentos que acrediten que el investigado sobre el que ya se sigue un proceso iniciado por impago de pensiones tiene unas cuentas bancarias abiertas en un paraíso fiscal que acreditarían su solvencia como uno de los aspectos determinantes de la comisión del delito de impago de pensiones.
Por el contrario, nos encontraríamos ante un descubrimiento casual propiamente dicho, en el caso de que tras un registro informático acordado por un posible delito de estafa informática del art. 248.2.a) se descubran imágenes que revelen la posible comisión de un delito abusos sexuales o contra la intimidad.

parcialmente común, no necesariamente se enmarcan en el mismo escenario, ni dan lugar a las mismas consecuencias»[341]. Realizaremos un análisis de ambos supuestos.

1. Utilización de la información obtenida en una diligencia de investigación como medio de investigación o prueba en proceso distinto

El uso de las informaciones obtenidas en un procedimiento distinto, se regulará con arreglo a lo dispuesto en el art. 579 bis LECrim. Así lo dispone el art. 588 bis i LECrim, que, a fin de evitar innecesarias repeticiones, se remite a lo que, para lo relativo a la información obtenida en procedimientos distintos y hallazgos casuales, viene acordado unos preceptos antes en el capítulo relativo a la «detención y apertura de la correspondencia escrita y telegráfica».

En efecto, el art. 579 bis LECrim, introducido igualmente por la reforma operada por la LO 13/2015, dispone en su apartado 1 que el resultado de la detención y apertura de la correspondencia escrita y telegráfica «podrá ser utilizado como medio de investigación o prueba en otro proceso penal».

Por tanto, de conformidad con los preceptos citados, el resultado de cualquier medida de investigación tecnológica, no solo podrá ser usado como medio de investigación en otro proceso penal, sino también como prueba, pudiendo por tanto cualquier hallazgo casual ser usado como medio de investigación a fin de aportar nuevos hechos a un proceso que se encuentra en fase de instrucción, e igualmente como elemento probatorio que incorporado válidamente al proceso pueda servir para fundar una sentencia condenatoria.

Sin embargo, con anterioridad a la susodicha reforma, no puede afirmarse que esta práctica fuese llevada a cabo pacíficamente, al plantearse ante los tribunales la legitimidad de la medida de investigación en el segundo proceso, donde se pretendía hacer valer el medio de investigación o la prueba, poniéndose en duda tal legitimidad en aquellos casos en los que no existía constancia en el nuevo procedimiento de las actuaciones relativas a la adopción de la medida en el procedimiento penal precedente.

[341] NADAL GÓMEZ, I., «El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal», *Revista General de Derecho Procesal*, n.º 40, 2016, p. 43.

Tal planteamiento no tuvo un tratamiento uniforme por parte de la jurisprudencia hasta el Acuerdo del Pleno no jurisdiccional de la Sala de lo Penal del Tribunal Supremo de 26 de mayo de 2009 al que ahora nos referiremos.

Así, por ejemplo, el TS, en Sentencia de 24 de septiembre de 2001, declaró la nulidad de la intervención, tanto como medio de prueba como de investigación, por la ausencia en los autos de toda la documentación que constaba en el procedimiento donde inicialmente se acordó la intervención, acreditativa de la solicitud policial de intervención y de la propia autorización judicial, estimando asimismo que la denuncia por parte de la defensa de tal irregularidad podría ser efectuada en cualquier fase del procedimiento[342]. De un modo similar, se pronunció el TS en la Sentencia de 24 de abril de 2003, en la que se justificó la nulidad de la medida de investigación en el hecho de que las razones, datos o indicios que tuviera inicialmente la policía para solicitar la intervención inicial no obraban en las actuaciones[343].

Sin embargo, el TS fue modulando su criterio, y así, en STS 187/2009, de 3 de marzo, FJ 1.º, declaró que «…no es procedente presumir que las actuaciones judiciales y policiales son ilegítimas e irregulares y por ende vulneradoras de derechos

[342] STS 1673/2001, de 24 de septiembre, FJ 1.º, que declaró: «La ausencia en los autos de toda la documentación acreditativa de la solicitud policial de intervención y de la propia autorización judicial convierte en insubsanablemente nula la propia intervención policial por falta del presupuesto habilitante de la autorización judicial que exige de forma inexcusable el art. 18-3º de la Constitución. No se trata de una irregularidad procesal sino de la falta de la autorización y control judicial, indispensable para el sacrificio de un derecho fundamental […]. Esta ausencia puede ser denunciada en cualquier momento del proceso, e incluso apreciada de oficio por esta Sala casacional como manifestación del control de legalidad que le corresponde, por lo que no se puede estimar desleal que la defensa lo manifieste en un momento procesal —en el informe oral—- en el que ya es imposible su subsanación, pues tal estrategia —sin duda hábil—, no puede ocultar que, en definitiva lo que se está denunciando es una inactividad probatoria, que por su naturaleza de cargo, le corresponde inequívocamente a la acusación, y aquella denuncia no le convierte en obligado a subsanar la falta de actividad de la parte contraria, ni menos, puede darse "por supuesta" la existencia de la autorización judicial a la vista de la remisión por la policía de las transcripciones de las intervenciones efectuadas obrante a los folios 338 a 655, porque sobre ser presupuesto para la validez tal autorización, su ausencia, impide además en esta sede casacional toda verificación de los requisitos de legalidad constitucional determinantes de la validez, a saber, la judicialidad de la medida, con las consecuencias que de ello se derivan, su excepcionalidad y su proporcionalidad…».

[343] STS 498/2003, de 24 de abril, FJ 2.º que declaró que «ausente en las actuaciones de estos datos iniciales así como la correspondiente autorización judicial que fuera dada, no existe medio de verificar el cumplimiento de los requisitos de legalidad constitucional indispensables para contrastar la legitimidad de la intervención, lo que difunde hacia el resto de investigaciones derivadas de la primera una radical imposibilidad de tener en cuenta los hallazgos efectuados ni como fuente de prueba, ni tampoco como prueba en sí misma».

fundamentales, mientras no conste lo contrario»[344]. Esta sentencia, citó la STS 503/2008, de 17 de julio, declarando que, conforme a la misma, se refrenda la doctrina citada, la cual «no permite premiar la mala fe procesal o, cuando menos, no impone preceptivamente la obligación de acreditar la regularidad de una injerencia en la intimidad más allá de las comprobaciones obrantes en la causa, si son suficientes para adoptar otras intervenciones diferentes con las que pueda existir una relación de precedente»[345].

Además, la STS 187/2009 justificó la validez de las diligencias de investigación en la circunstancia de que el recurrente guardó silencio esperando hasta el momento del informe final para efectuar su alegación relativa a la falta de motivación de las intervenciones, en un momento en el que ya no era posible incorporar los correspondientes testimonios a la causa, y así tener los datos necesarios para juzgar su legitimidad constitucional[346].

---

[344] La STS 187/2009 añadió que «…debe partirse de que salvo prueba en contrario hay que suponer que los jueces, policías, autoridades y en general funcionarios públicos han adecuado su actuación a lo dispuesto en las leyes y en la Constitución. Sería absurdo presumir que como no constan las actuaciones iniciales obrantes en una causa distinta hay que entender que no hubo autorización judicial de la intervención o la misma fue inmotivada o injustificada. Como bien apunta el Fiscal ni el derecho a la presunción de inocencia ni el principio procesal "in dubio pro reo" llega hasta el punto de tener que presumir por mandato constitucional que, salvo que se acredite lo contrario, las actuaciones de las autoridades son ilegítimas e ilícitas».

[345] La STS 503/2008, de 17 de julio, la cual resolvió el recurso de casación interpuesto en relación con el lamentablemente conocido caso de los atentados terroristas del 11 de marzo de 2004, declaró que «…aunque no existan razones para una sospecha sistemática contra la acción de la autoridad, más allá de las que justifican el control sobre el ejercicio del poder, en el examen de estas cuestiones debe partirse de la integridad e indemnidad de los derechos fundamentales, de forma que la constitucionalidad de su restricción debe quedar acreditada. Dicho de otra forma, el principio general en un sistema democrático es la vigencia de los derechos fundamentales y la excepción, que debe estar justificada, su restricción por parte de los poderes públicos».

[346] Señaló finalmente a este respecto la STS 187/2009, de 3 de marzo, que respecto a la autorización judicial inicial «…no consta se haya pronunciado resolución alguna que la invalide o la declare inconstitucional o de otro modo irregular. Junto a ello no puede pasar desapercibido que el recurrente pudo cómodamente pedir testimonios de aquella causa para que en la presente se pudieran tomar en consideración, concretamente, los autos allí dictados con sus correspondientes oficios policiales que sirvieran de referencia, y es lo cierto que ni siquiera ha intentado este medio probatorio. En consecuencia, el tribunal de instancia ha dispuesto de unos referentes policiales contundentes e inequívocamente incriminatorios, que justificaban la restricción del derecho a la intimidad […]. A falta de otros datos, que indujeran a dudar de las actuaciones […], no es posible declarar inconstitucional o de otro modo irregular el auto o autos habilitantes emitidos en aquel proceso».

Por su parte, la STS 326/2009, de 24 de marzo, señaló que: «la nueva causa penal no puede constituir un cauce procesal idóneo para que el Juzgador examine, en todo caso, y con carácter previo, la regularidad constitucional de las restricciones de los derechos fundamentales ordenadas en otro proceso, y se pronuncie sobre su validez y eficacia jurídicas, con lo que, además, se daría ocasión a posibles resoluciones jurisdiccionales contradictorias sobre el particular. Ello no puede ser obstáculo, sin embargo, para que cualquiera de las partes que pudiera tener una duda o una razón fundada sobre la posible irregularidad o ilegalidad de las intervenciones telefónicas previas pueda instar en la segunda causa, para superar la duda o esclarecer la cuestión de legalidad de la injerencia, con las obligadas consecuencias que de ello pudieran derivarse, en su caso, para el segundo proceso, las diligencias que considere pertinentes al efecto (como sería el testimonio de particulares del otro proceso), sin olvidar, por lo demás, las exigencias inherentes al principio de buena fe y lealtad procesal en la defensa de sus legítimos intereses con la que siempre deben actuar las partes en el proceso».

Después de estas sentencias discrepantes, a fin de unificar criterios, el Pleno de Sala Segunda del TS dictó el Acuerdo de 26 de mayo de 2009[347], seguido en las resoluciones posteriores.

La primera sentencia dictada por el TS tras el referido acuerdo realizó una exégesis del mismo concluyendo lo siguiente: «a) que no existen nulidades presuntas; b) que la prueba de la legitimidad de los medios de prueba con los que pretenda avalarse la pretensión de condena, incumbe a la parte acusadora; c) pese a ello, la ley no ampara el silencio estratégico de la parte imputada, de suerte que si en la instancia no se promueve

[347] En el Acuerdo del Pleno de la Sala Segunda del TS, se acordó lo siguiente:
«En los procesos incoados a raíz de la deducción de testimonios de una causa principal, la simple alegación de que el acto jurisdiccional limitativo del derecho al secreto de las comunicaciones es nulo, porque no hay constancia legítima de las resoluciones antecedentes, no debe implicar sin más la nulidad.
En tales casos, cuando la validez de un medio probatorio dependa de la legitimidad de la obtención de fuentes de prueba en otro procedimiento, si el interesado impugna en la instancia la legitimidad, de aquel medio de prueba, la parte que lo propuso deberá justificar de forma contradictoria la legitimidad cuestionada.
Pero, si, conocido el origen de un medio de prueba propuesto en un procedimiento, no se promueve dicho debate, no podrá suscitarse en ulteriores instancias la cuestión de la falta de constancia en ese procedimiento de las circunstancias concurrentes en otro relativas al modo de obtención de las fuentes de aquella prueba».

el debate sobre la legalidad de una determinada prueba, esa impugnación no podrá hacerse valer en ulteriores instancias»[348].

El legislador, con la reforma operada por la LO 13/2015, ha seguido lo dispuesto en mencionado Acuerdo del Pleno no jurisdiccional de la Sala de lo Penal del Tribunal Supremo y, en definitiva, ha establecido que para que el resultado de una medida de investigación pueda ser usado como otra medida o como prueba en otro procedimiento, deberá seguirse el procedimiento establecido en el apartado 2 del mencionado art. 579 bis, conforme al cual «se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia» y se incluirán entre los antecedentes indispensables, en todo caso, «la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen».

En palabras de NADAL GÓMEZ, esta norma establece que se cumpla «con una serie de requisitos que confluyen fundamentalmente en exigir la legitimidad de la injerencia que dio origen a descubrimiento y de las actuaciones posteriores que deben llevarse a cabo una vez identificado éste»[349].

En definitiva, el precepto consagra la necesidad de constatar la legalidad precedente y subsecuente en la obtención del hallazgo casual, como requisito ineludible para otorgarle cualquier valor en el mismo o en otro proceso, pudiendo afirmar igualmente, como así lo hace la Instrucción 2/2017 de la FGE, que la incorporación de los testimonios tras la entrada en vigor de la LO 13/2015 es preceptiva siempre, y

[348] Vid. STS 777/2009, de 24 de junio, FJ 1.º Previamente la sentencia declaró que «…es evidente que la ausencia de determinados documentos y la imposibilidad de acreditar su verdadera existencia, pueden desplegar un efecto invalidante respecto de la legitimidad de la medida de intervención telefónica (art. 11 LOPJ). Sin embargo, la legitimidad del sacrificio del derecho previsto en el art. 18.3 de la CE no puede ponerse en entredicho por la circunstancia de que falten algunos de los antecedentes de los que pudiera traer causa el acto limitativo cuestionado. La afirmación de que como no puede presumirse que las intervenciones anteriores fueran legítimas, las posteriores son nulas, sin que puedan tenerse en cuenta el resto de los medios de prueba, admite otro enfoque. La nulidad de los actos procesales sólo puede basarse en algunas de las causas estrictamente reguladas en el art. 238 de la LOPJ, con la consecuencia de la pérdida de efectos que impone el art. 11 de la misma ley. Sin embargo, declarar la nulidad de unas escuchas porque no consta la legitimidad de todas aquellas actuaciones procesales, practicadas en otros procedimientos y a las que se atribuye —sin explicar el por qué— la condición de antecedentes, supone desenfocar el contenido material del derecho que se dice vulnerado. Estaríamos alentando la creación de la nulidad presunta, categoría carente de cobertura en nuestro sistema procesal».

[349] NADAL GÓMEZ, I., «El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal», cit., pp. 3-4.

especialmente cuando la diligencia de investigación hubiera sido impugnada por la defensa[350].

No obstante lo anterior, se ha planteado la cuestión relativa al momento procesal en el que se han de incorporar los testimonios a las actuaciones. De conformidad con el Acuerdo del Pleno de la Sala II del TS de 26 de mayo de 2009 y la STS 777/2009, de 24 de junio, anteriormente mencionados, quedó sentado que el «el silencio estratégico» de la parte imputada impedirá que pueda ser tenida en cuenta la impugnación de la validez de una prueba obtenida en una diligencia de investigación en instancias ulteriores, si tal impugnación no se promovió en la instancia.

Sin embargo, no se encuentra debidamente resuelto el problema relativo a si la impugnación debe plantearse durante la fase de instrucción, al momento de incorporarse el medio de investigación o prueba al proceso, o como máximo hasta la fase de calificación del delito, o podría hacerse valer en cualquier fase del procedimiento incluida su posible formulación en la fase de cuestiones previas en el procedimiento abreviado o incluso en general en las conclusiones definitivas o en el informe oral.

A este respecto, cabe señalar que en la STS 469/2016, de 31 de mayo, se dictaron dos votos particulares en cada uno de los sentidos indicados. Concretamente, en uno de ellos se declaró que la impugnación en la fase de cuestiones previas no resulta procesalmente operativa sin quebranto del principio de contradicción y defensa de la contraparte, mientras que en sentido contrario se declaró que las partes acusadoras deberían haber previsto la eventual impugnación así como que no es posible exigir a la defensa que exponga sus cartas a fin de que la acusación pueda prevenirse del uso de las mismas[351].

---

[350] FISCALÍA GENERAL DEL ESTADO, *Instrucción 2/2017, sobre procesos incoados a raíz de la deducción de testimonios de una causa principal*, 2017, pp. 6-7, Consultado en https://www.fiscal.es/documents/20142/e823a65b-d869-3c12-4fdc-3329dbfcbd88, el 10 de junio de 2020.

[351] En la referida STS 469/2016, los dos votos particulares fueron formulados por los magistrados, Sres. Llarena Conde y Andrés Ibáñez. El magistrado Sr. Llarena Conde, en su voto particular, estimó que la impugnación sobre la validez de la intervención en la fase de cuestiones previas una vez iniciado el juicio oral, se hacía de manera tardía y de un modo que hace inviable atender su análisis, lo cual justificó declarando que: «La denuncia en la fase de cuestiones previas del supuesto vicio de nulidad que ahora analizamos, aun cuando es una posibilidad aparentemente contemplada en el artículo 786.2 de la LECRIM por venir referida a una vulneración de derecho fundamental, no resulta procesalmente operativa sin quebranto del principio de contradicción y defensa de la contraparte, considerando: 1. Que en esa fase de cuestiones previas sólo puede proponerse la prueba que pueda practicarse en el acto (art. 786.2 LECRIM), previsión que descansa en que las partes conozcan con antelación los extremos que son objeto de debate,

Para resolver esta cuestión, consideramos en primer lugar, que si bien es cierto que no se puede exigir a la defensa que muestre sus cartas, no se debe identificar la estrategia de cada una de las partes con los trámites de proposición de prueba y su impugnación, los cuales deben estar sujetos a un trámite que respete los principios de contradicción e igualdad de partes, que (con las salvedades previstas en cuanto a la posibilidad de acordar en el juicio oral pruebas de oficio o a propuesta de las partes, cuando se consideren pertinentes, o en el trámite de cuestiones previas en el procedimiento abreviado, en cuyo caso podrían ser impugnadas en el momento de su proposición o admisión formulando en su caso la oportuna protesta) solo se verían respetados con la impugnación como máximo en los escritos de calificación en el procedimiento ordinario (art. 656 LECrim) o de defensa (art. 784.1 LECrim).

En este sentido no se ajustaría a las reglas de la buena fe, exigida por el art. 11 de la LOPJ en su primer inciso, que se pretenda impugnar la validez de una diligencia de investigación o medio de prueba —cuya incorporación al proceso se efectuó en fase de instrucción o en el escrito de calificación o acusación con conocimiento de la defensa—, una vez iniciado el juicio oral cuando ya ha transcurrido un lapso de tiempo considerable, teniendo en cuenta, además, que las causas de suspensión se encuentran tasadas por los arts. 745 y 746 LECrim, sin que pueda acomodarse el caso que nos

---

para poder pertrecharse de las pruebas que resulten oportunas para ello, 2. Que la alegación por la defensa del posible quebranto del derecho constitucional, necesariamente se produce cuando la acusación ha desplegado ya sus opciones procesales de proposición de nueva prueba y 3. Que cualquier posibilidad de suspensión del juicio oral —por la afectación que supone para las partes, para los colaboradores de la justicia y para el propio funcionamiento de los Juzgados y Tribunales— queda restringida a los supuestos contemplados en los artículos 744, 745 y 746 LECRIM. Cuando no se haya hecho ya en la fase de Diligencias Previas, el acuerdo de Sala antes referido obliga a que la denuncia de la supuesta ilegitimidad de la prueba, se haga en cuanto se tenga conocimiento de que ha sido propuesta como medio de prueba, lo que entiendo no puede ser en otro momento que en el escrito de calificación provisional de la defensa…». Por su parte, el magistrado Sr. Andrés Ibáñez, consideraba que la impugnación debía entenderse realizada tempestivamente en el trámite de cuestiones previas y por tanto debió atenderse la misma, argumentando que «…en un caso como el de esta causa, el fiscal debería haber previsto la eventualidad (por lo demás nada extraordinaria) de una impugnación como la que en efecto se produjo. Del mismo modo que el acusador interesado en hacer valer en una causa las interceptaciones telefónicas practicadas en otra, tendrá buenas razones para esperar algo tan previsible como el cuestionamiento basado en la ausencia de alguna documentación relativa a las mismas o en un déficit de motivación de las decisiones correspondientes…», añadiendo que «…exigir a una defensa que exponga sus cartas a tiempo de que la acusación pueda prevenirse frente al uso posible de ellas, no es una cuestión de lealtad, sino que equivale a imponerle una actitud procesalmente suicida. Un —dialéctica y procesalmente aberrante— deber de colaboración con aquella en propio perjuicio».

ocupa en ninguna de ellas[352], así como que, con carácter general, las irregularidades procesales deben ser alegadas tan pronto como sean conocidas.

Ahora bien, lo anterior no impide que la diligencia de investigación aportada tras el hallazgo casual como medio de investigación o prueba con el que se trate de desvirtuar la presunción de inocencia, deba estar rodeada de todas las garantías que impidan concluir que se ha producido la lesión de algún derecho fundamental, y muy especialmente que se han cumplido las exigencias de especialidad, idoneidad, necesidad, excepcionalidad y proporcionalidad. De no ser así, nos encontraríamos ante una prueba ilícita (art. 11.1 segundo inciso LOPJ) y por tanto debería quedar excluida de la valoración probatoria por exigirlo así el derecho a un proceso con todas las garantías proclamado por el art. 24.2 de la CE.

De todo lo anterior se deduce que recaerá sobre la parte acusadora la carga de procurar la aportación al nuevo proceso de testimonio de los antecedentes indispensables, y en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen, tal y como exige el referido art. 579 bis.2 LECrim.

Por lo que respecta a la impugnación, siguiendo a CASTILLEJO MANZANARES «no es suficiente con la simple alegación de la existencia de alguna infracción referida a la medida limitativa realizada en un proceso penal precedente, sino que resulta necesario que el encausado formule una impugnación a este respecto con expresión de las razones de la misma»[353].

---

[352] Mantiene la misma opinión CASTILLEJO MANZANARES, aunque con la salvedad, que no compartimos por las razones expuestas, relativa a la posibilidad de realizar la impugnación en la fase de cuestiones previas en el procedimiento abreviado. Señala esta autora que: «No cabe la impugnación de la legitimidad de la fuente de prueba *per saltum* en la alzada cuando no se solicitó en la instancia. Tampoco cabe su formulación en las conclusiones definitivas o en el informe oral. Lo procedente será manifestarlo en la instrucción, en el escrito de calificación provisional o en el trámite de cuestiones previas. Nótese que no cabe solicitar la práctica de diligencias de al inicio del juicio oral puesto que concluida la instrucción y consentido el auto de conclusión sin haber solicitado su revocación, no cabe la retroacción del procedimiento resucitando una competencia para la investigación del delito que ya no tiene el juez de instrucción y que nunca podrá tener la Audiencia Provincial». Vid. CASTILLEJO MANZANARES, R., «Hallazgos casuales y medidas tecnológicas de investigación», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 1, 2018, p. 32, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[353] Cita la autora la STS 428/2014, de 28 de mayo, la cual declaró que: «…no basta una impugnación genérica como la que se realizó aquí en los escritos de conclusiones de dos defensas. No se ajusta a las exigencias de la buena fe procesal ese cuestionamiento puramente estratégico y no concretado. De la

2. Los descubrimientos casuales

Todo lo expuesto en el apartado anterior relativo a la utilización en otro procedimiento de la información obtenida en una diligencia de investigación como medio de investigación o prueba en otro procedimiento distinto, es aplicable igualmente en aquellos casos en los que en el transcurso de la investigación sea descubierto un nuevo delito.

Es decir, tanto lo manifestado en el Acuerdo del Pleno no jurisdiccional de la Sala de lo Penal del TS de 26 de mayo de 2009 y su desarrollo jurisprudencial en el sentido de otorgar valor a unas actuaciones judiciales y policiales que en principio deben considerarse ajustadas a derecho mientras no se pruebe lo contrario, como las anteriores consideraciones acerca de la impugnación en su caso de la validez de la diligencia en la instancia y el momento procesal oportuno para hacerlo, como la necesidad de aportar los testimonios previstos en el art. 579 bis.2 LECrim, hemos de entenderlas totalmente aplicables en el caso de que el hallazgo casual determine la existencia de un nuevo delito.

Pero lo que ahora pretendemos en este nuevo apartado es el estudio de la problemática que supone la investigación de la nueva infracción penal en relación con la que ya se estaba investigando, la cual ha tenido una evolución jurisprudencial, fundamentalmente con base a tres criterios principales, como son: el principio de especialidad y prohibición de la novación del tipo delictivo, el criterio de la flagrancia y el criterio de la conexidad.

2.1. El principio de especialidad y prohibición de la novación del tipo delictivo

Como señala ARMENTA DEU, a partir del ATS de 18 de junio de 1992 se sentó una doctrina conforme a la cual si no se interrumpía la medida y se ampliaba el auto o se dictaba otro específico al efecto, la vulneración del derecho fundamental derivaba en la

---

lectura del párrafo antes transcrito, no cabía inferir una queja por la no incorporación de los antecedentes de las escuchas. No se aducía y ni siquiera se insinuaba la posibilidad de que las conversaciones que fundaron las intervenciones no contasen con respaldo judicial y legal suficiente. Desarrollar y detallar luego esa queja al inicio del juicio oral en esos términos anulaba toda capacidad de reacción y atentaba a la lealtad procesal». Vid. CASTILLEJO MANZANARES, R., «Hallazgos casuales y medidas tecnológicas de investigación», cit., p. 32.

nulidad, no sólo de lo actuado, sino de todo aquello con lo que guardara relación de causalidad[354].

Por tanto, el primer criterio que el TS tuvo en cuenta para dar validez al hallazgo casual se ciñó al respeto del principio de especialidad, prohibiendo una novación del tipo penal investigado, es decir, el descubrimiento tendría validez, siempre y cuando la intervención inicial no se hubiese realizado de forma prospectiva, con la ilegítima finalidad de propiciar el descubrimiento de cualquier infracción penal usando la doctrina del hallazgo casual, y por tanto se hacía necesaria la interrupción de la medida y la ampliación del auto inicial o el dictado de un nuevo auto que, respetando las exigencias del principio de proporcionalidad, autorizase la continuación de la medida de investigación en relación con el hallazgo casual.

No obstante, el TS declaró igualmente que, aunque lo procedente tras el descubrimiento casual fuese una ampliación de la intervención, ello no impedía que el descubrimiento pudiese servir lícitamente como *notitia criminis*, determinando las actuaciones procedentes en orden a la evitación o investigación del nuevo delito[355].

Sin embargo, la jurisprudencia no ha mantenido un criterio uniforme y fue modulando las exigencias del principio de especialidad. En este sentido señala LÓPEZ BARJA DE QUIROGA que, para la validez del hallazgo casual, «puede decirse que básicamente, junto con algún otro criterio —en ocasiones no específicamente expresado—, la jurisprudencia ha utilizado dos criterios: el del delito flagrante y el de la regla de la conexidad»[356].

2.2. El criterio de la flagrancia

En cuanto al criterio de la flagrancia[357], como uno de sus primeros exponentes, podemos citar la STS 462/1999, de 22 de marzo, FJ único, que, estimando el motivo de

[354] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 195.

[355] Vid. STS 835/1996, de 31 de octubre, FJ 2.º Más recientemente la STS 279/2014, de 20 de febrero, FJ 1.º declaró con mención a otras sentencias anteriores que «…en los supuestos en que se investiga un delito concreto y se descubre otro distinto, no puede renunciarse a investigar la *notitia criminis* incidentalmente descubierta en una intervención dirigida a otro fin, aunque ello pueda hacer precisa una nueva o específica autorización judicial o una investigación diferente de la del punto de arranque».

[356] LÓPEZ BARJA DE QUIROGA, J., *Tratado de Derecho Procesal Penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2010, p. 1247.

[357] Dispone el art. 795.1.1.ª de la LECrim que «…se considerará delito flagrante el que se estuviese cometiendo o se acabare de cometer cuando el delincuente sea sorprendido en el acto. Se entenderá

impugnación en virtud del cual se instaba el abandono de la aplicación estricta del criterio de la especialidad en los casos en los que la aparición de un posible delito distinto del investigado constituyese una situación de flagrancia que exija inmediata intervención[358], declaró que, en estos casos, «el hallazgo casual de efectos que pudieran ser constitutivos de un objeto delictivo obliga a los funcionarios de la policía judicial que realizan la investigación y, en su caso, a los funcionarios de la administración de justicia, a su intervención y a la realización de aquellas diligencias necesarias para la investigación del delito para su persecución»[359]. Por su parte, la STS 981/2003, de 3 de julio, FJ 2.º, declaró que la recogida de un hallazgo casual, cuando el descubrimiento se instala en la nota de flagrancia, «no es sino consecuencia de la norma general contenida en el art. 286 de la Ley Procesal»[360].

2.3. El criterio de la conexidad

En relación con el criterio de la conexidad, cabe señalar que el mismo sirvió igualmente para suavizar las exigencias del principio de especialidad o prohibición de la novación del tipo penal.

---

sorprendido en el acto no sólo al delincuente que fuere detenido en el momento de estar cometiendo el delito, sino también al detenido o perseguido inmediatamente después de cometerlo, si la persecución durare o no se suspendiere mientras el delincuente no se ponga fuera del inmediato alcance de los que le persiguen. También se considerará delincuente in fraganti aquel a quien se sorprendiere inmediatamente después de cometido un delito con efectos, instrumentos o vestigios que permitan presumir su participación en él».

[358] La referida STS 462/1999 declaró asimismo que, si para el caso de que el hallazgo casual participase de la naturaleza de la flagrancia, «…el Juzgado de instrucción proporcionó en la investigación un mandamiento de entrada y registro para la intervención de objetos de procedencia ilícita y se obtuvieron efectos que podían constituir el objeto de un delito contra la salud pública, la intervención de los mismos se enmarca en una correcta actuación por parte de los funcionarios de policía judicial toda vez que el registro se practicó con observancia de la legalidad, constitucional y procesal, existió la debida proporcionalidad y los efectos intervenidos lo fueron casualmente, lo que se corrobora por la suspensión del registro para que en la diligencia intervinieran perros para ayudar a la intervención de sustancias tóxicas».

[359] Cabe señalar que la STC 41/1998, de 24 de febrero, FJ 22.º, había declarado 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».

[360] Establece el art. 286 de la LECrim que: «Cuando el juez de instrucción o el municipal se presentaren a formar el sumario, cesarán las diligencias de prevención que estuviere practicando cualquier Autoridad o agente de policía; debiendo éstos entregarlas en el acto a dicho juez, así como los efectos relativos al delito que se hubiesen recogido, y poniendo a su disposición a los detenidos, si los hubiese».

De este modo, en el caso de que por el juez ordenante de la medida inicial se considere que el nuevo delito descubierto con el hallazgo casual tiene conexidad[361] con el inicialmente investigado, estaría legitimado para dictar una nueva resolución autorizando la medida para la investigación del nuevo delito conexo, sin que por ello resultase vulnerado el principio de especialidad.

En este sentido, el TS ha declarado que solo se vulnera el principio de especialidad cuando se produce una novación del tipo penal investigado, pero no cuando existe una adición o suma[362]. Con esta expresión relativa a la «adición o suma», aclara NADAL GÓMEZ, la jurisprudencia viene a decir que «la aparición de hechos nuevos que puedan suponer la comisión de delitos diferentes de los investigados pero conexos con éstos, no impide que pueda continuarse con su investigación en el mismo proceso»[363].

Ahora bien, tal y como puso de manifiesto la Circular 1/1999 de la FGE, cuando exista conexidad entre el delito descubierto y el inicialmente investigado «deberá darse una orden judicial ampliatoria del ámbito de la escucha telefónica y proseguir la investigación en la misma causa»[364]. Es decir, con independencia de que exista o no conexidad, lo que finalmente resulta necesario tal y como también ha declarado el TS, es que la continuidad en la investigación de un hecho delictivo nuevo, casualmente detectado, sea objeto de una renovada autorización judicial[365].

---

[361] Ha de tenerse en cuenta que tras la reforma operada por la Ley 41/2015, de 5 de octubre, de modificación de la LECrim para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, se ha modificado el régimen de la competencia por conexidad, quedando suprimida la aplicación automática de la conexidad cuando se diese alguno de los supuestos objetivos que se establecían en el art. 17 de la LECrim, en virtud de los cuales se entendían conexos *ex lege* dos o más delitos y por imperativo legal debían enjuiciarse en un solo proceso. Ahora se añade un elemento de tipo subjetivo, en virtud del cual, una vez que concurra alguno de los supuestos objetivos de conexidad, el juez deberá valorar si como dice el actual art. 17.1 de la LECrim, la investigación y la prueba en conjunto de los hechos resultase conveniente para el esclarecimiento de los hechos y la determinación de las responsabilidades procedentes, y ello siempre y cuando no suponga excesiva complejidad o dilación para el proceso.

[362] Vid. SSTS 545/1998, de 13 de enero de 1999, FJ 2.º y 393/2012, de 29 de mayo FJ 2.º

[363] NADAL GÓMEZ, I., «El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal», cit., p. 38.

[364] FISCALÍA GENERAL DEL ESTADO, *Circular 1/1999, de 29 de diciembre, sobre la intervención de las comunicaciones telefónicas en el seno de los procedimientos penales*, 1999, p. 15. Consultada en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/cir01-1999.pdf?idFile=27c35845-e6ba-4472-b36d-98908744e752, el 11 de julio de 2018.

[365] Vid. STS 1313/2009, de 16 de diciembre, FJ 1.º

Así lo declaró igualmente la STC 49/1996, de 26 de marzo, FJ 4.º, que, resolviendo un recurso de amparo en relación con un procedimiento en el que se acordó la medida de investigación para el esclarecimiento de un presunto delito de tráfico de drogas, descubriéndose durante la misma un posible delito de cohecho, declaró que «…debió ponerse de manifiesto al juez este inesperado dato»[366].

2.4. Situación actual

Con los anteriores criterios principales relativos al principio de especialidad, la flagrancia y la conexidad delictiva, se fue conformando la doctrina sobre el hallazgo casual, pudiendo afirmar que la jurisprudencia avanzó en orden a conceder validez a los hallazgos casuales, si bien, como señalaba ÁLVAREZ DE NEYRA KAPPLER, aunque se daban pasos cada vez más decididos a admitir los resultados de los descubrimientos casuales, los argumentos formulados para ello no llegaban a ofrecer una solución integral, sino que se trataba más bien de soluciones fragmentarias y casuísticas[367]. En cualquier caso, también es cierto que la situación, tras la consolidación jurisprudencial de los referidos criterios, quedó más clarificada.

Ya en época más reciente, podemos encontrar que el TS resume en una de sus sentencias dicha doctrina, razonando que «el hallazgo casual, es decir, el elemento probatorio novedoso que no está inicialmente abarcado por el principio de especialidad, puede ser utilizado en el propio o distinto procedimiento, bien por tratarse de un de un delito flagrante o bien por razones de conexidad procesal, siempre que, advertido el hallazgo, el juez resuelva expresamente continuar con la investigación para el esclarecimiento de ese nuevo delito, ante la existencia de razones basadas en los principios de proporcionalidad e idoneidad»[368].

En cualquier caso, con la reforma operada por la LO 13/2015 consideramos que queda superada tal fragmentación, dado que, en la nueva regulación se introducen

---

[366] La STC 49/1996 estimó el recurso de amparo, declarando en el 7.º y último FJ que: «En consecuencia, ha de concluirse que no ha habido actividad probatoria que puede considerarse suficiente a los efectos de desvirtuar el derecho a la presunción de inocencia del que inicialmente gozaba el recurrente. Las Sentencias de la Audiencia Provincial de Barcelona y de la Sala Segunda del Tribunal Supremo, dictadas con carencia de pruebas constitucionalmente válidas, deben ser anuladas».

[367] ÁLVAREZ DE NEYRA KAPPLER, S., «Los descubrimientos casuales en el marco de una investigación penal (Con especial referencia a las diligencias de entrada y registro en domicilio)», *Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, n.º 2, 2011, p. 25, nota al pie 54.

[368] Vid. STS 777/2012, 17 de octubre, FJ 2.º

diversas cautelas, principalmente la exigencia de que, para la continuación de la medida, se dicte una nueva autorización del juez que resulte competente para la investigación del nuevo delito descubierto.

En efecto, el n.º 3 del art. 579 bis LECrim dispone que «la continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente…». En caso de ser juez competente otro distinto al que investiga el delito inicial, se deberá deducir testimonio para su remisión al mismo, en los términos previstos en el apartado 2.º del art. 579 bis LECrim. Por otra parte, el juez competente, continúa disponiendo el n.º 3 del art. 579 bis LECrim, «…comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento».

Con este contenido, la ley exige que el juez competente verifique la legalidad de la actuación previa. Como afirma RICHARD GONZÁLEZ, con esta norma «…se pretenden evitar peticiones de medidas de intervención que persiguen una indagación general en la intimidad de una persona con base en un pretexto dirigido a obtener una orden judicial»[369].

De esta forma, con la regulación actual, al exigirse en todo caso una nueva resolución judicial que examine la imposibilidad de que el posible hallazgo casual se hubiera previsto con la medida inicial, se respeta el principio de especialidad, si bien partiendo de una presunción de validez de la diligencia acordada inicialmente y consecuentemente del hallazgo casual. Como dice SÁNCHEZ YLLERA, «solo cuando la actuación policial trata de eludir el control judicial y la posible evaluación de la adecuación de la injerencia podrá entenderse que la misma, en lo que afecta al hallazgo casual, es ilegítima»[370].

---

[369] Añade este autor, refiriéndose a las prohibidas investigaciones prospectivas, que «naturalmente que esta posibilidad debe quedar cercenada mediante el riguroso examen de la petición inicial. Ahora bien, ante la aparición de indicios de la comisión de delitos absolutamente distintos de los investigados hará bien el juez de instrucción en analizar si la autorización inicial estaba debidamente fundamentada o bien encubría una investigación o causa general que está proscrita en nuestro ordenamiento jurídico». Vid. RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», cit., p. 17.

[370] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art . 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 22.

Por ello, con la finalidad de que no se altere la situación del procedimiento inicial y sean respetados los intereses y derechos de todas las partes, el último inciso del n.º 3 del art. 579 bis, ha incluido para los supuestos en los que deban incoarse nuevas diligencias en las que resulte competente otro juez, la razonable previsión de que la declaración del secreto sumarial sea respetada en el nuevo proceso, disponiendo a tal efecto que, asimismo, «se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce».

Por último, consideramos que, sin perjuicio de que puedan darse otros problemas en la práctica, con el nuevo art. 579 bis LECrim, aplicable a todos los supuestos de diligencias de investigación tecnológica, unido a la amplia doctrina jurisprudencial elaborada con anterioridad, quedan resueltas las principales cuestiones que se planteaban acerca de los hallazgos casuales y su utilización en otro procedimiento distinto. Como señala MARCHENA GÓMEZ, «lo decisivo, al fin y al cabo, es que no quede duda alguna de la validez de la prueba cuya funcionalidad pretende proyectarse a un segundo proceso»[371].

[371] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 281.

CAPÍTULO IV. DISPOSICIONES COMUNES A LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA EN LA LECRIM (II): ASPECTOS PROCESALES

I. Autorización judicial

En relación con la autorización judicial, deben ser examinados dos apartados principales como son: la solicitud de dicha autorización y la resolución del tribunal.

1. Solicitud de autorización

La solicitud que se efectúe por el Ministerio Fiscal o la Policía Judicial para la práctica de una medida de investigación tecnológica deberá sujetarse a una serie de requisitos que, sin embargo, han de considerarse como los estrictamente necesarios para poder iniciar las diligencias indagatorias.

En efecto, conforme ha recordado la jurisprudencia del TS, en el momento inicial del procedimiento, en el que ordinariamente se acuerda la intervención, «no resulta exigible una justificación fáctica exhaustiva, pues se trata de una medida adoptada, precisamente, para profundizar en una investigación no acabada, por lo que únicamente pueden conocerse unos iniciales elementos indiciarios»[372].

Por otra parte, de acuerdo con lo indicado por VELASCO NÚÑEZ, la omisión en la solicitud de algún dato que no resulte imprescindible para que el tribunal pueda realizar su juicio ponderativo, no supone ningún impedimento para la legalidad de la adopción de la medida, sin perjuicio de que por el juez pueda recabar la información complementaria que considere oportuna[373].

Estudiaremos dichos requisitos, establecidos en el art. 588 bis b.2 LECrim, clasificándolos en objetivos y subjetivos.

---

[372] Vid. STS 714/2018, de 16 de enero de 2019, FJ 1.º, en la que se citan las SSTS 1240/1998, de 27 de noviembre, 1018/1999, de 30 de septiembre, 1060/2003, de 21 de julio, 248/2012, de 12 de abril y 492/2012, de 14 de junio.

[373] VELASCO NÚÑEZ, E., «Investigación Tecnológica de Delitos: Disposiciones Comunes e Interceptaciones Telefónicas y Telemáticas», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 6, Consultado en https://www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada, el 7 de marzo de 2018.

1.1. Requisitos subjetivos

Se concretan en la necesidad de consignar en la solicitud de autorización judicial, la identidad del investigado o de cualquier otro afectado por la medida —si tales datos fuesen conocidos—, los datos del identificación del investigado, la unidad investigadora de la Policía Judicial que se hará cargo de la intervención y el sujeto obligado que llevará a cabo la medida —en caso de conocerse—. Realizaremos un breve análisis de cada uno de ellos.

1.1.1. Identidad del investigado o de cualquier otro afectado por la medida

El apartado 1.º del art. 588 bis b.2 LECrim, establece la obligación de reflejar la identidad del investigado, siempre que sus datos resulten conocidos. Por tanto, el precepto deja abierta la posibilidad de que tanto la concreta identidad del investigado o de cualquier otro afectado por la medida no se consigne en la solicitud.

De este modo, se ha recogido la doctrina jurisprudencial que se estableció desde la STC 150/2006, de 22 de mayo, conforme a la que, para la legitimidad de la intervención, no es necesaria una delimitación subjetiva con la identificación del investigado. Esta resolución, declara en su FJ 3.º que, «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»[374]. De igual modo, la STC 219/2009, de 21 de diciembre, FJ 4.º, señala que «lo relevante para preservar el principio de proporcionalidad es "la aportación de aquellos datos que resulten imprescindibles para poder constatar la idoneidad y estricta necesidad de la intervención y excluir las escuchas prospectivas"».

El TS se hizo eco de la anterior jurisprudencia, citándola en algunas sentencias en las que se pronuncia en idéntico sentido. Así, por ejemplo, la STS 712/2012, de 26 de

[374] Para justificar esta doctrina, la STC 150/2006, de 22 de mayo, declara asimismo en su FJ 3.º que «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 éstos se cometen en el seno de estructuras delictivas organizadas».

septiembre, FJ 2.º, declara, con mención de antecedentes del propio TS[375], que «la previa identificación del titular de un número que luego resulta intervenido, no es indispensable para la legitimidad de la injerencia».

Debe tenerse en cuenta, por otra parte, que, con la salvedad de los delitos privados, la instrucción puede abrirse sin que exista investigado, dado que, puesta en conocimiento de la autoridad judicial la *notitia criminis*, el juez de instrucción competente deberá iniciar la fase de instrucción incluso cuando no se tenga autor conocido, y ello por cuanto la finalidad de la instrucción conforme al art. 299 LECrim es precisamente, además de averiguar y hacer constar la perpetración de los delitos, averiguar y hace constar la culpabilidad de los delincuentes, asegurando sus personas[376].

Cuestión distinta es que para concluir con éxito la instrucción sea necesario que el presunto o presuntos culpables se encuentren identificados, ya que de no ser así el procedimiento no podría continuar, procediendo el dictado de un auto de sobreseimiento provisional (arts. 641.2.º y 779.1.1.º LECrim)[377].

---

[375] Señala concretamente la STS 712/2012, de 26 de septiembre, que «así lo hemos proclamado en varios precedentes, de los que las SSTS 309/2010, 31 de marzo y 493/2011, 26 de mayo, son muestra elocuente».

[376] Vid. la STS 712/2012, de 26 de septiembre, FJ 2.º, en la que se señala que «el objeto del proceso no responde a una imagen fija. Antes al contrario, se trata de un hecho de cristalización progresiva, con una delimitación objetiva y subjetiva que se verifica de forma paulatina, en función del resultado de las diligencias. Esta idea la expresa con absoluta claridad, en el ámbito de la fase de investigación, el art. 299 de la LECrim , cuando recuerda que durante esa etapa del proceso se practican las actuaciones encaminadas a "... averiguar y hacer constar la perpetración de los delitos, con todas las circunstancias que puedan influir en su calificación y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos". Ninguna vulneración de derechos constitucionales puede asociarse a una actuación jurisdiccional que entronca con la esencia misma del proceso penal. La ampliación de las imputaciones inicialmente acordadas, con fundamento en conversaciones que son ofrecidas a la autoridad judicial, algunas de la cuales no permiten identificar a uno los interlocutores, no es sino la consecuencia de asociar a las acciones delictivas que van poniéndose de manifiesto durante la investigación, la persona que haya de ser considerada responsable».

[377] Dispone el art. 641 de la LECrim que procederá el sobreseimiento provisional: «…2.º cuando resulte del sumario haberse cometido un delito y no haya motivos suficientes para acusar a determinada o determinadas personas como autores, cómplices o encubridores». De forma similar en sede del procedimiento abreviado el art. 779.1.1.º de la LECrim dispone que «…1.ª Si estimare que el hecho no es constitutivo de infracción penal o que no aparece suficientemente justificada su perpetración, acordará el sobreseimiento que corresponda. Si, aun estimando que el hecho puede ser constitutivo de delito, no hubiere autor conocido, acordará el sobreseimiento provisional y ordenará el archivo».

Por otro lado, y de igual modo, el art. 588 bis b.2.1.º LECrim establece que la petición habrá de contener la identidad de cualquier otra persona afectada, si bien permite que pueda omitirse la misma cuando no fuese conocida.

La mención a otras personas afectadas ha de entenderse principalmente dirigida a aquellos casos en los que la investigación se lleva a cabo en relación con un dispositivo electrónico perteneciente a una tercera persona, cuando aquel es usado por el investigado para almacenar, transmitir o recibir información[378].

Así lo señaló el ATS de 18 de junio de 1992 al declarar que la investigación puede dirigirse contra el terminal «que corresponda como titular a la persona procesada, o contra la que existan indicios graves de criminalidad, o también en relación con el que, más o menos, habitualmente lo utilice»[379]. Asimismo, cabe señalar que, en relación con la identidad de las demás personas afectadas, resulta igualmente de aplicación la doctrina de las de las anteriormente citadas SSTC 150/2006 y 219/2009, en las que se menciona la posibilidad de intervenir terminales de los que el investigado sea titular o usuario.

1.1.2. Datos de identificación del investigado

En conexión con el apartado anterior, lo que si necesariamente ha de concretarse, son los datos que permitan una identificación de la persona que está siendo investigada, al establecer el art. 588 bis b.2.3.º LECrim, que la petición habrá de contener «los datos de identificación de investigado».

Se trata de una previsión, que a nuestro juicio, no muestra una apropiada redacción legislativa, por lo que por algunos autores se ha entendido la misma como una reiteración o incluso contradicción[380] de lo dispuesto en el apartado 1.º del art. 588 bis

[378] Afirma a este respecto RODRÍGUEZ ÁLVAREZ: «Esta previsión parte de un hecho incontestable: que no siempre será sencillo determinar quién puede hacer uso del dispositivo intervenido (piénsese, e. g., en una línea telefónica o de Internet común a los habitantes de una vivienda). Vid. RODRÍGUEZ ÁLVAREZ, A., «Intervención de las comunicaciones telefónicas y telemáticas y smartphones», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, p. 161.

[379] Vid. Auto de 18 de junio de 1992 - ROJ: ATS 3773/1992, FJ 3.º

[380] Así, por ejemplo, GARCIMARTÍN MONTERO afirma que «se aprecia en este apartado una cierta reiteración del Art. 588 bis b 2.1.º LECrim que ya exige que se proporcione la identidad del «investigado o de cualquier otro afectado». Vid. GARCIMARTÍN MONTERO, R., «*Los medios de investigación tecnológicos en el proceso penal*», cit., p. 49. Por su parte, LÓPEZ CAUSAPÉ afirma que cabe observar una

b.2, al que nos hemos referido en el anterior apartado, en el que se dispone la necesidad de consignar en la petición del Ministerio Fiscal o la Policía Judicial, la identidad del investigado, siempre que fuese conocida.

Consideramos desafortunada la redacción del precepto, por cuanto lo que el legislador ha pretendido, no es tanto que se consignen «los datos de identificación del investigado», sino «los datos que puedan permitir la identificación del investigado», siendo este el espíritu del precepto, en el que ya no se admite que tales datos puedan omitirse.

En este sentido, en aquellos casos en los que se inste al juez competente, la práctica de una intervención en la que no se conozca con precisión los datos que identifiquen de una forma precisa a la persona sospechosa, se deberá facilitar algún dato que pueda permitir tal identificación, circunstancia que, de forma incuestionable, exigirá un mayor grado de motivación, tanto en la petición policial como en la resolución judicial.

Esta interpretación es a nuestro juicio la correcta, si tenemos en cuenta, que la jurisprudencia ya había permitido una identificación parcial, con el uso solamente de nombres de pila o sobrenombres, como así se deduce de la STS 490/2014, de 17 de junio, FJ 5.º, que declaró que, «no es necesaria, de otra parte, la identificación plena del usuario de un teléfono para su intervención».

Asimismo, la STS 832/2001, de 14 de mayo, FJ 1.º —a la que se refirió la anteriormente citada STS 490/2014—, declaró que, «además de la exigencia sobre concreción del hecho delictivo investigado, es necesaria la especificación personal, esto es, la determinación de la persona o personas cuya actividad criminal se investiga […] a fin de que en la medida de lo posible la observación […], no alcance a personas no sometidas a investigación», añadiendo que «esa determinación no significa forzosamente la identificación de la persona con sus nombres y apellidos, dada la

---

cierta contradicción entre los requisitos 1º y 3º, dado que el 1º condiciona la identidad del investigado o de cualquier otro afectado por la medida a que tales datos sean conocidos, mientras el 3º exige que la solicitud contenga los datos de identificación del investigado o encausado. Esta contradicción, la interpreta en el sentido de que la identidad del investigado debe consignarse en todo caso en la solicitud y que la exención de tal obligación, si el dato no es conocido, afectaría solo a terceros afectados por la medida, lo cual guardaría relación con la redacción del requisito 2º de la resolución judicial que contempla el artículo 588 bis c.3 b). Vid. LÓPEZ CAUSAPÉ, E., «Las medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», cit., p. 6.

posibilidad de que en ese momento se ignoren…» y que «basta entonces con la referencia personal que resulta de los propios indicios criminales valorados para la intervención […], en principio por aquella persona determinada —identificada nominalmente o no— cuya actividad criminal se investiga»[381].

1.1.3. Unidad investigadora que se hará cargo de la intervención

De acuerdo con lo dispuesto en el apartado 5.º del art. 588 bis b.2 LECrim, deberá reflejarse en la petición «la unidad investigadora de la Policía Judicial que se hará cargo de la intervención»[382].

Acerca de este requisito, poco más puede añadirse a lo indicado doctrinalmente, cuando se apunta que «se trata de una exigencia que adquiere todo su sentido, tanto desde una perspectiva ordenadora de la comunicación entre las fuerzas policiales y el órgano judicial, como por el deseo legislativo de hacer explícitos los presupuestos que hacen posible el efectivo control judicial»[383].

---

[381] La STS 832/2001, de 14 de mayo, concluyó este apartado declarando que «en definitiva, en la relación de los indicios criminales disponibles contra alguna persona deben estar las determinaciones relativas a ésta, sin que ello signifique su nominal identificación individual, que puede constituir precisamente el objeto de la investigación».

[382] Explica LANZAROTE MARTÍNEZ que, dentro del concepto de Policía Judicial han de entenderse incluidos no solo las FCSE cuando desempeñen funciones de Policía Judicial de acuerdo con lo previsto en el art. 547 LOPJ sino también de los agentes de Vigilancia Aduanera que tienen la consideración de agentes facultados conforme al art. 6.2 de la Ley 25/2007, de 18 de octubre en el desarrollo de sus competencias como Policía Judicial de acuerdo con el apartado 1 del art. 283 LECrim, habiendo reconocido la Sala II del TS tal carácter de Policía Judicial al servicio de vigilancia aduanera desde el Acuerdo plenario de 14 de noviembre de 2003. Afirma asimismo el citado autor que por el contrario, el personal del Centro Nacional de Inteligencia, en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, no pueden entenderse incluidos en la expresión utilizada por el precepto de «unidad investigadora de la Policía Judicial que se hará cargo de la intervención» a la vista de que sus funciones se cumplen en ámbitos distintos al proceso penal. Como refuerzo de esta afirmación cita la STS 1094/2010, de 10 diciembre, que declaró que «las actividades de los agentes del CNI no están funcionalmente subordinadas al esclarecimiento de hechos aparentemente constitutivos de delito. Su cometido no es otro que facilitar al Gobierno "las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones"». Vid. LANZAROTE MARTÍNEZ, P., «La nueva regulación de las intervenciones telefónicas y telemáticas: Algunas cuestiones claves y otras discutibles», cit., p. 74.

[383] Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 234.

Aun así, ha de tenerse en cuenta, que de acuerdo con lo declarado por el TC, es suficiente que la petición identifique la unidad policial que ejecutará la intervención, sin que sea necesaria la identificación, ya sea por su número o por su nombre, de los agentes integrantes de dicha unidad[384].

1.1.4. Sujeto obligado que llevará a cabo la medida, en caso de conocerse

El art. 588 bis b.2 LECrim, termina disponiendo en el 8.º y último de sus apartados, que será necesario consignar en la petición del Ministerio Fiscal o de la Policía Judicial «el sujeto obligado que llevará a cabo la medida».

Cabe señalar que por el Consejo Fiscal de la FGE, en el informe al anteproyecto de la LO 13/2015, se consideró superfluo este requisito al señalar que «no se acierta a comprender su significación, sobre todo cuando el numeral 5º comprende a la unidad investigadora de la Policía Judicial que se hará cargo de la intervención» y añadió que «parece que pudiera referirse a la compañía prestadora del servicio, pero entendemos que tal extremo no es imprescindible, y por ello, en aras a la simplificación, podría suprimirse»[385].

Sin embargo, de acuerdo con lo afirmado por algunos autores, entre los que podemos mencionar a RICHARD GONZÁLEZ, «la Ley prevé la existencia de diversos sujetos obligados a ejecutar o colaborar de algún modo con la medida de investigación. Así sucederá en el supuesto de una interceptación telefónica en la que será precisa la colaboración de la empresa suministradora del servicio o en el supuesto de la intervención de computadoras en cuyo caso puede ser necesaria la colaboración de la empresa suministradora de acceso a Internet o bien de la empresa propietaria de la computadora que deba ser objeto de intervención»[386].

---

[384] Vid. STC 166/1999, de 27 de septiembre, FJ 7.º, que declaró que «a efectos de la determinación del alcance subjetivo de la medida, es suficiente que la autorización se efectúe para funcionarios del Grupo de Estupefacientes de la Policía Judicial, sin que sea necesario que se identifique por su número o nombre a quienes en particular habrán de llevarla a cabo».

[385] Vid. CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 63.

[386] RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», cit., p. 15.

Por su parte, GARCIMARTÍN MONTERO, señala que «esta norma alude a la posibilidad, recogida en otras normas de la LECrim, de que no sea la policía la encargada de ejecutar la medida sino que esta se encomiende a otra persona, bien porque posee la información necesaria, bien por poseer conocimientos especializados que se pudieran requerir para ejecutar la medida»[387].

En efecto, la vigente LECrim establece el deber de colaboración de terceras personas, que no siempre han de tener la condición de prestadores de servicios de telecomunicaciones.

Así, aunque en el ámbito de la interceptación de las comunicaciones telefónicas y telemáticas, el art. 588 ter e, establece el deber de colaboración de todos los prestadores de servicios de telecomunicaciones y demás personas que de cualquier modo contribuyan a facilitar las comunicaciones[388], no es menos cierto que, para el registro de dispositivos de almacenamiento masivo de información, el art. 588 sexies c.5, impone la obligación de facilitar la información que resulte necesaria a las autoridades y agentes encargados de la investigación, a cualquier persona que conozca el funcionamiento del sistema informático objeto de registro o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo, salvo que suponga una carga desproporcionada para el afectado[389].

Por su parte, el art. 588 septies b, establece en el ámbito de los registros remotos sobre equipos informáticos, el deber de colaboración, además de los prestadores de

---

[387] GARCIMARTÍN MONTERO, R., «*Los medios de investigación tecnológicos en el proceso penal*», cit., p. 50.

[388] Dispone el art. 588 ter e LECrim:

1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones.
2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.
3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia.

[389] La excepción al deber de colaboración consistente en la circunstancia de que la obligación suponga «una carga desproporcionada», constituye un término muy amplio, que ha sido criticado doctrinalmente por su falta de concreción. Nos ocuparemos de este tema en el apartado del capítulo V dedicado al «deber de colaboración de terceros».

servicios, de los titulares o responsables del sistema informático o base de datos objeto del registro, imponiendo además la obligación de facilitar la información necesaria para el buen fin de la diligencia, a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo[390].

Además, el artículo 588 octies (al que dedicaremos el último apartado de este capítulo, por su especial relevancia), establece el deber de conservación de datos, hasta que se obtenga la autorización judicial para su cesión, no solo a las operadoras[391], sino a cualquier persona física o jurídica.

Finalmente, debe subrayarse que, conforme dispone el apartado 8.º del art. 588 bis b.2 LECrim, la mención del sujeto obligado que llevará a cabo la medida, ha de consignarse en la petición del Ministerio Fiscal o la Policía Judicial, «en caso de conocerse». Con ello, el legislador ha dejado abierta la posibilidad, de que la identificación de la persona que ha de colaborar se identifique con posterioridad, siempre en los términos establecidos en los preceptos referidos en los apartados anteriores.

1.2. Requisitos objetivos

Los requisitos de carácter objetivo que deberá contener la solicitud al órgano judicial para la autorización de la medida de investigación tecnológica, se concretan en la descripción del hecho objeto de la investigación, la exposición de las razones que justifican la necesidad de la medida, la existencia de indicios de criminalidad, los medios de comunicación empleados que permitan la ejecución de la medida, así como su extensión y duración. Realizaremos unas sucintas consideraciones en relación con cada uno de ellos.

---

[390] Tanto el art. 588 sexies c.5 LECrim, para los registros de dispositivos de almacenamiento masivo, como el art. 588 septies b LECrim, para los registros remotos de dispositivos informáticos, eximen de las obligaciones de colaboración mencionadas, al investigado y a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el art. 416.2 LECrim, no pueden declarar en virtud del secreto profesional. En ambos casos se establece que, la colaboración deberá prestarse, bajo apercibimiento de incurrir en delito de desobediencia.

[391] La obligación de conservación y cesión de datos por parte de las operadoras así como la Ley 25/2007, de conservación de datos, fueron examinadas en el primer capítulo, con motivo del análisis de la confrontación entre las medidas de investigación tecnológica y el derecho fundamental a la protección de datos de carácter personal. Vid. supra apdos. III.4.4.2 y ss. del capítulo I, pp. 61-84.

1.2.1. Descripción del hecho objeto de la investigación

El primero de los requisitos establecidos en el art. 588 bis b.2, que deberá hacerse constar en la solicitud para la autorización judicial de la medida, se establece en el apartado 1.º de dicho precepto, que comienza señalando que la petición habrá de contener «la descripción del hecho objeto de investigación».

Como no podría ser de otro modo, para que el tribunal pueda calificar jurídicamente los hechos[392], juzgando su gravedad, trascendencia social o el ámbito tecnológico de producción, dando así cumplimiento al principio de proporcionalidad[393], resulta indispensable que se informe al juez sobre tales hechos, realizando una descripción de los mismos en la correspondiente solicitud.

1.2.2. Exposición de las razones que justifican la necesidad de la medida

Con este requisito de la solicitud de autorización judicial, exigido por el apartado 2.º del art. 588 bis b.2 LECrim, se pretende la justificación de los principios de excepcionalidad y necesidad, que ya han sido examinados anteriormente[394]. Por tanto, deberá acreditarse que no existen otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, así como que sin el recurso a la medida solicitada, se vería gravemente dificultado el descubrimiento o la comprobación del hecho investigado.

Baste señalar a este respecto, de acuerdo con lo afirmado por MARCHENA GÓMEZ, que cualquier otra diligencia de investigación menos gravosa para los derechos fundamentales resultará siempre preferible a la intervención de las comunicaciones y por extensión a los registros informáticos, y por ello «el principio de necesidad ha de

[392] Como veremos más adelante, la LECrim exige que la resolución judicial concrete la calificación jurídica del hecho punible objeto de investigación.

[393] Vid. supra apdo. I.4 del capítulo III, pp. 149-151, donde al analizar la el principio rector de la «proporcionalidad», señalamos que «la gravedad del hecho» es uno de los criterios para llevar a cabo la ponderación de los intereses en conflicto exigida por dicho principio, esto es, para determinar si una vez tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros.

[394] Vid. supra apdo. I.3 del capítulo III, pp. 147-149.

convertirse en un elemento decisivo en la motivación del acto jurisdiccional habilitante»[395].

1.2.3. Existencia de indicios de criminalidad

Dispone el art. 588 bis b.2.2.º LECrim, que la petición del Ministerio Fiscal o Policía Judicial habrá de contener: «…los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia».

Además de para dar cumplimiento al principio de proporcionalidad, (dado que, la existencia de indicios de criminalidad, es uno de los criterios a tener en cuenta para estimar proporcionada la medida)[396], es este un requisito igualmente exigido para que se cumpla el principio de especialidad, habida cuenta que, siendo necesario conforme a este último principio, que cualquier medida de investigación tecnológica esté relacionada con la investigación de un delito concreto, no permitiéndose aquellas medidas que estuvieran dirigidas a vigilar conductas sin que existan indicios claros de la posible comisión de un delito, resulta necesario que existan unos indicios que sean suficientes para inferir que existe un delito cometido o que se va a cometer[397].

En este sentido, de conformidad con la opinión de DELGADO MARTIN «el Estado podrá restringir un derecho fundamental solo en aquellos supuestos en los que exista un grado suficiente de imputación de un delito, es decir cuando existan razones objetivas que permitan afirmar la probabilidad de que ese sujeto esté cometiendo o haya cometido un delito»[398], añadiendo el citado autor que, «únicamente la concurrencia de esos indicios legitima al Estado para rebasar el ámbito intangible de la libertad personal y la intimidad en el desarrollo de la investigación»[399], y concluyendo que, «en otro caso, se

[395] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 237.
[396] Vid. supra apdo. II.3.2.2.1 del capítulo II, pp. 123-124.
[397] Vid. supra, en relación con la exigencia de la existencia de indicios para que se cumpla el principio de especialidad, el apartado I.1 del capítulo III, pp. 144-145.
[398] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 348.
[399] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 348.

estaría otorgando a los órganos estatales una patente de corso para inmiscuirse en la vida privada de los ciudadanos»[400].

En definitiva, como ha declarado la jurisprudencia, la solicitud policial debe recoger indicios que proporcionen «una base real y por tanto lo suficientemente objetiva de la que puede inferirse que se ha cometido o se va a cometer el delito para cuya investigación se solicita la intervención…»[401].

1.2.4. Medios de comunicación empleados que permitan la ejecución de la medida

El apartado 3.º del art. 588 bis b.2 LECrim, establece que la petición del Ministerio Fiscal o Policía Judicial hará constar cuales son los medios de comunicación empleados que permitan la ejecución de la medida. Ahora bien, el precepto dispone que tal reseña se realizará «en su caso», lo que, obviamente, quiere decir que no siempre será necesario para la ejecución de una medida de investigación tecnológica el uso de un concreto medio de comunicación.

Como es notorio, en la actualidad, los medios de comunicación tecnológicos no quedan reducidos a las comunicaciones telefónicas, sino que, con la irrupción de las TIC, se ha impuesto el concepto de las «comunicaciones telemáticas», entendidas como aquellas que se producen a distancia mediante el uso de la informática. Dentro de ellas podemos destacar las que tienen lugar mediante correo electrónico, en las redes sociales (facebook, twiter, youtube, etc.), whatsapp, videoconferencia y foros de conversación y chats en internet.

Alguno de estos medios de comunicación, deberá reflejarse en la solicitud policial, en los supuestos de ejecución de una medida de intervención de las comunicaciones telemáticas, lo cual facilitará la tarea del juez para dar cumplimiento al principio de idoneidad, definiendo el ámbito objetivo de la medida (art. 588 bis a.3 LECrim)[402].

---

[400] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 348.

[401] Vid. STS 558/2005, de 27 de abril, FJ. 2.º

[402] Como dijimos en el apartado I.2 del capítulo III, pp. 145-147, al examinar el principio de idoneidad, el legislador, supedita para la utilidad de la medida, los aspectos esenciales que determinarán que la misma

Sin embargo, en lo concerniente a los registros informáticos, no es necesario el uso de estos medios de comunicación, sin perjuicio de que, en relación con los registros remotos sobre equipos informáticos, es necesaria la utilización de un software mediante el que se ejecutará el control de la información, que deberá ser instalado remotamente en el equipo informático del investigado, respecto del cual —como se verá en el apartado correspondiente del capítulo V—, el legislador ha establecido que ha de ser especificado en la resolución judicial (art. 588 septies a.2 c LECrim).

1.2.5. Extensión de la medida

Otro de los requisitos a consignar en la solicitud de autorización judicial, contemplado en el apartado 4.º del art. 588 bis.2 LECrim, se concreta en la extensión de la medida, o lo que es lo mismo, en la fijación de su alcance, es decir, que se especifique la concreta información que se requiere para culminar la investigación, sin que proceda el acceso a más datos que los estrictamente necesarios, evitando así cualquier intrusión improcedente en la privacidad de la persona afectada.

Para ello, el referido precepto determina que se consignara la extensión «con especificación de su contenido». De este modo, ya no es posible, como pudo suceder con anterioridad a la LO 13/2015, que la intervención se extienda obligadamente a todos los datos que pudieran obtenerse en cualquier intervención tecnológica.

Por ello, la solicitud policial o del Ministerio Fiscal deberá especificar cuáles son los contenidos o datos necesarios para el esclarecimiento de los hechos (contenido de comunicaciones, datos de tráfico, localización geográfica, una concreta conversación con determinada persona, archivos de texto, video o audio, etc.), sin que proceda extender la medida a otros contenidos que, sin ser necesarios para el buen fin de la investigación, podrían vulnerar los derechos a la vida privada, tanto del investigado como de terceros.

1.2.6. Forma de ejecución

En cuanto a la forma de ejecución de la medida, tal y como señala SANTOS MARTÍNEZ, la LECrim guarda silencio en relación a esta cuestión, lo cual no genera mayor problema, dado que, de conformidad con lo apuntado por el referido autor, «no es

---

es apta y adecuada para conseguir el fin perseguido, como son las cosas y las personas sobre las que habrá de llevarse a cabo la investigación (ámbito objetivo y subjetivo).

menester de la ley procesal establecer aquellos sistemas más idóneos para proceder a ejecutar las medidas de investigación tecnológica»[403].

Pero es lo cierto, como indica MARCHENA GÓMEZ, que «al juez de instrucción no le debería ser ajeno el procedimiento técnico aplicable para la eficacia de la interceptación», por lo que los agentes solicitantes deberán explicar de forma comprensible y al alcance de no iniciados en cuestiones técnicas, la forma mediante la que se llevará a cabo la actuación[404].

En el ámbito de los registros informáticos, por lo que respecta al registro de dispositivos de almacenamiento masivo, con carácter general, entendemos que se explicará la forma en la que se realizará el volcado de datos, identificando los equipos que se utilizarán para ello. En el registro remoto de equipos informáticos, se especificará el software que será instalado en el equipo del investigado, así como el programa y procedimiento mediante el que se accederá remotamente al mismo, todo ello, como se ha dicho, de una forma comprensible para personas indoctas en tecnología informática.

1.2.7. Duración

El Ministerio Fiscal o la Policía Judicial en su solicitud deberán reflejar el tiempo estimado que podrá durar la intervención, conforme al apartado 6.º del art. 588 bis b.2, dado que, cuando se restringe un derecho fundamental en el marco de una investigación policial, de tener esta limitación una duración indefinida, estaríamos ante una actuación desproporcionada y contraria al principio de seguridad jurídica.

El juez, en el auto que acuerde la práctica de la diligencia, deberá finalmente establecer la duración, dentro de los límites máximos fijados por la LECrim para cada medida de investigación.

En relación con los aspectos concernientes a la duración de la medida, nos remitimos a lo ya estudiado en el capítulo anterior[405].

---

[403] SANTOS MARTÍNEZ, A. M., «Examen de las disposiciones comunes de las medidas de investigación tecnológica», cit., p. 4.

[404] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 247.

[405] Vid. supra apdos. III.1, 2 y 3 del capítulo III, pp. 167-172.

2. Resolución judicial

Determinados requisitos que deben concretarse en la resolución, coinciden con algunos de los exigidos en la solicitud, examinados anteriormente. Por ello, aun cuando se pueda producir alguna puntual reiteración, nos ocuparemos del estudio de los aspectos inherentes a la resolución judicial, como son: la necesaria audiencia del Ministerio Fiscal, el plazo máximo para la adopción de la resolución, el hecho punible objeto de investigación y su calificación jurídica, la expresión de los indicios racionales en los que se funde la medida, su extensión, motivación relativa al cumplimiento de los principios rectores, la forma y periodicidad con la que el solicitante informará al juez sobre los resultados obtenidos con su ejecución y el deber de colaboración de terceros.

2.1. Necesaria audiencia del Ministerio Fiscal

De conformidad con el art. 588 bis c.1, el juez de instrucción autorizará o denegará la medida solicitada mediante auto motivado, oído el Ministerio Fiscal.

No se trata de una cuestión novedosa el hecho de que el Fiscal deba ser oído previamente al acuerdo de cualquier diligencia de investigación, dado que, de conformidad con el art. 306 LECrim, le corresponde la inspección directa en la formación del sumario por los jueces de instrucción, como así lo ha puesto de manifiesto la doctrina[406] y la jurisprudencia[407].

Sin embargo, aunque en principio este inciso podría considerarse superfluo, estimamos que con el mismo, el legislador ha pretendido que cuando los juzgados de instrucción registren una modalidad de expediente judicial no contemplado por la ley, usado en la práctica forense desde años atrás bajo el nombre de «diligencias

[406] Señala MONTERO AROCA: «A pesar de las palabras el Fiscal no "inspecciona" la labor del juez, ni éste puede considerarse un subordinado suyo. El procedimiento preliminar judicial está en manos del juez de instrucción y la pretendida "inspección" se reduce a que el Ministerio fiscal se constituya como parte en aquél, formulando las alegaciones y solicitando los actos de investigación que considere oportunos. Sus privilegios consisten en que el juez de instrucción debe darle parte de la incoación de la instrucción (art. 308) y en que para él el sumario no puede decretarse secreto. El fiscal no "informa"; alega como todas las partes». Vid. MONTERO AROCA, J., «Los conceptos esenciales», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, p. 77.

[407] De acuerdo con lo declarado por la STS 272/2017, de 18 de abril, con cita de otras (SSTS 138/2006, 1013/2007, 578/2009, 309/2010 o 385 y 694/2011), «el Fiscal no necesita de un acto formal de invitación al proceso puesto que su presencia es institucional y conforme al artículo 306 LECrim, los Jueces de instrucción formaran los sumarios bajo la inspección directa del Fiscal del Tribunal competente».

indeterminadas», se confiera traslado al Ministerio Fiscal, evitando de este modo una práctica respecto de la que el TC ha declarado que, de producirse, el proceso se mantendría dentro de un «constitucionalmente inaceptable secreto»[408].

En cualquier caso, aun cuando existen algunas opiniones doctrinales muy críticas con las diligencias indeterminadas, su uso no ha sido vedado por la jurisprudencia, existiendo sectores doctrinales que se pronuncian en favor de las mismas, con el denominador común de que, en todo caso, se confiera traslado al Ministerio Fiscal de su incoación[409].

2.2. Plazo máximo para la adopción de la resolución

La resolución se dictará en el plazo máximo de veinticuatro horas desde que se presente la solicitud (art. 588 bis c.1).

En relación con este reducido plazo para adoptar una decisión este calado, compartimos la opinión de LÓPEZ CAUSAPÉ, quien afirma que no en todos los supuestos está justificada esta premura[410], añadiendo que, en numerosas ocasiones, resulta muy

[408] Vid. STC 49/1999, de 5 de abril, FJ 6º.

[409] En relación las diligencias indeterminadas, puede consultarse un estudio realizado por este autor, en el que, con mención de la doctrina y jurisprudencia existente hasta ahora sobre la materia, y habida cuenta de la disparidad de criterios entre los propios tribunales en cuanto a su utilización, se propone, mejor que la prohibición de las mismas, su regulación legal. En ella debería establecerse la obligatoriedad, en todo caso, de la notificación al Ministerio Fiscal de la apertura de las diligencias, dada su condición de garante de los derechos de los ciudadanos. Vid. ESPÍN LÓPEZ, I., «La necesidad de una adecuada regulación de las Diligencias Indeterminadas en el Proceso Penal», *Acta Judicial - Revista del Ilustre Colegio Nacional de Letrados de la Administración de Justicia*, n.º 6, 2020.

[410] LÓPEZ CAUSAPÉ, E., «Las medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», cit., pp. 7-8. Afirma este autor que: «Este plazo parece atender a las exigencias de urgencia de atención de solicitudes de interceptación de comunicaciones telefónicas o telemáticas en curso, de captación y grabación de comunicaciones orales o de colocación de dispositivos de captación de imagen, seguimiento y localización. Sin embargo, en muchos casos tal urgencia no concurre en las solicitudes de diligencias de instrucción relacionadas con la aportación de datos electrónicos conservados por las operadoras prestadoras de tales servicios, o con la identificación de los equipos o dispositivos desde los que se realiza una concreta conexión a través de una dirección IP, o con el registro del contenido de dispositivos de almacenamiento masivo. Por otra parte, en muchas ocasiones tales solicitudes se producen en el ámbito de la instrucción de causas penales ya iniciadas siendo extremadamente difícil cumplir el plazo indicado fuera del servicio de guardia, máxime ante la exigencia de audiencia al Ministerio Fiscal. Debe considerarse por ello inadecuado el establecimiento de tal plazo tan perentorio en las disposiciones comunes, limitando así la posibilidad de valorar la urgencia de cada una de las solicitudes de medidas de investigación tecnológica solicitadas. Cabe igualmente plantearse cuáles serían las consecuencias de

dificultoso el cumplimiento de dicho requisito por el Juzgado de instrucción, máxime teniendo en cuenta la preceptiva audiencia del Ministerio Fiscal, por lo que considera inadecuada la fijación de este plazo con carácter general[411].

En el mismo sentido, SANTOS MARTÍNEZ se refiere a la conveniencia de cuestionarse si el plazo legal es suficiente para tomar una decisión ponderada, fruto de la reflexión, señalando que «a fin de evitar situaciones que comprometan la validez de la decisión judicial una solución podría ser reservar el plazo de veinticuatro horas a aquellas medidas que precisen una respuesta urgente —debiendo así anunciarlo el peticionante en su solicitud y valorarlo de forma preliminar el juez de instrucción— estableciendo para el resto de peticiones el carácter de actuaciones con tramitación preferente pero sin que queden sujetas a plazo concreto»[412].

Por nuestra parte, estimamos, en línea con las anteriores opiniones, que sería más aconsejable la fijación de un plazo más amplio con carácter general, que permitiría que el exigente ejercicio de la potestad jurisdiccional en un asunto de tan alta trascendencia como es la tutela de los derechos fundamentales, se llevase a cabo con un más completo estudio y reflexión, lo que no haría otra cosa que reforzar la garantía del respeto a los mismos.

No obstante, debería fijarse un plazo de veinticuatro horas para aquellas diligencias que por su propia naturaleza, o según las circunstancias de cada caso, exigiesen una intervención urgente, la cual debería ponerse de manifiesto en la solicitud, informando al juzgado de dicha circunstancia, a fin de ser examinada en el mismo día de su presentación por el juez de instrucción.

En todo caso, sí consideramos conveniente la fijación de un plazo con carácter general para el dictado de la resolución judicial, sin que este quede a discreción del tribunal instructor, dada la relevancia de esta decisión, consistente en la adopción —o en

---

exceder tal plazo en la resolución de la solicitud, entendiendo en todo caso improbable que pueda afectar a la validez de lo resuelto».

411 LÓPEZ CAUSAPÉ, E., «Las medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», cit., pp. 7-8.

412 Señala este autor que «podrían darse situaciones donde, como consecuencia de una elevada carga de trabajo, el estricto cumplimiento del plazo diera lugar a la adopción de decisiones mero formularias, susceptibles de comprometer la viabilidad de la actuación y, por ende, llegar a ser declaradas nulas por no dar cumplimiento a los requisitos legales». Vid. SANTOS MARTÍNEZ, A. M., «Examen de las disposiciones comunes de las medidas de investigación tecnológica», cit., p. 12.

su caso denegación— de una concreta intervención, limitativa de derechos fundamentales, para el esclarecimiento de un hecho delictivo, pudiendo establecerse, por ejemplo, un plazo de tres días, que permitiría un idóneo estudio por el juez de instrucción competente, pero sin el riesgo de que se produzcan dilaciones indebidas en un asunto de esta especial relevancia.

Por otra parte, se hace necesario referirse en este apartado, al art. 588 bis c.2 LECrim, que dispone que «siempre que resulte necesario para resolver sobre el cumplimiento de alguno de los requisitos expresados en los artículos anteriores, el juez podrá requerir, con interrupción del plazo a que se refiere el apartado anterior, una ampliación o aclaración de los términos de la solicitud».

Por tanto, el juez, únicamente en aquellos casos en los que considere, y así lo motive en la correspondiente resolución, que la petición de intervención carece de alguno de los requisitos que se exigen por la LECrim en la solicitud de autorización judicial, o en su caso si albergase cualquier duda acerca de los mismos o en relación con los principios rectores proclamados en el art. 588 bis a, podrá requerir al Ministerio Fiscal o Policía Judicial una ampliación o aclaración, con suspensión del plazo de veinticuatro horas para autorizar o denegar la práctica de la diligencia, el cual se reanudará tan pronto como sea facilitada la ampliación o aclaración.

No se fija en la LECrim un plazo en el que el Ministerio Fiscal o la Policía Judicial deberán facilitar la ampliación o aclaración, entendiendo que si partimos de la fijación de un plazo tan perentorio para que el juez deba resolver la solicitud, del mismo modo debería fijarse un plazo como máximo de la misma duración para que se facilitase tal ampliación o aclaración. No obstante, esta apreciación no impide que mantengamos nuestra opinión anteriormente mencionada, en relación con el establecimiento de un plazo de veinticuatro horas solamente para los supuestos de carácter urgente.

2.3. Hecho punible objeto de investigación, calificación jurídica y expresión de los indicios racionales en los que se funde la medida

Por imperativo del apartado a) del art. 588 bis c.3 LECrim, la resolución judicial que autorice la medida, deberá concretar «el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que se funde la medida». Por tanto, conforme dijimos anteriormente, el juez de instrucción no está

autorizado por la vigente LECrim para motivar el auto por remisión a la solicitud del Ministerio Fiscal o la Policía Judicial[413].

La concreción del hecho objeto de investigación, constituye una garantía del cumplimiento del principio de especialidad, y en tal sentido, tal y como apunta SÁNCHEZ MELGAR, no deberá realizarse con vaguedades «sino con la precisión que resulte de la descripción de los aspectos fácticos que le participe quien le solicite la medida, o con los datos de ampliación que sean consecuencia de sus exigencias»[414].

En cuanto a la calificación del presunto delito objeto de la investigación, compartimos la opinión de la Circular 1/2019 de la FGE, cuando señala que la misma «resulta de las exigencias propias del principio de proporcionalidad que, en relación con alguna de las medidas que regula la Ley, se ha reflejado en el establecimiento de catálogos cerrados de comportamientos delictivos»[415]. En efecto, tal y como hemos tenido la oportunidad de analizar en apartados anteriores[416], la gravedad del hecho es uno de los criterios para llevar a cabo la ponderación necesaria para un correcto juicio de proporcionalidad, por lo que se hace necesaria una pertinente calificación jurídico-penal del hecho objeto de investigación, para poder justificar el cumplimiento del principio de proporcionalidad.

Finalmente, para una completa motivación, la resolución judicial deberá referirse a los indicios racionales en los que se funde la medida, lo que culminará la justificación del cumplimiento de los principios de especialidad y proporcionalidad. También en relación con los indicios, nos remitimos a lo ya examinado anteriormente, tanto al estudiar el principio de proporcionalidad como al examinar el contenido de la solicitud policial[417].

En los referidos apartados, examinamos con alguna referencia jurisprudencial, el tema relativo a la intensidad de los indicios que permita la adopción de la medida, respecto de lo cual, baste apuntar, para concluir con este importante requisito de la

---

[413] Vid. supra apdo. II.1.2 del capítulo III, pp. 153-156.

[414] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 27.

[415] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., p. 10.

[416] Vid. supra apdo. II.3.2.2.2 del capítulo II, pp. 124-126 y apdo. I.4 del capítulo III, pp. 149-151.

[417] Vid. supra apdo. II.3.2.2.1 del capítulo II, pp. 123-124 y apdo. I.1.2.3 de este capítulo, pp. 203-204.

resolución judicial, que, conforme ha declarado el TC, no es necesario «cimentar la resolución judicial en un indicio racional de comisión de un delito, bastando una noticia *criminis* alentada por la sospecha fundada en circunstancias objetivas de que se pudo haber cometido, o se está cometiendo o se cometerá el delito o delitos en cuestión»[418].

2.4. Extensión de la medida de injerencia y motivación relativa al cumplimiento de los principios rectores

Al referirnos anteriormente al contenido de la solicitud de autorización judicial, indicamos que uno de los elementos a consignar en la misma, se concretaba en la extensión de la medida con especificación de su contenido. Este aspecto, de conformidad con el art. 588 bis c.3 c) LECrim, debe reflejarse en la resolución judicial, disponiendo este precepto que, además del alcance, deberá especificar la motivación relativa al cumplimiento de los principios rectores establecidos en el art. 588 bis a LECrim.

El juez, por tanto, tendrá la obligación de ponderar la necesidad de acordar la medida en toda la extensión solicitada por el Ministerio Fiscal o Policía Judicial, o bien determinar la que, para dar cumplimiento a los principios rectores comunes a todas las diligencias de investigación tecnológica, sea suficiente para una debida observancia de los mismos, en relación con el caso concreto que se esté investigando. De este modo, trayendo a colación lo dicho anteriormente, no será posible una remisión al oficio policial o del Ministerio Fiscal para la ponderación, sino que, el juez deberá razonar acerca de lo que se necesita y la forma de obtenerlo, limitándose a los datos relacionados con la causa, ya sean —como dijimos anteriormente en el apartado relativo a la solicitud de autorización— conversaciones concretas, datos de tráfico, localización geográfica o archivos de texto, video, audio; sin que proceda la extensión de la medida a datos que no sean estrictamente necesarios, que podrían limitar indebidamente los derechos a la vida privada del investigado o de terceros.

Para poder realizar esta ponderación, teniendo en cuenta que nos encontramos ante una resolución judicial en la que quedarán limitados derechos fundamentales, de conformidad con lo declarado por el TC de forma reiterada, los juzgados y tribunales

[418] Vid. STC 239/1999, de 20 de diciembre, FJ 5.º

tienen un deber reforzado de motivación[419]. Resulta relevante en este punto la SAP 311/2000, Sección 2.ª de Madrid, de 26 de abril que, conforme a la doctrina del TC, declaró que la relevancia constitucional de la motivación «deriva de su funcionalidad, en la medida en que constituye una eficaz profilaxis frente a la arbitrariedad judicial, en cualquier caso, y adquiere una importancia especial cuando están comprometidos derechos y libertades fundamentales…».

Por otra parte, si para acordar una medida de investigación tecnológica se deben respetar los principios rectores que rigen las mismas, es decir, los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, no plantea discusión el hecho de que la resolución que acuerde tal medida, deberá justificar que tales principios se cumplen. En consecuencia, conforme afirman MELÓN MUÑOZ Y OTROS «todas las actuaciones que supongan injerencia en el ámbito de los derechos fundamentales requieren como presupuesto previo —a falta del consentimiento del titular del derecho afectado, que en algunos casos puede convertir la diligencia en absolutamente inútil— la autorización judicial mediante resolución motivada»[420].

Además, para que las resoluciones judiciales limitativas de derechos fundamentales cumplan el deber de motivación, estas deben reflejar las exigencias del principio de proporcionalidad, erigiéndose como una garantía judicial que a su vez constituye un mecanismo de orden preventivo, destinado a proteger el derecho, y no como en otras intervenciones judiciales previstas en la Constitución a reparar su violación cuando se produzca[421]. Asimismo, ese deber reforzado de motivación viene impuesto por encontrarse en juego un derecho fundamental sustantivo, que solamente puede considerarse preservado cuando la decisión judicial de restringirlo ha sido debidamente razonada[422].

---

[419] Vid. STC 196/2002, de 28 de octubre, FJ 5.º la cual declaró que sobre las resoluciones judiciales que inciden en el contenido de un derecho fundamental sustantivo «pesa un deber de motivación reforzada, por comparación con el específicamente derivado del derecho a la tutela judicial efectiva proclamado en el artículo 24.1 CE». Por su parte la STC 116/1998, de 2 de junio, con cita de varias sentencias previas estableció que dicho deber reforzado de motivación se ha de dar en los siguientes supuestos: «a) cuando se vean afectados otros derechos fundamentales; b) cuando se trata de desvirtuar la presunción de inocencia, en especial a la luz de pruebas indiciarias; c) cuando se atañe "de alguna manera a la libertad como valor superior del ordenamiento jurídico"; d) o, en fin, cuando el juez se aparta de sus precedentes».

[420] MELÓN MUÑOZ, A.; MARTÍN NIETO, P. Y OTROS, *Memento Procesal Penal*, Madrid, Francis Lefebvre, 2017, p. 1668.

[421] Vid. STC 136/2000, de 29 de mayo, FFJJ 3.º y 4.º

[422] Vid. STC 12/2007, de 15 de enero FJ 2.º

El TS se ha pronunciado del mismo modo en numerosas ocasiones, en el sentido de que, tratándose de la restricción de derechos fundamentales, no es suficiente la intervención de un juez, sino que es exigible que tal intervención esté razonada y justificada de forma suficiente[423].

Con la reforma legal operada por la LO 13/2015, el apartado c) del art. 588 bis c LECrim, ha establecido que la motivación deberá darse en relación con el cumplimiento de los principios rectores establecidos en el art. 588 bis a. Con ello el texto legal pasa a exigir una necesidad de motivación respecto de los principios fijados como pórtico legal de las diligencias de investigación tecnológica, y que se concretan en los de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, lo cual consideramos plausible, dado que un examen con la debida justificación del cumplimiento de cada uno de ellos, es la única forma de garantizar el respeto a los derechos fundamentales así como a la presunción de inocencia.

Cabe señalar por último que, de no respetarse los principios constitucionales, siempre podría dudarse de la licitud de la medida, resultando en todo caso perjudicados, si la prueba fuese declarada ilícita, ya no solo los derechos de la víctima, sino los de toda la sociedad en su conjunto, dado que serían absueltas personas respecto de las que, en muchos casos, de no haberse producido la ilicitud de la prueba, no cabría duda de su culpabilidad. Por ello, en definitiva, no podrá prescindirse en la motivación realizada en el auto que acuerde la adopción de la medida de ninguno de los principios que rigen las diligencias de investigación.

2.5. Forma y periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

El presupuesto de la jurisdiccionalidad de la medida, no queda cumplido únicamente con el dictado de una resolución motivada, sino que es necesario un efectivo control posterior en relación con la ejecución de la misma.

[423] Vid. STS 454/2015, de 10 de julio. En esta resolución el TS declaró asimismo con abundante cita de sentencias del TC que «forman parte del contenido esencial del art. 18.3 CE las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga. Éstas deben explicitar, en el momento de la adopción de la medida, todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida pues, por la propia finalidad de ésta, la defensa no puede tener lugar en el momento de su adopción».

En este sentido, el apartado f) del art. 588 bis c.3 LECrim, obliga al juez instructor que fije en la resolución la forma (si se efectuará por escrito, telemáticamente, verbalmente, etc.) y la periodicidad con la que será informado acerca de las incidencias (parece razonable que se fije un plazo de quince días para intervenciones, como la del registro remoto de equipos informáticos, las cuales pueden prolongarse hasta tres meses), y en general de la evolución de la intervención, sin perjuicio de la facultad del juez de solicitar la información que estime oportuna en cualquier momento.

Se trata de un requisito que se hace necesario para el control de la medida. Sin embargo, de acuerdo con la opinión expresada en la Circular 1/2019 de la FGE, «la simple omisión no necesariamente afecta a la validez de la medida si ha existido efectivo control judicial»[424].

2.6. Finalidad perseguida con la medida

La obligación de dejar constancia en el auto judicial de la finalidad de la medida, de conformidad con el apartado g) del art. 588 bis c.3 LECrim, forma parte de la justificación del cumplimiento del principio de proporcionalidad. En este sentido, cabe recordar que, para el cumplimiento de este fundamental principio, el resultado perseguido con la restricción del derecho fundamental, es uno de los parámetros a tener en cuenta para ponderar los intereses en conflicto, es decir, para determinar si el sacrificio de los derechos e intereses afectados no es superior al beneficio que de su adopción resulte para el interés público y de terceros (art. 588 bis a.5 LECrim).

Por ello, en definitiva, de acuerdo con lo señalado por SANTOS MARTÍNEZ, «se trata de concretar qué se pretende lograr», pudiendo encontrarse entre las finalidades perseguidas, «el descubrimiento o la comprobación del hecho investigado, la determinación de su autoría, la averiguación del paradero de sus autores o la localización de los efectos del delito»[425].

---

[424] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., p. 15.

[425] SANTOS MARTÍNEZ, A. M., «Examen de las disposiciones comunes de las medidas de investigación tecnológica», cit., p. 15.

2.7. Deber de colaboración de terceros

Ya nos ocupamos del sujeto obligado que llevará a cabo la medida, en el apartado anterior relativo a la solicitud de autorización judicial, al que nos remitimos[426].

Se hace necesario, sin embargo, realizar unas consideraciones en relación con la mención de dicho sujeto en la resolución judicial, dado que, en caso de estimarse necesario por el juez competente la participación de un sujeto concreto para llevar a cabo la medida, deberá consignarse en la resolución judicial, con expresa mención, cuando proceda, del deber de colaboración y de guardar secreto, bajo apercibimiento de incurrir en un delito de desobediencia [art. 588 bis c.3 h) LECrim].

En relación con el apercibimiento de poder incurrir en un delito de desobediencia, no es una cuestión pacífica, si nos encontramos ante una obligación o quizás una carga desproporcionada para unas personas que no se concretan en el texto legal.

A este respecto, algunos autores afirman, refiriéndose a la policía o fiscalía, «…que son estos sujetos públicos sobre los que recae la carga de la investigación y persecución de los delitos, sin que pueda depositarse sobre el tercero colaborador una carga que legalmente no tiene»[427].

Sin embargo, el Convenio de Budapest establece en el art. 19.4 que «cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2».

Por otra parte, no ha de olvidarse que el art. 118 CE, establece la obligación de prestar la colaboración requerida por los jueces y tribunales en el curso del proceso y en la ejecución de lo resuelto. En virtud de ello, estimamos que el deber de colaboración de terceros, se ajusta la legalidad constitucional, siempre que sea respetuoso con los

[426] Vid. supra apdo. I.1.1.4 de este capítulo, pp. 199-201.

[427] Vid. RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», cit., p. 16.

derechos fundamentales del tercero obligado, y se justifique dicha obligación como indispensable para el buen fin de la intervención.

3. Fuentes confidenciales y denuncias anónimas

Para concluir este apartado relativo a las formalidades que han de cumplirse en relación con la autorización judicial de la investigación, cabe hacer una breve mención a los casos en los que se insta una autorización judicial como consecuencia de una información obtenida de una fuente confidencial y aquellos en los que la información se recibe tras una denuncia anónima.

Por lo que respecta a las fuentes confidenciales, tal y como ha declarado el TS, son aquellas informaciones obtenidas por la Policía en la fase preliminar de sus investigaciones, tales como la colaboración ciudadana, sus propias investigaciones e, incluso, datos suministrados por colaboradores o confidentes policiales[428].

Aclara GIMENO SENDRA, que «el confidente policial es una persona perteneciente a círculos delictivos, que bien por propia iniciativa, bien por encargo de las autoridades penales, suministra información a las Fuerzas y Cuerpos de Seguridad en el marco de las primeras diligencias, guiado por el propósito de obtener beneficios económicos o procesales»[429].

En relación con las fuentes confidenciales, ha de destacarse en primer lugar que, conforme declaró la jurisprudencia del TEDH, es admisible de forma excepcional la utilización de estas informaciones, únicamente como medio de investigación, sin que puedan servir de base como prueba de cargo para una sentencia condenatoria[430].

---

[428] Vid. STS 1047/2007, de 17 de diciembre, FJ 3.º

[429] Señala el referido autor que «el recurso a la confidencia constituye una práctica forense habitual en todos los Estados y tiempos, pero, en el nuestro, sin cobertura legal», y añade que «su mayor problema reside en la ocultación de la identidad del confidente a fin de evitar, no sólo posibles atentados vengativos contra su persona, sino también no "quemar, mediante la revelación de su identidad, una fuente de información policial futura"». Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 355.

[430] En este sentido se pronunció la STEDH de 20 de noviembre de 1989, Caso Kostovski v. Paises Bajos, la cual declaró que «el Convenio no impide apoyarse, en el período de la instrucción preparatoria, en fuentes como los informantes anónimos; pero el uso posterior de estas declaraciones, como pruebas suficientes para formar una convicción, suscita un problema diferente. En el caso de autos, llevó a limitar los derechos de la defensa de manera opuesta a las garantías del artículo 6. De hecho, el Gobierno reconoce que la condena del demandante se fundó "de forma decisiva" en las declaraciones anónimas».

Por tanto, si el conocimiento de la comisión de un delito tiene su origen en una fuente confidencial, para justificar la medida deberá existir una previa investigación a los efectos de verificar la veracidad de la imputación[431], pudiéndose iniciar una investigación sobre la base de informaciones confidenciales anónimas, «siempre que sean razonablemente creíbles y a continuación se lleven a cabo diligencias de investigación tendentes a confirmar la sospecha, obteniendo datos indiciarios de que se está cometiendo o se va a cometer un delito»[432].

Del mismo modo, por lo que respecta a la denuncia anónima, se ha planteado la cuestión de si la misma, permite acordar la adopción de una diligencia de investigación restrictiva de derechos fundamentales. El TS se ha pronunciado en sentido negativo, declarando que una información anónima, no puede fundamentar por sí sola, una investigación que implique el sacrificio de derechos fundamentales[433], dado que, «solo la investigación policial encaminada a verificar en términos razonables la verosimilitud de lo denunciado anónimamente, puede justificar la intervención»[434].

II. Secreto de las actuaciones

Con la sencilla rúbrica «Secreto» dispone el art. 588 bis d, que «la solicitud y las actuaciones posteriores a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa». Lo más relevante de este precepto, ya no es tanto el hecho de que se ordene la tramitación en

[431] En la STS 661/2013, de 15 de julio, FJ 4.º se declaró la necesidad de la investigación policial tras la información confidencial para verificar la realidad de la imputación. En concreto y para el caso que se enjuiciaba se declaró que «en el presente caso, no estamos ni de lejos ante una mera información anónima. Hay una laboriosa tarea policial de depuración. Informaciones previas y pesquisas policiales posteriores para comprobar aquellas son dos vectores que confluyen y se complementan recíprocamente».

[432] Vid. STS 32/2014, de 30 de enero, FJ 1.º

[433] Vid. STS 1487/2005, de 13 de diciembre, la cual se refirió a la STS 416/2005, de 31 de marzo, en la que se declaró que «la existencia de una información anónima no puede considerarse, en principio, suficiente para restringir un derecho fundamental a personas que ni siquiera consta su mención nominativa en aquella, pues un anónimo no es por sí mismo fuente de conocimiento de los hechos que relata, sino que en virtud de su propio carácter anónimo, ha de ser objeto de una mínima investigación por la Policía a los efectos de corroborar, al menos en algún aspecto significativo, la existencia de hechos delictivos y la implicación de las personas a las que el mismo se atribuye su comisión».

[434] Vid. STS 181/2014, de 11 de marzo, FJ. 3.º Como curiosidad, cabe señalar que esta resolución matizó que «la razón de que no sirva la sola y mera denuncia anónima, la encontramos en el viejo brocardo "quien oculta el rostro para acusar, también es capaz de ocultar la verdad en lo que se acusa"».

pieza separada y secreta, sino el que se puntualice que ello lo será sin necesidad de que se acuerde expresamente el secreto de la causa.

Como dice MORENO CATENA «…sigue vigente la norma que ordena que toda actuación de la que resulte la imputación de un delito deberá ponerse inmediatamente en conocimiento de los presuntamente inculpados…»[435], mientras que, «…en aplicación del principio de especialidad, esta pieza separada secreta prevista en la ley se mantendría en tal condición, y operaría con sus propios plazos, independientes de las previsiones de secreto del sumario…»[436].

En realidad, lo que ha querido el legislador con este inciso, ha sido dotar de legalidad a una cuestión que ya había sido abordada jurisprudencialmente. En efecto, el TS ha tenido la oportunidad de pronunciarse sobre este asunto. Concretamente, en la resolución de un recurso, en el que por los recurrentes se invocaba indefensión por no haberles sido notificada la resolución que acordaba la adopción de la medida a pesar de no haber sido declarado el secreto del sumario, entendiendo que se vulneraban los arts. 302 y 118 LECrim, así como que el Juzgado de instrucción debió declarar el secreto de las actuaciones para que la medida fuese secreta. El TS resolvió el recurso en el sentido de que el secreto de la diligencia se ha de considerar como «elemento esencial implícito a la misma y presupuesto de su efectividad y utilidad»[437].

Otro problema radicaría en la circunstancia de que, una vez notificada la existencia del procedimiento penal al investigado, se acordase una medida de investigación tecnológica, planteándose entonces el interrogante relativo a si las medidas

[435] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 295.

[436] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 295.

[437] STS 704/2009, de 29 de septiembre, FJ 4.º en la que declaró igualmente que el secreto debe verse comprendido en la diligencia y no sólo por la necesidad inmanente de la propia diligencia «sino porque su notificación le privaría de practicidad a la misma, y uno de los condicionamientos de la medida injerencial es su utilidad, y el juez no puede contradecirse dictando una medida inútil, que por tal razón sería improcedente e inadecuada hasta el punto de arrastrar la nulidad de la misma y un instructor no dicta conscientemente una medida nula». Además por lo que respecta a la invocada vulneración de los arts. 302 y 118 de la LECrim declaró que la aplicación estricta de los arts. 302 y 118 L.E.Cr . «no atribuye el derecho a conocer el procedimiento, porque se dio un requisito (la adopción de una medida cautelar) pero no concurría el otro "imputación de un acto punible", lo que no puede hacerse sin conocer el resultado final de las escuchas o incluso valorando otros datos incriminatorios de la investigación. No teniendo, pues, el investigado la condición de denunciado, querellado o imputado ni estando personado en la causa carece del derecho a ser notificado de la medida investigadora adoptada».

de investigación tecnológica pueden acordarse o prolongarse en secreto, mientras dure el sumario ya incoado y notificado a los investigados.

Se trata de lo que doctrinalmente se ha denominado «derecho a no autoincriminarse» o dicho en palabras de SÁNCHEZ YLLERA, se trata de la cuestión sobre «los límites que el derecho a no autoincriminarse y a no declarar contra sí mismo deben poner frente a la actuación investigadora subrepticia de los agentes estatales, en caso de utilización de agentes encubiertos o captación tecnológica de las comunicaciones mantenidas por los ya imputados»[438].

Este es un asunto, que no ha sido desarrollado debidamente tanto doctrinal como jurisprudencialmente. No obstante, puede traerse a colación, la STC 145/2014, de 22 de septiembre, que se refirió a este problema[439], en un caso en el que se instalaron micrófonos ocultos en los calabozos donde un sospechoso permanecía detenido, donde partiendo de la declaración de que «la verdad no puede ser hallada en el proceso penal a cualquier precio sino que se encuentra limitada por el escrupuloso respeto a los derechos fundamentales», la referida sentencia determinó finalmente que las escuchas obtenidas entre los detenidos en los calabozos no eran ilegales por no estar regulada su prohibición, pero además porque no se está obteniendo la información de forma incorrecta, como sí lo sería si la Policía Judicial hubiera utilizado algún tipo de subterfugio para sonsacar información.

Como ya examinamos en su momento, conforme a las exigencias del principio de proporcionalidad, cuando el sacrificio de los derechos e intereses en conflicto no sea superior al beneficio que de su adopción resulte para el interés público y de terceros, deberán adoptarse las medidas de investigación necesarias para el descubrimiento de los delitos, sin que el derecho a no autoincriminarse pueda ser extrapolado a la restricción

[438] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art . 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., pp. 19-20.

[439] La STC 145/2014, de 22 de septiembre, FJ 6.º cita para referirse al derecho a la no autoincriminación con carácter general las SSTEDH de 17 de diciembre de 1996, caso Saunders c. Reino Unido; y 5 de noviembre de 2002, caso Alian c. Reino Unido, declarando la primera de ellas que «la finalidad del derecho a no autoincriminarse es proporcionar a un acusado la protección contra una coacción impropia por parte de las autoridades y evitar así errores judiciales y garantizar los fines del art. 6» y la segunda que: «El derecho a no autoincriminarse afecta en primer lugar al respeto a la voluntad de la persona acusada a permanecer en silencio y presupone que la acusación en un proceso penal busca probar el caso contra el acusado sin recurso a pruebas obtenidas por medios no previstos legalmente desafiando la voluntad del acusado».

de las medidas de investigación por el hecho de estar iniciada la instrucción y puesto en conocimiento del investigado.

Por ello, no compartimos las opiniones que postulan la extensión del derecho a este supuesto. Sin embargo, ello no justifica en modo alguno que la Policía Judicial pueda llevar a cabo actuaciones contrarias a las reglas de la buena fe, en cuyo caso, a nuestro juicio sí que entraría en juego el derecho, como por ejemplo en el caso que expone la citada STC, de que la Policía Judicial utilizase una tercera persona para sonsacar información al investigado.

Pero en todo caso, consideramos que no es admisible, que el derecho a la no autoincriminación pueda invocarse cuando se produzcan conversaciones espontáneas, no impidiéndose, por tanto, en estos casos, que pueda acordarse cualquiera de las medidas de investigación tecnológica cuando la instrucción está iniciada y notificada al investigado, siempre que tenga lugar antes del inicio de la fase de juicio oral. A ello puede añadirse que, teniendo el investigado conocimiento de su derecho al silencio, no se le puede eximir de la responsabilidad de lo que pueda decir de forma desinhibida.

Por todo lo expuesto, sin necesidad de mayores consideraciones, entendemos plausible la previsión legal de tramitar la medida de investigación en pieza separada y secreta con independencia del secreto del sumario, lo cual fortalece la seguridad jurídica, además de contribuir a una reducción de los recursos judiciales en aras a la necesitada agilización de la Administración de Justicia.

III. Destrucción de registros

Tal y como señaló el Consejo Fiscal de la FGE en su informe al Anteproyecto de Ley Orgánica que culminó con la reforma operada por la LO 13/2015, «de nuevo se aborda un tema que estando huérfano de tratamiento legislativo, precisaba una regulación»[440]. Efectivamente, en el ámbito de las escuchas telefónicas la jurisprudencia TEDH había dictaminado que la ley nacional, dentro de su contenido mínimo, debía

[440] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, *Informe 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 tecnológica*, 2015, p. 86, Consultado en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/INFORME_CF_MODIFICACIÓN_LECrim_23-01-2015.pdf?idFile=7c2cd525-01bf-4cc0-864a-29dc8ee0dae9, el 7 de marzo de 2018.

referirse a las circunstancias en las que se puede realizar el borrado o la destrucción, sobre todo tras un sobreseimiento o absolución[441], lo cual ha sido declarado igualmente por el TC[442].

En cualquier caso, con anterioridad a la previsión normativa, que ha tenido lugar con la LO 13/2015, el TS consolidó una jurisprudencia en virtud de la cual se debía proceder al borrado o eliminación de las grabaciones, impidiendo así cualquier uso gubernativo no autorizado en relación con el investigado o incluso con terceras personas implicadas o no en los hechos enjuiciados, lo que supondría un menoscabo de su derecho a la intimidad.

Así, la STS 293/2011, de 14 de abril, FJ 9.º, declaró que «si no se adoptan las necesarias cautelas, podría resultar posible el almacenamiento de una cantidad ingente de datos relativos a la actividad de numerosas personas, implicadas o no en hechos delictivos, que quedarían fuera del control directo y exclusivo de la autoridad judicial»[443].

Por su parte, la STS 565/2011, de 6 de junio, FJ 3.º, declaró que «…la legitimidad del sistema no excluye la necesidad de que, dada la naturaleza invasiva e incisiva del sistema, se refuerce la motivación de las resoluciones que autorizan este sistema y se adopten por los tribunales, además, algunas medidas encauzadas a la destrucción de las grabaciones una vez que ya no se precisan para operar probatoriamente en la causa»[444].

---

[441] Vid. STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España, apdo. 46, en la que se señalaba que la necesidad de dicha previsión normativa ya fue declarada en la STEDH de 24 de abril de 1990, caso Kruslin c. Francia.

[442] Vid. STC 49/1999, de 5 de abril, FJ 5.º

[443] La STS 293/2011 añadió que «el acceso a tales datos se ha producido solamente sobre la base de una autorización judicial emitida con la finalidad de proceder a la investigación de unos hechos concretos, y, con independencia de las cautelas y medidas de seguridad que se derivan del propio sistema, todo el material obtenido queda íntegramente a la exclusiva disposición de la autoridad judicial. Es por ello que los Tribunales en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar de oficio en sus sentencias la destrucción de las grabaciones originales que existan en la unidad central del sistema SITEL y de todas las copias, conservando solamente de forma segura las entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido».

[444] Vid. SSTS 207/2012, de 12 de marzo, FJ 6.º; 794/2012, de 11 de octubre, FJ 2.º; y 143/2013, de 28 de febrero, FJ 5.º

Consecuencia de esta doctrina jurisprudencial la FGE dispuso en la Circular 1/2013 que «los Sres. Fiscales deberán velar porque se destruyan en ejecución de sentencia las grabaciones originales…»[445].

Sin embargo, tal y como afirma MARCHENA GÓMEZ, estas resoluciones del TS no sirvieron para que en la práctica judicial se acordase la eliminación de esa ingente acumulación de información —a lo que añadimos que tampoco surtió efecto la orden emitida por la FGE a los Sres. Fiscales—, por lo que el legislador ha querido acabar con esa despreocupación a través de una fórmula legislativa que tiende a equilibrar el interés del Estado en su conservación y el del ciudadano afectado en su destrucción[446].

La LECrim establece en el apartado primero del art. 588 bis k LECrim, aplicable a todas las medidas de investigación tecnológica, que «una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo custodia del secretario judicial».

De este modo, en un primer momento el texto legal establece como consecuencia de la terminación del procedimiento, una vez firme esta, el borrado o eliminación de los registros originales que obren en poder de las FCSE, lo cual ha de ser ordenado por el tribunal en la propia sentencia, o en su caso en los autos de sobreseimiento libre o cuando se acuerde que la infracción penal ha prescrito.

En un segundo momento, y una vez transcurrido un plazo fijado legalmente, se deberá proceder igualmente a la destrucción de las copias conservadas en poder del letrado de la Administración de Justicia, disponiendo a tal efecto el apartado 2 del art. 588 bis k LECrim, que «se acordará la destrucción de las copias conservadas cuando 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».

---

[445] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., pp. 43-44.

[446] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 283.

Se ha planteado doctrinalmente la confusión que se produce al emplearse los términos «borrado y eliminación» en el primer apartado y el término «destrucción» en el segundo[447]. No obstante, consideramos que la mención legal de dichos términos no debe ofrecer mayores dificultades interpretativas, dado que, siendo aplicable el precepto a todas las medidas de investigación tecnológica, podría suceder que en la primera fase existan archivos informáticos respecto de los que únicamente proceda su borrado, o soportes como discos duros, DVD, o cualquier otro dispositivo de almacenamiento que deba ser eliminado o destruido, debiendo a estos efectos considerar equivalentes los términos «eliminación y destrucción».

Por otra parte, ha sido objeto de cierta controversia la previsión relativa a que el tribunal podrá ordenar la conservación de la información, siempre que a su juicio fuese precisa la misma, tal y como se establece *in fine* en el mencionado apartado 2 del art. 588 bis k LECrim, respecto de lo que, doctrinalmente, se ha señalado que, no obstante ser una norma precautoria, no tiene demasiado fundamento lógico[448] que el legislador no de criterio ni ponga límite alguno a esta evaluación judicial[449], así como que no se establezca un plazo máximo de conservación, lo cual está en contra de la finalidad del art. 588 bis k LECrim, que es justamente la contraria: que originales y copias se conserven únicamente por tiempo limitado[450].

En cualquier caso, compartimos la opinión de autores como MARCHENA GÓMEZ, que sostienen que la facultad del tribunal de conservar las copias únicamente debe referirse a los casos de sobreseimiento libre y sentencia absolutoria, señalando que resulta, con carácter general, de difícil aceptación y carece de justificación, que cinco años después de que la pena haya sido definitivamente ejecutada o cuando el delito o la

[447] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 31.

[448] Señala RICHARD GONZÁLEZ, que «lo que parece estar diciendo la Ley es que el Tribunal que decreta un sobreseimiento libre o una sentencia absolutoria puede decidir que las grabaciones que no han conducido a acreditar el delito sea por su falta de "criminalidad" o bien porque aun pudiendo tener valor han sido declaradas ilícitas deben conservarse "por si acaso". Esto suena a aquello tan conocido, por desgracia, de dictar sobreseimientos provisionales en lugar de libres respecto de causas que es evidente que no se van a reabrir por falta de indicios racionales de criminalidad». Vid. RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 276.

[449] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art . 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 23.

[450] GARCIMARTÍN MONTERO, R., «*Los medios de investigación tecnológicos en el proceso penal*», cit., p. 74.

pena hayan prescrito, pueda prevalecer el interés del Estado en conservar conversaciones de un encausado, cuando se trata de un material incriminatorio que ha sido desechado por el tribunal sentenciador y que ha agotado su funcionalidad en el proceso en el que ha sido objeto de valoración[451].

Sin embargo, dado que el legislador no ha regulado con claridad los casos en los que pudieran ser conservadas las copias, debemos indagar acerca de los supuestos en los que podrá ser acordada tal conservación, considerando que la ley debería haber contemplado los mismos, dejando en manos de la discrecionalidad de jueces y tribunales, únicamente si tales supuestos se cumplen, favoreciendo así la seguridad jurídica en una materia de tanta importancia donde están en juego los derechos fundamentales del acusado e incluso de terceras personas, principio de seguridad jurídica, que a nuestro juicio sufre cierto menoscabo al establecerse una fórmula tan intederminada como la ya mencionada: «…siempre que no fuera precisa su conservación a juicio del Tribunal».

Doctrinalmente se ha señalado que «el contenido de los derechos afectados y las exigencias de garantía y proporcionalidad, tantas veces expuestas, permite concluir que la excepción únicamente estará justificada cuando dicha información sea útil para el esclarecimiento de hechos delictivos distintos a los juzgados —conexidad—, o para determinar la participación en el hecho investigado de sospechosos no afectados por la resolución que al mismo le ha puesto fin»[452] o que «solo en el caso de que se tratara de una decisión de sobreseimiento libre de carácter parcial o de una sentencia absolutoria respecto de uno de los investigados, mas no para el resto, podría estar justificada la negativa judicial a la destrucción»[453].

A tales supuestos, podrían añadirse aquellos en los que como consecuencia de la intervención tecnológica se produjese un hallazgo casual que pudiera ser constitutivo de un delito independiente que no pudiera ser enjuiciado por conexidad, ante lo cual el juez

[451] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., pp. 285-286.
[452] SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», cit., p. 23.
[453] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 286.

ordenaría la conservación y remisión al juez competente del oportuno testimonio y de la copia conservada.

Como hemos dicho anteriormente, doctrinalmente se ha propuesto que igualmente se debería fijar el plazo por el que la información fuese conservada excepcionalmente por ser este el espíritu de la norma. Sin embargo, si nos atenemos a los casos que hemos indicado como únicos supuestos en los que se podrían conservar las copias, nos encontramos en todos ellos ante la necesidad de que por el juez que instruye el caso se continúe con la investigación o en su caso de que se remitan el testimonio de particulares necesario y copia conservada al juez competente, por lo que operarían los plazos generales de prescripción[454] en atención al principio de legalidad en relación con el *ius puniendi* del Estado.

En virtud de lo expuesto, consideramos que, *de lege ferenda*, en aras de la seguridad jurídica y en atención a los derechos fundamentales en juego —los derechos a la vida privada del art. 18 CE—, deben establecerse los supuestos que hemos mencionado[455] como aquellos en los que únicamente podrán conservarse las copias obtenidas como consecuencia de la diligencia de investigación tecnológica practicada, una vez que se dicte resolución firme que ponga fin al proceso.

Finalmente, cabe referirse al apartado 3.º del art. 588 bis k LECrim, de conformidad con el cual «los tribunales dictarán las órdenes oportunas a la Policía

[454] Dispone el art. 131 del CP lo siguiente:
«1. Los delitos prescriben: A los veinte años, cuando la pena máxima señalada al delito sea prisión de quince o más años. A los quince, cuando la pena máxima señalada por la ley sea inhabilitación por más de diez años, o prisión por más de diez y menos de quince años. A los diez, cuando la pena máxima señalada por la ley sea prisión o inhabilitación por más de cinco años y que no exceda de diez. A los cinco, los demás delitos, excepto los delitos leves y los delitos de injurias y calumnias, que prescriben al año.
2. Cuando la pena señalada por la ley fuere compuesta, se estará, para la aplicación de las reglas comprendidas en este artículo, a la que exija mayor tiempo para la prescripción.
3. Los delitos de lesa humanidad y de genocidio y los delitos contra las personas y bienes protegidos en caso de conflicto armado, salvo los castigados en el artículo 614, no prescribirán en ningún caso.
Tampoco prescribirán los delitos de terrorismo, si hubieren causado la muerte de una persona.
4. En los supuestos de concurso de infracciones o de infracciones conexas, el plazo de prescripción será el que corresponda al delito más grave.

[455] Estos supuestos se concretan en los siguientes: a) esclarecimiento de hechos delictivos distintos a los juzgados que guarden conexidad, b) determinación de la participación en el hecho investigado de sospechosos no afectados por la resolución que al mismo le ha puesto fin, c) continuación de las actuaciones respecto de otros investigados o acusados en los casos de sobreseimiento libre o sentencia absolutoria respecto de alguno de ellos, y d) necesidad de investigación de la posible comisión de un nuevo delito tras un hallazgo casual que no guardase conexidad.

Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados». El precepto no ofrece ninguna duda interpretativa, aunque son llamativas algunas opiniones doctrinales, tales como que «este precepto solamente puede comprenderse dentro de un marco de cierta penuria económica afectante a los órganos judiciales, pues, en puridad, la propia Administración de Justicia debería contar con los medios necesarios para ejecutar tal destrucción, sencilla por otra parte»[456], que «no deja de ser paradójico que la inicial suspicacia se convierta en confianza ciega en el momento de acordar la destrucción de una información tan sensible»[457] o que «nada garantiza, en cualquier caso, que se destruyan las copias entregadas a las partes»[458].

IV. La orden de conservación de datos como medida de aseguramiento

1. Naturaleza

Termina la LECrim el título VIII del libro II, con un capítulo, el X, dedicado a las «medidas de aseguramiento», integrado por un único precepto, el art. 588 octies, que se presenta bajo la rúbrica «orden de conservación de datos». Como puede apreciarse, este precepto se encuentra fuera del capítulo IV y, por tanto, regulado de forma independiente a las disposiciones comunes a las diligencias de investigación tecnológica, que hemos examinado en este capítulo.

Sin embargo, en nuestra opinión, se trata de una materia completamente afín a las disposiciones comunes, que sin mayores problemas podría haber sido incluida en el capítulo dedicado a las mismas, puesto que, como de forma muy acertada sostiene CABEZUDO RODRÍGUEZ, los medios de investigación tecnológica «han de combinarse con medidas aseguratívas que garanticen la existencia de los referidos datos e informaciones y su conservación íntegra, amenazada por la volatilidad que les caracteriza, sustrayéndolos a cualquier eventualidad ya fuera incontrolable o deliberada»[459], o como dice ARMENTA DEU «en clara conexión con la eventual

[456] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 32.
[457] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 286.
[458] VEGAS TORRES, J., «Las medidas de investigación tecnológica», cit., p. 22.
[459] CABEZUDO RODRÍGUEZ, N., «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», cit., pp. 52-53.

volatilidad de la información en muchas de las medidas a las que se ha hecho referencia y con la necesidad de cohonestar la urgencia de la situación y la necesidad (como principio rector de estas medidas) de obtener autorización judicial con carácter previo, se contempla la posibilidad de adoptar "medidas de aseguramiento"»[460].

De este modo, nos encontramos ante una medida de prevención, que tiene por objeto salvaguardar cualquier información almacenada en un sistema informático, habida cuenta de la inestabilidad, que caracteriza con carácter general, a los datos contenidos en el espacio virtual, y ello a fin de evitar la pérdida o modificación del que podría constituir relevante material probatorio, evitando así malograr la investigación[461].

En definitiva, y dicho de una forma más concisa, puede afirmarse que la orden de conservación de datos, es una medida preventiva, común a todas las diligencias de investigación tecnológica, que tiene como finalidad la protección de una fuente de prueba ubicada en un sistema informático de almacenamiento.

2. Contenido

De conformidad con el art. 588 octies LECrim, cualquier persona física o jurídica, podrá ser requerida por el Ministerio Fiscal o la Policía Judicial para «la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión», todo ello «con arreglo a lo dispuesto en los artículos precedentes», por lo que entendemos, que el citado precepto se erige como una disposición común a todas las medidas de investigación tecnológica. Además, conforme aclara la Circular 1/2019 de la FGE, se trata de una medida que

[460] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 206.

[461] En este sentido, se pronunció el preámbulo de la LO 13/2015, al señalar en su apartado IV que «por lo que se refiere a las diligencias de investigación tecnológica, la reforma contempla como medida de aseguramiento la orden de conservación de datos, cuyo fin es garantizar la preservación de los datos e informaciones concretas de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión. De este modo su posterior aportación como medio de prueba o, en su caso, su análisis forense no se verá frustrado por la desaparición, alteración o deterioro de unos elementos inherentemente volátiles».

«puede adoptarse en relación con cualquier delito, pueda o no calificarse como ciberdelito, siempre que se trate de la obtención de evidencias digitales»[462].

Debe reseñarse que el precepto recoge lo dispuesto en el art. 16 del Convenio de Budapest, que en su apartado primero dispone que cada parte firmante del convenio «adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación».

De forma distinta a lo previsto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (que conforme estudiamos en el capítulo I, establece la posibilidad de dirigir una orden a las compañías operadoras prestadoras de servicios de comunicación[463]), el precepto que nos ocupa dispone que el mandato para la conservación y protección de datos o informaciones concretas, podrá ser dirigido a cualquier persona física o jurídica[464].

A este respecto, cabe señalar que, conforme afirma RIOS PINTADO, que la orden de conservación puede ir dirigida a la conservación de cualquier género de datos informáticos que se encuentren a disposición del obligado[465], mientras que la Ley 25/2007, se refiere a la conservación de datos de tráfico. Se trata de una distinción que se tuvo en cuenta por el Convenio de Budapest, que al ocuparse de la conservación de

---

[462] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., p. 26.

[463] Vid. supra apartado III.4.4.2 y ss. del capítulo I, pp. 61-84.

[464] Señala MARCHENA GÓMEZ que «nace así otra categoría legal de sujetos obligados, no necesariamente vinculada a la prestación de un servicio de telecomunicaciones, que se asocia a la condición de sujeto en cuyo poder obre un sistema informático de almacenamiento y que nace a partir del requerimiento de conservación formulado por el Fiscal o los agentes facultados». Vid. MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 334.

[465] RÍOS PINTADO, J. F., «La Reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (Arts. 588 ter J y 588 octies de la Ley de Enjuiciamiento Criminal)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 19, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Rios Pintado.pdf?idFile=9bb2604a-0ca5-432c-8124-f51611957c7b, el 10 de junio de 2020.

datos informáticos, distingue respectivamente en sus artículos 16 y 17, entre «datos informáticos almacenados» y «datos sobre el tráfico»[466].

El art. 588 octies LECrim, prescribe que el requerimiento podrá efectuarlo el Ministerio Fiscal o la Policía Judicial, lo que obviamente no impide que también pueda efectuarlo el juez competente, estableciendo en el párrafo tercero que «el requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado 3 del art. 588 ter e».

Por tanto, el obligado podrá incurrir en un delito de desobediencia, en caso de no cumplir las obligaciones de conservación y protección de la información, así como de guardar secreto respecto de la orden encomendada.

De esta forma, se da cumplimiento a lo acordado en el Convenio de Budapest, que en el art. 16.2 dispone que cada Estado interviniente adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a los sujetos obligados a conservar y a proteger la integridad de los datos informáticos, mientras que el art. 16.3 establece que del mismo modo se adoptarán por los Estados las medidas necesarias para que los sujetos obligados mantengan en secreto sobre el procedimiento.

En otro orden de cosas, no se establece por el precepto, si quedan eximidas las personas dispensadas de la obligación de declarar por razón de parentesco o secreto profesional, si bien ha de interpretarse que las mismas no pueden ser obligadas, en el entendimiento que nos encontramos ante una medida de aseguramiento común a todas

[466] Asimismo, el Convenio de Budapest, al ocuparse en su art. 1 de la definición de los términos relevantes del convenio, establece la distinción entre unos y otros tipos de datos, al disponer que a los efectos del Convenio:
«... b) por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función; (…)
d) por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente».

las diligencias de investigación tecnológica, en las que si se acuerda la referida exoneración[467].

Señala a este respecto MARCHENA GÓMEZ, que si bien el art. 588 octies LECrim no contiene una regla de exclusión que limite el deber de colaboración en los casos de parentesco o secreto profesional, similar a la prevista para los dispositivos de almacenamiento masivo en el art 588 sexies c.5 LECrim, no encuentra obstáculo alguno «para atribuir plena vigencia a ese límite, tanto por la identidad sustancial con el supuesto allí regulado, como por la operatividad de la dispensa general que proclama el art. 416.2 LECrim»[468].

Sin embargo, existen opiniones como la de la Circular 1/2019 de la FGE, que entienden que, ante el silencio de la Ley en este apartado, ha de estimarse que no estarán exceptuados del cumplimiento de la obligación de conservación de datos, ni los parientes del investigado ni quienes resulten amparados por el secreto profesional, como podría ser el abogado del investigado.

Nos parece excesivo este criterio, dado que, aun siendo cierto el silencio guardado por la LECrim, hemos de tener en cuenta que el fundamento de la exención del deber de prestar colaboración en el ámbito en los registros informáticos —respecto de los que la orden de conservación de datos es una diligencia común—, es el mismo que el de la obligación de no declarar prevista en el art. 416.1 LECrim, que no es otro que el de la «no exigibilidad de otra conducta», con la finalidad de proteger las relaciones familiares proclamadas en el art. 39 CE, así como el derecho a la intimidad familiar consagrado con el carácter de fundamental en el art. 18 CE.

Y de forma similar, puede afirmarse en relación con el abogado, exento de la obligación de declarar conforme al art. 416.2 LECrim —siempre que exista constancia de que asiste al investigado—, justificándose la exención en el respeto al derecho fundamental del art. 24.2 CE a la asistencia de letrado, teniendo en cuenta, además, que el art. 542.3 LOPJ, reproducido por el art. 32.1 del Real Decreto 658/2001, de 22 de junio, por el que se aprueba el Estatuto General de la Abogacía Española, establece que

[467] Así, tanto para los registros de dispositivos de almacenamiento masivo, como para los registros remotos sobre equipos informáticos, se establece tal exención, respectivamente en los arts. 588 sexies c.5 y art. 588 septies b.2 LECrim.

[468] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 335.

«los abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos».

Por todo lo anterior, estimamos que lo expresado en este punto por la Circular 1/2019 de la FGE, podría considerarse inconstitucional, por lo que, teniendo en cuenta que, la orden de conservación de datos puede imponerse por la Policía Judicial y el Ministerio Fiscal, sin necesidad de autorización judicial, a fin de evitar posibles abusos, consideramos que tal criterio debería ser modificado por la FGE.

Finalmente, debe recordarse que, atendiendo a las reglas del principio de especialidad, proclamado como principio rector de todas las diligencias de investigación tecnológica en el art. 588 bis a.2 LECrim[469], la orden de conservación de datos, solo podrá efectuarse, en el marco de una investigación abierta por la posible comisión de un delito concreto[470], no procediendo ningún tipo de investigación prospectiva, que contravendría tal principio y frustraría la investigación.

En este sentido, si bien es cierto, que con la orden de conservación de datos no se vulnera en principio ningún derecho fundamental, no por ello, conforme señala RODRÍGUEZ LAINZ, la decisión de retención «habrá de entenderse ajena a un mínimo de justificación que la aparte del mero voluntarismo o arbitrariedad»[471].

En consecuencia, la LECrim debería establecer algún tipo de cautela para evitar los posibles excesos que pudieran cometerse al impartir órdenes a los ciudadanos, que para nada son comparables a las que se dan a las compañías operadoras para la conservación de datos de tráfico.

---

[469] Vid. supra, apdo. I.1 del capítulo III, pp. 144-154.

[470] En relación con esta cuestión, afirma RÍOS PINTADO que, al requerimiento de conservación, se le exige determinación y concreción, señalando que para evitar una decisión arbitraria, el mandato ha de producirse en el marco de una investigación. Vid. RÍOS PINTADO, J. F., «La Reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (Arts. 588 ter J y 588 octies de la Ley de Enjuiciamiento Criminal)», cit., pp. 19-20.

[471] RODRÍGUEZ LAINZ, J. L., «Sobre la Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales: La regulación de las medidas de investigación tecnológica», *Ponencias de formación continuada - Ministerio Fiscal*, 2015, p. 20, Consultado en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia Sr Rodriguez Lainz.pdf?idFile=b9f4cc67-da93-4aa5-8eee-1507857092b8, el 18 de abril de 2019.

Como dice MARCHENA GÓMEZ, «una cosa es tratar de dar respuesta a la inmensa volatilidad de esos datos y otra bien distinta es hacerlo otorgando un poder incontrolado a los agentes facultados que, si bien se mira, permitirá la consolidación de un sistema en paralelo de conservación y cesión de datos»[472].

En nuestra opinión, no existirían mayores problemas en obtener una autorización judicial para esta medida de aseguramiento, para la que podría establecerse, sin ningún obstáculo, un plazo prudencial que permitiese un adecuado estudio por parte del juez competente, así como la apertura de un procedimiento judicial, lo que impediría cualquier vulneración del principio de especialidad, todo ello sin perjuicio de establecer unos determinados supuestos de urgencia en los que la Policía Judicial o el Ministerio Fiscal podrían impartir la orden de conservación de datos.

Por ello, con base en todo lo anterior, realizaremos dos propuestas:

En primer lugar, aunque nuestra interpretación del precepto es clara, estimamos que, *de lege ferenda*, en aras de una mayor seguridad jurídica y con la finalidad de evitar actuaciones desproporcionadas, debería incluirse por el legislador en una próxima reforma, un segundo apartado del art. 588 octies LECrim, en el que se establezca la exención de la obligación de conservar los datos, de las personas dispensadas de la obligación de declarar por razón de parentesco conforme al art. 416.1 LECrim y de las que, de conformidad con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional.

En segundo lugar, consideramos que debería exigirse la necesidad de resolución judicial para la orden de conservación de datos, a fin de evitar cualquier riesgo de intromisión no permitida, sin perjuicio de establecer unos determinados supuestos de urgencia en los que la Policía Judicial podría impartir la orden de conservación de datos.

3. Plazo de conservación

En cuanto al plazo de conservación, el párrafo II del art. 588 octies LECrim, dispone que «los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días».

[472] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 332.

Se fija así, un plazo máximo en el que el sujeto obligado deberá conservar los datos o información concreta, que a diferencia del plazo de doce meses que se establece como máximo en la Ley 25/2007 para las operadoras de los servicios de comunicación, se fija en 180 días, siempre que se acordase la prórroga.

Aun cuando doctrinalmente no se ha considerado adecuado el plazo inicial y de prórroga, entendiéndose «desmesurado» por algunos autores[473] y por otros «claramente excesivo»[474], no compartimos esta opinión, ya que, de acuerdo con lo señalado por RIOS PINTADO, «el art. 588 octies lo que regula es una medida cautelar para impedir que se pierdan determinados datos, y ese riesgo que se pretende precaver no tiene por qué producirse precisamente cuando la investigación policial haya avanzado y se tenga una idea cabal de los hechos ejecutados y de la extensión de las informaciones a recabar»[475].

Así, teniendo en cuenta que en el momento de la orden de conservación, la investigación podría encontrarse en un momento inicial, siendo necesarias otras indagaciones policiales, o incluso paralelas medidas de investigación tecnológica, no nos parecen desproporcionados los plazos fijados por el legislador.

Por otra parte, ha de tenerse en cuenta que también en este caso, se han seguido las indicaciones del Convenio de Budapest, que en su art. 16.2 *in fine,* establece precisamente un máximo de noventa días para la conservación y protección de los datos, disponiendo que los estados pueden prever que la orden sea renovable.

Sin embargo, no es menos cierto, que el Convenio de Budapest, establece en su art. 15 la necesidad de supervisión judicial, cuando así lo exija la naturaleza del procedimiento de que se trate. En este sentido, en nuestra opinión, al igual que en la de otros autores[476], la orden de conservación de datos, exige cuando menos, un control

[473] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 332.

[474] RODRÍGUEZ LAINZ, J. L., «Sobre la Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales: La regulación de las medidas de investigación tecnológica», cit., p. 20.

[475] RÍOS PINTADO, J. F., «La Reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (Arts. 588 ter J y 588 octies de la Ley de Enjuiciamiento Criminal)», cit., p. 20.

[476] RIOS PINTADO sostiene que «hubiera sido necesario prever algún sistema de control de la actuación policial, de manera tal que la Policía tuviera que comunicar al juez o al Ministerio Fiscal, las ordenes de retención dictadas y los motivos que las hacen necesarias». Vid. RÍOS PINTADO, J. F., «La Reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (Arts. 588 ter J y 588 octies de la Ley de Enjuiciamiento Criminal)», cit., pp. 20-21. Por su parte,

judicial, con el objetivo primordial de vigilar el correcto cumplimiento de los principios rectores que han de regir toda diligencia de investigación.

Por todo ello, como adición a las propuestas ya efectuadas en este apartado dedicado a la orden de conservación de datos como medida de aseguramiento, añadiremos la necesidad de incluir la obligatoriedad del control judicial de esta diligencia de investigación, común a todas las medidas de investigación tecnológica.

RODRÍGUEZ LAINZ estima que «debería haberse establecido un deber de dación de cuenta que permitiera un control judicial de la decisión de retención para aquellos supuestos en que finalmente no se presentara la correspondiente solicitud a la autoridad judicial». Vid. RODRÍGUEZ LAINZ, J. L., «Sobre la Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales: La regulación de las medidas de investigación tecnológica», cit., p. 20.

CAPÍTULO V. LOS REGISTROS INFORMÁTICOS

I. Introducción

A lo largo de este trabajo, hemos analizado los distintos aspectos que conforman lo que podríamos denominar «la parte general» de las diligencias de investigación tecnológica. Su estudio se hacía necesario para poder llevar a cabo un análisis minucioso de cualquiera de tales medidas.

Efectivamente, han sido examinadas en los capítulos anteriores cuestiones generales como son: la incidencia de la investigación tecnológica en los derechos fundamentales a la vida privada, el desarrollo jurisprudencial de los requisitos constitucionales para su validez y las disposiciones comunes establecidas en la LECrim, tras su regulación legal por la reforma operada por la LO 13/2015, para todas las diligencias de investigación tecnológica.

Procede ahora, por tanto, entrar a examinar, dentro de lo que podríamos denominar «la parte especial» de estas medidas de investigación, las que son objeto de este trabajo; es decir, los registros informáticos. Se concretan en dos modalidades: los registros de dispositivos de almacenamiento masivo de información y los registros remotos de equipos informáticos.

Para ello, siguiendo la sistemática establecida en la LECrim —que regula respectivamente los dos tipos de registros informáticos, en los capítulos VIII y IX del título VIII del libro II—, nos referiremos a continuación, en primer lugar, a los aspectos comunes de ambas modalidades, aun con la reseña de puntales discordancias que no impiden su tratamiento conjunto. Finalmente, nos ocuparemos, en sendos apartados, de las particularidades propias de cada una de ellas.

Realizaremos su estudio de este modo, porque, de acuerdo con lo señalado por la Circular 5/2019 de la FGE, «el legislador ha optado por distinguir entre un registro estático, el de los dispositivos de almacenamiento masivo de información, y un registro dinámico, el registro remoto sobre equipos informáticos, que, si bien presentan numerosas notas comunes, también ofrecen aspectos singulares que invitan a su tratamiento independiente»[477].

[477] FISCALÍA GENERAL DEL ESTADO, *Circular 5/2019, sobre registro de dispositivos y equipos informáticos*, 2019, p. 3, Consultado en https://www.fiscal.es/documents/20142/282a82d1-da36-8e8d-4dbc-c1bc0f02c6f0, el 4 de junio de 2020.

II. Aspectos comunes

1. Finalidad de los registros de dispositivos de almacenamiento masivo y de los registros remotos

Aunque puede parecer una obviedad, el primer aspecto común de los registros de dispositivos de almacenamiento masivo y de los registros remotos, es que, en ambos casos, la finalidad de la medida consiste en obtener información que se encuentre en dispositivos informáticos o repositorios telemáticos de datos.

En efecto, tanto el art. 588 sexies a.1, como el art. 588 septies a.1 de la LECrim, se refieren respectivamente al «acceso de los agentes facultados a la información» y al «examen a distancia y sin conocimiento de su titular».

En cuanto a los dispositivos que pueden ser objeto de registro, la LECrim enumera, para las dos modalidades de registros informáticos, distintos tipos que, en todos los casos, podrían incluirse en un concepto amplio de dispositivo electrónico. Así, en el art. 588 sexies a, para los registros de dispositivos de almacenamiento masivo de información, se establecen como equipos que pueden ser objeto de registro «ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos». En el art. 588 septies a, para los registros remotos de equipos informáticos, se dispone que serán susceptibles del examen a distancia el contenido de «un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos».

Se trata de un elenco de instrumentos, que, en definitiva, tal y como señala LÓPEZ-BARAJAS PEREA, comprenden un concepto amplio que está sujeto a la evolución propia de los sistemas de comunicación y que «abarca todos aquellos instrumentos que incluyen entre sus funcionalidades la de servir de soporte para el almacenamiento masivo de datos»[478].

[478] LÓPEZ-BARAJAS PEREA, I., «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos», *IDP: Revista de Internet, Derecho y Política*, n.º 24, 2017, p. 71.

Siguiendo a DELGADO MARTÍN, este conjunto de equipos e instrumentos, puede esquematizarse en tres grupos[479]:

- Ordenadores: dispositivos que permiten el tratamiento automatizado de datos en ejecución de un programa o software.

- Instrumentos de comunicación telefónica o telemática: dispositivos que posibilitan la transmisión de datos (comunicación telemática) y/o de la voz (comunicación telefónica).

- Dispositivos de almacenamiento masivo de información digital: instrumentos que permiten el archivo de datos en formato electrónico (*computer data*).

A ellos hay que añadir los repositorios telemáticos de datos, nombre que el legislador ha dado a la denominada «nube» o «*cloud computing*», que consiste en la puesta a disposición de espacio digital ofrecido por las grandes compañías a sus clientes, pudiendo estos almacenar, en dispositivos propiedad de estas compañías, grandes cantidades de datos a los que pueden acceder a través de internet. Por tanto, los repositorios telemáticos de datos o *cloud computing*, pueden considerarse dispositivos de almacenamiento masivo, a los que no se accede de forma directa mediante un dispositivo informático, sino de forma telemática, es decir, a distancia[480].

2. Extensión de la medida

Una de las novedades de la LO 13/2015, que adquiere una especial relevancia, es la relativa a la extensión o alcance de la medida de investigación tecnológica, importancia que se ve incrementada al tratarse de los registros informáticos, donde se presenta el fenómeno del entorno virtual como aquel en el que convergen los distintos derechos a la vida privada.

Como explicamos, en general, para todas las medidas de investigación tecnológica[481], con esta previsión el legislador ha determinado la obligación del juez competente de especificar de forma motivada, la concreta información que se requiere

[479] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 368.
[480] No está de más señalar que, de conformidad con el DRAE, el término «tele-» es un elemento compositivo, cuyo significado es «a distancia».
[481] Vid. supra apdos. I.1.2.5 y I.2.4 del capítulo IV, pp. 205 y 212-214.

para culminar una investigación, sin que proceda el acceso a más datos que los estrictamente necesarios, evitando, de este modo, cualquier intrusión improcedente en la privacidad de la persona afectada.

La STS 342/2013, de 17 de abril, FJ 8.º, tras señalar que en esta materia no caben las interpretaciones extensivas ni la elasticidad como fuente inspiradora a la hora de delimitar los exactos términos de la autorización concedida, declaró que «nuestro sistema no ampara autorizaciones implícitas, ni mandamientos de intromisión en el espacio de exclusión que definen los derechos fundamentales que no estén dibujados con la suficiencia e indispensable claridad».

Asimismo, doctrinalmente, ciñéndose al ámbito de los registros informáticos, LÓPEZ-BARAJAS PEREA ha señalado que «el juez no puede limitarse a autorizar que se aprehenda todo el material informático que se encuentre sino, únicamente, el que tenga relación con la causa»[482].

Esta doctrina, acerca de la limitación en la ejecución de los registros informáticos, ha sido reconocida por el TEDH, que en algunas de sus resoluciones ha declarado vulnerado el derecho a la vida privada del art. 8 del CEDH, al haberse efectuado registros indiscriminados sobre todos los datos obrantes en los equipos informáticos. Entre ellas, puede destacarse la de 3 de julio de 2012, caso Robathin c. Austria, dado que, conforme explica RODRÍGUEZ LAINZ, lo determinante para declarar vulnerado el derecho, no fue el registro indiscriminado no autorizado —que igualmente hubiera supuesto la censura de la medida por su extralimitación como así sucedió en otros casos resueltos por el alto Tribunal europeo—, sino la falta de proporcionalidad de la injerencia, al no contener la resolución habilitante un razonamiento suficiente[483].

En cualquier caso, ello no ha de estar reñido con la posibilidad de que, en determinados supuestos más complejos, sea necesario un examen completo de los dispositivos, dado que, como correctamente afirma VELASCO NUÑEZ, «investigar supone

[482] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant Lo Blanch, 2019, p. 156.

[483] En relación con la jurisprudencia del TEDH sobre la extensión de la medida de injerencia en los registros informáticos, RODRÍGUEZ LAINZ realiza una reseña de diversas sentencias del alto Tribunal europeo. Vid. RODRÍGUEZ LAINZ, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», cit., pp. 33-38.

averiguar hechos punibles sobre hipótesis fácticas que pueden ensancharse o minorar, esto es, irse perfilando»[484] teniendo en cuenta, además, que, en determinadas ocasiones, la investigación supondrá «indagar actividades delictivas, muchas veces dinámicamente, en un claro sistema de progresión»[485].

Ahora bien, ha de precisarse, reiterando la doctrina del TEDH mencionada anteriormente, que sería contrario al principio de proporcionalidad, el acuerdo de registro de forma indiscriminada sobre todos los archivos digitales que se encontrasen en un ordenador, sin que se llevase a cabo en la resolución una adecuada ponderación de los intereses en conflicto. Es decir, que el posible sacrificio de tres derechos fundamentales, como son: la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal (que a su vez convergen en el fenómeno —que no derecho reconocido expresamente de forma legal— del entorno virtual, que puede describir detalladamente el perfil ideológico de una persona), no sea superior al beneficio que de su adopción resulte para el interés público y de terceros.

Esta ponderación, conforme ha declarado reiteradamente la jurisprudencia, ha de realizarse *ex ante*. No es posible, por tanto, la ratificación posterior de una intervención que inicialmente no hubiese respetado el principio de proporcionalidad, lo que, como estamos viendo ocurriría si no se determinase con precisión la extensión de la medida en el auto inicial.

La STS 77/2019, de 12 de febrero, FJ 2.º, con mención de otras resoluciones[486], ha declarado que «en los autos que restringen derechos fundamentales, el tipo de juicio requerido cuando aparece cuestionada por vía de recurso la existencia de los presupuestos habilitantes de la medida limitativa y la corrección jurídica de su autorización ha de operar con rigor intelectual con una perspectiva *ex ante*, o lo que es lo mismo, prescindiendo metódicamente del resultado realmente obtenido como consecuencia de la actuación policial en cuyo contexto se inscribe la medida

[484] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 1, 2018, p. 12, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[485] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 12.

[486] SSTS 974/2012, de 5 de diciembre; 83/2013, de 13 febrero; y 877/2014, de 22 diciembre.

cuestionada»[487], indicando igualmente que lo contrario, la justificación *ex post*, «equivaldría a la pura y simple derogación del artículo 11.1 de la Ley Orgánica del Poder Judicial e, incluso, de una parte, si no todo, del artículo 24 CE»[488].

Por otra parte, las previsiones establecidas legalmente en cuanto al alcance o la extensión de la medida, pueden considerarse reglas comunes a ambas modalidades de registros informáticos, por su carácter consustancial a la idéntica finalidad de los mismos, como es la obtención de pruebas digitales a localizar en equipos e instrumentos informáticos.

En este sentido, con carácter general, parece razonable la opinión puesta de manifiesto por la Circular 1/2019 de la FGE, al señalar que «cuando se trate del registro de dispositivos de almacenamiento masivo de información deberá indicarse, con precisión, si el registro se extenderá a todo el dispositivo y a toda clase de archivos o si quedará limitado a alguna parte del mismo; en los registros remotos sobre equipos informáticos deberá precisarse también el alcance y extensión de la injerencia en relación con las posibilidades que ofrezca la técnica de registro que se utilice»[489].

Por lo que respecta al registro de dispositivos de almacenamiento masivo de información, el art. 588 sexies c.1, dispone que la resolución del juez «… fijará los términos y el alcance del registro…».

Para el cumplimiento de este precepto, la Circular 5/2019 de la FGE ha señalado que «la delimitación del alcance del registro que debe hacer el juez tendrá una proyección tanto subjetiva como objetiva»[490]. En efecto, deberán precisarse los sujetos afectados por el registro, dado que, aunque lo normal es que la intervención se dirija únicamente al investigado, puede darse el caso de que el registro afecte igualmente a

---

[487] Argumenta la STS 77/2019. que un resultado obtenido mediante una aproximación extrajurídica e ingenua «no es el metro con el que se ha de medir la adecuación normativa de la injerencia. De otro modo, lo que coloquialmente se designa como éxito policial sería el único y máximo exponente de la regularidad de toda clase de intervenciones; cuando, es obvio, que tal regularidad depende exclusivamente de que éstas se ajusten con fidelidad a la Constitución y a la legalidad que la desarrolla».

[488] En relación con este último inciso, relativo a la posible vulneración del art. 24 CE, la STS 77/2019 cita la STS 926/2007, de 13 de noviembre.

[489] FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*», cit., p. 12.

[490] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 22.

terceros, cuando se trate de dispositivos compartidos o de los que sean titulares otras personas. En cualquier caso, lo más relevante a los efectos de determinar el alcance o extensión de la medida, es su delimitación objetiva[491].

Por tanto, el juez mediante una motivación respetuosa con los principios rectores (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad), deberá especificar los datos que resultan necesarios para la investigación. De este modo, aun cuando sea necesaria la aprehensión de todo el material informático**,** una vez que se practique el volcado y posterior registro, este deberá contraerse únicamente a los archivos digitales (voz, imagen, texto, audio, video o en su caso datos que revelen el momento de emisión o recepción de un mensaje, datos bancarios, de ubicación, etc.), que se especifiquen por el juez en el auto acordando la intervención.

Debe reseñarse que es esta una cuestión controvertida, que hará necesario un tratamiento más específico a la hora de analizar determinados aspectos en el próximo capítulo, referentes a la eficacia probatoria de las diligencias de registros informáticos, dado que la extracción de determinados archivos puede constituir un proceso de gran complejidad técnica[492], que hará necesaria la incautación de todos los dispositivos para que, posteriormente, sean examinados por la Sección de Informática Forense de la Comisaría de Policía Científica[493].

En estos casos, y ante las dudas que podrían generarse en cuanto a la cadena de custodia, autores como LÓPEZ-BARAJAS PEREA, han afirmado que deberían «arbitrase las medidas que garanticen la exclusión de la información que pueda afectar a datos

---

[491] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 22-23.

[492] A modo de ejemplo en relación con la extremada complejidad que puede suponer en algunos casos el registro de dispositivos informáticos, puede citarse la referencia que realiza VELASCO NÚÑEZ, referente a la intervención en un conocido caso de corrupción política seguido ante la Audiencia Nacional, en el que se ocuparon inicialmente 63 discos duros; 46 pen drives; 58 tablets y móviles y 13 DVD/CDs, que al clonarse dieron 43,5 terabytes de información. Vid. VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., pp. 10-11.

[493] LLORENTE VEGA, M. J., «Informática forense», en *Policía científica - 100 Años de Ciencia al Servicio de la Justicia*, Madrid, 2011, pp. 275-302, Consultado en http://www.interior.gob.es/documents/642317/1203227/Policía+Científica+-100+años+de+Ciencia+al+servicio+de+la+justicia+%28NIPO+126-11-081-7%29.pdf/b983385f-ec1c-48c0-a6fe-98ede304c2fc, el 13 de julio de 2019.

especialmente sensibles»[494]. En este sentido, la referida autora señala, a nuestro juicio de forma muy acertada, que pudiendo y debiendo utilizarse los avances tecnológicos para reducir el ámbito de la injerencia, «es posible diseñar un software que tenga por objeto exclusivo descifrar una comunicación telemática entre terminales móviles, garantizando que no se accede a ningún otro contenido alojado en el terminal e, incluso, a ninguna otra comunicación»[495], a lo que podemos añadir que, del mismo modo y en sentido inverso, podrían crearse aplicaciones informáticas mediante las que se garantizase el acceso únicamente a determinados contenidos digitales, impidiendo cualquier acceso a datos relativos a comunicaciones telemáticas.

Podemos adelantar a este respecto que, lo indicado anteriormente, unido a la creciente intervención de equipos e instrumentos informáticos en la investigación de los delitos, plantea, sin perjuicio de la existencia de la Sección de Informática Forense de la Comisaría de Policía Científica y de los informes periciales privados que fuesen aportados por las partes, la posibilidad de la creación de un cuerpo de informáticos forenses al servicio de la Administración de Justicia, con el paralelo establecimiento de un organismo encargado de la adecuada custodia de los dispositivos[496] cuando puedan contener archivos digitales que acrediten la comisión de delitos, este último con la finalidad de garantizar la plenitud de los datos, facilitando un informe pericial con todas las garantías, y ante todo asegurar el acceso controlado a los datos que puedan resultar limitativos de los derechos fundamentales a la vida privada.

En cuanto a los registros remotos sobre equipos informáticos, el art. 588 septies a.2 b LECrim) establece que la resolución judicial deberá especificar «el alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos relevantes para la causa…».

Así, de forma similar a la expuesta para los dispositivos de almacenamiento y mediante una resolución respetuosa con los principios rectores, deberán fijarse cuáles son los archivos que han de aprehenderse, remitiéndonos en lo esencial a todo lo que acabamos de exponer.

---

[494] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», cit., p. 156.

[495] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», cit., p. 156.

[496] De la existencia de un organismo encargado de la adecuada custodia de los dispositivos informáticos, nos ocuparemos en el capítulo VI, en el epígrafe dedicado a la cadena de custodia.

Al igual que dijimos anteriormente, podría plantearse la cuestión relativa a las dificultades en cuanto a la forma en la que deberá llevarse a cabo la aprehensión, excluyendo el acceso a los datos no necesarios para la investigación susceptibles de vulnerar derechos fundamentales, y ello dada la distinta naturaleza de ambos tipos de registro informático. En los registros remotos, obviamente, no es posible la incautación de dispositivos de almacenamiento para un examen posterior, sino que todo el examen, sin perjuicio de la descarga de archivos, ha de ejecutarse en tiempo real, es decir, mediante una interactuación desde el ordenador de los agentes policiales investigadores con el equipo informático investigado, que, necesariamente, debe estar conectado a la red internet o, en su caso, a una red privada, desconociendo el usuario de dicho equipo que se está llevando a cabo la investigación.

Realizaremos más adelante unas consideraciones de forma individualizada en cuanto a la forma de ejecución de la medida para cada una de las modalidades, en las que, *mutatis mutandis*, resulta de aplicación todo lo expuesto anteriormente.

3. Derechos fundamentales afectados

En el capítulo I nos ocupamos de los derechos fundamentales a la vida privada del art. 18 CE, abordando el estudio de los mismos, con carácter general, desde la perspectiva de la investigación tecnológica. Procede ahora referirnos a las particularidades que se derivan de la posible restricción de estos derechos fundamentales como consecuencia de los registros informáticos, habida cuenta de las especiales características que los definen y que los distinguen del resto de las diligencias de investigación tecnológica.

Como ya sabemos, los derechos fundamentales a la vida privada que pueden resultar limitados, son los derechos a la intimidad, secreto de las comunicaciones y protección de datos de carácter personal, de los arts. 18.1, 18.3 y 18.4 CE, los cuales constituyen un aspecto común a ambas categorías de registros informáticos, por cuanto independientemente de la forma de ejecución de estas, estimamos que los derechos mencionados podrían resultar vulnerados del mismo modo en ambos casos; es decir, practicando un registro de archivos digitales en un instrumento o equipo informático.

Cierto es que, en relación con el derecho al secreto de las comunicaciones, durante la ejecución de un registro remoto podrá intervenirse una comunicación telemática a través de cualquiera de los distintos tipos de conversaciones online

permitidos por las redes sociales en general, pero ello no impide el tratamiento conjunto de los derechos fundamentales afectados, dado que en los registros de dispositivos de almacenamiento, igualmente podría ser localizado un mensaje recibido vía correo electrónico o a través de redes sociales que se encontrase sin abrir y leer por el destinatario, en cuyo caso resultaría vulnerado el derecho al secreto de las comunicaciones.

De acuerdo con lo declarado por el TS, «el ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar —de hecho, normalmente albergará— información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones»[497].

En el mismo sentido, ha de tenerse en cuenta la declaración que, poco después, el TC realizó refiriéndose a los *smartphones*, al señalar que, «…la versatilidad tecnológica que han alcanzado los teléfonos móviles convierte a estos terminales en herramientas indispensables en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también a los derechos al honor, a la intimidad personal y a la propia imagen (art. 18.1 CE), e incluso al derecho a la protección de datos personales (art. 18.4 CE)»[498 y 499].

---

[497] Vid. STS 342/2013, de 17 de abril, FJ 8.º

[498] STC 115/2013, de 9 de mayo, en la cual añade que lo ya señalado «…implica que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento deba ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de la ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad».

[499] Aunque en esta sentencia el TC resuelve un recurso planteado en relación con unos hechos relativos al registro de un teléfono móvil y, por tanto, se refiere a la versatilidad tecnológica de los teléfonos móviles,

De acuerdo con ello, adquieren especial relevancia las reglas relativas a la precisión de la extensión o alcance de la medida, examinadas en el apartado anterior, al poder ser transgredidos derechos fundamentales que, tal y como vimos en el capítulo I, no tienen constitucionalmente el mismo grado de protección, circunstancia que se presenta especialmente entre los derechos a la intimidad y secreto de las comunicaciones[500].

En atención a todo ello, realizaremos unas consideraciones en relación con la posible transgresión de cada uno de los referidos derechos a la privada, como consecuencia de la ejecución de los registros informáticos.

3.1. Derecho a la intimidad

Aun cuando pueden resultar vulnerados otros derechos, como el secreto de las comunicaciones y la protección de datos de carácter personal, el primer derecho que puede resultar restringido como consecuencia de un registro informático, y el que más se identifica, sin duda, con la denominación que, bajo el nombre «derechos a la vida privada», se da a los derechos del art. 18 CE, no es otro que el derecho a la intimidad, pues es enorme la cantidad de datos relativos a la vida privada que, de una forma normal, conservan en la actualidad la gran mayoría de los ciudadanos en sus dispositivos informáticos.

El derecho a la intimidad puede situarse en un vértice superior en relación con los demás derechos a la vida privada. Así, de conformidad con lo afirmado por autores como RODRÍGUEZ LAINZ, la protección constitucional que se brinda al domicilio, las comunicaciones y los datos de carácter personal, prevista en los apartados 2 a 4 del art. 18 CE, es claramente gregaria, del derecho a la intimidad personal y familiar del apartado 1 del mismo precepto. Ello ha encontrado acomodo en una línea jurisprudencial que tuvo su punto de arranque en la STS 940/2012, de 27 de noviembre,

---

esta referencia se puede hacer extensiva a todos los dispositivos de almacenamiento, dado que se refiere a las «herramientas de recopilación y almacenamiento», y por tanto queda comprendida dentro del ámbito de los registros informáticos que nos ocupan en este trabajo. En cualquier caso, puede afirmarse que actualmente el *smartphone*, se está convirtiendo en uno de los más representativos dispositivos de almacenamiento de información.

[500] Vid. supra apdo. III.3.1 del capítulo I, pp. 32-38.

en la que se define al secreto de las comunicaciones como una manifestación concreta del derecho a la intimidad[501].

De este modo, por lo que respecta a los registros informáticos llevados a cabo en el marco de una investigación policial, el TC ha declarado que dentro del ámbito de la intimidad constitucionalmente protegido se encuentran «el cúmulo de la información que se almacena por un titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.)», añadiendo que «…además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano»[502].

Por su parte, el TEDH determinó que «no cabe lugar a dudas de que el acceso a los archivos del ordenador personal del demandante y la condena resultante constituyen una "injerencia de las Autoridades públicas" en el derecho a la vida privada del interesado. Una tal intromisión vulnera el Convenio si no se cumplen los requisitos del apartado 2 del art. 8. Se debe por tanto determinar si la misma estaba "prevista por la ley", basada en uno o varios de los fines legítimos respecto de dicho apartado y "necesaria, en una sociedad democrática"»[503].

Llegados a este punto, y a diferencia del derecho al secreto de las comunicaciones y el derecho a la protección de datos de carácter personal, podemos afirmar que, con la práctica de cualquier registro informático, siempre quedará afectado el derecho a la intimidad.

Es cierto, no obstante, que podrán darse distintos grados de injerencia, atendiendo a los concretos datos guardados por el investigado en el dispositivo, si bien esta circunstancia no es posible preverla mediante el necesario juicio de proporcionalidad que, *ex ante*, ha de realizarse por el juez competente, por lo que en ningún caso podrá considerarse que un registro informático constituye una injerencia leve en la intimidad, lo que, como veremos más adelante, hará que nos mostremos

[501] RODRÍGUEZ LAINZ, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», cit., p. 24.
[502] Vid. STC 173/2011, de 7 de noviembre, FJ 3.º
[503] Vid. STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España, apdo. 28. Esta sentencia fue dictada en virtud del recurso interpuesto ante el TEDH como consecuencia de la denegación de amparo por el TC en la Sentencia 173/2011, de 7 de noviembre, citada anteriormente.

críticos y, en todo caso, partidarios de una interpretación restrictiva en relación con los supuestos de intervención policial urgente.

3.2. Derecho al secreto de las comunicaciones

En el ámbito de los registros informáticos, para el examen de los casos en los que podría quedar vulnerado el secreto de las comunicaciones, debe distinguirse, en primer lugar, entre la intervención sobre equipos que se encuentren conectados a internet o a una red de telefonía, lo que ocurrirá cuando se realice un registro sobre un teléfono móvil u ordenador con acceso a internet, y aquellos casos en los que se examina la información contenida en un dispositivo de almacenamiento que no está conectado, como así sucedería, por ejemplo, cuando se registrase un disco duro externo.

En el primer supuesto, la vulneración de derecho podría producirse si se observasen por los investigadores los listados de números de llamadas realizadas o recibidas, así como las comunicaciones telemáticas que se produzcan en programas de correo electrónico, mensajería instantánea o conversaciones privadas llevadas a cabo a través de programas de redes sociales.

Nos debemos plantear nuevamente el tema de la extensión de la medida, y por tanto, si en la resolución habilitante han de entenderse incluidos los accesos a todos los datos o programas relacionados con comunicaciones telefónicas o telemáticas. Dicho de otro modo, si la autorización de acceso a tales datos o programas ha de entenderse implícitamente incluida en la resolución judicial.

Por nuestra parte, entendemos que no cabe tal posibilidad, principalmente por la necesidad de autorización judicial que preside la injerencia en el derecho al secreto de las comunicaciones en todo caso[504]. A ello hay que añadir que, de conformidad con el art. 588 ter a LECrim, la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el art. 579.1 LECrim, o delitos cometidos a través de instrumentos

[504] Únicamente con la salvedad de los supuestos previstos en el art. 588 ter d.3, esto es, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida, en cuyo caso deberá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, poniéndole en conocimiento inmediatamente o en el plazo máximo de veinticuatro horas, del juez competente, quien en un plazo máximo de setenta y dos horas revocará o confirmará tal actuación.

informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[505], no existiendo para el registro de dispositivos de almacenamiento masivo limitación alguna en cuanto a los delitos a investigar.

El texto legal debería incluir una previsión expresa en cuanto a la necesidad de que, en la resolución que habilite el registro de un dispositivo de almacenamiento masivo de información, se especifique, con una motivación respetuosa con las reglas expresamente establecidas para la interceptación de las comunicaciones telefónicas y telemáticas en los distintos apartados del art. 588 ter a, si se autoriza el acceso a aquellos programas o datos que supongan una restricción del derecho al secreto de las comunicaciones.

Por lo que respecta a los registros informáticos de equipos o instrumentos informáticos que no se encuentren conectados a una red de telefonía o a la red internet, es posible igualmente que el derecho al secreto de las comunicaciones resulte transgredido, lo que se pone especialmente de manifiesto en relación con el correo electrónico.

En efecto, tal y como vimos en el capítulo I, al estudiar la delimitación entre los derechos a la intimidad y secreto de las comunicaciones, concluimos como tesis más congruente que, con independencia de que un mensaje haya sido leído o una llamada haya finalizado, no lleva aparejada una desprotección del derecho al secreto de las comunicaciones en relación con los datos que han quedado almacenados o se han originado como consecuencia del proceso de comunicación, como podría ser el listado de llamadas efectuadas registrado en un teléfono[506]. Todo ello, sin perjuicio de los criterios jurisprudenciales relativos a si quedaría afectado el derecho al secreto de las comunicaciones o el derecho a la intimidad, una vez que los mensajes de correo electrónico han sido leídos por su destinatario.

En relación con esta cuestión, tal y como aclara MARCHENA GÓMEZ, teniendo en cuenta que en cualquier programa de gestión de correo electrónico se agolpan mensajes

[505] Los delitos establecidos en el art. 579.1 LECrim, por cuya investigación sería posible acordar la intervención de las comunicaciones telefónicas o telemáticas, son los siguientes:
1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo.
[506] Vid. supra apdo. III.3.1 del capítulo I, pp. 32-38.

recibidos y abiertos, no abiertos y eliminados sin abrir, «resultará mucho más seguro estimar que el acceso a esos mensajes, ya sean los que se hallen en el servidor pendientes de descarga como los que se encuentren almacenados en el ordenador del sospechoso, abiertos o no, requiere una resolución jurisdiccional ajustada a las exigencias constitucionales y legales que legitiman la injerencia en el secreto de las comunicaciones»[507].

A ello podemos añadir que los mensajes de correo electrónico incorporan en muchos casos un archivo adjunto de texto, audio o video, respecto del que no es posible saber si ha sido abierto por el destinatario, archivos adjuntos que forman parte del contenido de la limitación que impone el derecho al secreto de las comunicaciones.

En efecto, tal y como precisa ALONSO SALGADO, el específico análisis del correo electrónico «entraña más dificultades de las de inicio evidentes» y ello, por cuanto «más allá de las implicaciones de su intervención, deben precisarse los umbrales del concepto que identifica esta forma de comunicación»[508]. En este sentido, la Directiva 2002/58/CE del Parlamento europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, dispuso que por correo electrónico deberá entenderse «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».

Por otro lado, debe recordarse que, conforme ha declarado la STC 115/2013, de 9 de mayo, FJ 4.º, puede afectar al secreto de las comunicaciones el acceso a cualquier función del teléfono móvil que pudiera desvelar procesos comunicativos, lo que, de

[507] Señala MARCHENA GÓMEZ que «la doctrina constitucional sentada en la importante STC 70/2002 no puede entenderse sin conexión al supuesto de hecho que motivó el pronunciamiento del Tribunal Constitucional». En efecto, a diferencia de un correo electrónico, como añade el citado autor, «se trataba de discernir si la lectura y examen por un agente de la autoridad, sin autorización judicial, de una carta sin sobre hallada en el interior de una agenda de la persona detenida, podía considerarse vulnerador del derecho al secreto de las comunicaciones». Vid. MARCHENA GÓMEZ, M., «Dimensión jurídico-penal del correo electrónico», *Diario La Ley - Sección Doctrina*, n.º 6475, 2006, p. 19.

[508] ALONSO SALGADO, C., «Algunos elementos problemáticos de la intervención del correo electrónico como diligencia de investigación en el sistema penal español: Un camino de claroscuros», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, p. 126.

acuerdo con lo señalado por DELGADO MARTÍN, «puede extenderse a cualquier dispositivo electrónico»[509].

Por todo ello, consideramos, en línea con lo ya expuesto, que la intervención del correo electrónico, con independencia de la lectura previa de los mensajes por el investigado, ha de estimarse, *ex ante*, una injerencia en el derecho al secreto de las comunicaciones.

3.3. Derecho a la protección de datos de carácter personal

Como tuvimos la oportunidad de poner de manifiesto, al estudiar en el capítulo I el derecho a la protección de datos de carácter personal[510], y de conformidad con lo establecido por el art. 4.1 del RGPDUE, se entiende por «datos personales», toda información sobre una persona física identificada o identificable («el interesado»), considerando como tal «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Por su parte, nuestro TC, en la Sentencia 292/2000, de 30 de noviembre[511], FJ 6.º, definió lo que ha de entenderse por datos de carácter personal, al declarar que estos comprenden «cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal» es decir aquellos datos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».

Partiendo de esta premisa, parece muy probable que, con un registro informático en el que no se aplicasen en su ejecución de una forma estricta, las reglas que en orden

[509] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 126.
[510] Vid. supra apdo. III.4 del capítulo I, pp. 47-54.
[511] La citada STC fue citada en el apdo. III.4.3 del capítulo I, pp. 58-59.

al alcance o extensión de la medida hubiesen sido acordadas por el juez competente, podría resultar vulnerado el derecho a la libertad informática consagrado en el art. 18.4 CE. Ahora bien, acabamos de decir que «parece muy probable», sin que podamos afirmar que tal injerencia se produciría con seguridad, como sí lo hicimos en relación con el derecho a la intimidad.

Realmente, descendiendo a la práctica de los registros informáticos, no parece posible que resulte vulnerado el derecho a la protección de datos del propio investigado, si atendemos al concepto de datos de carácter personal indicado anteriormente, así como el contenido protegido por el derecho (que no es otro que el derecho a la autodeterminación informativa o *habeas data,* consistente en la facultad de cualquier persona para ejercer con independencia el control sobre sus propios datos personales).

Además, esta tesis se refuerza, si tenemos en cuenta que, de conformidad con los arts. 11.2.a) y 22.2 LOPD 1999[512], no será necesario el consentimiento del interesado cuando «la cesión está autorizada en una ley», así como que «la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad».

De este modo, consideramos que el acceso indebido, por no estar debidamente autorizado, a datos personales del investigado, supondría una injerencia en su derecho a la intimidad personal o familiar, pero no su derecho a la autodeterminación informativa, sin perjuicio de su derecho al acceso, rectificación, cancelación y oposición de los datos tratados con fines jurisdiccionales, de conformidad con lo dispuesto en los arts. 236 bis a 236 decies de la LOPJ[513].

[512] Los citados preceptos se encuentran vigentes hasta tanto no se trasponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Vid. Disposición Transitoria Cuarta de la LOPD 2018.

[513] Estos preceptos integran el capítulo I Bis del título III del libro III de la LOPJ, incorporados por la LO 7/2015, de 21 de julio.

Cuestión distinta sería el tratamiento de los datos vinculados a un proceso de comunicación, que, conforme fue examinado en el capítulo I[514], se integrarían dentro de la protección del derecho al secreto de las comunicaciones.

Y, por otro lado, también debe ser tratada de forma diferente la posible vulneración del derecho a la protección de los datos de terceras personas que pudieran encontrarse en los equipos o dispositivos informáticos registrados, dado que, dependiendo de la profesión del investigado, podrían localizarse bases de datos relativas, por ejemplo, a clientes, historias clínicas, procesos judiciales, integrantes de un equipo deportivo, etc. En estos casos, es donde se pone de manifiesto la necesidad de una protección del derecho a la autodeterminación informativa, y cobran nuevamente especial importancia las reglas sobre el alcance o extensión de la medida, por lo que estimamos que, dentro de la mejora legislativa que hemos propuesto en relación con esta materia, se incluyese una referencia a la protección del derecho a la protección de datos de terceros, quienes podrían, desde luego, ejercer los derechos de acceso, rectificación, cancelación y oposición, cuando los datos no fuesen necesarios para la investigación y su incorporación al proceso se encontrase debidamente motivada por la correspondiente resolución judicial.

En cualquier caso, debe reseñarse, por último, que no existen diferencias sustanciales, para todo lo que concierne a los registros informáticos, entre este derecho y el derecho a la intimidad, si tenemos en cuenta además que, conforme al art. 18.4 CE, el principal objeto del derecho a la protección de datos es garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En tal sentido ha de interpretarse la declaración jurisprudencial relativa a que los datos identificativos de un titular o de un terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones, sino en el marco del derecho a la intimidad personal, con la salvaguarda que puede dispensar la legislación referente a la protección de datos de carácter personal[515], por lo que, en lo que respecta a la autorización judicial para la práctica de las diligencias de registros informáticos, hemos de entender que el tratamiento de la protección de datos, no es sino una modalidad o extensión del derecho a la intimidad.

[514] Vid. supra apdo. III.4.4 del capítulo I, pp. 59-84.
[515] Vid. nota al pie n.º 117, en la que se cita la STS 247/2010, de 18 de marzo, p. 60.

3.4. Referencia al entorno virtual. Remisión

Por lo que respecta al entorno virtual, nos referimos al mismo en el capítulo I[516], al que nos remitimos, donde, no obstante la doctrina que propugna la existencia de un nuevo derecho al que se ha denominado «derecho al entorno virtual», pusimos de manifiesto que, para que podamos hablar de la efectiva existencia de un derecho, estimamos preciso un desarrollo legislativo del art. 18.4 CE, en el aspecto relativo al aprovechamiento por los órganos de persecución penal de los sistemas de almacenamiento y comunicación de datos digitales para la investigación y prueba de los delitos, que reconociese, por tanto, al «entorno virtual» como un nuevo derecho, del mismo modo que en su día se hizo en relación con el derecho a la protección datos de carácter personal, en el entendimiento de que la expresión del art. 18.4 CE «la ley limitará el uso de la informática», incluye el uso que de la misma pueda hacerse en la investigación del delito.

Cierto es que, el fenómeno del entorno virtual es una realidad indiscutible que, en lo que se refiere a las diligencias de investigación tecnológica, ha de ser tratada legalmente con los registros informáticos, por poder obtenerse con ocasión de los mismos datos de distinta índole que pueden dibujar un perfil de una determinada persona, que revelen su ideología, preferencias, o, en definitiva, un perfil altamente descriptivo de su personalidad.

Cabe preguntarse si, en caso de resultar desvelado dicho perfil personal, lo que realmente se está vulnerando es el derecho a la intimidad personal, o, sencillamente, el derecho a la vida privada proclamado como tal por el art. 8 CEDH.

Se afirma jurisprudencial y doctrinalmente, que el legislador ha otorgado a los datos reveladores del perfil personal del investigado un tratamiento unitario, configurando un derecho de nueva generación, y que, por tanto, el nuevo art. 588 sexies ha refrendado la doctrina del entorno virtual[517].

Sin embargo, no compartimos tales opiniones y estimamos que, de la reforma operada por la LO 13/2015, si bien se puede desprender un tratamiento unitario de los

[516] Vid. supra apdo. IV del capítulo I, pp. 84-92.
[517] Vid. notas al pie núms. 165, 167 y168, pp. 86-88.

datos que pueden encontrarse, no se puede afirmar que se esté reconociendo o refrendando la existencia de un derecho «al entorno virtual».

Lo que se ha producido con la referida reforma ha sido consolidar legalmente la necesidad de autorización judicial para un registro informático, pero no porque podría configurarse un perfil descriptivo de la personalidad e ideología del afectado, sino, básicamente, por existir el riesgo de que con los mismos se transgrediese el derecho al secreto de las comunicaciones, para el que, como ya sabemos, se exige en todo caso resolución judicial. Y asimismo, y aquí es donde puede entenderse conferido un tratamiento unitario a las distintas categorías de datos obrantes en un dispositivo informático, porque en ningún caso, en un juicio *ex ante* se podría hablar de injerencia leve sobre el derecho a la intimidad o el derecho a la protección de datos de carácter personal, sino de una restricción grave, que siempre, y con la salvedad de los supuestos de urgencia, exigiría autorización judicial, conforme a la jurisprudencia del TC.

De este modo, en nuestra opinión, cuando como consecuencia de la recopilación de diversos datos, pueda configurarse un perfil altamente descriptivo de la personalidad de su titular, se estaría vulnerando el derecho a la intimidad, o como hemos dicho, atendiendo al art. 8 CEDH, el derecho a la vida privada.

No cabe duda de que hay que proteger el fenómeno del entorno virtual. Pero tal protección irá encaminada a la preservación de la intimidad, secreto de las comunicaciones y a la libertad informática, hasta tanto no exista un desarrollo legal de la referida realidad. En tal sentido, se ha pronunciado la jurisprudencia menor, que, al referirse a la necesidad de la autorización judicial específica para un registro informático con independencia de la ya otorgada para la entrada y registro domiciliario, declaró que «de lo que se trata es, una vez reconocida la inviolabilidad del entorno digital como una manifestación del derecho a la intimidad, que ese reconocimiento tenga una trascendencia jurídica, que en este caso sería la habilitación específica»[518].

Se hace necesaria, por tanto, la autorización judicial. No por encontrarnos ante un derecho, que, como hemos tenido oportunidad de afirmar, debe tener un reconocimiento legal, sino porque puede quedar afectado cualquiera de los tres derechos a la vida privada. Por tanto, en primer lugar, siempre es necesaria la autorización cuando puede ser vulnerado el derecho al secreto de las comunicaciones; y, en segundo lugar, la

[518] Vid. SAP 8/2016, Sección 1.ª de Guadalajara, de 4 de abril, FJ 1.º

limitación del derecho a la intimidad nunca tendrá el carácter de leve, único caso en el que se ha autorizado la intervención policial directa, fuera de los casos de urgencia.

Entendemos que nuestra opinión viene avalada por la doctrina del TC. Este se ha mostrado especialmente proclive a poner límites a las posibilidades de análisis indiscriminado de la información contenida en dispositivos de almacenamiento masivo de datos, ante el alto riesgo de afectación de la privacidad de las personas afectadas, pero no ha llegado a pronunciarse claramente en favor de la existencia de un derecho al entorno virtual[519].

Por todo ello, hasta tanto no se produzca su reconocimiento legal, entendemos que con los registros informáticos realizados como consecuencia de la investigación de un delito y la consecuente intromisión en el entorno virtual de las personas investigadas, podrán quedar afectados los derechos a la vida privada; es decir, la intimidad, el secreto de las comunicaciones o la protección de datos de carácter personal. A ellos quedará reconducida la injerencia, y ello hasta tanto el pretendido derecho al entorno virtual no tenga un reconocimiento legal expreso.

4. El deber de colaboración de terceros

Los arts. 588 sexies c.5 y 588 septies b.2 LECrim imponen la obligación de facilitar la información que resulte necesaria para el buen fin de la diligencia, a cualquier persona que conozca el funcionamiento del sistema informático objeto de registro o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo.

MARTÍN RÍOS afirma que esta norma trata de dar una solución a aquellos casos en los que los agentes policiales en el curso de una investigación se enfrentan a información cifrada, en las que resulta necesaria una clave de acceso. La dificultad se incrementa cuando la contraseña se establece antes del inicio del sistema operativo o se ha procedido a la completa encriptación de un disco duro, llegando en algunos casos a convertirse en un problema irresoluble[520]. De este modo, debe distinguirse este deber de

[519] Así lo afirma RODRÍGUEZ LAINZ, mencionando la STC 173/2011, de 7 de noviembre. Vid. RODRÍGUEZ LAINZ, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», cit., p. 28.

[520] MARTÍN RÍOS, P., «La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información ¿un supuesto de autoincriminación?», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, pp. 149-150.

terceras personas ajenas a las prestadoras de servicios de la comunicación, del exigido a estas.

Esta obligación surgirá como consecuencia de la orden que tales personas reciban de las autoridades y agentes encargados de la investigación. Del texto legal se desprende con claridad que el mandato a terceras personas podrá ser impartido directamente por el Ministerio Fiscal o la Policía Judicial, sin necesidad de autorización judicial.

Los terceros afectados tendrán la obligación de guardar secreto acerca de las actividades requeridas, y podrán incurrir en un delito de desobediencia en caso de no facilitar la información.

Estas disposiciones no serán aplicables 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 art. 416.2 LECrim, no pueden declarar en virtud del secreto profesional. En el mismo sentido, cuando el suministro de la información por parte del tercero le suponga a este una carga desproporcionada, no estará obligado a colaborar.

La Circular 5/2019 de la FGE se refiere al establecimiento por el legislador de dos limitaciones al deber de colaboración: una subjetiva, que restringiría los sujetos de los que se puede demandar la colaboración, y otra objetiva, que exime del deber cuando la colaboración resulte especialmente gravosa[521].

En relación con la limitación subjetiva, y por lo que respecta a la exención de la persona del investigado del deber de colaboración, resalta MARTÍN RÍOS, a fin de evitar supuestos de autoincriminación, la importancia de que el mismo sea puntual y debidamente informado acerca de tal exoneración, ya que solo ese conocimiento permitirá el adecuado ejercicio de su derecho, afirmando igualmente que la presencia de su abogado incrementaría las posibilidades de que se facilitase adecuadamente dicha información[522].

---

[521] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 50.

[522] MARTÍN RÍOS, P., «La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información ¿un supuesto de autoincriminación?», cit., p. 157.

Por lo que respecta a la limitación objetiva, se concreta en aquellos casos en los que de las órdenes impartidas a terceros en virtud del deber de colaboración, pudiera derivarse una carga desproporcionada para el afectado, cuestión sobre la Circular 5/2019 de la FGE subraya la indeterminación del concepto[523].

De acuerdo con esta afirmación, consideramos que hubiera sido aconsejable una mayor concreción por parte del legislador. Se afirma, no obstante, en la Circular 5/2019 de la FGE, que el art. 19.4 del Convenio de Budapest utiliza un concepto equivalente, al referirse a la obligación de facilitar la información necesaria dentro de lo razonable, refiriéndose asimismo al informe explicativo del citado instrumento internacional ratificado por España, el cual cita como ejemplo de falta de racionalidad, los casos en los que «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»[524].

Con base en lo anterior, prosigue la FGE en la referida Circular, deberán valorarse las circunstancias concurrentes en cada caso concreto, si bien, en orden a evitar cualquier tipo de injerencia en la vida privada de terceras personas, el juez, además de la proporcionalidad de la medida, «deberá valorar, conforme a los criterios generales que se establecen en la LECrim, la proporcionalidad de la exigencia de colaboración», y por ello «habrá de justificar que el sacrificio de los derechos e intereses de la persona afectada no resulte superior al beneficio que para el interés público y de terceros resulte del cumplimiento de ese deber de colaboración»[525].

---

[523] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 51.

[524] Además del referido supuesto señalado por el informe explicativo del Convenio de Budapest, la Circular 5/2019 de la FGE afirma que se podrían añadir aquellos casos en los que, por ejemplo, la facilitación de información supusiera desvelar secretos industriales que pudieran perjudicar una actividad empresarial del afectado, como resultaría de facilitar información sobre los sistemas de seguridad de un determinado teléfono o dispositivo informático. Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 51.

[525] Como ejemplo de juicio de proporcionalidad, en el que deberán ceder, de ordinario, los intereses particulares de la persona requerida, la Circular 5/2019 se refiere a los casos de delitos especialmente graves, en los que esté comprometida la vida de alguna persona o la seguridad pública (como ocurriría en los delitos de terrorismo). Por el contrario, deberán valorarse con mayor intensidad los intereses del requerido, cuando se trate de delitos de menor importancia o cuando los datos que el registro pueda proporcionar a la investigación no sean especialmente determinantes. Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 51-52.

Sin embargo, no ha sido tenido en cuenta que, como hemos expresado anteriormente, la orden podría ser dada directamente por la Policía Judicial, por lo que cabe la posibilidad de que el mandato se imparta sin una debida atención a los criterios de proporcionalidad mencionados. Ello nos lleva a estimar la necesidad de que sean concretados legalmente los casos en los que, por suponer una carga desproporcionada, no será posible exigir la información a terceras personas, quedando en tales casos supeditada la emisión de la orden al juicio de proporcionalidad que, motivadamente, deberá reflejar en la correspondiente resolución judicial el juez competente.

Por otra parte, resulta paradójico que la referida limitación objetiva únicamente se establece para los registros de dispositivos de almacenamiento masivo en el art. 588 sexies c.5 LECrim, pero no así para los registros remotos de equipos informáticos en el art. 588 septies b.2 LECrim, en el que nada se expresa acerca de no ser posible la petición de información cuando de ello se derive una carga desproporcionada. Ello podría permitir determinados excesos en la investigación, por lo que consideramos oportuna, *de lege ferenda,* la misma incorporación al texto legal que acabamos de mencionar anteriormente.

Finalmente, cabe señalar, como expusimos en el capítulo anterior dedicado a las disposiciones comunes a todas las diligencias de investigación tecnológica, que ha sido objeto de cierta controversia el hecho de si nos encontramos ante una obligación o quizás una carga desproporcionada para unas personas que no se concretan en el texto legal[526].

En relación con ello, cabe recordar que, atendiendo a lo dispuesto en el ya citado art. 19.4 del Convenio de Budapest así como a la obligación impuesta por el art. 118 CE de prestar la colaboración requerida por los jueces y tribunales en el curso del proceso y en la ejecución de resuelto, el deber de colaboración de terceros se ajusta a la legalidad constitucional siempre que sea respetuoso con los derechos fundamentales del tercero obligado, y se justifique dicha obligación como indispensable para el buen fin de la intervención.

[526] Vid. supra apdo. I.2.7 del capítulo IV, pp. 216-217.

5. Afectación de terceras personas

5.1. Planteamiento de la cuestión

En consonancia con lo afirmado por LÓPEZ-BARAJAS PEREA[527], los principios de especialidad e idoneidad imponen una delimitación subjetiva de la injerencia estatal que excluya las intervenciones prospectivas o de límites difusos, y aunque la regla general se centra en la persona sometida a investigación, el legislador de 2015 ha dispuesto expresamente que podrán acordarse las medidas de investigación tecnológica, aun cuando afecten a terceras personas.

Tanto la jurisprudencia del TC como del TS ya habían puesto de manifiesto que la normalidad de un acto jurisdiccional de injerencia, no puede ser cuestionada por la circunstancia de que el terminal investigado no sea titularidad del investigado[528]. Por otra parte, esta regulación constituía una necesidad que ya fue puesta de manifiesto por la STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España, al declarar que para cumplir el requisito de la previsibilidad de la ley se requiere que la legislación interna incluya la definición de las categorías de personas sobre las que se ha de adoptar la medida.

La incorporación legal de esta posibilidad, se ha producido mediante una norma de carácter general, el art. 588 bis h LECrim, que dispone que las medidas de investigación tecnológica podrán afectar a terceras personas, si bien «en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas». Sin embargo, resulta llamativo que la referida afectación a terceros, se ha producido para las intervenciones de comunicaciones telefónicas y telemáticas (art. 588 ter c LECrim) o para la captación de imágenes en lugares públicos (art. 588 quinquies a LECrim), pero no ha tenido lugar la misma para los registros informáticos.

---

[527] LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley», cit., p. 112.

[528] Vid. STS 48/2013, de 23 de enero, FJ 2.º, que, en relación con el criterio favorable a la posibilidad de que la persona investigada no sea la titular del terminal objeto de injerencia, se refirió a numerosos precedentes del propio TS y del TC, concretamente las SSTC 49/1999, 5 de abril; 299/2000, 11 de diciembre; 17/2001, 19 de enero; 136/2006, 8 de mayo; y SSTS 474/2012, 6 de junio; 759/1995, 3 de junio; 1181/2000, 3 de julio; 934/2004, 15 de julio; 463/2005, 13 de abril; 918/2005, 12 de julio y 1154/2005, 17 de octubre.

Ello nos lleva a plantearnos si era necesaria dicha previsión legal o, si por el contrario, la misma hubiera sido superflua por resultar directamente de aplicación el art. 588 ter c LECRIM.

5.2. Aplicación del art. 588 ter c a las diligencias de registros informáticos

Aun cuando en una primera aproximación podría inferirse la posible afectación de terceras personas con la ejecución de un registro informático y, por ello, que el legislador debería haber previsto dicha circunstancia incorporando una previsión en los arts. 588 sexies y septies LECrim, consideramos que la misma no es necesaria, por resultar de aplicación el art. 588 ter c, el cual regula la posible afectación a terceros en el ámbito de la intervención de las comunicaciones telefónicas y telemáticas.

Mantenemos este criterio, dado que lo determinante en relación con la afectación de terceros, es la posibilidad de que sea intervenido un equipo informático de otra persona distinta al investigado, y no tanto la afectación de los derechos a la vida privada de terceras personas, que siempre deberá ser tenida en cuenta por el juez al autorizar cualquier registro informático.

Por tanto, existiendo la posibilidad de que con estas diligencias de investigación pueda resultar vulnerado el derecho al secreto de las comunicaciones, conforme a lo ya estudiado, resulta de aplicación lo dispuesto en el art. 588 ter c LECrim, ubicado en el capítulo dedicado a la intervención de las comunicaciones telefónicas y telemáticas, más aún si tenemos en cuenta que la comunicación telemática es propia de dispositivos informáticos. Cierto es, no obstante, que hubiera sido conveniente, en el ámbito de los registros informáticos, una remisión a dicho precepto, a fin de evitar cualquier duda interpretativa[529].

El art. 588 ter c LECrim, permite la intervención de medios de comunicación telemática pertenecientes a una tercera persona. De acuerdo con lo afirmado por GONZÁLEZ-MONTES SÁNCHEZ, en este caso «se deberá de justificar de forma sólida la

[529] En este sentido se pronuncia BACHAMIER WINTER, al señalar que «en suma, si bien hay argumentos para aplicar por analogía lo dispuesto para las interceptaciones de comunicaciones, habría sido preferible que el legislador hubiera clarificado en qué condiciones puede procederse al registro remoto del ordenador de un tercero, y qué sucede si ese tercero no se encuentra en ninguna de las situaciones descritas en el art. 588 ter (c) LECrim». Vid. BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 12.

vinculación existente entre el tercero y el investigado así como las razones por las cuales se considera que los medios de comunicación de éste son los que sirven de base para la comisión del delito», y para el caso de no estar debidamente justificados estos extremos, «el instructor deberá garantizar escrupulosamente el derecho a la intimidad y al secreto de las comunicaciones del tercero no investigado en el proceso penal»[530].

Para que pueda acordarse la intervención del equipo perteneciente a un tercero, el precepto exige que se cumpla alguno de los siguientes supuestos:

1.º Que exista constancia de que el sujeto investigado se sirve de los equipos pertenecientes a la tercera persona para transmitir o recibir información.

2.º Que el tercero titular del equipo colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad.

Finalmente, dispone el art 588 ter c LECrim, que también será posible la intervención del equipo de un tercero, cuando este sea utilizado por el presunto o los presuntos sospechosos de forma maliciosa, sin el conocimiento de su titular. Nos encontramos en este caso ante la posibilidad de intervención del equipo informático de una víctima de un delito contra la intimidad de los previstos en el título X del libro II del CP[531]. En relación con este apartado, hay que tener en cuenta que el tercero es «víctima» del delito del art. 197 bis CP, pero, a su vez, su terminal puede estar siendo utilizado para la comisión de otros delitos. Por otro lado, asociado también al art. 588 ter c LECrim, debe traerse a colación lo dispuesto en el párrafo II del art. 588 ter b.2 LECrim, que dispone que «también podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad».

Por último, ha de tenerse en cuenta que el art. 588 ter i LECrim —que consideramos igualmente aplicable en el ámbito de los registros informáticos—, ordena la notificación a las personas intervinientes en las comunicaciones interceptadas, el hecho de la práctica de la injerencia, estableciendo igualmente que se les informará de

[530] GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», cit., p. 33.

[531] Concretamente el art. 197 bis CP castiga al que «por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo».

las concretas comunicaciones en las que hubiesen participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Y termina disponiendo este artículo, que si la persona notificada lo solicita, se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

Como dice SÁNCHEZ MELGAR, al referirse a este último apartado del referido precepto, en una opinión que compartimos, la posibilidad ofrecida al tercero afectado de poder pedir copia de la grabación o transcripción «acarreará numerosos inconvenientes prácticos», pero es igualmente cierto que «tal notificación puede servir de freno frente a cualquier exceso en la adopción de la medida»[532].

6. El acceso a repositorios telemáticos de datos o a otros sistemas informáticos

6.1. Aspectos generales

Tanto para los registros de dispositivos de almacenamiento masivo como para los registros remotos, la LECrim prevé la posibilidad de ampliar el registro, respecto del que inicialmente hubiera sido acordado.

Concretamente en lo que concierne a los dispositivos de almacenamiento, ha de tenerse en cuenta que el art. 588 sexies a LECrim, al ocuparse de los distintos equipos e instrumentos que pueden ser objeto de la intervención, menciona «el acceso a repositorios telemáticos de datos», mientras que el art. 588 sexies c.3 LECrim regula el régimen de esta eventual ampliación del registro, refiriéndose de forma genérica a datos almacenados en «otro sistema informático o en una parte de él».

Por su parte, en el ámbito de los registros remotos, el art. 588 septies a.3 LECrim, alude de igual modo a los datos almacenados «en otro sistema informático o en una parte del mismo».

De este modo, dentro de la expresión «otro sistema informático o una parte del mismo», el legislador está englobando, tanto los repositorios telemáticos de datos o

[532] SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», cit., p. 30.

cloud computing, como aquellos otros sistemas informáticos que se encuentren conectados al equipo investigado mediante una red privada, como así puede ocurrir en una red de ordenadores de una empresa o cualquier institución.

Con esta regulación, se ha incorporado a nuestra legislación lo previsto en el Convenio de Budapest, que en su art. 19.2 establece la obligación de los estados firmantes de adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, se pueda ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

El acceso a los repositorios telemáticos de datos, plantea la cuestión relativa a la necesidad de autorización judicial independiente de la inicialmente otorgada para el registro del dispositivo o dispositivos, ya que el legislador se refiere a la posibilidad de ampliación del registro cuando esta no hubiera sido prevista inicialmente.

De este modo, puede ocurrir que el registro de un repositorio telemático de datos o sistema informático concretos o, en su caso, ya que el precepto no se opone a ello, el registro genérico de cualquier sistema al que se pueda tener acceso desde el sistema inicial o que se encuentre disponible para este, se disponga inicialmente en la misma resolución que acuerde el concreto registro informático.

Pero también es probable que no se hubiera adoptado tal previsión en la resolución inicial. En este caso, de conformidad con los arts. 588 sexies c.3 y 588 septies a.3 LECrim, los agentes policiales deberán poner en conocimiento del juez las razones por las que se considera que los datos buscados se encuentran en otro sistema informático o en una parte de él, pudiendo en este caso el juez, de forma motivada, acordar la ampliación del registro.

Finalmente, cabe la posibilidad, de conformidad con lo dispuesto en el art. 588 sexies c.3 LECrim, de que, en caso de urgencia, la Policía Judicial o el Ministerio Fiscal puedan llevar a cabo la ampliación del registro en relación con los repositorios telemáticos u otros sistemas informáticos a los que se tenga acceso desde el sistema inicial, sin previa autorización judicial, si bien deberán informar al juez de la actuación realizada, de la forma en la que se ha efectuado y su resultado, inmediatamente, y en

todo caso dentro del plazo máximo de veinticuatro horas, pudiendo el juez, también de forma motivada, revocar o confirmar tal actuación.

El registro urgente sin autorización judicial es una posibilidad prevista para los registros de dispositivos de almacenamiento masivo y no así, de forma totalmente congruente con su naturaleza, para la diligencia de registro remoto de equipos informáticos. Por esta razón, nos ocuparemos de este problema más adelante, en el apartado dedicado a los supuestos de intervención policial urgente en los registros de dispositivos de almacenamiento masivo de información.

6.2. Registros transfronterizos

El acceso a repositorios telemáticos de datos o a otros sistemas informáticos no ofrece mayores problemas cuando los datos se encuentran en nuestro país. Sin embargo, la cuestión adquiere cierta dificultad cuando el material digital buscado se encuentra en un sistema que se sitúa en otro país. Son los llamados registros transfronterizos.

En estos casos, ha de acudirse de forma obligada a la normativa referente a la cooperación judicial internacional. A este respecto, si bien existen numerosos instrumentos bilaterales suscritos por España con otros países[533], el Convenio de Budapest tuvo en cuenta esta posibilidad, dado que el art. 32 del mismo establece dos supuestos en los que se podrá llevar a cabo un acceso transfronterizo a datos almacenados en un servidor informático.

El primero de tales casos se producirá cuando los datos buscados se encuentren a disposición del público (fuente abierta), en un servidor ubicado en uno de los países firmantes del convenio: el país que se encuentre investigando no precisará de autorización del país donde se encuentren ubicados los datos.

El segundo tendrá lugar cuando se trate de datos informáticos que no se encuentran a disposición del público, siendo necesario en esta ocasión, para poder

[533] Cabe reseñar que, fruto del convenio entre el Consejo General del Poder Judicial, la Fiscalía General del Estado y el Ministerio de Justicia, se creó el Prontuario de Auxilio Judicial Internacional, como una herramienta que pretende responder a las cuestiones más suscitadas en el quehacer diario de los operadores judiciales. Esta herramienta, si bien tiene una zona privada para que los tribunales puedan obtener los formularios correspondientes, permite, de forma pública identificar los convenios internacionales u otras normas jurídicas aplicables en materia de cooperación judicial internacional. Puede accederse al mismo en la página web http://www.prontuario.org/portal/site/prontuario.

acceder a los datos, obtener el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos.

En caso de no obtenerse dicho consentimiento, deberá acudirse a los mecanismos de cooperación internacional. A este respecto, de conformidad con los arts. 31.2 y 23 del Convenio de Budapest, la parte requerida dará respuesta a la solicitud aplicando «los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos».

En todo caso, debe tenerse en cuenta que la posibilidad de acceder a datos que se encuentren en una fuente abierta, lo es solamente respecto de las partes que han suscrito el Convenio de Budapest, como así lo indica la Guidance Note nº 3 emitida por Cybercrime Convention Committee (T-CY) de fecha 3 de diciembre de 2014[534].

Algunos autores han criticado el contenido del Convenio de Budapest, por no facilitar la investigación del delito cuando la información se encuentra en servidores ubicados en otro país, considerando que el art. 32 constituye una dificultad para una efectiva persecución del delincuente.

Así, VELASCO NUÑEZ afirma que no se alcanza a ver por qué el legislador europeo impone esa traba, señalando que la cooperación jurisdiccional a la que remite el Convenio podría ser inoperativa e ilusoria[535], añadiendo que para nada afecta al principio de soberanía ver una información en otro país, si técnicamente es posible hacerlo desde el nuestro y se cuenta con una autorización judicial, que es lo que efectivamente

[534] El Comité de la Convención sobre Ciberdelincuencia (T-CY) representa a los Estados Parte del Convenio de Budapest, teniendo como objetivo, de conformidad con el art. 46 del Convenio, facilitar el uso efectivo y la implementación del Convenio, así como el intercambio de información y la consideración de futuras enmiendas, todo ello conforme a lo expuesto en su página web https://www.coe.int/en/web/cybercrime/tcy. En este sentido, el Comité, en su octava sesión plenaria (diciembre de 2012), decidió emitir las «Guidance Notes» o notas de orientación, destinadas a facilitar el uso efectivo y la implementación de la Convención de Budapest sobre ciberdelincuencia, también a la luz de los desarrollos legales, políticos y tecnológicos, representando tales notas el entendimiento común de las partes con respecto al uso de la Convención. Puede accederse a las referidas notas en la web https://www.coe.int/en/web/cybercrime/t-cy-reports.

[535] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 23.

garantiza la protección de derechos fundamentales, entre los que, de cualquier forma, no se encuentra el de la soberanía[536].

URIARTE VALIENTE entiende que si la policía accede a datos desde el territorio español, aun cuando se encuentren alojados en un servidor ubicado en otro país, puede presumirse que la policía está actuando en España y que, por lo tanto, no existen problemas de jurisdicción. Señala que si se considera que, por ejemplo, un delito de pornografía infantil se ha cometido en nuestro país, aun cuando los archivos están en la nube, no deben ponerse obstáculos para considerar que nuestra jurisdicción alcanza el acceso a esos datos. Y añade que, si se tiene en cuenta que el reciente proyecto de Código Procesal Penal, preveía el recurso a la cooperación jurídica internacional para el acceso a los datos ubicados físicamente fuera del territorio español, mientras que el actual articulado guarda silencio sobre dicho extremo, no existe obstáculo alguno para la actuación directa por los órganos judiciales españoles con independencia del lugar donde se encuentren los archivos[537].

Finalmente, SÁNCHEZ RUBIO señala que la reforma de la LECrim de 2015 debería haber abordado este punto relativo a la cooperación judicial internacional para los registros informáticos y señala que de producirse una reforma en este sentido, debiera preverse la posibilidad de que el acceso a información contenida en sistemas de *cloud computing* se autorice por las autoridades judiciales españolas siempre que nuestros tribunales tengan jurisdicción para conocer de la causa que se está investigando[538].

Por nuestra parte, estimamos que si existe autorización del juez español, en el orden interno no debe existir problema alguno respecto a la validez de los datos obtenidos. Cuestión distinta es la posible responsabilidad internacional de nuestro Estado en virtud de lo establecido en el Convenio de Budapest.

---

[536] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 23.

[537] URIARTE VALIENTE, L. M., «25 cuestiones prácticas acerca de las medidas de investigación tecnológica en la LECrim», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 39, Consultado en https://www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada, el 2 de marzo de 2019.

[538] SÁNCHEZ RUBIO, A., «Los registros remotos sobre equipos informáticos: La investigación del "hacker legal"», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, p. 213, nota al pie n.º 11.

En cualquier caso, lo cierto es que existe un instrumento internacional en vigor para nuestro país que no puede obviarse en caso de una nueva reforma legal. Muy probablemente, lo acordado en el Convenio de Budapest pueda estar desfasado en la actualidad, por lo que estimamos necesario un esfuerzo de los Estados Parte a fin de que, mediante un nuevo Protocolo, se actualicen los contenidos, logrando así ampliar el ámbito de los registros de repositorios telemáticos transfronterizos, en la consideración de que, la realidad del año 2020 difiere mucho de lo que fue pactado en el año 2001.

III. El registro de dispositivos de almacenamiento masivo de información

El imparable auge de la informática en general ha permitido que grandes cantidades de información puedan ser almacenadas en los distintos dispositivos de almacenamiento existentes (discos duros, dvd, pen-drive, etc.)[539], así como en repositorios telemáticos de datos. Ello ha ocasionado que determinados hechos relevantes representados en documentos electrónicos, que podrían permitir la incriminación de los posibles delincuentes, se encuentren almacenados en dichos instrumentos informáticos, por lo que, para llegar a obtener la verdad material en la investigación de los delitos, en numerosas ocasiones no existe otra alternativa que la de llevar a cabo un registro informático a fin de obtener tales datos almacenados.

[539] Tal y como señala MARTÍN MARTÍN DE LA ESCALERA, de la redacción de los arts. 588 sexies a y b, se desprende que «la regulación del registro de dispositivos de almacenamiento masivo de la información no se dirige únicamente al establecimiento de las garantías necesarias para el acceso a lo que en sentido estricto constituye un dispositivo de almacenamiento masivo de la información, entendiendo por tales aquellos instrumentos informáticos cuya función y efecto es precisamente la de guardar o registrar información del usuario a largo plazo tales como discos externos, USBs, pendrives, CDs, DVDs, memorias digitales…etc. Por el contrario, tal normativa es de aplicación al acceso a cualquier tipo de dispositivo electrónico que tenga capacidad de guardar información, aun cuando sea de modo temporal y de forma secundaria a las funciones que constituyen su objetivo primario, tal sería el caso de los teléfonos móviles, tablets….etc En base a lo cual cualquier dispositivo o instrumento tecnológico que, sin tener porqué constituir en sí mismo un dispositivo de almacenamiento masivo, pueda contener o proporcionar datos de los que extraer las evidencias electrónicas relacionadas con la actividad delictiva puede ser objeto material de esta medida». Vid. MARTÍN MARTÍN DE LA ESCALERA, A. M., «El registro de dispositivos de almacenamiento masivo de la información», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, p. 5, Consultado en:
https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Martín Martín de la Escalera, Ana Mª.pdf?idFile=bf66c357-e4d4-4701-8a4d-83d6c103ebe5, el 7 de mayo de 2018.

Examinaremos en distintos apartados las particularidades de esta medida de investigación tecnológica.

1. Dispositivos incautados durante el registro domiciliario

El legislador de 2015, inicia la regulación del registro de dispositivos de almacenamiento masivo de información, distinguiendo entre los registros realizados con ocasión de un registro domiciliario, de aquellos que puedan llevarse a cabo tras la incautación de un dispositivo fuera del domicilio del investigado. Se trata de una cuestión que no siempre fue pacífica, en la que tuvo lugar un cambio de criterio jurisprudencial, tal y como expondremos a continuación.

1.1. Registros informáticos realizados con anterioridad a la LO 13/2015

Con anterioridad a la LO 13/2015, tuvo lugar una particular controversia, en relación a si era preceptivo el requisito de la jurisdiccionalidad para el registro de un dispositivo de almacenamiento masivo de información con independencia de la entrada y registro domiciliario.

No se planteaba si el dispositivo informático de almacenamiento, ya fuese un ordenador de sobremesa o una pequeña tarjeta de memoria, debía intervenirse —dado que tal intervención deviene preceptiva por imperativo del art. 282 LECrim, cuando existan sospechas de que la memoria del dispositivo informático pudiese contener pruebas del delito—, sino si era preceptiva autorización judicial para registrar su contenido.

Ya hemos dicho que para las injerencias en el derecho a la intimidad no siempre se hace necesaria la reserva jurisdiccional cuando no medie el consentimiento del afectado siempre y cuando se respete el principio de proporcionalidad y se trate de una intromisión leve. Pero precisamente por la copiosa cantidad de datos que pueden ser almacenados en los dispositivos informáticos —que pueden desvelar cuestiones relativas a las preferencias, ideologías y en general aspectos configuradores de la personalidad de un ciudadano—, aun cuando se respetase el principio de proporcionalidad no puede decirse que se trate de una injerencia leve, sino todo lo contrario, el registro supondría una grave intromisión en el derecho a la intimidad de cualquier persona. A ello hay que añadir la circunstancia de que, con el registro, podría quedar vulnerado eventualmente el derecho al secreto de las comunicaciones, habida cuenta de la posible existencia de

mensajes de correo electrónico, whatsapp, etc., que no hubieran sido abiertos y leídos por los afectados[540].

Con todo, es lo cierto que la jurisprudencia de TS se pronunció en algunas ocasiones permitiendo que la autorización para la entrada y registro domiciliario sirviese de soporte para el registro de dispositivos de almacenamiento. Así, por ejemplo, la STS 691/2009, de 5 de junio, FJ 3.º, declaró la legitimidad constitucional de la intervención y registro de un soporte de almacenamiento —concretamente un CD en el que figuraba la inscripción «ordenador de tráfico copia de seguridad»—, que almacenaba información que sirvió como prueba en el juicio, señalando que a la vista de la referida inscripción, conforme a la que el dispositivo contenía información oficial, no personal, «el acceso a su contenido no implica injerencia en datos personales o íntimos, sino que bien cabría calificarlo como documento en soporte diferente al papel y encuadrable en el concepto de que de tal da el art. 26 del Código Penal, y la lectura de su contenido al no afectar ni a la intimidad ni a la privacidad, no requería resolución judicial habilitadora al efecto».

En un sentido similar, cabe mencionar, la STS 256/2008, de 14 de mayo, FJ 2.º, en la que se estimó que no había nada que objetar a la intervención de unos ordenadores localizados en una entrada y registro domiciliario, al entender que el auto acordando la entrada y registro domiciliario habilitaba a la policía para la incautación del material informático que pudiera encontrarse, siendo con esa cobertura con la que se ordenó el análisis de los ordenadores que ya se encontraban a disposición del juzgado.

Esta doctrina quedó superada tras el reconocimiento del fenómeno del entorno virtual[541], respecto del cual ya existía alguna opinión doctrinal que propugnaba la judicialidad de la «inspección o recogida de dispositivos y soportes de almacenamiento

[540] Señala MARCHENA GÓMEZ que «habría que distinguir un primer grupo integrado por el correo electrónico ya enviado y recibido pero aún no leído —se hallen los mensajes en el servidor o descargados en el ordenador del destinatario—, así como por los mensajes todavía en proceso de transferencia» indicando que la intervención jurisdiccional de este primer bloque de mensajes quedaría sujeta al régimen general del secreto de las comunicaciones, con lo que se exigiría en todo caso el presupuesto de legitimación representado por la previa autorización judicial. Y se refería asimismo a un segundo bloque «compuesto por los mensajes de correo electrónico no enviados y los ya enviados, recibidos y leídos que se encuentren almacenados en el ordenador personal», el cual se regiría por las normas generales sobre limitación al derecho a la intimidad, con la consiguiente modulación de los términos de la injerencia. Vid. MARCHENA GÓMEZ, M., «Dimensión jurídico-penal del correo electrónico», cit., pp. 18-19.

[541] Vid. supra apdo. IV.1 del capítulo I, pp. 84-86.

masivo de datos»[542] siendo fundamental para el cambio de criterio algunas resoluciones del TC, entre las que cabe destacar la STC 173/2011, de 7 de noviembre, la cual tuvo en cuenta la jurisprudencia del TEDH para declarar que el registro de un ordenador debería estar legitimado por el consentimiento de su titular y en su defecto por resolución judicial[543].

Finalmente, el definitivo giro jurisprudencial y el establecimiento de la necesidad de autorización judicial para el registro de cualquier dispositivo informático, viene constituido por la relevante STS 342/2013, de 17 de abril, seguida por numerosas resoluciones posteriores, en la que partiendo de la base de que un ordenador u otro dispositivo de almacenamiento masivo de información no puede ser considerado una simple pieza de convicción[544], se declaró que cualquier acceso por la Policía Judicial a dicha información en el marco de la investigación de un delito, deberá contar con el presupuesto de una resolución judicial que motivadamente autorice la intervención[545].

---

[542] Vid. GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», cit., pp. 893-894.

[543] La STC 173/2011, de 7 de noviembre, menciona en su FJ 4.º la STEDH de 22 de mayo de 2008, caso Iliya Stefanov c. Bulgaria, refiriéndose a lo declarado en la misma del siguiente modo: «El registro de la oficina de un Abogado, incluyendo los datos electrónicos, equivale a una injerencia en su "vida privada", lesiva por ello del art. 8 del Convenio (§ 34). No obstante reconocer el Tribunal que concurría en este caso un objetivo legítimo (investigación penal por delito de extorsión) y que existía una previa autorización judicial, siendo así que "los registros del PC y las incautaciones deben, por regla general, llevarse a cabo en virtud de una orden judicial" (§ 39), razona que la expresada orden se había elaborado en términos excesivamente amplios, ejecutándose además de manera desproporcionada por la policía, por lo que se había afectado al secreto profesional, por cuanto "retiró todo el equipo del solicitante, incluyendo sus accesorios, así como todos los disquetes que se encontraban en su oficina", resultando que durante el tiempo que permaneció este material en su poder "ningún tipo de garantías existen para asegurar que durante el periodo intermedio el contenido completo del disco duro y los discos no fueron inspeccionados o copiados" (§ 42). De lo expuesto, parece desprenderse que cualquier injerencia en el contenido de un ordenador personal —ya sea por vía de acceso remoto a través de medios técnicos, ya, como en el presente caso, por vía manual— deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados».

[544] Esta afirmación relativa a que un dispositivo informático de almacenamiento no puede considerarse estrictamente como una pieza de convicción, ha sido tenida en cuenta por el legislador para la regulación llevada a cabo en la LO 13/2015, al señalar en su preámbulo que «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».

[545] Vid. nota al pie n.º 166, p. 87.

Estimamos que no se entienden muy bien las dudas que, inicialmente, tuvo la jurisprudencia, pues la analogía con el registro de papeles y documentos es evidente. Lo único que cambia es el tipo de soporte: papel o documento electrónico. La única justificación podríamos encontrarla en el carácter novedoso de las TIC.

En cualquier caso, es lo cierto que el requisito de la jurisdiccionalidad no tardó en imponerse, por la evidente injerencia que se produce en el derecho a la intimidad de las personas, así como, posiblemente, en el derecho al secreto de las comunicaciones, debiendo recordarse, que todo acceso a los datos digitales contenidos en un equipo informático, supondría una intromisión grave en el derecho a la intimidad, y nunca leve, por lo que siempre sería exigible el requisito de la jurisdiccionalidad.

1.2. La regulación actual

Tras la reforma operada por la LO 13/2015, para el supuesto de que 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, el art. 588 sexies a, establece la «necesidad de motivación individualizada», disponiendo que 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.

Cabe reseñar que el hecho de que se exija una motivación individualizada, no impide que se acuerde en la misma resolución que acuerda la entrada y registro, como así lo ha señalado VELASCO NUÑEZ[546], quien afirma que «la ley no impide hacerlo en una y la misma resolución si, como suele ocurrir, la previsibilidad de encontrar dispositivos tecnológicos en ese espacio reservado es razonable».

De este modo, en línea con esta última afirmación, ha de tenerse en cuenta que tal y como establece el texto legal, la previa autorización judicial será posible cuando sea previsible la aprehensión de dispositivos informáticos de almacenamiento. Por tanto, en aquellos casos en los que no exista tal previsibilidad, habrá que estar a lo dispuesto en el apartado 2 del art. 588 sexies a, que dispone que «la simple incautación de cualquiera

[546] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 6.

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»[547].

En consecuencia, de acuerdo con lo dispuesto en este último precepto, se infiere que en estos casos, en los que se encuentren equipos informáticos sin que se hubiera autorizado previamente el registro de su contenido, no existe ningún problema en que el juez autorice el registro del dispositivo o los dispositivos durante el mismo acto de la diligencia de entrada y registro, o bien pueda hacerlo posteriormente tras la intervención de los mismos.

2. Dispositivos incautados fuera del domicilio

Para el caso de que un dispositivo de almacenamiento masivo sea incautado fuera del domicilio del investigado, lo cual se producirá, principalmente, cuando tras la detención de un presunto delincuente le sea intervenido su teléfono móvil, ordenador portátil o cualquier dispositivo de almacenamiento como una micro-tarjeta de memoria, deberá ponerse en conocimiento del juez competente dicha intervención, a fin de que, en su caso pueda autorizarse el registro.

En relación con este tema, cabe mencionar, por resultar paradójico, habida cuenta de la antigüedad desde que se aplicó por primera vez la Cuarta Enmienda a la Constitución de los EEUU[548], que la primera sentencia del Tribunal Supremo de este

[547] Como señala la STS 864/2015, de 10 de diciembre, FJ 7.º «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».

[548] La Cuarta Enmienda a la Constitución de los EEUU fue promulgada el 15 de diciembre de 1791 con el fin de proteger a las personas de las investigaciones y aprehensiones arbitrarias de las fuerzas policiales, si bien fue aplicada por primera vez en un proceso judicial en la Sentencia del caso Jackson v. United States, de 13 de mayo de 1878, en la que se determinó que el secreto postal se encontraba protegido por la misma. Concretamente la Cuarta Enmienda reconoce que «el derecho del pueblo a la seguridad de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, corroborados mediante juramento o protesta, y describan expresamente el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o incautadas».

país que ha exigido una orden judicial para el acceso a la memoria de un teléfono móvil data de 2014. Concretamente se trata de la Sentencia dictada con fecha 24 de junio de 2014 en el caso Riley v. California, considerada como una *landmark ruling*[549], la cual determinó que «hay un elemento de omnipresencia que caracteriza a los teléfonos celulares pero no a los registros físicos, dado que antes de la era digital, las personas no llevaban un caché de información personal sensible con ellas a medida que avanzaban en sus actividades diarias» y señaló igualmente que «no es exagerado decir que muchos de los más del 90% de los adultos estadounidenses que poseen un teléfono celular mantienen en su persona un registro digital de casi todos los aspectos de sus vidas: de lo mundano a lo íntimo», todo ello para imponer la obligatoriedad de la reserva jurisdiccional al concluir finalmente que «antes del registro de un teléfono móvil incautado en un arresto, la policía debe obtener una orden judicial».

En España, cabe destacar que, con anterioridad a la reforma de 2015, para el registro de teléfonos móviles incautados de forma independiente a un registro domiciliario, el TS afirmó la legitimidad de la indagación en el teléfono móvil a fin de obtener el listado de llamadas, señalando que «esta diligencia no supone ninguna intromisión en el derecho a la intimidad, ya que han sido obtenidas en legal forma y sólo sirven para acreditar los usuarios de los teléfonos intercomunicados, sin entrar en el contenido de las conversaciones»[550].

Una vez llegada la tan esperada reforma de la LECrim, el vigente art. 588 sexies b, establece la obligatoriedad de la resolución judicial, al establecer que «la exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en

[549] Es el nombre con el que en EEUU se denomina a una «sentencia histórica» que servirá como precedente judicial.

[550] Vid. SSTS 1086/2003, de 25 de julio, FJ 3.º; y 1231/2003, de 25 de septiembre, FJ 8.º Esta última sentencia declaró asimismo en relación con el referido registro de un teléfono móvil que «no se trata de una intervención en el proceso de comunicación, ya entendido como transmisión de conversaciones, ni localización, al tiempo de su realización, de las llamadas efectuadas, de la identificación de usuarios, limitándose a la comprobación de unos números. Se trata de una comprobación de una agenda que contiene datos almacenados y que pudieron ser borrados por el titular o, incluso, bloqueados por el titular. Por otra parte, esa actuación no permite comprobar el destinatario de la llamada, ni el tiempo ni, en la mayoría de los supuestos las horas de su realización, tan sólo de una información obtenida de la memoria mediante una sencilla actuación sugerida por el aparato. Cumplidos los requisitos de proporcionalidad, no discutidos por el recurrente, la actuación policial se encuentra amparada por los preceptos de la Ley procesal (art. 287 y correspondientes informados por el art. 126 de la Constitución), toda vez que la investigación lo era por un delito grave y era necesaria para indagar los culpables de la conducta investigada».

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», añadiendo que «en tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos» y termina disponiendo que «si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización».

De este modo, el juez, tras una apropiada valoración de los principios de excepcionalidad, necesidad y proporcionalidad, determinará si, como dice el propio precepto, es indispensable el registro de los dispositivos intervenidos, lo cual se producirá cuando sea altamente previsible la localización de algún dato que se encuentre relacionado con el delito investigado o pueda valer para el esclarecimiento del mismo.

Obviamente, los agentes policiales serán los que, como consecuencia de las circunstancias de su investigación, deberán solicitar al juez el registro de los dispositivos intervenidos, exponiendo las razones por las que consideran que pueden ser localizados datos relevantes para la averiguación del delito, sin perjuicio de lo cual, el juez, bien tras dicha petición o por su propia iniciativa, deberá valorar la necesidad del acceso a la información.

Únicamente, en los casos que se consideren urgentes, los agentes podrán acceder a cualquier contenido de un teléfono móvil o cualquier otro dispositivo informático. No obstante, de todo lo relativo a las intervenciones urgentes, nos ocuparemos más adelante, en un apartado dedicado a estos supuestos.

3. Resolución judicial

En cuanto a la resolución judicial que el juez dicte a fin de autorizar la práctica de la diligencia, nos remitimos al estudio de la misma llevado a cabo, con carácter general, en el capítulo IV, dedicado a los aspectos procesales comunes a todas las diligencias de investigación tecnológica[551].

No obstante, puede reseñarse que el art. 588 sexies c.1, dedica unas líneas a la resolución judicial que autorice los registros de dispositivos de almacenamiento masivo, disponiendo que «la resolución del juez de instrucción mediante la que se autorice el

[551] Vid. supra apdo. I.2 del capítulo IV, pp. 207-217.

acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos», añadiendo que «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».

Se ocupa el precepto de establecer el contenido mínimo de la resolución, el cual, no obstante, comprende aspectos como la extensión o alcance de la medida, o cuestiones relativas a la prueba, que han sido o precisan ser examinados en otros apartados de este trabajo.

Finalmente, baste recordar que, en todo caso, será necesaria para su validez una suficiente motivación de la resolución y respeto a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

4. Inexistencia de tipos delictivos concretos

La LECrim no fija delitos concretos respecto de los que se pueda acordar la medida de registro de dispositivos de almacenamiento masivo, a diferencia de la de registro remoto de equipos informáticos y, por tanto, tal y como afirma VELASCO NUÑEZ, y teniendo en cuenta que la ley no excluye donde no ha querido expresamente excluir, pudiendo hacerlo, entendemos que no hay delitos excluidos de ser investigados a través de esta medida, a diferencia de lo que ocurre con los registros remotos de equipos informáticos[552].

Se trata de una cuestión que, a juicio de MORENO CATENA, resulta llamativa, puntualizando este autor que «pareciera que con independencia de la gravedad o de la naturaleza delictiva de los hechos que se estuvieran investigando, solamente a partir de la necesidad y de la proporcionalidad se concretaría la autorización de esta medida»[553].

En efecto, a la vista de la inexistencia de tipos delictivos en los distintos apartados del art. 588 sexies LECrim, y su inclusión en otras diligencias de investigación tecnológica, queda claro que, para cualquier delito, incluido un delito leve,

[552] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 5.
[553] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 301.

podría ser acordado un registro de un dispositivo de almacenamiento masivo de información.

Se plantea por tanto la cuestión de si el legislador debiera haber incluido un catálogo de delitos, o al menos un límite penológico para poder acordarse la práctica de la medida. En este sentido, MAESO VENTUREIRA afirma que «es criticable que el legislador no haya limitado a la investigación de delitos concretos la posibilidad de acordar una medida potencialmente tan invasiva de derechos fundamentales como la que nos ocupa», agregando que «ni siquiera ha excluido los delitos leves».[554]

Ciertamente nos encontramos ante una medida que supone una fuerte injerencia en los derechos a la vida privada, y en la que, a diferencia de otras diligencias como la intervención de las comunicaciones telefónicas o el registro remoto de equipos informáticos, no se incluye una previsión legal que coadyuve al cumplimiento del principio de proporcionalidad, mediante el establecimiento de unos tipos delictivos de cierta gravedad que permitan la adopción de una investigación tan invasiva, dejando en manos del criterio judicial, el cumplimiento del tan señalado principio rector de proporcionalidad.

Podríamos preguntarnos, ¿por qué es mucho más invasiva la diligencia de registros remotos que el registro directo de dispositivos de almacenamiento, como así se afirma mayoritariamente? La respuesta se encuentra en la circunstancia de que un registro remoto se realiza clandestinamente con carácter dinámico[555], mientras que el registro directo se hace con conocimiento del investigado sin que pueda examinarse en tiempo real su actividad en el equipo informático objeto de la intervención.

Así, debe reconocerse que, por las circunstancias citadas, el registro remoto tiene un grado de injerencia superior. Pero si se reflexiona sobre la cuestión, y sin perjuicio de la posible, pero no segura en todos los casos, mayor lesividad, pronto se observa que la intervención del dispositivo será siempre sorpresiva para el investigado y por tanto, no siempre y en todo caso ha de ser menos invasiva en los derechos a la vida privada, que

[554] MAESO VENTUREIRA, A., «Medidas de investigación tecnológica en el proceso penal tras la reforma efectuada por la Ley Orgánica 13/2015», en Pérez Machío, A.I., Goizueta Vértiz, J. (dirs.), *Tiempo de reformas: perspectiva académica y realidad judicial*, Bilbao, Servicio Editorial de la Universidad del País Vasco, 2017, p. 53.

[555] Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 52-53.

el registro remoto, debiéndose tener en cuenta que el registro puede afectar igualmente al derecho al secreto de las comunicaciones.

Por ello, consideramos que, *de lege ferenda,* debería establecerse un catálogo de delitos que de forma similar a otras diligencias de investigación, establecieran unos límites para llevar a cabo la medida con el fin de coadyuvar para el cumplimiento del principio de proporcionalidad, sin perjuicio de la motivación de la resolución judicial en relación con la ponderación entre la gravedad del delito, derecho sacrificado y el beneficio obtenido para el conjunto de la sociedad.

5. El consentimiento del titular

Como quiera que el registro de dispositivos de almacenamiento, a diferencia de los registros remotos, nunca se realiza con desconocimiento del investigado, cabe la posibilidad de que este preste su consentimiento a la práctica de la diligencia, no siendo necesario por ello, en estos casos, recabar la autorización del juez competente.

Así lo ha declarado desde tiempo atrás la jurisprudencia del TS, dejando sentado que «el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno»[556].

La misma jurisprudencia ha declarado que, en lo que respecta a la forma de prestación del consentimiento, este no precisa ser expreso, si bien con la salvedad de que, salvo casos excepcionales, la mera falta de oposición por parte del investigado no podrá entenderse como un consentimiento tácito[557]. A este respecto, cabe destacar que el TS admitió el consentimiento prestado, al permitirse expresamente la retirada de los equipos informáticos por parte de la Policía Judicial, entendiendo que ello implica una aceptación tácita del análisis de su contenido[558].

Asimismo, la jurisprudencia ha declarado que este consentimiento puede ser revocado en cualquier momento, si bien ha señalado que el derecho a la intimidad resultará vulnerado cuando la injerencia en el ámbito propio y reservado del sujeto, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la

[556] Vid. STS 97/2015, de 24 de febrero, FJ 2.º, donde se citan otras sentencias anteriores.
[557] Vid. STS 97/2015, de 24 de febrero, FJ 2.º
[558] Vid. STS 864/2015, de 10 de diciembre, FJ 6.º

conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida[559].

Por otra parte, ha de tenerse en cuenta que, si el investigado está detenido, será obligatoria la asistencia de su letrado para prestar el consentimiento, siendo necesario en todo caso que se le facilite información precisa sobre la finalidad y consecuencias de su otorgamiento así como de su derecho a no prestarlo, si bien no será necesaria la asistencia de letrado para la práctica del registro.

Consideramos que es aplicable en este punto a los registros informáticos la doctrina elaborada en relación con la entrada y registro domiciliario, de conformidad con la que, el consentimiento devendrá ineficaz cuando, encontrándose detenido el investigado, sea prestado sin la asistencia de su letrado, dado que «el detenido puede sentirse condicionado o presionado por dicha situación, incluso desconocer la posibilidad de negarse a autorizar la entrada, así como las consecuencias que pudieran derivarse de dicho acto», concluyéndose que «esta falta de asistencia del Abogado, constituye una vulneración del artículo 17.3 CE, con los efectos previstos en el artículo 11.1 LOPJ, esto es, la ineficacia total de dicho consentimiento y por tanto, la imposibilidad de conferir validez al resultado de la entrada y registro efectuado, sin perjuicio de la posibilidad de acreditar por otros medios, lo que se descubrió en el registro, cuya diligencia, debe ser radicalmente nula»[560].

Finalmente, conviene recordar, aun cuando después de lo dicho pueda parecer una cuestión obvia, que, de conformidad con lo establecido en el último párrafo del art. 588 sexies c.5 LECrim, las autoridades y agentes encargados de la investigación no podrán ordenar al investigado que facilite información para el acceso al equipo informático, por lo que, evidentemente, no tendrá la obligación de prestar el consentimiento ni tampoco la de facilitar claves de acceso.

6. Supuestos de intervención policial urgente

Dispone el art. 588 sexies c.4 que «en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen

[559] Vid. SSTS 864/2015, de 10 de diciembre, FJ 7.º y 287/2017, de 19 de abril, FJ 2.º, citando ambas las SSTC 159/2009, de 29 de junio, FJ 3.º y 196/2004, de 15 de noviembre, FJ 2.º

[560] Vid. por todas STS 550/2001, de 3 de abril, FJ 2.º y 234/2016, de 17 de marzo, FJ 1.º

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». Y termina disponiendo el precepto 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».

Sin embargo, tal y como afirma LÓPEZ-BARAJAS PEREA, no se concreta en la norma cómo se ha de determinar la urgencia del caso, ni tampoco se refiere a los casos en los que concurre un interés constitucionalmente legítimo[561]. Nos ocuparemos a continuación de estas cuestiones.

6.1. Acerca del interés constitucionalmente legítimo

Conforme ha señalado el TS, los derechos fundamentales a la vida privada no son absolutos, ya que en toda sociedad democrática existen determinados valores que, dependiendo de cada caso concreto, pueden justificar, con las debidas garantías, su limitación.

Esta jurisprudencia ha declarado que «entre estos valores se encuentra la prevención del delito, que constituye un interés constitucionalmente legítimo y que incluye la investigación y el castigo de los hechos delictivos cometidos, orientándose su punición por fines de prevención general y especial»[562].

Por tanto, puede afirmarse que la investigación de un delito, constituye un interés constitucionalmente legítimo que puede limitar los derechos fundamentales a la vida privada. Pero para que pueda producirse la restricción sin necesidad de autorización judicial, como venimos indicando, es necesario que concurra un supuesto urgente, lo que nos lleva preguntarnos cuando se da tal circunstancia como consecuencia de un registro informático.

[561] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», cit., p. 142.
[562] Vid. STS 714/2016, de 26 de septiembre, FJ 6.º

6.2. Justificación de los supuestos de urgencia que permiten la intervención directa de la Policía Judicial

Hemos mencionado anteriormente que la práctica de un registro informático, supondrá, cuando menos, una injerencia en el derecho a la intimidad, que nunca podrá considerarse leve, por lo que siempre se hará necesaria la autorización judicial.

No obstante, la LECrim ha permitido, conforme a lo dispuesto en el art. 588 sexies c.4, que en los supuestos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida, la Policía Judicial pueda llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado.

Ha de ponerse de relieve previamente, que la necesaria intervención del juez, para la autorización de una medida de investigación restrictiva de derechos fundamentales, también denominada «judicialidad o jurisdiccionalidad de la medida», no puede decirse que fuese una cuestión pacífica en relación con la intromisión en el derecho fundamental a la intimidad.

En efecto, a diferencia de las intromisiones en el derecho al secreto de las comunicaciones o la inviolabilidad domiciliaria, en las que los arts. 18.2 y 3 CE exigen la resolución judicial previa, no se proclama de igual modo desde el texto constitucional el mismo requisito de reserva jurisdiccional para la protección del derecho a la intimidad del art. 18.1 CE[563], lo cual suscitó cierta controversia doctrinal con anterioridad a la promulgación de la LO 13/2015.

Así, aun cuando la regla general, ya puesta de manifiesto en la STC 37/1989, era que la injerencia en el derecho a la intimidad exige resolución judicial[564], posteriormente la jurisprudencia constitucional estableció que la «urgencia» pudiese considerarse, en

---

563 Conforme afirma ORTIZ PRADILLO la entrada y registro domiciliario se permite sin autorización judicial en los casos de flagrancia (art. 18.2 CE) mientras que no siendo posible acudir a la flagrancia respecto de las injerencias en el secreto de las comunicaciones, el art. 18.3 exige en todo caso la autorización judicial, con la salvedad de los supuestos de intervenciones urgentes en los casos de delitos relacionados con la actuación de bandas armadas o elementos terroristas previstos en el art. 588 ter d.3.
ORTIZ PRADILLO, J. C., «Desafíos legales de las diligencias de investigación tecnológica», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, pp. 307-308.

564 La STC 37/1989, de 15 de febrero declaró en su FJ 7.º que la afectación del ámbito de la intimidad «es posible sólo por decisión judicial que habrá de prever que su ejecución sea respetuosa de la dignidad de la persona y no constitutiva, atendidas las circunstancias del caso, de trato degradante alguno».

determinados casos, un criterio a tener en cuenta por la Policía Judicial para ejecutar una medida limitativa leve del derecho fundamental a la intimidad. Así, por ejemplo, la STC 70/2002, de 3 de abril, FJ 10.º, declaró que «la regla general es que el ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad […] esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad»[565].

Estos pronunciamientos fueron criticados doctrinalmente, no por el hecho de permitirse una actuación policial en casos de urgencia, sino por la inconcreción del concepto de urgencia. Así, por ejemplo, ORTIZ PRADILLO afirmó que «legitimar tales actuaciones policiales bajo la genérica alusión a motivos de urgencia y necesidad […] resulta extremadamente escueta y confusa, y puede dar lugar a una interpretación fraudulenta de la legalidad»[566]. Asimismo, autores como ASENCIO MELLADO señalaron que «es ineludible que el legislador proceda con urgencia a desarrollar las normas imprescindibles para acotar el ámbito de la restricción de derechos por parte del Estado,

[565] Puede mencionarse igualmente la STC 115/2013, de 9 de mayo, FJ 5.º, en la que considerando que la intromisión en el derecho a la intimidad puede llevarse a cabo en supuestos de urgencia por parte de las FCSE sin necesidad de autorización judicial, declaró justificado el acceso a la agenda de contactos de contactos de un teléfono móvil habida cuenta de que se trataba de un caso urgente al haberse detenido a los presuntos culpables de un delito de tráfico de drogas, quienes emprendieron la huida al ser sorprendidos por los agentes de policía.

[566] Señalaba este autor que «bastaría detener al sospechoso bajo la excusa de un pretendido control de identidad en determinados lugares o establecimientos públicos, e incautarle su terminal de telefonía móvil para indagar sobre las llamadas efectuadas o recibidas, en vez de tener que solicitar la necesaria autorización judicial para recabar de las operadoras esos mismos datos de tráfico, con la consiguiente obligación de tener que explicitar ante el órgano jurisdiccional las sospechas (si acaso existen) sobre dicho sujeto y su presunta relación con los hechos investigados». Y añadía que «habría que delimitar con mayor detalle los supuestos en los que se entiende que existe tal urgencia, como por ejemplo, en aquellos casos en los que exista un peligro inminente para la vida, la libertad o la integridad física de las personas […] o cuando se trate de delitos flagrantes. De lo contrario, y sin el debido respaldo legal, corremos el riesgo de justificar posibles fraudes y abusos en las garantías de los derechos fundamentales en aras de una falaz eficacia en la persecución criminal». Vid. ORTIZ PRADILLO, J. C., «Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas», *La Ley Penal - Sección Jurisprudencia aplicada a la práctica*, n.º 75, 2010, p. 12.

estableciendo expresamente los requisitos que deben concurrir en todo caso y las correspondientes excepciones»[567].

Estas críticas, se han reiterado ahora, tras la promulgación de la LO 13/2015, fundamentalmente porque, como señala ASENCIO GALLEGO, «las referencias a la urgencia son tan difusas, como subjetivas y, por tanto, susceptibles de valoración en exceso dependiente incluso de los órganos competentes en el caso»[568]. Por su parte, CASTILLEJO MANZANARES ha señalado que «dejar en manos de la policía semejante decisión a la vista de lo que se considere un interés constitucionalmente legítimo, teniendo en cuenta los derechos afectados, no parece aceptable»[569].

En cuanto a nuestra posición en relación con esta materia, mantenemos al igual que los anteriores autores, una postura crítica con la falta de definición legal de los supuestos de urgencia, entendiendo que sería necesaria una mejora de la LECrim en este sentido.

Cierto es que, de conformidad con lo establecido en el art. 5.2.c) LOFCS, en el ejercicio de sus funciones las FCSE deberán actuar con la decisión necesaria, y sin demora cuando de ello dependa evitar un daño grave, inmediato e irreparable; rigiéndose al hacerlo por los principios de congruencia, oportunidad y proporcionalidad en la utilización de los medios a su alcance. Ahora bien, ello no está reñido con una mayor concreción de los casos que permitan una actuación urgente sin autorización judicial por parte de la Policía Judicial, cuando de registros informáticos se trate, teniendo en cuenta que, en estos casos, nunca estaríamos ante una injerencia leve.

Ha sido mencionada doctrinalmente la STC 173/2011, de 7 de noviembre, en la que se estimó necesaria la actuación policial sin necesidad de autorización judicial, en un supuesto en el que la policía registró los archivos de un ordenador que había sido dejado para reparar en un establecimiento informático, cuando, tras las operaciones de reparación, se detectó por los técnicos la existencia de archivos con contenido pedófilo,

---

[567] ASENCIO MELLADO, J. M., «La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales», *Diario La Ley - Sección Doctrina*, n.º 8009, 2013, p. 2.

[568] ASENCIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la Ciberdelincuencia», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, p. 64.

[569] CASTILLEJO MANZANARES, R., «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», cit., p. 22.

procediéndose a denunciar los hechos ante la policía, que, seguidamente, procedió al registro sin autorización judicial[570].

Sin embargo, el TEDH en la Sentencia de 30 de mayo de 2017, caso Trabajo Rueda c. España, resolviendo la demanda interpuesta ante el alto Tribunal europeo, tras la anterior desestimación por el TC, determinó que en el referido caso se había producido la violación del art. 8 CEDH, y consecuentemente el derecho a la vida privada del demandante por el registro sin autorización judicial del equipo informático, y declaró que «el TEDH no alcanza a detectar las razones por las que la espera de una previa autorización judicial, que podía obtenerse con relativa rapidez, habría obstaculizado la investigación llevada a cabo por la policía sobre los hechos denunciados»[571].

Por nuestra parte, consideramos que puede llegarse un poco más lejos, y afirmar que para la práctica de un registro informático no será necesario, en la mayoría de los casos, una actuación inmediata por parte de la Policía Judicial, pudiendo esperar veinticuatro horas para que el juez competente pueda resolver motivadamente la solicitud con respeto de los principios rectores, especialmente, en este caso, del principio de proporcionalidad.

Compartimos en este punto la opinión de ASENCIO GALLEGO, cuando afirma que «siendo el criterio de la urgencia de carácter procesal y superior a la flagrancia, que tiene connotaciones penales, es lo cierto que se constituye en un dato excesivamente abierto e impreciso, tanto que TIEDEMANN ha llegado a considerar que suele en la práctica elevarse a norma común de comportamiento, de modo que la policía, mediante una amplísima interpretación califica de urgente lo que no es»[572] y añade que «por ello,

---

[570] La STC 173/2011, de 7 de noviembre, declara en su FJ 7.º que «si bien la intervención policial desplegada no contó con la previa autorización judicial, circunstancia ésta que ha llevado a considerar, tanto al recurrente como al Fiscal, que se había producido en este caso una vulneración del derecho a la intimidad personal, podemos afirmar que nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia, pues existen y pueden constatarse razones para entender que la actuación de la policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad».

[571] Vid. STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España, apdo. 42.

[572] ASENCIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la Ciberdelincuencia», cit., p. 64. Este autor cita la obra de TIEDEMANN, «El Derecho Procesal Penal», en *Introducción al Derecho Penal y al Derecho Procesal Penal*, con ROXIN Y ARZT, Barcelona, 1989, pág. 180.

el control judicial posterior debe ser estricto en evitación de tal ampliación desmesurada de un criterio que, de modo estricto, puede cumplir, por el contrario, una función adecuada a las necesidades procesales»[573].

Por ello, estimamos que deberían reducirse los casos de urgencia, en los que la Policía Judicial podría proceder a un registro informático sin necesidad de autorización judicial, únicamente a aquellos supuestos excepcionales, en los que, como ha señalado el TEDH, «la policía en misión e averiguación no puede esperar una autorización judicial sin obstaculizar el correcto desarrollo y el fin de dicha averiguación»[574]. No se trata por tanto, de descender hasta el establecimiento de todos los concretos supuestos de urgencia, tarea que sería muy complicada.

Por otro lado, también nos parece excesiva la solución que se adoptó en el Anteproyecto de la LO 13/2015, en el que en su art. 588 quinquies c.4, se preveía únicamente para «los casos de emergencia o de riesgo de catástrofe o cuando la medida tenga por objeto la localización de personas en situación de urgencia vital y existan razones fundadas que hagan imprescindible la medida», respecto de lo cual, el Consejo Fiscal de la FGE, en su informe al Anteproyecto, estimó que se regulaba «de modo demasiado restrictivo el supuesto habilitante»[575], opinión a la que se adhirió el Consejo de Estado en su informe al mismo Anteproyecto[576].

En todo caso, estimamos que el concepto de «urgencia» se encuentra establecido de forma muy difusa, por lo que consideramos oportuna una regulación más detallada, más aun si tenemos en cuenta que cuando es solicitada una medida limitativa de derechos fundamentales, el juez debe acordarla en el urgente plazo máximo de veinticuatro horas (art. 588 bis c.1 LECrim).

---

[573] ASENCIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la Ciberdelincuencia», cit., p. 64.

[574] Vid. STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España, apdo. 32.

[575] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 116.

[576] CONSEJO DE ESTADO, «*Dictamen 97/2015, 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 tecnológica*», cit., p. 19.

Por ello, estimamos que, *de lege ferenda*, debería prescribirse legalmente que únicamente se justificaría la urgencia para los registros informáticos, permitiendo la actuación de la Policía Judicial o el Ministerio Fiscal sin necesidad de autorización judicial, en aquellos casos en los que, ante la posibilidad del fracaso de la investigación, la intervención sea absolutamente inaplazable.

6.3. La urgencia en relación con el acceso a los repositorios telemáticos de datos

Distinto tratamiento han de tener los registros de repositorios telemáticos de datos de los que nos hemos ocupado anteriormente[577], para los que el art. 588 sexies c.3 LECrim, prevé que la Policía Judicial o el Ministerio Fiscal puedan llevarlos a cabo en caso de urgencia, informando igualmente al juez competente en el plazo máximo de veinticuatro horas, quien, de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

Estimamos que tal intervención será proporcionada, de acuerdo con lo señalado por la Circular 5/2019 de la FGE, «ante situaciones de peligro inminente de que la información pueda desaparecer, ya que, al resultar accesible a través de internet para cualquier persona que conozca las claves de acceso, podría ser borrada por cualquier tercero que tuviera conocimiento de la detención del investigado»[578]. Ello siempre que la intervención inicial viniera autorizada judicialmente, o bien tras una intervención policial inmediata, en caso de que, como hemos indicado, esta fuera absolutamente inaplazable.

Ahora bien, esto no impide que, en aras de una mayor seguridad jurídica y de una mayor calidad y previsibilidad de la ley, esta circunstancia relativa a las situaciones de peligro inminente en la que pueda desaparecer la información, pueda ser recogida legalmente, a fin de evitar actuaciones desproporcionadas. Aunque es cierto que la actuación ha de ser convalidada por el juez, la regulación actual no está exenta de riesgos de intervenciones en las que se podría invocar una urgencia que no existe, con la consecuente e indeseable para todos, nulidad de la prueba.

---

[577] Vid. supra apdo. II.6 de este capítulo, pp. 266-271.

[578] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 38.

7. Forma de ejecución

7.1. Copia de los datos

En cuanto a la forma de ejecución para el registro de dispositivos de almacenamiento masivo, ha de tenerse en cuenta que el art. 588 sexies c.1 LECrim prevé que la resolución del juez podrá autorizar la realización de copias de los datos informáticos.

Aunque se establezca de este modo, es decir, como una facultad del juez, parece que lo más normal será que sea efectuada una copia de los archivos digitales que se precisen, la cual podrá efectuarse o bien mediante una copia selectiva de datos, o bien mediante un clonado o volcado integral de los mismos.

Tal y como precisa URIARTE VALIENTE, la primera forma tiene como nota principal, la facilidad y rapidez de obtención, aunque su inconveniente estriba en la posibilidad de manipulación, con la consiguiente menor garantía de autenticidad. Por su parte, afirma el citado autor, el volcado completo de los datos resulta mucho más lento y el análisis y manejo posterior de la información copiada será mucho más tedioso, pero de esta manera se conseguirá un análisis mucho más profundo de la información que pudiera existir en el dispositivo, a lo que hay que añadir una mayor seguridad para la inmutabilidad de la prueba[579].

En cualquier caso, todo lo que se refiere al aseguramiento de la prueba será examinado en el apartado relativo a la cadena de custodia, dentro del siguiente y último capítulo, dedicado a la eficacia probatoria.

7.2. Regla general relativa a la evitación de incautación de los soportes físicos que contengan los datos o archivos informáticos

El art. 588 sexies c.2 LECrim, establece que «se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda

[579] URIARTE VALIENTE, L. M., «Nuevas técnicas de investigación restrictivas de derechos fundamentales», *Ponencias de formación continuada - Ministerio Fiscal*, 2015, pp. 31-32, Consultado en https://www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada, el 2 de marzo de 2019.

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».

Conforme señala MARCHENA GÓMEZ, ante la existencia de supuestos en que los dispositivos de almacenamiento masivo de datos desplieguen una utilidad no necesariamente asociada a la actividad delictiva que ha justificado su intervención, «el legislador quiere que, en la medida de lo posible, una vez obtenida la copia de esos datos, aquellos instrumentos recuperen su utilidad»[580].

Por su parte, DELGADO MARTÍN considera que también es posible la incautación provisional del dispositivo, procediéndose a devolución una vez practicada la diligencia con condiciones adecuadas[581].

No obstante, esta regla relativa a la evitación de la incautación de los soportes físicos, queda condicionada a que estos «no constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen».

Estos casos, en los que se hace necesaria la incautación de dispositivos, quedan perfectamente explicados por la Circular 5/2019 de la FGE, en la que se señala que «el soporte constituirá el objeto del delito cuando recaiga sobre él la acción del sujeto activo o resulte afectado directamente por el daño causado por la conducta delictiva (delitos de daños informáticos, por ejemplo) o cuando contenga los archivos informáticos de contenido delictivo (delitos de pornografía infantil o contra la propiedad intelectual)»[582].

Por su parte, «los soportes físicos podrán ser considerados instrumentos del delito cuando hayan sido directamente utilizados como medio para su perpetración; será el caso, por ejemplo, de los ordenadores utilizados para cometer estafas a través de internet o el teléfono móvil empleado para realizar grabaciones que supongan intromisiones ilícitas en la intimidad»[583].

---

[580] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 378.

[581] DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», cit., p. 10.

[582] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 32-33.

[583] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 32-33.

Finalmente, la existencia de otras razones que lo justifiquen, «aparece como una cláusula genérica de cierre que permitiría valorar como excepción a la regla general cualquier otra circunstancia específica que pudiera darse en un caso concreto, como, por ejemplo, que los soportes físicos contengan datos o archivos informáticos que pertenecieran a un tercero o que el titular o propietario del soporte no tuviera derecho a conservar»[584], añadiendo que «en la determinación de estas razones deberá ponderarse siempre la importancia de las mismas en relación con el perjuicio que genera la incautación del dispositivo»[585].

IV. Los registros remotos sobre equipos informáticos

1. Consideraciones previas

Una vez examinados los aspectos comunes de las dos modalidades de registros informáticos, así como las especialidades de los registros de dispositivos de almacenamiento masivo, procede ocuparnos de los registros remotos sobre equipos informáticos, cuyas particularidades puede afirmarse que derivan de dos notas esenciales que caracterizan a esta moderna medida de investigación, como son, de acuerdo con la opinión puesta de manifiesto en la Circular 5/2019 de la FGE, la clandestinidad y el carácter dinámico del registro[586].

Aun resultando obvio, no está de más recordar, como así lo ha hecho RICHARD GONZÁLEZ, que no debe confundirse esta medida de investigación con la investigación ordinaria de la policía por internet que se fundamenta en la atribución genérica a la policía de la potestad y el deber de averiguar los delitos públicos conforme al art. 282 LECrim, afirmando que en cumplimiento del mandato establecido en dicho precepto y dado el carácter de lugares públicos que tienen internet y las redes sociales de acceso libre, para la investigación dentro de estos lugares virtuales la Policía Judicial no precisa de ninguna autorización judicial[587].

---

[584] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 32-33.

[585] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 32-33.

[586] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., pp. 52-53.

[587] RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 197.

Tal como señala BACHAMAIER WINTER, esta diligencia de registro remoto se encuentra admitida en diversos países europeos, como Alemania, Francia, Italia, República Checa, Bélgica, Holanda o Suecia[588], siendo de destacar que, desde hace años, el Consejo de la Unión Europea venía recordando a los estados miembros la conveniencia de regular esta medida de investigación[589]. En tal sentido, señala el preámbulo de la LO 13/2015 que se trata de una «diligencia ya presente en buena parte de las legislaciones europeas».

De todas las regulaciones europeas, resulta relevante poner de relieve, tal y como afirma LÓPEZ-BARAJAS PEREA, el caso alemán, donde parte de la doctrina había defendido la legitimidad de los registros remotos con base en la regulación de las entradas y registros tradicionales regulados en los parágrafos 102 y siguientes de la ley procesal penal y en la cláusula general recogida en el parágrafo 161 del mismo texto[590].

Conforme explica LORENZ, aun a pesar de su fuerte controversia el registro remoto fue aplicado por las autoridades de seguridad. Sin embargo, la Sentencia del Tribunal Supremo alemán de 31 de enero de 2007 lo declaró inadmisible en los procesos penales por falta de fundamento legal. Previamente a esta sentencia, el Estado federado (Land) de Westfalia-Rin del Norte, había habilitado a sus autoridades del servicio secreto para la aplicación del registro oculto *on line* a través de la Ley de 20 de diciembre de 2006[591].

No obstante, mediante la Sentencia del 27 de febrero de 2008 el Tribunal Constitucional Federal declaró nula dicha ley. Esta sentencia, de acuerdo con lo señalado por LÓPEZ LOMA, determinó que un registro online solo sería admisible cuando haya un peligro concreto, causado por una persona determinada, subrayando en su

[588] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., pp. 5-8.

[589] La autora hace referencia a la indicada recomendación del Consejo de la Unión Europea, en el «Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting, 27-28 de noviembre de 2008», disponible en: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ jha/104344.pdf. Vid. BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», nota al pie nº. 4.

[590] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», cit., p. 163.

[591] LORENZ, D., «El registro oculto de ordenadores como desafío en la dogmática de los derechos fundamentales y la reciente respuesta por la Constitución alemana», *Revista Española de Protección de Datos*, n.º 5, 2008, pp. 13-14.

fundamento jurídico 66 que, además, «la búsqueda "*on line*" debería estar sujeta a exigencias rigurosas en cuanto a la proporcionalidad» y señalando que «en vista de su intensidad de invasión, tal medida solo puede ser la última opción»[592].

Pese a las referidas controversias, este medio de investigación ha sido introducido a nivel federal por Ley de 25 de diciembre de 2008. Ahora bien, tal y como apunta BACHMAIER WINTER, la ley alemana configura el registro remoto como medida en el ámbito de la seguridad o prevención de delitos, tanto en el ámbito de inteligencia, como por las fuerzas de seguridad, sin que hasta este momento, se regule como diligencia de investigación penal en su Código Procesal Penal[593].

De este modo, afirma la referida autora, «junto con Francia e Italia, España es uno de los pocos países de la Unión europea que regula expresamente el registro remoto de equipos informáticos a través de la instalación de software espía como una medida de investigación criminal»[594].

La reforma operada por la LO 13/2015 ha incluido en la LECrim esta medida de investigación, regulándola en tres artículos, 588 septies a), b) y c). De conformidad con lo dispuesto en el apartado 1 del primero de dichos preceptos, el examen a distancia, de forma remota y telemática y sin conocimiento de su titular de un equipo informático, podrá ser autorizado por el juez competente, mediante la utilización de datos de identificación y códigos, así como con la instalación de un software.

---

[592] LÓPEZ LOMA, L., «El registro oculto on line y su conflicto con los derechos fundamentales según la doctrina alemana tras la Sentencia del Tribunal Constitucional Federal de 27 de febrero de 2008», *Revista Española de Protección de Datos*, n.º 5, 2008, p. 227.

[593] Señala la referida autora que conforme a los datos del estudio llevado a cabo por el Instituto Max Planck de derecho penal de Friburgo, en materia de interceptación de las comunicaciones en la Unión europea, en Alemania, como en la República Checa, la instalación de software no se regula expresamente en el ámbito del proceso penal, lo cual crea la incertidumbre acerca de si tal medida está autorizada o no. Por su parte, en Bélgica, Holanda y Suecia se permite acceder de forma remota a equipos informáticos, pero ello deberá realizarse mediante la instalación física en el ordenador del software que se precisa, no permitiéndose instalar el spyware a través del acceso remoto, es decir, solo se permite la vigilancia remota una vez que se instala directamente el programa espía. Finalmente, afirma que en el Reino Unido el registro remoto de equipos informáticos no es una medida novedosa, pues, a pesar de no estar regulada en el ámbito del proceso penal, sí se encuentra prevista desde hace tiempo en la normativa policial. Vid. BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., pp. 7-8.

[594] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 7.

Esta inicial lectura de la novedosa regulación, nos lleva al examen de la primera de las peculiaridades de los registros remotos, como son las modalidades de intervención.

2. Modalidades de intervención

Tal y como acabamos de indicar, de conformidad con lo dispuesto en el art. 588 septies a.1 LECrim, la entrada de forma remota en un equipo informático, puede realizarse, bien mediante la utilización de datos de identificación y códigos, o bien a través de la instalación de un software (troyano[595]).

Además, doctrinalmente, se ha planteado la posibilidad de incluir entre las modalidades, los denominados *keylogger,* instrumentos que almacenan cada una de las pulsaciones que se hagan en el teclado de un ordenador y que pueden ser hardware, esto es, adaptadores que se conectan en dicho ordenador o en su teclado; o bien software, es decir, programas ejecutables que se instalan en el ordenador investigado sin que el usuario se dé cuenta, que guardan cada tecla presionada en el teclado, y cuya información puede ser transmitida al investigador por una red local o de telecomunicación[596].

Teniendo en consideración estas aportaciones doctrinales, quizás hubiera sido más aconsejable que el legislador hubiera seguido la opinión del Consejo Fiscal de la FGE, que, en su Informe al Anteproyecto de la LO 13/2015, consideró inoportuna la concreción de los medios técnicos mediante los que se podría efectuar el registro remoto, señalando que «debería bastar con la previsión legal de la posibilidad de acceso remoto a los equipos o en todo caso una fórmula más abierta en la que sea posible encuadrar cualquier otro mecanismo o instrumento que en el futuro pueda ser utilizado con esa misma finalidad y con idénticas garantías», y ello, teniendo en cuenta el vértigo con el que evolucionan estas tecnologías[597].

---

[595] La tercera acepción del término «troyano» del DRAE, dice, «dicho de un virus: capaz de alojarse en una computadora u otro dispositivo electrónico para captar información y transmitirla a usuarios ajenos».

[596] Vid. DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», cit., pp. 12-13.

[597] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 121.

En cualquier caso, nos referiremos a los métodos de intervención previstos en la LECrim tras la referida reforma legal.

2.1. Utilización de datos de identificación y códigos

De acuerdo con lo señalado por URIARTE VALIENTE, «existen ciertos programas informáticos de gestión que permiten el manejo a distancia de ordenadores previamente conectados, exigiendo para ello la correcta identificación del equipo que pretende la conexión mediante determinados códigos. Igualmente, el acceso a determinados sistemas informáticos, repositorios o bases de datos, puede realizarse a distancia con la simple utilización de los datos de identificación o códigos correctos por parte del equipo que pretenda el acceso»[598].

Por tanto, esta modalidad de intervención exigirá la participación de terceras personas que, conocedoras de los datos de identificación del equipo o en su caso el nombre de usuario y la contraseña, los faciliten a fin de que los agentes puedan entrar en una red privada con el perfil de la persona investigada. Del mismo modo, los datos para el acceso podrán ser facilitados por las operadoras prestadoras de servicios de la sociedad de la información[599].

En este punto ha de recordarse que, conforme dijimos en el segundo epígrafe de este capítulo[600], en el ámbito de los registros informáticos rige el deber de colaboración de terceros (arts. 588 sexies c.5 y 588 septies b.2 LECrim), el cual se ajusta a la legalidad constitucional siempre que sea respetuoso con los derechos fundamentales del tercero obligado, y se justifique dicha obligación como indispensable para el buen fin de la intervención.

En este sentido, siempre que se cumplan los principios rectores, especialmente los de necesidad y proporcionalidad, podrá instarse la facilitación de los datos de

[598] URIARTE VALIENTE, L. M., «Nuevas técnicas de investigación restrictivas de derechos fundamentales», cit., p. 35.

[599] Afirma RODRÍGUEZ LAINZ, en relación con la obligación de cooperación de las operadoras para esta diligencia, que esta posibilidad «se presenta cada vez más compleja y dificultosa, frente a la cada vez más generalizada utilización por los diseñadores de sistemas operativos aplicados a dispositivos de técnicas que hacen a las claves impenetrables incluso frente a los propios operadores». Vid. RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», *Diario La Ley*, n.º 8896, 2017, p. 4.

[600] Vid. supra apdo. II.4 de este capítulo, pp. 259-263.

identificación y códigos, no solo a las operadoras, sino a otras personas conocedoras de los mismos, tales como administradores de redes privadas o gestores de redes wifi, con la excepción de las personas que estén dispensadas de la obligación de declarar por obligación de parentesco, y aquellas que, de conformidad con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional.

Finalmente, debe recordarse que, los obligados, de conformidad con lo dispuesto en el art. 588 septies b.4 LECrim, quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e LECrim, es decir, podrán incurrir en un delito de desobediencia.

2.2. Instalación de un software espía

En cuanto a la segunda de las modalidades establecidas legalmente para los registros remotos, esta consiste en la instalación de un troyano en el equipo informático objeto de la intervención, mediante el que los agentes policiales podrán acceder a los datos almacenados, al igual que, en tiempo real, a la observación y grabación de la actividad que lleva a cabo la persona investigada, tales como las visitas a páginas web, ejecución de programas o las telecomunicaciones llevadas a cabo por la misma. En definitiva, supone un acceso a todas las funcionalidades y datos del equipo, así como el espionaje de toda su actividad.

Cabe señalar, como así lo hace VELASCO NUÑEZ, que la instalación de estos programas, supone un proceso muy complejo que no siempre tiene éxito. Tal y como afirma SÁNCHEZ RUBIO, «debe partirse de la idea de que la instalación de troyanos por parte de la policía no es una labor ni sencilla ni ágil, sino que requerirá un intenso trabajo de estudio previo, análisis del objetivo, preparación y programación de la herramienta que se vaya a instalar [...] aun dedicando todo el tiempo preciso, no siempre será factible acceder al dispositivo que se desea investigar»[601].

Efectivamente, de acuerdo con lo señalado por VELASCO NUÑEZ, para poder ejecutar con éxito las sofisticadas técnicas de intrusión, hay que conocer el

[601] SÁNCHEZ RUBIO, A., «Los registros remotos sobre equipos informáticos: La investigación del "hacker legal"», cit., p. 211.

funcionamiento de los antivirus que, mediante modernas técnicas heurísticas, detectan los programas intrusos[602].

RODRÍGUEZ LAINZ, por lo que respecta a las intervenciones mediante instalación de troyanos, se ha referido a las mismas como «vías realmente dificultosas para acceder remotamente a los entresijos de un dispositivo o sistema informático conectado a una red»[603] así como a la «complejidad que representa su utilización en un horizonte que cada vez tiende más y más a blindar determinados dispositivos móviles frente a estas posibles vías de intrusión»[604]. Asimismo, ha señalado que, no obstante las estrategias utilizadas para poder penetrar en el equipo investigado, tales como el aprovechamiento de la conexión del dispositivo a determinada red pública o privada, valiéndose de canales de compartición como el bluetooth, mediante la incorporación como adjunto a un determinado mensaje de mensajería instantánea o acceso o descarga de información, la garantía de éxito de la operación de introducción del troyano puede llegar a exigir una manipulación manual del dispositivo que permita desactivar determinados niveles o protocolos de protección preestablecidos o activados por el propio usuario, abriendo así las puertas a la penetración del programa espía, resaltando en definitiva la complejidad de la misma[605].

Por otra parte, MIRANDA WALLACE afirma que, además de poder fallar el método común de infectar los ordenadores de los investigados por software espía, podrían fácilmente dañarse los equipos de formas impredecibles e inesperadas, pudiendo encontrarnos ante casos de responsabilidad patrimonial de la Administración[606].

---

[602] VELASCO NÚÑEZ, E.; VILLÉN SOTOMAYOR, M., «Medios tencológicos de investigación penal», *Conclusiones de Seminarios-Consejo General del Poder Judicial*, n.º 4, 2015, p. 10.

[603] RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 3.

[604] RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 3.

[605] RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 4.

[606] Si bien es cierto que, en caso de ocasionarse daños informáticos con ocasión de la intervención policial en un registro remoto, podría plantearse la responsabilidad patrimonial de la Administración, en nuestra opinión es una cuestión dudosa, dado que conforme al art. 32 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, puede darse el caso de que el particular «tenga el deber jurídico de soportar el daño». Vid. MIRANDA WALLACE, D., «Registro remoto de equipos informáticos. Comentario crítico al artículo 588 septies LECRIM», *Revista General de Derecho Procesal*, n.º 42, 2017, pp. 9-10.

Llegados a este punto, probablemente la ejecución de esta medida sería más fácil en relación con los equipos informáticos de delincuentes autores de delitos menos graves, por cuanto es de suponer que sus dispositivos estarán menos protegidos que los de organizaciones criminales o los de delincuentes que cometen los delitos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. Pero, como quiera que el catálogo cerrado de delitos respecto de los que puede ser acordado este tipo de registro —de los que nos ocuparemos más adelante—, excluye a aquellos pequeños delincuentes, es previsible la dificultad que supondrá su ejecución, que no obstante ser técnicamente posible, probablemente, por el momento, quedará reservada para la investigación de los delitos de mayor trascendencia social, teniendo en cuenta, además, como señala VELASCO NUÑEZ, que la instalación de software espía requiere ataques persistentes avanzados, específicamente dirigidos al investigado que son realmente caros y de difícil consecución[607].

Cabe señalar, no obstante, que el uso de nuevos troyanos, especialmente diseñados, que no se encuentren en los catálogos actualizados de los programas antivirus[608], cuando se trate de delitos especialmente graves, dado el alto coste que puede suponer este proceso así como la también difícil infiltración en las organizaciones criminales de la figura del agente encubierto, podrán facilitar la ejecución de esta medida de investigación.

En todo caso, las mencionadas complicaciones que se encuentran para la práctica de un registro remoto de equipos informáticos, son probablemente la causa de que esta diligencia no se haya llevado a la práctica lo suficiente, no habiendo tenido que pronunciarse los tribunales sobre ningún conflicto jurídico derivado de un registro informático practicado bajo esta modalidad de intervención[609]. Se sigue manteniendo así

[607] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 26.

[608] Una afirmación similar se realiza en la Circular 5/2019 de la FGE, que señala que «puede ocurrir, sin embargo, que no se utilice un programa de uso público, sino un programa desarrollado específicamente para su utilización policial con esta finalidad. Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 61.

[609] A la fecha del depósito de esta tesis, no se ha encontrado, en ninguna de las distintas bases de datos consultadas, sentencias o autos que hayan resuelto alguna cuestión jurídica en relación con esta medida de investigación. Asimismo no se ha localizado ninguna cita de alguna de estas resoluciones en la bibliografía utilizada.

a día de hoy, la afirmación que, poco después de la LO 13/2015, realizó CONDE-PUMPIDO TOURON al señalar que «el análisis de esta medida es complejo en este momento inicial, dado que no existe doctrina jurisprudencial, y su aplicación genera sobre todo una serie de problemas técnicos que no es fácil prever cómo se van a resolver»[610].

En todo caso, y aun tratándose de una materia respecto de la que habrá que estar atentos a su evolución, ha de valorarse positivamente su regulación, aplaudiendo de este modo la valentía del legislador, al haber dado por cumplido el necesario requisito de una adecuada previsión legal para la ejecución de una medida tan restrictiva de derechos fundamentales, todo ello sin perjuicio de que nuevas investigaciones en el campo de la informática coadyuven al perfeccionamiento de esta diligencia, que tan necesaria resulta para combatir el crimen organizado.

3. Interceptación de las comunicaciones telemáticas mediante registro remoto

Ya sabemos que mediante un registro informático, en general, podrán ser intervenidas determinadas comunicaciones telemáticas. Además, si nos ceñimos a los registros remotos se trata de una posibilidad, que incluso personas legas en cuestiones técnicas informáticas podrían calificar como indudable. Como ha señalado RODRÍGUEZ LAINZ, «que a través de un registro remoto pueda accederse a comunicaciones ya consumadas o a su rastro es una realidad que difícilmente puede negarse; y ello aunque el legislador haya guardado silencio sobre la posibilidad de tener que ponderar esa posible afectación»[611].

Y es que, en efecto, el legislador no ha previsto en el art. 588 septies LECrim, la posibilidad de la intervención de las comunicaciones mediante un registro remoto, respecto del que, como veremos más adelante, incluso ha establecido un catálogo de delitos que difiere del previsto para la intervención de las comunicaciones telefónicas y telemáticas. Ello no obstante, se plantea una cuestión que precisa ser contestada en este

[610] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 14.

[611] RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 11.

trabajo: ¿Permite la LECrim llevar a cabo una intervención de las comunicaciones telemáticas mediante un registro remoto?

Inicialmente, como ya hemos indicado en primer párrafo de este apartado, se podría pensar que un registro remoto permitiría en todo caso intervenir las comunicaciones, dado que, al visualizar de forma clandestina la actividad de una persona de forma remota, sus comunicaciones telemáticas serían fiscalizadas.

No obstante, hemos de tener en cuenta que la intervención de las comunicaciones telefónicas y, con la LO 13/2015, también telemáticas, tienen una regulación específica en un capítulo independiente, de la que resultan algunas diferencias que ponen de manifiesto que aquella reflexión inicial era desacertada.

Así, existen diferencias de bastante relevancia, entre las que podemos mencionar las siguientes:

a) La que se refiere al catálogo de delitos en virtud del que se pueden acordar ambas medidas —de la que nos ocuparemos, por su importancia, en el apartado siguiente—.

b) La posibilidad de la intervención de las comunicaciones sea ordenada por el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, en casos de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, posibilidad que no se establece para los registros remotos.

c) La duración máxima de la medida, es de un mes prorrogable por iguales periodos hasta un máximo de tres meses, mientras que para la intervención de las comunicaciones es de tres meses prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Por ello, nos adherimos a la opinión de BACHMAIER WINTER, quien afirma que «al regular el registro remoto de equipos informáticos, la intención del legislador no ha sido cubrir también la interceptación en tiempo real de las telecomunicaciones»[612].

[612] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 15.

En este sentido, consideramos que dentro del espíritu de la regulación, no es posible encontrar la voluntad de que la misma sea dirigida a la intervención de las comunicaciones —en nuestro caso fundamentalmente telemáticas—, sino el de establecer una modalidad de registro informático, que tiene por objeto los contenidos digitales de un dispositivo mientras este se encuentre conectado a una red, para poder realizarlo sin el conocimiento del investigado, siendo esta la nota esencial —además de las peculiaridades propias de la naturaleza de cada uno de ellos—, que lo distingue de los registros de dispositivos de almacenamiento masivo de información.

Pero, no obstante todo lo anterior, cabría preguntarse si sería posible la intervención de las comunicaciones telemáticas, como las que el investigado mantuviese mediante aplicaciones de mensajería o redes sociales. En este caso, nuestra respuesta ha de ser afirmativa. Para sustentar este criterio cabe decir que el art. 588 ter b LECrim, se refiere de forma genérica a «terminales o medios de comunicación» mientras que el art. 588 ter d.1 c), establece que se deberán hacer constar en la solicitud de autorización «los datos necesarios para identificar el medio de telecomunicación de que se trate». Además, es obvio que la intervención de una telecomunicación deberá efectuarse, al igual que un registro remoto, con carácter dinámico y de forma clandestina, por lo que, en nuestra opinión, no existe ningún impedimento legal para que una intervención de las comunicaciones telemáticas, pudiera efectuarse mediante un acceso remoto a través de software espía.

Esta posibilidad, respecto de la que ha de predicarse una muy estricta motivación en cuanto al alcance de la intervención, plantea otra duda: la relativa a si habrá que acogerse a las particularidades de la regulación de la intervención de las comunicaciones o por el contrario a la de los registros remotos. En este punto, se plantea una situación compleja en la que estimamos que el juez competente podría aplicar ambas regulaciones, justificando debidamente el uso de una o de la otra.

Es posible que la intervención de las comunicaciones se lleve a efecto simultáneamente con un registro remoto, en cuyo caso nos parece acertada la opinión de RODRÍGUEZ LAINZ, cuando afirma que al intervenir las comunicaciones mediante el acceso remoto, independientemente de someter al dispositivo a un registro remoto completo, es preciso el respeto de las exigencias previstas para ambas regulaciones, si bien «con una preponderancia de las propias de lo que no dejaría de ser un registro remoto ampliado al flujo de comunicaciones del dispositivo en cuestión [...] ello habría de afectar a los dos puntos esenciales en fricción con el supuesto de las injerencias sobre

comunicaciones: la pertenencia del hecho investigado al catálogo de delitos definidos en el art. 588 septies a.1, y la limitación temporal a no más de tres meses del tiempo de vigencia de la medida»[613]. Por el contrario, en el caso de que se acordase una intervención exclusiva de las comunicaciones telemáticas mediante un acceso remoto a un equipo informático, entendemos que debería preponderar la normativa relativa a la interceptación de las comunicaciones, como sería el caso de la aplicación del catálogo de delitos previsto para la misma o su duración.

4. Especialidades en cuanto a los delitos respecto de los que pueden ser acordados los registros remotos de equipos informáticos

Otra de las peculiaridades que distingue los registro remotos de los de almacenamiento masivo, se produce como consecuencia del establecimiento de un catálogo de delitos respecto de los que únicamente podrá ser acordada la medida[614].

En efecto, de conformidad con lo expuesto en el preámbulo de la LO 13/2015, al referirse a los registros remotos en su apartado IV, «…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 *números clausus* los delitos que la pueden habilitar». De este modo, no resulta posible la ampliación de este elenco de infracciones penales a otras conductas delictivas, aun cuando estas pudieran considerarse graves.

Este listado se detalla en el art. 588 septies a.1 LECrim, conforme al que la intervención podrá acordarse por el juez competente, «…siempre que persiga la investigación de alguno de los siguientes delitos: a) Delitos cometidos en el seno de organizaciones criminales; b) Delitos de terrorismo; c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente; d) Delitos cometidos

[613] Afirma el referido autor que, no obstante, «surgiría la duda sobre la difícil situación jurídica de los delitos contra la Constitución, de traición y relativos a la defensa nacional, o los cometidos contra menores o personas con capacidad modificada judicialmente que, no pudiendo integrarse en las otras tres modalidades de dicho precepto, no superaran el umbral del concepto de delito grave manejado por el art. 579.1,1.º LECrim», concluyendo que «es lógico pensar que lo que no pudiera obtenerse en el curso de una interceptación de comunicaciones no debería hacerse accesible por el hecho de que se emplee la técnica del registro remoto». Vid. RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 12.

[614] En el apartado III.4 de este capítulo nos ocupamos de la inexistencia de tipos delictivos concretos para las intervenciones mediante el registro de dispositivos de almacenamiento masivo de información, pp. 279-281.

contra la Constitución, de traición y relativos a la defensa nacional; e) Delitos cometidos a través de instrumentos informáticos o cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación».

Ha de tenerse en cuenta que la fijación de este grupo de delitos, si bien es cierto que inicialmente trata de garantizar el respeto al principio de proporcionalidad, no asegura su cumplimiento hasta tanto la resolución judicial lleve a cabo de forma motivada la oportuna ponderación entre el derecho sacrificado y el beneficio obtenido para el interés público, atendiendo a la entidad de las sospechas existentes y a la gravedad de los hechos desde el punto de vista de su trascendencia social.

Por otra parte, de acuerdo con la opinión puesta de manifiesto por la Circular 5/2019 de la FGE, cabe señalar que «la relación de delitos que establece el artículo supone un catálogo cerrado no susceptible de ser ampliado a otros comportamientos delictivos, por muy graves que estos pudieran ser».

El catálogo de delitos plantea algunas dudas, cuyo examen desglosaremos en dos apartados: el primero, relativo a la inclusión de todo tipo de delitos cometidos a través de las TIC; el segundo, dedicado a los puntos de conflicto en relación con los delitos para los que puede ser acordada la intervención de las comunicaciones.

4.1. Problemas en relación con la inclusión de los delitos cometidos a través de las TIC

De los delitos fijados legalmente para poder practicar esta diligencia, así como de la explicación ofrecida en el preámbulo de la LO 13/2015, parece claro que la intención del legislador ha sido delimitar el ámbito de esta medida a la investigación de delitos de especial gravedad, dada la fuerte injerencia que supone su aplicación sobre los derechos a la vida privada.

Sin embargo, esta afirmación puede predicarse de los cuatro primeros apartados de la enumeración, pero no así del apartado e) referido a delitos cometidos a través de instrumentos informáticos o cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación, respecto del que, doctrinalmente, se han planteado dudas acerca de su inclusión de forma generalizada, dado que, con esta regulación, podría acordarse la práctica de un registro remoto para cualquier delito cometido a través de medios tecnológicos, con independencia de que se tratase de un delito menos grave o incluso un delito leve.

Señala a este respecto CONDE-PUMPIDO TOURÓN, que «hay que tener en cuenta que muchos de los delitos que se pueden cometer en el mundo real, también pueden cometerse en el virtual: amenazas, coacciones, delitos contra la libertad sexual o contra el honor, violencia de género, tráfico de personas y de drogas, terrorismo, etc.»[615], añadiendo que «además existen los delitos propios del mundo virtual, como la distribución de ficheros de pornografía infantil, la piratería informática, el sabotaje a sistemas informáticos, la entrada no autorizada en redes y sistemas, la difusión de datos de terceros sin su consentimiento etc.»[616].

Por otra parte, SÁNCHEZ RUBIO señala que «ha de recordarse que la norma no se refiere solamente a los delitos que afecten directamente a las nuevas tecnologías, por ejemplo los daños informáticos, sino a los delitos tradicionales cometidos a través de instrumentos informáticos, por ejemplo las amenazas cometidas a través de correo electrónico, que constituyen en realidad delitos de escasa gravedad que solo difieren de los delitos tradicionales en cuanto al medio de comisión, sin que este medio altere sustancialmente el daño causado al bien jurídico protegido por el tipo, que sigue siendo el mismo»[617].

Son estas circunstancias las que sustentan opiniones en contra de la inclusión de este apartado. Así, BUENO DE MATA afirma que «se deja una puerta peligrosamente abierta a través de una tipología indeterminada […] que pensamos se debería eliminar para evitar el uso de esta herramienta de manera analógica a discrecionalidad del juzgador»[618]. Por su parte, SÁNCHEZ RUBIO señala que «la utilización de una medida tan intrusiva como el registro remoto puede ser manifiestamente desproporcionada pues aumenta con creces la previsión del art. 55.2 CE, que solo contempla la restricción del

[615] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 17.
[616] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 17.
[617] SÁNCHEZ RUBIO, A., «Los registros remotos sobre equipos informáticos: La investigación del "hacker legal"», cit., p. 211.
[618] BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», cit., p. 5.

secreto de las comunicaciones para casos de delitos de bandas armadas o terroristas»[619]. Y en similar sentido, CONDE-PUMPIDO TOURÓN concluye que «es por ello por lo que la extensión generalizada del registro remoto a los delitos cometidos mediante instrumentos informáticos es desproporcionada, y exigirá una interpretación muy restrictiva»[620].

Sin perjuicio de las anteriores posiciones doctrinales, debe señalarse que la inclusión de este apartado en el catálogo de delitos, se debe al compromiso de España, como consecuencia de la ratificación del Convenio de Budapest, en el que, en su art. 14, se acordó por los estados firmantes establecer las medidas necesarias para la investigación de los delitos enumerados en los arts. 2 a 11 del Convenio y «otros delitos cometidos por medio de un sistema informático».

No obstante, tal y como explica BACHAMIER WINTER, los estados pueden formular reserva en relación con la interceptación en tiempo real sobre los contenidos de las comunicaciones establecida en el art. 21, en relación con las que los estados miembros solo vendrían obligados a adoptarlas cuando se trate de «una serie de delitos graves que deberán definirse en su derecho interno»[621].

De este modo lo aclara el Informe Explicativo del Convenio de Budapest[622], que en sus apartados 212 y 214 justifica la posibilidad de que las partes puedan formular reservas, dado que algunos estados podrían considerar que los delitos establecidos en el convenio no son lo suficientemente graves como para permitir la interceptación de datos relativos al contenido[623]. Así, el apartado 214 de dicho informe, asumiendo que la interceptación de datos relativos al contenido es un tema delicado, dispone que «el

[619] SÁNCHEZ RUBIO, A., «Los registros remotos sobre equipos informáticos: La investigación del "hacker legal"», cit., p. 211.

[620] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 17.

[621] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 13.

[622] El Informe Explicativo del Convenio de Budapest puede consultarse en el siguiente enlace de la web del Consejo de Europa: https://rm.coe.int/16802fa403. Página visitada el 3 de diciembre de 2019.

[623] Tanto en el Convenio de Budapest como en su Informe Explicativo, se distingue entre datos sobre el tráfico y datos sobre el contenido, refiriéndose estos últimos a los datos que pueden obtenerse como consecuencia de la ejecución de una medida de investigación tecnológica. En el caso de los registros remotos, podría tratarse del contenido de comunicaciones o archivos digitales de cualquier clase que pudieran servir como elemento probatorio.

Convenio deja que el ámbito de aplicación de esta medida se determine atendiendo a lo dispuesto en el derecho interno», permitiendo la posibilidad de que los países firmantes «puedan formular una reserva con el fin de restringir la aplicabilidad de la disposición anterior».

Sin embargo, termina disponiendo el referido apartado 214 que «las Partes deberían considerar la aplicación de ambas medidas a los delitos establecidos por el convenio en la sección 1 del capítulo II, con el fin de contar con un medio eficaz para la investigación de estos delitos informáticos y los delitos relacionados con la informática». Por ello, afirma BACHAMAIER WINTER, que aun cuando el Convenio de Budapest permite a los estados miembros definir el ámbito de aplicación de las interceptaciones en tiempo real de datos relativos al contenido, pudiéndolo ceñir únicamente a la investigación de delitos calificados como graves conforme a su ordenamiento interno; al mismo tiempo «anima a los estados a que autoricen estas medidas en la investigación de todo delito relacionado con la informática»[624].

En el caso de España, el legislador de 2015 aceptó esta propuesta, y, como dijimos anteriormente, ha incluido dentro del ámbito de los registros remotos la investigación de cualquier delito relacionado con las TIC. No obstante, la primera conclusión a la que se podría llegar como consecuencia de esta nueva regulación, sería que, en virtud de las exigencias del principio de proporcionalidad, no puede ser acordada una medida de investigación tecnológica para la investigación de hechos que no revistan la suficiente gravedad. De este modo, para la investigación de cualquier delito cometido por medios tecnológicos no siempre podría ser acordado un registro remoto de equipos informáticos, como así ocurriría en relación con unas amenazas leves cometidas por medio de correo electrónico o programas de mensajería como *whatsapp* u otros similares.

Pero lo cierto es que, tal y como examinamos al estudiar el principio de proporcionalidad[625], la jurisprudencia ha considerado justificado este importante principio rector de las diligencias de investigación tecnológica cuando se trate de la investigación de los delitos cometidos por medios informáticos. Así, citamos, entre otras, la STS 811/2015, de 9 de diciembre, que en su FJ 1.º, señaló que, tratándose de la

[624] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., pp. 13-14.
[625] Vid. supra apdo. II.3.2.2.2 del capítulo II, pp. 124-127.

investigación de delitos cometidos por medios informáticos, las medidas han de considerarse proporcionadas «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». Asimismo, declaró que, «en esta clase de delitos, la posible volatilidad de las pruebas documentales puede aconsejar claramente en numerosos supuestos una rápida intervención tendente a su más pronta ocupación, sin las demoras que produciría una investigación más amplia».

Con todo, llegados a este punto, no debe olvidarse que existen otros principios rectores que han de respetarse, debiendo destacar en este caso el principio de necesidad que, conforme a lo ya estudiado, ha sido desglosado en dos: excepcionalidad y necesidad propiamente dicha[626]. Así, no se cumplirá el principio de excepcionalidad, en caso de acordarse un registro remoto, cuando estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles para el esclarecimiento del hecho. Por su parte, en relación con el cumplimiento del principio de necesidad en sentido estricto, difícilmente la investigación de determinados delitos menos graves o leves se vería gravemente dificultada sin el recurso a una diligencia tan lesiva como esta, respecto de la que, para que se respetase el principio de necesidad, debería tener el carácter de insustituible.

Por ello, nuestra opinión ha de ser favorable, en relación con la decisión del legislador de incluir en el catálogo de delitos en virtud de cuya investigación podría acordarse un registro remoto, en general, los delitos cometidos a través de las TIC, teniendo en cuenta que los principios de excepcionalidad y necesidad no permitirían siempre y en todo caso la intervención.

En línea con ello, compartimos la opinión de BACHMAIER WINTER cuando señala que «el acceso remoto a los datos del ordenador solo debería autorizarse si la policía no logra determinar la localización física de esos datos, pues solo entonces devendría necesario»[627]. Por tanto, añade la referida autora, «si se sabe dónde se encuentran los datos y se puede acceder a ellos directamente mediante el registro del dispositivo de almacenamiento, la medida de entrada y registro, complementada con la autorización

[626] Vid. supra apdo. I.3 del capítulo III, pp. 147-149.

[627] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 23.

para registrar el ordenador, haría innecesario recurrir al acceso remoto del ordenador mediante *spyware*»[628].

Sin embargo, todo ello no obsta que, dado el tiempo transcurrido desde la reforma legal, pudiera matizarse el contenido de este apartado, delimitando, dentro de los delitos cometidos a través de medios tecnológicos, aquellos cuya investigación podría dar lugar a un registro remoto.

En este sentido, nos parece correcta la opinión de GARCÍA MOLINA, cuando señala como posible solución que se especifique que esta medida solo podrá adoptarse siempre que se persiga alguno de estos delitos, cuando pueda ser calificado como delito grave conforme al art. 13.1 CP o cuando los hechos presenten caracteres de delito sancionado con pena cuyo máximo sea igual o superior a un número determinado de años de prisión[629], opinión análoga a la de CÓNDE-PUMPIDO TOURÓN, quien afirma que «este último apartado es muy problemático, generando una importante inseguridad jurídica»[630] añadiendo que, por ello, «debe ser interpretado de modo muy restrictivo, limitándose a delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación, de especial gravedad»[631].

De este modo, consideramos que, *de lege ferenda*, debería adoptarse una solución de este tipo que, teniendo en cuenta que sus límites deberían fijarse teniendo en cuenta el necesario cumplimiento de los principios de excepcionalidad y necesidad dentro del marco de lo acordado en el Convenio de Budapest, supondría un fortalecimiento de la seguridad jurídica dentro del respeto a los derechos fundamentales.

---

[628] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 24.

[629] GARCÍA MOLINA, P., «El registro, físico o remoto, de dispositivos de almacenamiento masivo de información y de equipos informáticos de abogados», en Bueno de Mata, F. (coord.), *Fodertics 5.0*, Albolote (Granada), Editorial Comares, 2016, p. 132.

[630] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 17.

[631] CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», cit., p. 17.

4.2. Puntos de conflicto en relación con los delitos establecidos para la intervención de las comunicaciones

Con la LO 13/2015 se ha dado una nueva regulación a la interceptación de las comunicaciones telefónicas y telemáticas, a la que se ha dedicado el capítulo V del título VII del libro II de la LECrim, en el que como acaba de decirse se prevé la posibilidad de intervenir no solo las comunicaciones telefónicas, sino las telemáticas.

Como ya hemos tenido oportunidad de indicar anteriormente, resulta obvio que con la vigilancia en tiempo real de la actividad cibernética de una persona, podrán observarse sus comunicaciones, ya sean mediante correo electrónico, chats, programas de mensajería instalados en teléfonos móviles, foros de conversación o redes sociales.

Sin embargo, en relación con el catálogo de delitos establecido para la intervención de las comunicaciones telefónicas y telemáticas[632], aunque este coincide en algunos tipos con el establecido para los registros remotos, existen algunas diferencias relevantes, que han dado lugar a que doctrinalmente se afirme que «la comparativa entre los delitos cuya persecución permite el empleo de una u otra técnica de investigación tecnológica plantea igualmente situaciones un tanto absurdas, en las que el principio de proporcionalidad, tan implicado en el especial rigor con que el legislador ha querido proteger el empleo de la técnica del registro remoto, queda aparentemente en entredicho»[633].

En efecto, ambas intervenciones pueden llevarse a cabo para la investigación de delitos de terrorismo, los cometidos en el seno de organizaciones criminales y aquellos perpetrados a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación.

Pero, como decíamos, de un modo ciertamente controvertido, el legislador ha regulado las dos medidas de investigación con las siguientes diferencias en el listado de tipos delictivos, en cuya averiguación podrían ser acordadas:

---

[632] Los delitos para cuya investigación puede ser acordada la intervención de las comunicaciones telefónicas y telemáticas, se establecen en el art. 588 ter a LECrim, que se remite al art. 579.1 LECrim donde se establecen los delitos que deben ser investigados para la intervención de la correspondencia escrita y telegráfica.

[633] RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», cit., p. 9.

a) Para la intervención de las comunicaciones telefónicas y telemáticas se incluyen los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. Asimismo puede acordarse respecto de delitos cometidos en el seno de un grupo criminal. Para estas infracciones penales la LECrim no permite que sea acordado un registro remoto.

b) En sentido contrario, para los registros remotos se incluyen los delitos cometidos contra menores o personas con capacidad modificada judicialmente, los cometidos contra la Constitución, de traición y relativos a la defensa nacional. Para estos delitos, sin embargo, sí podrá acordarse una intervención de las comunicaciones, dado que se encuentran penados con pena con límite máximo de, al menos, tres años de prisión.

Por tanto el conflicto se encuentra fundamentalmente en la circunstancia de que un registro remoto no pueda acordarse para todos los delitos que tengan establecida pena con límite máximo de, al menos, tres años de prisión y los cometidos en el seno de un grupo criminal, y que, sin embargo, para la investigación de estos delitos sí que pueda acordarse una intervención de las comunicaciones.

Ante esta singular situación, parece claro que la intención del legislador al regular el registro remoto de equipos informáticos, no ha sido cubrir también la interceptación en tiempo real de las telecomunicaciones, lo cual ya pusimos de manifiesto anteriormente[634]. Ahora bien, de acuerdo con lo que explicamos, consideramos que no existe ningún inconveniente legal en que se pueda acordar una intervención de las comunicaciones telemáticas mediante un acceso remoto a un equipo informático.

Como quiera que, en nuestra opinión, nos encontramos ante una regulación, cuando menos confusa, estimamos que para ofrecer una solución a la misma cabe plantearse la cuestión de si un registro remoto por sí mismo supone una injerencia superior en los derechos a la vida privada, que la que supondría una intervención de las comunicaciones telefónicas o telemáticas. Esta pregunta ya la planteamos[635], a fin de comparar el grado de injerencia de un registro remoto en relación con un registro de dispositivos de almacenamiento masivo, llegando a la conclusión de que, aunque no

[634] Vid. supra apdo. IV.3 de este capítulo, pp. 300-303.
[635] Vid. supra apdo. III.4 de este capítulo, pp. 279-281.

siempre y en todo caso ha de ser así, con carácter general, la clandestinidad y el carácter dinámico del registro remoto, hacen que, *ex ante,* deba considerarse un mayor grado de intromisión en los derechos fundamentales de esta modalidad de registro informático.

Pero lo cierto es que, a esta misma conclusión no podría llegarse si comparamos el registro remoto con la intervención de las comunicaciones telefónicas y telemáticas, que también tienen la nota característica de la clandestinidad y el carácter dinámico. En este sentido se pronunció el Consejo Fiscal de la FGE, señalando que «podría entenderse que esta diligencia no es más invasiva que la de grabación de conversaciones, por lo que desde esta perspectiva no tendría que restringirse su ámbito más de lo que se restringe esta otra diligencia»[636].

Por ello, *de lege ferenda,* estimamos que, en relación con el catálogo de delitos en virtud de los que se podría acordar la medida de investigación, debería establecerse una regulación similar para la intervención de las comunicaciones telefónicas y los registros remotos, en el entendimiento de que no puede apreciarse un mayor grado de injerencia en los derechos fundamentales a la vida privada de una en relación con la otra. En este sentido, consideramos que el problema quedaría resuelto, incluyendo en el catálogo de delitos establecidos para los registros remotos los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión y los delitos cometidos en el seno de grupos criminales.

5. Especialidades respecto de la resolución que autorice el registro

Además de los requisitos generales ya estudiados, que rigen el contenido de la resolución judicial de toda medida de investigación tecnológica y que se encuentran regulados en el art. 588 bis c LECrim, el art. 588 septies a.2 se ocupa de los elementos que específicamente deberán figurar en la resolución que autorice un registro remoto, estableciendo los siguientes:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

---

[636] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 119.

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Algunos de estos requisitos de la resolución judicial ya han sido examinados con carácter general para todas las medidas de investigación tecnológica, así como en el apartado II de este capítulo dentro de los aspectos comunes a las dos modalidades de registros informáticos. Así ocurre con los dispositivos que pueden ser objeto de intervención, el alcance o extensión de la medida o la autorización para la realización y conservación de copias de los datos informáticos.

Cabe destacar, como especialidades dentro del el ámbito de los registros remotos, los siguientes aspectos:

- En primer lugar, se exige que conste la forma en la que se procederá al acceso y el software mediante el que se ejecutará la medida. Se trata de elementos que deberán ser expuestos en la petición que se efectúe por los equipos policiales de investigación al juez competente, y cuya constancia refuerza el derecho de defensa del investigado, quien tendrá la posibilidad de impugnar la intervención cuando esta no se ajuste a lo estrictamente acordado[637]. No obstante, la eventual impugnación por parte del investigado, será a posteriori, habida cuenta de que las diligencias de investigación de este tipo son secretas.

[637] Señala a este respecto la Circular 5/2019 de la FGE que «con el conocimiento de estos datos podrá el investigado comprobar si efectivamente el programa utilizado permite únicamente lo que el juez haya autorizado o, por el contrario, va más allá, lo que podría generar vicios de la medida por haberse extralimitado en la intromisión judicialmente autorizada». Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 61.

- En segundo término, cabe subrayar la necesidad de que se especifiquen los agentes autorizados para la ejecución de la medida, lo que adquiere especial importancia en orden a la probanza de todos los aspectos relevantes de la intervención, tanto para la acusación o acusaciones como para la defensa, dado que, lo normal será que los agentes sean citados como testigos para la celebración del juicio oral, donde serán sometidos a las preguntas de todas las partes.

- Finalmente, se han de hacer constar las medidas precisas para la inaccesibilidad o supresión de determinados datos del sistema informático al que se ha tenido acceso. Se trata de una previsión dirigida a aquellos casos en los que se encuentren archivos digitales que sean considerados instrumentos o efectos del delito, como puede ocurrir con imágenes o videos pedófilos o archivos digitales relacionados con un delito contra la propiedad industrial. A diferencia de los registros de dispositivos de almacenamiento masivo, donde lo normal será que, cuando se den estos supuestos, se intervengan los equipos informáticos, tratándose de un registro remoto no es posible esta intervención, por lo que tales archivos deberán hacerse inaccesibles o suprimirse del sistema informático objeto del registro, obviamente preservando previamente la integridad de dichos datos mediante las medidas que igualmente deberán consignarse en la resolución judicial.

6. Exclusión de la posibilidad de intervención urgente por parte de la Fiscalía o la Policía Judicial

El legislador, a diferencia de lo establecido para los registros de dispositivos de almacenamiento masivo de información, no ha previsto la posibilidad de que pueda llevarse a cabo un registro remoto con carácter de urgencia, comunicándolo posteriormente a la autoridad judicial.

En nuestra opinión, esta particularidad se debe a dos razones: en primer lugar, a la conveniencia de que la procedencia de una diligencia de un carácter tan invasivo sobre los derechos fundamentales a la vida privada, sea examinada por el juez competente, quien deberá motivar el cumplimiento de los principios constitucionales rectores aplicables a las medidas de investigación tecnológica, y muy especialmente los de proporcionalidad y necesidad; y, en segundo lugar, por cuanto no parece que sea necesario establecer dicha posibilidad en una medida que previamente a su ejecución siempre requerirá una investigación pormenorizada, que permita bien la obtención de

datos de identificación y códigos, o en su caso el estudio de la forma en la que se instalará un programa espía en el equipo investigado.

Podría, no obstante, suscitarse el interrogante relativo a la causa por la que sí se permite la intervención urgente para la interceptación de las comunicaciones telefónicas y telemáticas por parte del Ministro del Interior, o, en su defecto, por el Secretario de Estado de Seguridad, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida (art. 588 ter d.3 LECrim), y, sin embargo, no se permite esta actuación para los registros remotos, cuando lo cierto es que se trata, como ya hemos puesto de manifiesto anteriormente[638], de medidas que suponen una injerencia semejante en los derechos fundamentales a la vida privada.

Incluso cabría plantearse, teniendo en cuenta que una intervención de las comunicaciones puede practicarse mediante un acceso remoto, si para los registros remotos podría ser de aplicación lo dispuesto en el referido art. 588 ter d.3 LECrim, aun cuando, como dice dicho precepto, con la obligación de comunicar la intervención inmediatamente, y en todo caso, dentro del plazo máximo de veinticuatro horas 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, pudiendo el juez, también de forma motivada, revocar o confirmar la actuación en un plazo máximo de setenta y dos horas desde que fue ordenada.

Tal y como dijimos anteriormente, en el apartado de este mismo epígrafe dedicado a la interceptación de las comunicaciones telemáticas mediante registro remoto, en el caso de que se acordase una intervención exclusiva de las comunicaciones telemáticas mediante un acceso remoto a un equipo informático, debería preponderar la normativa relativa a la interceptación de las comunicaciones[639].

Por tanto, en nuestra opinión, no existe impedimento legal para que pueda acordarse la interceptación urgente de comunicaciones telemáticas mediante un registro remoto de acuerdo con el art. 588 ter d.3 LECrim. Ahora bien, esto solo será posible cuando el registro se ciña, única y exclusivamente, a una intervención de las comunicaciones telemáticas, sin que, en ningún caso pueda procederse de este modo,

[638] Vid. supra último párrafo del apdo. 4.2 de este mismo epígrafe, p. 312.
[639] Vid. supra los dos últimos párrafos del apdo. 3 de este mismo epígrafe, pp. 302-303.

cuando se pretenda un registro remoto informático propiamente dicho. Es decir, si el alcance de la medida se extendiera a la obtención de archivos digitales de cualquier tipo, excediendo una interceptación de comunicaciones, consideramos que no sería posible este procedimiento, sino que habría que instar al juez competente el dictado del correspondiente auto que permitiese la intervención.

Ciertamente, como señala BACHMAIER WINTER, «la regulación legal no es clara en este punto»[640]. No obstante, discrepamos parcialmente de la afirmación de esta autora, cuando señala que se inclina «por una interpretación garantista, que excluya la posibilidad de instalar *spyware* si no se ha obtenido previamente la debida autorización judicial»[641], a la cual nos adherimos, como acabamos de indicar, siempre que la intervención no se limite a la interceptación de las comunicaciones, sino que se pretenda la obtención de archivos digitales mediante un registro remoto.

En este sentido, consideramos que, donde la ley no ha distinguido, no debemos distinguir, y por ello, del mismo modo que para un registro remoto no es posible una intervención policial urgente sin la previa autorización judicial por no permitirlo expresamente la ley, para la interceptación de las comunicaciones no está prohibida la misma, siendo por otro lado necesario, en todo caso, un acceso remoto para tal interceptación.

7. Duración máxima de la medida

El preámbulo de la LO 13/2015, del mismo modo que lo hace en relación a los delitos respecto de los que puede ser acordado un registro remoto, justifica en su apartado IV, por el intenso grado de injerencia que implica su adopción, el reforzamiento del ámbito objetivo de la medida, «limitando la duración temporal». Como ya hemos estudiado con carácter general para todas las medidas de investigación tecnológica, y muy especialmente en lo que respecta a los registros remotos de equipos informáticos, de tener esta medida una duración indefinida, estaríamos ante una actuación desproporcionada y contraria al principio de seguridad jurídica[642].

---

[640] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 20.
[641] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 20.
[642] Vid. supra apdos. III.1, 2 y 3 del capítulo III, pp. 167-172.

El legislador, ha fijado esta duración en el art. 588 septies c LECrim, disponiendo que «la medida tendrá una duración máxima de un mes, prorrogable por iguales periodos hasta un máximo de tres meses». En todo caso, hay que tener presente lo dispuesto en el art. 588 bis e.1 LECrim, que en su segundo inciso dispone que las medidas «no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos».

Se trata de una duración, en nuestra opinión, demasiado breve, si tenemos en consideración que esta medida será utilizada únicamente en casos especialmente graves en los que seguramente será necesaria una mayor duración de la investigación. Pero, con independencia de la valoración que pueda tener este concreto plazo de intervención, cuya fijación afirma VELASCO NÚÑEZ que ha sido «consecuente con el miedo del legislador a la medida que ha regulado»[643], lo que llama la atención nuevamente, como en otros aspectos ya estudiados, es la diferencia existente entre este plazo y el establecido para la interceptación de las comunicaciones telefónicas y telemáticas, respecto de las que el art. 588 ter g LECrim, dispone que será de tres meses, prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

MARCHENA GÓMEZ se ha posicionado a favor de este plazo, señalando que aunque es cierto que la duración de la vigencia de esta medida se reduce frente a otras diligencias «lo impone así su propia naturaleza, cuya excepcionalidad forma parte de su esencia»[644], recordando que el Anteproyecto de LECrim de 2013 reducía todavía más el ámbito temporal de su validez, dado que en el art. 352 señalaba que su duración máxima no podía exceder de diez días[645].

En nuestra opinión, ya hemos indicado que no puede considerarse de una forma absoluta que un registro remoto suponga un mayor grado de injerencia en los derechos fundamentales a la vida privada, que una interceptación de las comunicaciones telefónicas o telemáticas, por lo que nos parece excesiva esta diferencia tan elevada en el

[643] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 33.
[644] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 390.
[645] MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», cit., p. 390.

plazo de duración, más aún habida cuenta de que ambas medidas únicamente pueden ser acordadas cuando se investiguen delitos de especial gravedad.

En este sentido se ha manifestado URIARTE VALIENTE, cuando muestra su desacuerdo en relación con la diferencia del plazo máximo de duración de los registros remotos en relación con otras medidas[646] y se remite a la opinión puesta de manifiesto en el Informe del Consejo Fiscal al Anteproyecto de la LO 13/2015, al señalar que esta duración máxima podría ser la misma que la prevista para las intervenciones telefónicas, recordando que la que la posibilidad de acordar esta diligencia se refiere a delitos de extrema gravedad, así como que no debe el Estado autolimitarse injustificadamente en el cumplimiento de su deber de investigar los delitos, siendo la eficacia del proceso penal un elemento del Estado de Derecho[647].

Por nuestra parte, estimamos, en línea con la opinión puesta de manifiesto por el Consejo de Estado en el Informe al Anteproyecto de la LO 13/2015, que pudiera ser aconsejable un moderado aumento del plazo de un mes, sin que, tratándose de registros informáticos, esté justificado que el plazo pueda llegar al establecido para las intervenciones telefónicas o telemáticas[648]. Cuestión distinta, en línea con lo estudiado anteriormente, sería el caso de una intervención de las comunicaciones telemáticas mediante un acceso remoto, en cuyo caso, una correcta interpretación exige la aplicación de la normativa prevista para la interceptación de las comunicaciones telefónicas y telemáticas.

En cuanto al *dies a quo* para el inicio de la intervención, no se efectúa mención alguna en el art. 588 septies LECrim, a diferencia, nuevamente, de lo previsto para otras medidas, en las que se establece que el plazo se computará desde la fecha de

[646] URIARTE VALIENTE, L. M., «Nuevas técnicas de investigación restrictivas de derechos fundamentales», cit., p. 39.
[647] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., pp. 122-123.
[648] CONSEJO DE ESTADO, «*Dictamen 97/2015, 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 tecnológica*», cit., p. 22.

autorización judicial[649]. Es cierto que en el caso de las intervenciones telefónicas, la interceptación es prácticamente inmediata una vez que se remite la oportuna comunicación a la operadora prestadora de servicios, lo que no ocurre con los registros remotos en los que, cuando se trata de la instalación de un programa espía, habida cuenta de la de la dificultad de su ejecución, esta puede exigir un tiempo adicional que podría superar el mes legalmente previsto. No ocurre así, sin embargo, cuando el acceso remoto se lleva a cabo mediante datos de identificación y códigos, en cuyo caso la Policía Judicial tendrá a disposición los mismos con carácter previo a la solicitud de la oportuna autorización judicial.

Algunos autores, como VELASCO NÚÑEZ, se han postulado a favor de que el plazo se inicie, en los casos de ejecución de la medida mediante software espía, desde que este «se instale y quede operativo»[650], atendiendo precisamente a la complejidad de dicho proceso. Por su parte, la FGE en la Circular 5/2019, considera que «los plazos que establece el art. 588 septies c, se computarán, tanto en su duración inicial como en la duración total, desde la fecha de la resolución judicial autorizante»[651], apoyando su opinión en la STC 205/2005, de 18 de julio, que declaró que posponer el inicio del cómputo del plazo al día en que la medida se haga realmente efectiva, «compromete la seguridad jurídica y consagra una lesión en el derecho fundamental, que tiene su origen en que sobre el afectado pesa una eventual restricción que, en puridad, no tiene un alcance temporal limitado, ya que todo dependerá del momento inicial en que la intervención tenga lugar»[652].

Aunque la mayor parte de la doctrina surgida como consecuencia de la interceptación de las comunicaciones telefónicas, ha resultado aplicable con carácter general a los registros informáticos, ello no puede predicarse de igual modo en relación con la duración de la medida de registros remotos, ni tampoco con una intervención de

[649] Así se encuentra previsto, no solo para la interceptación de las comunicaciones telefónicas y telemáticas en el art. 588 ter g LECrim, sino también para la medida de utilización de dispositivos técnicos de seguimiento y localización en el art. 588 quinquies c LECrim.

[650] VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», cit., p. 34.

[651] FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 70.

[652] La STC 205/2005, de 18 de julio, fue citada al estudiar la «duración de la medida» con carácter general para todas las medidas de investigación tecnológica. Vid. nota al pie n.º 333 y apdos. III.1, 2 y 3 del capítulo III, pp. 167-172.

las comunicaciones telemáticas, que no telefónicas, ya que las dificultades para el acceso remoto a un equipo informático nada tienen que ver con el acceso a las conversaciones telefónicas que, como decíamos, se produce de forma automática una vez que la operadora reciba la orden judicial. Por ello consideramos excesivamente riguroso el criterio relativo al comienzo de la medida desde la resolución judicial.

En todo caso, lo más relevante es la insuficiencia de la LECrim, dado que, probablemente por las dudas sobre donde fijar el inicio del plazo, el legislador, con cierto olvido de la seguridad jurídica, ha dejado a discreción de los jueces una cuestión que, en nuestra opinión, debiera estar regulada legalmente.

Tampoco nos parece admisible dejar el *dies a quo* a partir del imprevisible momento en el que se produzca la instalación del software. Tal y como expusimos en el apartado dedicado a las disposiciones generales[653], y como acabamos de mencionar, así lo declaró la STC 205/2005, de 18 de julio[654].

Ante tales consideraciones, lo más apropiado sería el establecimiento de una solución intermedia, como así la propone GARCIMARTÍN MONTERO, quien sugiere como respuesta a este problema «solicitar al juez en la petición inicial de autorización de la medida que el plazo de ejecución empiece a contar en el momento en que el registro esté preparado para practicarse, informando al juez del inicio de la ejecución cuando esta se produzca»[655].

Un remedio en estos términos, o bien, planteado de otro modo, que se regulase legalmente que deberá solicitarse autorización judicial para la instalación del software y que una vez verificado, se comunique inmediatamente al juez a fin de que pueda fijar la fecha de inicio, a partir de la que se computará el plazo de ejecución de la medida. Lo que si es cierto es que, en nuestra opinión, la regulación actual no respeta íntegramente la seguridad jurídica, y por ello, *de lege ferenda*, proponemos una regulación en el sentido indicado.

---

653 Vid. supra apdo. III.3 del capítulo III, pp. 170-172.

654 Vid. nota al pie n.º 652 y su texto correspondiente en relación con la STC 205/2005, de 18 de julio, p. 319.

655 GARCIMARTÍN MONTERO, R., «*Los medios de investigación tecnológicos en el proceso penal*», cit., p. 126.

Ello es consonante con la propuesta que hicimos al estudiar el cómputo del plazo como disposición general para todas las medidas de investigación tecnológica, en el sentido de que el día y hora concreto en el que la medida deberá iniciarse deba ser fijado en el auto judicial, así como, consecuentemente, el día y hora de su finalización, lo cual es más acorde con la legalidad constitucional, previniendo de este modo el transcurso de plazos excesivos entre el acuerdo y la ejecución de la intervención[656].

8. Control judicial de la intervención y extensión de la medida

A diferencia de los registros de almacenamiento masivo, en los que el control judicial se agota, por la propia naturaleza de la medida, con la práctica del volcado de datos, en los registros remotos de equipos informáticos cobra una trascendental relevancia el control por parte del juez competente, dada la fuerte restricción de los derechos fundamentales a la vida privada que se produce con la misma, y por tratarse de la diligencia de investigación tecnológica que tiene establecido el menor plazo de duración, incluidas las posibles prórrogas.

Poco queda que decir, tras el extenso estudio realizado en relación con el control judicial en el apartado II del capítulo III de este trabajo, dedicado a las disposiciones comunes a todas las medidas de investigación tecnológica. Sin embargo, existe una particularidad que, en relación con el control judicial en esta singular diligencia de registros remotos de equipos informáticos hay que resaltar, y que no es otra que la concerniente al cumplimiento de lo acordado en cuanto a la extensión o alcance de la medida.

Con anterioridad a la LO 13/2015, el TS había declarado, en el ámbito de la intervención de las comunicaciones, que «debe estar suficientemente garantizado que el destino y la destrucción o un eventual uso futuro de los resultados obtenidos, es decir, de la totalidad de las conversaciones telefónicas intervenidas, quedan bajo control judicial, pues la invasión de la intimidad ha sido acordada por el juez solamente respecto a la investigación de un concreto hecho delictivo»[657].

Actualmente, el art. 588 ter f LECrim, establece que la Policía Judicial «…pondrá a disposición del juez, con la periodicidad que este determine y en soportes

[656] Vid. supra último párrafo del apdo. III.3 del capítulo III, p. 172.
[657] Vid. STS 1200/2009, de 25 de noviembre, FJ 1.º apdo. 10.

digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas». Por su parte, el art. 588 ter i LECrim, regula el acceso de las partes a las grabaciones, disponiendo su apartado primero que «alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas» y añadiendo que «si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos», concluyendo este apartado que «la no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso»[658].

Una vez más, se pone de manifiesto la inseguridad del legislador en lo que a los registros remotos de equipos informáticos se refiere, habida cuenta de la inexistente regulación referente al control judicial sobre la extensión de la medida, de modo que, para poder llevar a cabo esta importante función, el juez tiene a su disposición el escueto art. 588 bis g LECrim[659] como disposición común a todas las medidas de investigación tecnológica, y los anteriormente citados arts. 588 ter f y 588 ter i LECrim, respecto de los que podrá plantearse su aplicación analógica, que, en una cuestión de esta trascendencia, aunque pudiendo ser válida, razones de seguridad jurídica no hacen de ella la solución más adecuada.

Ha de tenerse en cuenta, que en un registro remoto son muy diversos los elementos que pueden ser objeto de intervención y suponer una injerencia indebida en los derechos a la vida privada. La concreción de los recursos digitales que pueden

[658] Los apartados 2 y 3 del art. 588 ter i LECrim, disponen lo siguiente:

2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

[659] Cabe recordar que el art. 588 bis g LECrim, bajo la rúbrica «control de la medida», dispone que «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».

aprehenderse, conforme a lo ya estudiado[660], ha de estar especificada en la resolución judicial. Así, en la misma deberán puntualizarse los archivos digitales (audio, imagen, texto, video, bases de datos, ubicación, bancarios, etc.) que han de ser localizados, sin que el registro pueda extenderse más allá de lo acordado.

Es aquí donde adquiere una especial relevancia el control judicial. De este modo, la resolución judicial deberá expresar la forma y periodicidad con la que la Policía Judicial deberá informar de los datos obtenidos. Sin embargo, se echa en falta nuevamente en lo que respecta a los registros remotos, una regulación de estos aspectos, al igual que sí se ha llevado a cabo en relación con la interceptación de las comunicaciones telefónicas y telemáticas. Así lo ha puesto de manifiesto BACHMAIER WINTER, cuando ha señalado que, ante la cuestión relativa a como preservar el derecho a la intimidad de ciertos datos que no están relacionados con el delito, la respuesta no se encuentra en la ley[661].

En cualquier caso, por ahora, y sin perjuicio de que, *de lege ferenda*, estimamos necesaria una mejora legal en lo concerniente al control judicial de la extensión de la medida para los registros remotos, consideramos, tal y como hemos señalado anteriormente, que en este ámbito podría ser de aplicación analógica lo previsto para la intervención de las comunicaciones en los arts. 588 ter f y 588 ter i LECrim. En este sentido, en el plazo o día que el juez determine, deberá ponerse a su disposición el material intervenido dentro de la extensión o alcance acordado, con aplicación de las previsiones establecidas en dichos preceptos en cuanto al aseguramiento del material aprehendido y respetando las prevenciones establecidas en relación con el respeto a los derechos fundamentales a la vida privada, todo ello a fin de poder cumplir con los trámites igualmente establecidos para la incorporación al proceso de los datos relevantes para el proceso y la observancia del principio de contradicción.

9. El agente encubierto

Como hemos venido examinando en este epígrafe dedicado a los registros remotos, la ejecución de los mismos puede llegar a ser realmente compleja. Por ello, la

[660] Vid. supra apdo. II.2 de este capítulo, donde se estudia la extensión de la medida como uno de los aspectos comunes a ambas modalidades de registros informáticos, pp. 241-247.

[661] BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», cit., p. 32.

figura del agente encubierto, con carácter general, coadyuvará a la ejecución del registro remoto, y no tanto el recientemente creado agente encubierto informático, el cual no ha sido precisamente incorporado a la legislación, como veremos a continuación, pensando en esta diligencia de investigación tecnológica.

La regulación del agente encubierto con carácter general, tuvo lugar con la LO 5/1999 de 13 de enero, de modificación de la LECrim, que añadió un artículo 282 bis, con el objeto de combatir la delincuencia organizada, permitiendo el otorgamiento y la utilización de una identidad supuesta por plazo máximo de seis meses prorrogables por periodos de igual duración, a funcionarios de la Policía Judicial, quienes, de forma voluntaria y bajo un estricto control judicial, se infiltrarían en organizaciones criminales, con la finalidad de facilitar la investigación mediante la de adquisición y transporte de los objetos, efectos e instrumentos del delito y difiriendo la incautación de los mismos, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico. En definitiva, como señala VALIÑO CES, «se parte de que el grave problema social que representa la criminalidad organizada, demanda la adopción de técnicas especiales de investigación por parte de la policía, a fin de poder combatir eficazmente este tipo de manifestación criminal»[662].

El TS ha señalado que, con antecedente en el Derecho alemán, el término *undercover* o agente encubierto «será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operando, así como obtener pruebas sobre la ejecución de hechos delictivos»[663].

---

[662] VALIÑO CES, A., «El agente encubierto informático y la ciberdelincuencia: el intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil», en Bueno de Mata, F. (coord.), *Fodertics 5.0*, Albolote (Granada), Editorial Comares, 2016, p. 279.

[663] Vid. STS 1140/2010, de 29 de diciembre, FJ 6.º, que añade que debe aclararse que «es preciso diferenciar esta figura del funcionario policial que de forma esporádica y aislada y ante un acto delictivo concreto oculta su condición policial para descubrir un delito ya cometido o cuando -supuesto de las SSTS. 25.6.2007 y 6.2.2009- un funcionario policial lleva a cabo tareas de investigación antes de llegar a tener el carácter que regula el art. 282 bis, lo que no implica que no pueda servir válidamente como testigo respecto de lo visto y oído en tiempo anterior -lo que diferenciará uno y otro tiempo, es que la exención de responsabilidad penal, que regula el n.º 5 de dicho artículo, para actividades dotadas de proporcionalidad

Como igualmente ha declarado el TS, la reforma de LO 13/2015 ha introducido los apartados 6 y 7 del art. 282 bis de la LECrim, estableciendo la novedosa figura del agente encubierto informático, «tratando el legislador, una vez más, de adaptar el texto legal a la sociedad digitalizada en la que nos encontramos inmersos y enfocando su previsión a la investigación de los delitos llevados a cabo por la delincuencia organizada dispuestos en el apartado 4 del art. 282 bis[664]; de los designados en el art. 579 LECrim, a saber, delitos de terrorismo, delitos cometidos en el seno de una organización criminal o delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; o cualquier otro delito cometido a través de medios informáticos»[665].

Como señala ZARAGOZA TEJADA, la regulación del agente encubierto planteaba especiales problemas en lo que a la investigación de delitos cometidos a través de las nuevas tecnologías se refiere, dado que únicamente se permitía su intervención cuando se tratase de actividades relacionadas con la delincuencia organizada, y que estas se

---

con la finalidad de la investigación y que no constituyan provocación al delito, no será aplicable al periodo previo».

[664] El apartado 4 del art. 282 bis, a los efectos de la autorización del agente encubierto, considera como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los siguientes delitos:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

[665] Vid. STS 140/2019, de 13 de marzo, FJ 4.º

refirieran a delitos contenidos en el apartado 282 bis LECrim, quedando fuera determinadas modalidades delictivas cometidas a través de las TIC[666]. En este sentido, puntualiza VALIÑO CES, que la reforma llevada a cabo por la LO 13/2015 es el resultado de la necesidad ineludible de suplir lagunas de alegalidad, dando de este modo cobertura legal a la actuación del policía infiltrado en espacios no ya privados, sino íntimos del investigado, abarcando ámbitos de delincuencia cada vez más amplios, como es el caso del uso de internet y las nuevas tecnologías[667].

Para solventar este problema, el apartado 6 del referido precepto, con la particularidad de que la actuación de este nuevo agente, únicamente puede ser autorizada por el juez —a diferencia del agente encubierto en general, cuya actuación puede ser autorizada por el Ministerio Fiscal, aunque dando cuenta inmediata a aquel—, dispone que «el juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a». Por su parte, el párrafo segundo de dicho apartado, dispone que «el agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos».

De este modo, habida cuenta de la sensibilidad de los derechos fundamentales a la vida privada ante los avances tecnológicos, se otorga al agente encubierto informático una mayor amplitud en su cometido, permitiendo su actuación, en general, en relación con la investigación de los delitos previstos para poder autorizar tanto los registros remotos de equipos informáticos como la interceptación de las comunicaciones telefónicas y telemáticas, y ello con la finalidad de que, de conformidad con el apartado 5 del art. 282 bis LECrim, el agente se encuentre exento de responsabilidad criminal, siempre que las actuaciones llevadas a cabo guarden la debida proporcionalidad con la finalidad de la investigación y no constituyan una provocación al delito.

---

[666] ZARAGOZA TEJADA, J. I., «La modificación operada por la Ley 13/2015. El agente encubierto informático», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, pp. 18-21, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Zaragoza Tejada, Javier Ignacio.pdf?idFile=d16b7d76-2654-4b4e-abdf-b00f2540d57b, el 9 de junio de 2020.

[667] VALIÑO CES, A., «La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, p. 385.

BUENO DE MATA define esta figura como «un empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red y que causen una gran repulsa y alarma a nivel social»[668], añadiendo que «su función consistiría en la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales»[669].

Con base en todo lo anterior, puede apreciarse que el agente encubierto informático no ha sido creado pensando en la diligencia de registros remotos sobre equipos informáticos, sino más bien se encuentra orientado a la persecución de delitos, en virtud de cuya comisión circulan por la red archivos ilícitos, como puede ser el caso de los delitos de terrorismo, propiedad intelectual, y muy especialmente, los relativos a la prostitución y a la explotación sexual y corrupción de menores.

Sin embargo, como así lo ha puesto de manifiesto el Informe del Consejo Fiscal al Anteproyecto de la LO 13/2015, la dicción literal del precepto cuando señala que el agente «podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido» puede llevar a la interpretación de que un archivo ilícito «no es solamente aquel cuyo contenido puede vulnerar bienes jurídicamente protegidos, sino también el que contiene un software con un ejecutable cuyo cometido esté orientado a la investigación criminal»[670], dado que «un archivo ilícito puede tener muy distintas finalidades, algunas de las cuales pueden ser válidas para la investigación criminal como monitorizar las pulsaciones del teclado; realizar capturas de pantallas o control y seguimiento de acciones del usuario, pero otras tienen una naturaleza claramente

[668] BUENO DE MATA, F., «Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la LO 13/2015», en Bueno de Mata, F. (coord.), *Fodertics 4.0*, Albolote (Granada), Editorial Comares, 2015, p. 118.

[669] BUENO DE MATA, F., «Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la LO 13/2015», en Bueno de Mata, F. (coord.), *Fodertics 4.0*, Albolote (Granada), Editorial Comares, 2015, p. 118.

[670] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 28.

delictiva como la integración del dispositivo en una *botnet* (conjunto de robots informáticos que se ejecutan de manera autónoma y automática)»[671].

Autores como RICHARD GONZÁLEZ se refieren a la posibilidad de que los registros remotos se autoricen asociados a la figura del agente encubierto informático, señalando que «parece del todo punto lógico que la autorización de un agente encubierto que participa en las comunicaciones pueda estar respaldada o asociada a una medida de registro remoto previa, simultánea o posterior»[672]. Por su parte JIMÉNEZ SEGADO Y PUCHOL AIGUABELLA afirman en relación con los registros remotos, que «complementa esta medida, la posibilidad de autorizar judicialmente a la Policía Judicial de actuar con identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación»[673].

En efecto, existe una estrecha relación entre ambas intervenciones, ya que los canales cerrados de comunicación como foros, chats o grupos privados en redes sociales[674], pueden servir para obtener datos de identificación o códigos y, del mismo modo, podrían ser la vía adecuada para la instalación de software espía en un equipo informático.

Por ello, nos parece correcta la opinión puesta de manifiesto en el Informe del Consejo Fiscal al Anteproyecto de la LO 13/2015, que estima necesaria una regulación más detallada en la materia, dado que, no obstante suponer un avance necesario respecto a la regulación anterior, resulta en sí misma insatisfactoria, habida cuenta de que las potencialidades que ofrece la utilización del agente encubierto en las investigaciones *on-*

---

[671] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 28

[672] RICHARD GONZÁLEZ, M., «La Investigación y prueba de hechos y dispositivos electrónicos», cit., p. 21.

[673] JIMÉNEZ SEGADO, C.; PUCHOL AIGUABELLA, M., «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos», cit., p. 10.

[674] De acuerdo con lo señalado por CABEZUDO RODRÍGUEZ, cuando los rastreos o sondeos con fines preventivos o investigativos, llevados a cabo por las FCSE, se lleven a cabo dentro de la Red pública, no se requiere ninguna garantía adicional más que su previsión legal, que se viene a considerar comprendida dentro de las facultades propias de estos Cuerpos Policiales (art. 282 LECrim y art. 11.1 LOFCS), con el sustento que proporciona el Convenio de Budapest en su art. 32. Vid. CABEZUDO RODRÍGUEZ, N., «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», cit., pp. 36-37.

line, demanda de un tratamiento conjunto en aras a hacer posible una mayor coherencia que facilite la interpretación y aplicación de la norma reguladora[675].

No obstante, y sin perjuicio de que podría mejorarse la técnica legislativa regulando los aspectos más relevantes de la posible intervención del agente encubierto en el ámbito de los registros remotos informáticos, nos parece plausible la incorporación legal de esta figura, si tenemos en consideración que con la misma se garantiza, con la necesaria intervención judicial para su autorización, el respeto a los derechos fundamentales a la vida privada, que tan vulnerables se muestran dentro del entorno virtual.

10. Forma de ejecución

En cuanto a la forma de ejecución, de conformidad con lo establecido en el art. 588 septies a.2 b) LECrim, la resolución judicial que autorice el registro deberá especificar «la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información».

Por tanto, la Policía Judicial, con anterioridad a la solicitud de autorización, habrá tenido que llevar a cabo una investigación preliminar sobre el modo en el que se accederá al concreto equipo informático de forma remota y el software utilizado. En este momento, cobra especial importancia el agente encubierto, cuya actuación con la vigente regulación debería haber sido instada con anterioridad, a los efectos de poder obtener datos de identificación o códigos o asegurarse la confianza de la organización criminal a fin de poder instalar remotamente un software espía mediante el envío del mismo mediante programas de mensajería o correo electrónico. Como apuntábamos en el apartado anterior, una mejora legislativa, con un tratamiento conjunto de la medida de registros remotos y la intervención del agente encubierto informático, podría agilizar la intervención, si bien habrá que estar atentos a la evolución tanto de la propia diligencia en sí como de las aportaciones de la informática.

---

[675] CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, «*Informe 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 tecnológica*», cit., p. 29.

En cuanto a la forma en la que se procederá a la aprehensión de los datos relevantes para la causa, esta dependerá de lo acordado respecto del alcance o extensión de la medida. En efecto, a modo de ejemplo, la forma no será la misma si se acuerda la intervención de las comunicaciones realizadas por correo electrónico o por un programa de mensajería en un momento determinado, que si se pretende visualizar la actividad dentro de un canal cerrado de conversación. En el primer caso bastará el copiado de los mensajes, mientras que en el segundo la aprehensión se llevaría a efecto mediante la grabación mediante un programa de captura de pantalla en tiempo real.

De conformidad con los apartados c) y d) del art. 588 septies a.2 LECrim, se deberá especificar en la resolución judicial, la autorización, en su caso, para la realización y conservación de copias de los datos, y las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

Este último inciso, tendrá lugar en aquellos casos en los que, por la notoria ilicitud de los datos que puedan encontrarse en los equipos registrados, como en los casos de delitos contra la propiedad intelectual y los relativos a la prostitución y a la explotación sexual y corrupción de menores, se haga necesario impedir el acceso a determinados sitios web o en su caso eliminar del disco duro los archivos ilegales. Por su parte, tratándose de registros remotos, lo normal será autorizar la realización de copias de los datos que se obtengan, para su incorporación al proceso.

Finalmente, y del mismo modo que dijimos en su momento en el ámbito de los registros de dispositivos de almacenamiento masivo de información, lo referente a la conservación de los datos y las medidas para su preservación, será objeto de estudio en el apartado dedicado a la cadena de custodia dentro del siguiente capítulo de esta obra, relativo a la eficacia probatoria de las diligencias de registros informáticos, del que pasamos a ocuparnos a continuación.

CAPÍTULO VI. EFICACIA PROBATORIA DE LOS REGISTROS INFORMÁTICOS

I. Sinopsis

Hemos realizado un amplio recorrido desde el momento en el que ha de acordarse y ejecutarse una diligencia de investigación consistente en un registro informático, lo que nos ha llevado a examinar: los derechos fundamentales susceptibles de ser vulnerados, que han sido analizados desde una visión general aplicable a todas las diligencias de investigación tecnológica; las disposiciones comunes establecidas en la LECrim para todas ellas; y finalmente, han sido estudiadas, con ánimo de exhaustividad, todas las particularidades y cuestiones controvertidas, tanto de los registros de dispositivos de almacenamiento masivo, como de los registros remotos sobre equipos informáticos.

Llegados a este punto, procede ocuparnos de la eficacia probatoria de estas peculiares medidas de investigación. No es nuestra intención profundizar en el estudio la prueba, una de las materias de mayor enjundia del derecho procesal, cuyo examen, obviamente, excedería la finalidad de este trabajo.

Lo que pretendemos, siendo en definitiva uno de los objetivos de esta tesis, es realizar un detenido análisis de los aspectos que conforman el procedimiento a través del que el resultado de un registro informático practicado como una diligencia de investigación penal, deberá incorporarse válidamente a los autos, sin que, por tanto, dicha entrada al proceso penal pueda ser tachada de irregular.

Las cuestiones analizadas son las siguientes:

1.º La teoría sobre la prueba ilícita, dado que, de no practicarse la ejecución de la intervención de acuerdo con los principios rectores, se incurriría en ilegitimidad constitucional de la misma, lo que provocaría la no incorporación o, en su caso, la exclusión del proceso de la fuente de investigación.

2.º La cadena de custodia, que asegurará la integridad del material obtenido, así como su identidad con los datos obrantes inicialmente en los equipos registrados.

3.º Los medios de prueba válidos para la incorporación al juicio oral de las fuentes obtenidas con la diligencia de investigación.

4.º Finalmente, se hace necesario un breve examen sobre los aspectos procesales de la impugnación de la prueba digital, teniendo en cuenta que, de producirse la misma,

puede resultar necesaria, si así lo estima el tribunal, una prueba complementaria para la definitiva incorporación y consecuente valoración de la fuente de prueba.

Examinaremos en distintos apartados cada uno de ellos, si bien, con carácter previo, dedicaremos un epígrafe a realizar unas breves consideraciones en relación con la prueba en general y la prueba digital.

II. La prueba

1. Concepto y alcance constitucional

La CE proclama como derecho fundamental en el art. 24.2 dentro de las llamadas proyecciones del derecho a la tutela judicial efectiva[676], el derecho a la utilización de medios de prueba para la defensa, derecho que, conforme ha declarado la jurisprudencia del TC, «consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el juez o Tribunal»[677].

Como tal proyección del derecho a la tutela judicial efectiva, es este un derecho instrumental, dado que «es el medio que el Ordenamiento jurídico pone a disposición de

[676] VIDAL PRADO, C., «Derechos educativos. Derecho a la tutela judicial efectiva», en García-Atance y García de Mora, M. V., Gutierrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, p. 220.

[677] Vid. STC 30/1986, de 20 de febrero, FJ 8.º que declaró que «…cabe destacar que el art. 24.2 de la Constitución ha convertido en un derecho fundamental el de "utilizar los medios de prueba pertinentes" en cualquier tipo de proceso en que el ciudadano se vea involucrado. Este derecho fundamental, inseparable del derecho mismo a la defensa, consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el juez o Tribunal y, al haber sido constitucionalizado, impone una nueva perspectiva y una sensibilidad mayor en relación con las normas procesales atinentes a ello, de suerte que deben los Tribunales de Justicia proveer a la satisfacción de tal derecho, sin desconocerlo ni obstaculizarlo, siendo preferible en tal materia incurrir en un posible exceso en la admisión de pruebas que en su denegación.
Ello no implica, de conformidad con la doctrina constitucional que se cita, desapoderar al juzgador *a quo* de su potestad para pronunciarse sobre la pertinencia de las pruebas que las partes propongan, competencia ésta que, por lo que aquí importa, le confiere el art. 659 de la Ley de Enjuiciamiento Criminal; sino acoger, con el espíritu que informa el art. 24.2 de la Constitución en su virtualidad antes descrita, las peticiones de admisión a prueba en cuanto no sea manifiesta la ausencia de adecuación entre la que se propone y la cuestión debatida. Para prestar consistencia a una queja motivada en el indebido rechazo de un medio de prueba será, pues, necesario que se argumente por el demandante de amparo la trascendencia que dicha inadmisión, por la relevancia misma de los hechos que así se quisieron probar, pudo tener en la sentencia condenatoria, ya que sólo en tal caso —comprobado que el fallo pudo, acaso, haber sido otro si la prueba se hubiera admitido— podrá apreciarse también el menoscabo efectivo del derecho de quien por este motivo busca amparo».

las personas para defender sus bienes y derechos»[678]. A ello podemos añadir que difícilmente se podría hacer efectiva la justicia, como valor superior de nuestro ordenamiento jurídico proclamado en el art. 1 CE, de no admitirse este derecho a la utilización de los medios de prueba pertinentes.

Entre las numerosas definiciones que se han facilitado, uno de los autores clásicos del Derecho Procesal patrio, como es GÓMEZ ORBANEJA, define la prueba como «aquella actividad procesal encaminada a producir en el juez el convencimiento de la verdad o no verdad de la alegación de un hecho, o bien, a fijar los hechos necesitados de prueba como dados independientemente de ese convencimiento, en virtud de unas reglas de valoración legal: la prueba legal»[679].

De forma más moderna, nos parece acertado el concepto aportado con carácter general por BARONA VILAR, quien define la prueba como «la actividad procesal, de las partes (de demostración) y del juez (de verificación), por la que se pretende lograr el convencimiento psicológico del juzgador acerca de la verdad de los datos allegados al proceso»[680].

Por lo que respecta al ámbito del proceso penal, nos adherimos a la opinión de JIMÉNEZ CONDE, quien afirma que la prueba es aquella «actividad que llevan a cabo las partes y el tribunal, dirigida a formar la convicción de este último acerca de la verdad o certeza de los hechos relevantes en el proceso y que se relatan en los escritos de calificación»[681].

En cuanto a la doctrina del TC sobre el derecho a utilizar los medios de prueba pertinentes en el proceso penal, nos parece muy ilustrativa la STS 371/2017, de 23 de mayo, FJ 4.º, que lleva a cabo un resumen de la doctrina expuesta en las SSTC 86/2008, de 21 de julio y 80/2011, de 6 de junio, declarando, entre otras cuestiones, lo siguiente:

---

[678] REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», cit., p. 220.

[679] GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., *Derecho Procesal Civil, Vol. I*, Madrid, Artes Gráficas y Ediciones, 1979, p. 287.

[680] BARONA VILAR, S., «La prueba (I y II)», en Montero Aroca, J. y otros), *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, p. 374.

[681] JIMÉNEZ CONDE, F., *Introducción al Derecho Procesal Penal*, Murcia, Diego Marín Librero Editor, 2017, p. 123.

a) Nos encontramos ante un derecho fundamental de configuración legal. Para entenderlo lesionado será preciso que la prueba no admitida o no practicada se haya solicitado en la forma y momento legalmente establecidos, sin que en ningún caso pueda considerarse menoscabado este derecho cuando la inadmisión de una prueba se haya producido debidamente en aplicación estricta de normas legales cuya legitimidad constitucional no pueda ponerse en duda.

b) No es un derecho que tenga carácter absoluto, dado que no faculta para exigir la admisión de todas las pruebas que puedan proponer las partes en el proceso, sino que atribuye únicamente el derecho a la recepción y práctica de aquellas que sean pertinentes, correspondiendo a los órganos judiciales el examen sobre la legalidad y pertinencia de las pruebas solicitadas.

c) El órgano judicial ha de motivar razonablemente la denegación de las pruebas propuestas, de modo que puede resultar vulnerado este derecho cuando se inadmitan o no se practiquen pruebas relevantes para la resolución final del asunto litigioso sin motivación alguna, o la que se ofrezca resulte insuficiente, o supongan una interpretación de la legalidad manifiestamente arbitraria o irrazonable.

d) No toda irregularidad u omisión procesal en materia de prueba puede causar por sí misma una indefensión constitucionalmente relevante, pues la garantía constitucional contenida en el artículo 24.2 CE únicamente cubre aquellos supuestos en los que la prueba es decisiva en términos de defensa. En concreto, para que se produzca una violación de este derecho, es necesario en primer lugar que la denegación o la no práctica de las pruebas sea imputable al órgano judicial, y en segundo lugar que la prueba denegada o no practicada resulte decisiva.

2. La prueba digital

2.1. Ideas generales

Como afirma ABEL LLUCH, han sido numerosas las expresiones para aludir a las pruebas derivadas de las TIC. Señala este autor que «para aludir a las pruebas derivadas de las nuevas tecnologías de la información y comunicación [...] se han utilizado diversas expresiones, tales como, entre otras, prueba por soportes informáticos, prueba instrumental, prueba por medios reproductivos, prueba audiovisual, prueba por documentos electrónicos, prueba por registros, prueba tecnológica, documentos

multimedia, prueba documental electrónica y multimedia, documento procesal electrónico, la reproducción de la imagen y del sonido y los instrumentos informáticos, los nuevos medios reconocidos, medios de reproducción audiovisual y medios de archivo y reproducción de la información mediante instrumentos»[682].

Por nuestra parte, consideramos que la forma más apropiada de referirse a la prueba derivada de las TIC es la de «prueba digital» como así lo hacen algunos autores[683]. Estimamos más adecuada esta terminología, dado que, si nos atenemos al DRAE, lo digital es lo relativo a los medios[684]; es decir, para que algo pueda ser probado a través de las TIC se precisará la representación en medio digital de documentos electrónicos de texto, imagen, audio o sonido.

Por su parte, «electrónico» se refiere a todo lo referido a la electrónica[685]. En tal sentido, nos parece más acertado llamar «prueba digital» a la representación a través de medios digitales de todo aquello con lo que se pretende llegar a un convencimiento del juez o tribunal. A todas las fuentes que sean representadas a través de dichos medios digitales, las denominaremos documentos electrónicos.

Cabe a continuación preguntarse por el concepto de prueba digital. DELGADO MARTÍN la define como «toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio»[686]. En una línea similar, y partiendo de la definición que facilitamos de prueba en general, así como de lo mencionado anteriormente, afirmaremos que estaremos ante una prueba de contenido digital cuando los datos allegados al proceso tengan tal carácter, lo cual se producirá cuando dichos datos se contengan en documentos electrónicos.

---

[682] ABEL LLUCH, X., «Prueba electrónica», en Abel LLuch, X., Picó i Junoy, J. (dirs.), *La prueba electrónica*, Barcelona, Bosch Editor, 2011, pp. 21-22.

[683] Pueden mencionarse entre otros, DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit.; CUADRADO SALINAS, C., «Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa», *La Ley Penal - Sección Estudios*, n.º 107, 2014.; BUJOSA VADELL, L. M., «Tecnologías de la imagen y valoración de la prueba», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017; y MAGRO SERVET, V., «¿Como se aporta la prueba digital al proceso civil?», *Revista de Jurisprudencia - El Derecho*, n.º 2, Junio, 2015.

[684] Según la cuarta acepción de «digital» de la 23.ª edición del DRAE.

[685] Como igualmente se desprende de la 23.ª edición del DRAE.

[686] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 42.

2.2. Marco normativo

La prueba digital, al margen de las consideraciones sobre el documento electrónico que realizaremos más adelante, no tiene un reconocimiento expreso en la LECrim. Sin embargo, en la LEC, de aplicación supletoria al proceso penal y a los de las demás jurisdicciones[687], sí se prevé en el art. 382.1, disponiendo que «las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes».

Por su parte, los aspectos referentes a la práctica de prueba digital se encuentran reconocidos en nuestro ordenamiento procesal por el art. 299.2 LEC, que, al referirse a los medios de prueba de que se podrá hacer uso en juicio, dispone que «también se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

Cabe señalar que el art. 299.2 ha sido objeto de alguna crítica doctrinal. Así, por ejemplo, MONTERO AROCA afirma, en relación con este precepto, lo siguiente:

«1.º) Reitera inútilmente, pues los medios de reproducción de la palabra y del sonido son los mismos (la palabra es un sonido).

2.º) Confunde al intérprete, al hablar de "medios de prueba" y de "medios de reproducción", pues los primeros son una actividad procesal y los segundos una cosa física.

3.º) Es manifiesto que no se ha comprendido la distinción entre fuentes de prueba y medios de prueba, pues lo importante no es que diga que se considerarán fuentes de prueba los soportes físicos de grabaciones de imágenes o sonidos y los llamados documentos informáticos, lo que es sin duda obvio, sino que configurara un verdadero

[687] Cabe recordar que el art. 4 de la LEC establece el carácter supletorio de la LEC en relación con las demás leyes procesales, al disponer que «en defecto de disposiciones en las leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley».

medio de prueba, es decir, una actividad, a través del cual se aportaran esas fuentes al proceso»[688].

Consideramos que, *de lege ferenda*, debieran regularse los aspectos referentes a las fuentes de prueba digitales en la LECrim, con las particularidades propias del proceso penal, así como la reproducción de la imagen, el audio y el video, como el medio de prueba idóneo para la práctica de la prueba digital. De este medio de prueba, y de la necesidad de su regulación en la LECrim, nos ocuparemos más adelante en el epígrafe dedicado a los medios de prueba válidos para la incorporación de la prueba digital al proceso y, más concretamente, en el apartado dedicado a los medios de reproducción de la palabra, el sonido, la imagen e instrumentos de archivo.

No obstante todo lo anterior, a la vista de la ausencia de regulación en la LECrim y la escueta regulación de la LEC, y teniendo en cuenta el concepto que facilitamos en el último párrafo del apartado anterior, podemos concluir que el objeto de la prueba digital consistirá en los documentos electrónicos que se aporten al proceso. Teniendo en cuenta que legalmente no existe un medio concreto para ello, esta aportación podrá verificarse por cualquiera de los medios establecidos en la Ley, entre los que adquiere especial relevancia «la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo» conforme a lo dispuesto en el art. 299.2 LEC.

2.3. El documento electrónico

En consonancia con lo que acabamos de exponer, para la utilización en el proceso de un medio de prueba digital, deberá incorporarse al mismo un concreto documento electrónico.

Este, ha de ser contemplado, desde un punto de vista amplio, como un documento en el que de cualquier forma haya intervenido la informática en en su elaboración. Puede, en general, tratarse de un archivo de texto, de audio, de imagen o de video.

En realidad, el concepto de documento electrónico queda comprendido dentro del concepto de documento en general. En este sentido, tal y como ponen de manifiesto

[688] MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 7, 2000, pp. 46-47, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

INSA MÉRIDA Y LÁZARO HERRERO, en un buen número de países europeos, entre los que se encuentra España (además de Alemania, Bélgica, Finlandia, Francia, Irlanda, Italia, Luxemburgo, Portugal y Rumania), existe legalmente una equivalencia entre documento electrónico y documento en papel[689].

En efecto, en España, el CP facilita una definición de documento en este sentido, al disponer en el art. 26 que: «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».

Este concepto amplio del documento, en general, coincide, *mutatis mutandis*, en lo que se refiere a su estructura, con el que, en relación con el documento electrónico, se describe en el art. 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y con el del anexo que contiene las definiciones 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, en el que se establece que documento electrónico es la «información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado».

Por su parte, la jurisprudencia del TS también ha interpretado el concepto de documento electrónico en un sentido amplio, y tras recordar que:

a) El art. 230.2 LOPJ atribuye en el ámbito de la Administración de Justicia a los documentos emitidos por procedimientos electrónicos, informáticos y telemáticos la misma validez y eficacia que un documento original siempre que quede garantizada su autenticidad, integridad y los requisitos exigidos por las leyes procesales.

b) El artículo 135 LEC dispone que las oficinas judiciales y los intervinientes en un proceso estarán obligados al empleo de los sistemas telemáticos y electrónicos existentes en la Administración de Justicia y recibirán todos los escritos y demás documentos a través de esos sistemas.

Ha declarado que «lo que interesa de esos preceptos, al margen de su utilidad en el ámbito procesal, es el reconocimiento legal del documento electrónico como una

[689] INSA MÉRIDA, F.; LÁZARO HERRERO, C., «La admisibilidad de las pruebas electrónicas en los tribunales: Luchando contra los delitos tecnológicos», *Diario La Ley - Sección Doctrina*, n.º 6708, 2007, pp. 5-7.

nueva clase de documento con la misma eficacia jurídica que el documento tradicional», declarando asimismo que «el soporte papel ha sido superado por las nuevas tecnologías», y que «cualquier sistema que permita incorporar ideas, declaraciones, informes o datos susceptibles de ser reproducidos en su momento, suple con ventajas al tradicional documento escrito, siempre que existan instrumentos técnicos que permitan acreditar la fiabilidad y seguridad de los impresos en el soporte magnético»[690].

Con base en todo lo expuesto, concluiremos que, a los efectos de la prueba en el proceso, un documento electrónico viene constituido por cualquier información en forma electrónica que pueda ser reproducida o representada por medios digitales.

3. La preconstitución de la prueba

3.1. Consideraciones previas

Aun cuando hemos defendido la necesidad de una nueva LECrim más ajustada a la realidad de la época actual[691], no podemos sino elogiar el texto legal decimonónico, muy especialmente por el cambio radical, en pro de los derechos del justiciable, que supuso en aquel momento. Uno de los más relevantes aspectos que deben destacarse se concreta en la proclamación del principio, hoy vigente en nuestro sistema procesal penal, en virtud del que el tribunal penal solo queda vinculado a lo alegado y probado en el juicio oral.

Así lo afirmaba la exposición de motivos cuando, tras señalar que la nueva LECrim «proscribe y condena una preocupación hasta ahora muy extendida [...] de dar escaso o ningún valor a las pruebas del plenario, buscando principal o casi exclusivamente la verdad en las diligencias sumariales practicadas a espaldas del acusado»[692], declaró la idea fundamental de que «en el juicio oral y público es donde ha de desarrollarse con amplitud la prueba, donde las partes deben hacer valer en igualdad de condiciones los elementos de cargo y de descargo, y donde los magistrados han de formar su convicción para pronunciar su veredicto con abstracción de la parte del sumario susceptible de ser reproducida en el juicio»[693].

---

[690] Vid. STS 672/2019, de 15 de enero de 2020, FJ 4.º, que cita las SSTS 28/2007, de 11 de enero y 974/2012, de 5 de diciembre.
[691] Vid. supra apdo. III.4 del capítulo II, pp. 136-139.
[692] Vid. exposición de motivos LECrim, apdo. XIX.
[693] Vid. exposición de motivos LECrim, apdo. XX.

Este principio se plasmó en el art. 741 de la LECrim, que se mantiene en el apartado primero de la redacción actual, y que dispone que «el Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley».

En relación con este precepto, dice GÓMEZ ORBANEJA, que «si en la instrucción puede prescindirse en buena parte de los principios de publicidad y contradicción, es justamente porque del sumario no pasa al juicio absolutamente nada como adquirido»[694], y añade que «el tribunal ha de construir las premisas de hecho de la sentencia mediante la apreciación de las pruebas practicadas en el juicio, según dice terminantemente el artículo 741, disposición que a la vez que consagra la libre apreciación, limita con rigor el material apreciable»[695].

Sin embargo, señala ASENCIO MELLADO, «nuestros Jueces y Magistrados no asumieron el cambio de mentalidad que quiso imponer el legislador decimonónico y continuaron con la praxis inquisitiva de dictar sentencia en base a las actuaciones llevadas a cabo en la fase instructora, de modo que la doctrina no regateó palabras al calificar el juicio oral como "una parodia del proceso, cuyos sujetos tienen el máximo interés en que termine lo antes posible…" o "un auténtico escándalo cuya falta de contenido es un lamentable denominador común ... una oscura sombra chinesca del sumario..."»[696]. Y al mismo tiempo, como pone de manifiesto VEGAS TORRES, la jurisprudencia del TS, no corrigió dicha práctica, sino que, al contrario, la confirmó y avaló durante un largo periodo, sosteniendo que «los folios del sumario —incluso, los del atestado— pasaban al juicio como prueba documental que, conforme al art. 726 LECrim, el Tribunal sentenciador había de examinar por sí mismo y podía —y debía—

[694] GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., *Derecho Procesal Penal*, Madrid, Artes Gráficas y Ediciones, 1987, p. 264.

[695] GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., «*Derecho Procesal Penal*», cit., p. 264.

[696] ASENCIO MELLADO, J. M., *Prueba prohibida y prueba preconstituida*, Madrid, Editorial Trivium, 1989, p. 156. El autor cita en relación con las dos opiniones doctrinales mencionadas, las obras de SERRA DOMÍNGUEZ, M., «La instrucción de los procesos penal y civil: El sumario», en *Estudios procesales*, Barcelona, Editorial Ariel, 1969, p. 722 y VIVES ANTÓN, T. S., «Doctrina constitucional y reforma del proceso penal», *Revista del Poder Judicial*, n.º especial II: Justicia Penal, 1988, pp. 98-99.

tener en cuenta para la formación de su convicción sin necesidad de su lectura en el acto del juicio»[697].

No obstante, tras la entrada en vigor de la CE de 1978 cambia el panorama, dado que el TC comienza a hacerse cargo de este trascendental tema del Derecho Procesal. Ya en una de sus primeras sentencias, dejó sentado que «las pruebas a las que se refiere el propio art. 741 LECrim, son "las pruebas practicadas en el juicio", luego el Tribunal penal sólo queda vinculado a lo alegado y probado dentro de él (secundum allegata et probata)»[698].

Pero, siguiendo la explicación de ASENCIO MELLADO, nuestro TC, no se mostró ajeno al necesario conferimiento de valor probatorio de forma excepcional a determinadas diligencias sumariales y de este modo, fue «acomodando su doctrina a dicha situación y sancionando los presupuestos y requisitos que deben concurrir para su admisión»[699].

Fue con la STC 145/1985, de 28 de octubre, FJ 2.º, con la que el TC flexibiliza su anterior criterio y declara que la actividad probatoria ha de llevarse a cabo «normalmente» en el acto de juicio oral. Así, con el uso de este adverbio, el alto Tribunal dejó abierta la posibilidad de que, respecto de determinadas actuaciones sumariales, de imposible o muy difícil reproducción en el juicio oral, pudiera ser objeto de valoración la prueba preconstituida, término que, estrictamente en lo referente a la prueba preconstituida de actuaciones sumariales, es usado por primera vez, con la STC 80/1986, de 17 de junio, FJ 1.º, que declaró que «los únicos medios de prueba válidos para desvirtuar la presunción de inocencia son los utilizados en el juicio oral y los

[697] VEGAS TORRES, J., «La presunción de inocencia y el escenario de la prueba penal: STC 31/1981, de 28 de julio», *Persona y Derecho*, n.º 55, 2006, p. 748. Cita este autor en relación con la referida jurisprudencia, la STS de 10 de noviembre de 1972 - ROJ: STS 3584/1972, que en su primer considerando declaró que «no puede pretenderse, salvo caso de contradicciones entre lo manifestado en el juicio oral y lo contenido en tales folios, su lectura al Tribunal, porque supone repetición innecesaria e inocua de la prueba que los folios contengan, supone ordinariamente una pérdida de tiempo, que a nada conduce, como no sea a la dilación innecesaria del juicio; y es totalmente inconducente a formar el criterio del Tribunal su reiteración en el acto del juicio, puesto que el celo de aquél le llevará a tener conocimiento de todos los folios sumariales y en especial de aquellos en que las partes apoyan sus fundamentos de acusación y defensa; razones todas que concluyen en que sobre tal prueba no hubo denegación, sino admisión, y se practicó conforme está legalmente ordenado».

[698] Vid. STC 31/1981, de 28 de julio, FJ 3.º

[699] ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., p. 159.

preconstituidos que sean de imposible o muy difícil reproducción, siempre que en todo caso se hayan observado las garantías necesarias para la defensa».

Con ello, comienza a fraguarse la teoría de la prueba preconstituida, respecto de la que actualmente existe un amplio cuerpo consolidado, tanto doctrinal como jurisprudencial. Por ello, analizaremos la misma sin ánimo de exhaustividad, únicamente a los efectos de continuar con nuestro trabajo de aclarar las vicisitudes que conlleva la válida incorporación al proceso de la prueba obtenida como consecuencia de los registros informáticos.

3.2. Fundamento

La preconstitución de la prueba, como excepción a la práctica sin límites de toda la prueba en el acto de juicio oral conforme al art. 741 LECrim, tiene su fundamento, en la exigencia de asegurar los datos o elementos de convicción, respecto de los que existe un riesgo de pérdida o menoscabo. Así lo ha declarado el TC al señalar que «estando el proceso penal orientado a la búsqueda de la verdad material, es preciso asegurar que no se pierden datos o elementos de convicción, utilizando en este caso la documentación oportuna del acto y operando, en todo caso, con observancia de las garantías necesarias para la defensa»[700].

3.3. Prueba anticipada y prueba preconstituida

Nos referimos anteriormente a la preconstitución de la prueba con carácter general, como aquella prueba que, por su imposible o muy difícil reproducción en el juicio oral, ha de asegurarse con carácter previo a la celebración del mismo.

Ahora bien, en este concepto subyacen dos modalidades de preconstitución probatoria, como son la prueba anticipada y la prueba preconstituida, las cuales constituyen, en palabras de ARMENTA DEU, «dos especies de un mismo género que intentan responder al hecho de que sólo pueden tener valor probatorio los medios practicados en el juicio, cuando, sin embargo, existen circunstancias de muy diversa índole que lo hacen imposible, temporal o definitivamente, debiendo preservarse la

[700] Vid. STC 137/1988, de 7 de julio, FJ 2.º

fuente probatoria o acomodar la práctica probatoria con las garantías inexcusables a dichas circunstancias»[701].

3.3.1. Prueba anticipada

La prueba anticipada en sentido propio, es aquella que tiene lugar ante el órgano enjuiciador con anterioridad a la celebración del juicio oral. Su práctica se encuentra prevista, para el procedimiento ordinario, en el art. 657-III LECrim, que dentro del título dedicado a la calificación del delito, dispone que «podrán pedir además las partes que se practiquen desde luego aquellas diligencias de prueba que por cualquier causa fuere de temer que no se puedan practicar en el juicio oral, o que pudieran motivar su suspensión». Por su parte, en el procedimiento abreviado, queda igualmente regulada la posibilidad de solicitar prueba anticipada en los arts. 781.1-III y 784.2 LECrim, que respectivamente permiten a la acusación y la defensa solicitar la práctica anticipada de aquellas pruebas que no pueden llevarse a cabo durante las sesiones del juicio oral[702].

Los principios que han de presidir la práctica de la prueba en el juicio oral, es decir los de contradicción, oralidad, inmediación, concentración y publicidad[703], deben

---

[701] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 284.

[702] Dispone el art. 781.1-III que «en el escrito de acusación se podrá solicitar la práctica anticipada de aquellas pruebas que no puedan llevarse a cabo durante las sesiones del juicio oral…» mientras que el art. 784.2 establece que «en el escrito de defensa se podrá solicitar del órgano judicial que recabe la remisión de documentos o cite a peritos o testigos, a los efectos de la práctica de la correspondiente prueba en las sesiones del juicio oral o, en su caso de la práctica de prueba anticipada».

[703] Resultan muy instructivas las explicaciones de MONTERO AROCA, en torno a estos principios, con carácter general, como rectores del proceso. Afirma el referido autor lo siguiente:

a) En relación con el principio de contradicción, ha de entenderse como «un mandato dirigido al legislador para que, en las leyes conformadoras de los distintos procesos, estos queden regulados de modo que se respete el derecho fundamental de audiencia». De este modo «la existencia del principio de contradicción se frustraría si en la propia ley se estableciera la desigualdad de las partes», por lo que «el contradictorio tiene únicamente sentido cuando a las partes se reconocen los mismos derechos, cargas y deberes procesales».

b) En cuanto a la oralidad, respecto de la que hay que recordar que se proclama en el art. 120.2 CE, que dispone que «el procedimiento será predominantemente oral, sobre todo el materia criminal», tras señalar con carácter general, que este principio, en primer lugar, significa que en los actos procesales predomina lo hablado sobre lo escrito, como medida de expresión y comunicación entre los diferentes sujetos que intervienen en el proceso y que la fase decisiva del proceso penal, es decir, la del juicio oral, a diferencia de la primera fase de instrucción, responde completamente al principio de oralidad, afirma que «en el juicio oral y público es donde ha de desarrollarse con amplitud la prueba, donde las partes deben hacer valer en igualdad de condiciones los elementos de cargo y descargo, y donde los magistrados han de formar su convicción para pronunciar su veredicto con abstracción de la parte del sumario susceptible de ser reproducida en el juicio».

regir en la práctica de la prueba anticipada, con la salvedad, obviamente, del principio de concentración, por cuanto no podrá existir unidad de acto o sesiones consecutivas, dado que puede trascurrir cierto tiempo desde la práctica de la prueba anticipada hasta la celebración del juicio oral.

3.3.2. Prueba preconstituida

De acuerdo con lo declarado por el TS, un segundo supuesto distinto, porque ya supone un sacrificio de la inmediación, es el denominado «prueba preconstituida», cuya diferencia principal con la anticipada se centra en que esta última «no tiene lugar ante el tribunal juzgador sino ante el juez de instrucción, con lo cual la inmediación desaparece al menos como inmediación espacio temporal, y queda reducida a la percepción del soporte en que la prueba preconstituida se documente y refleje»[704].

Asimismo, la jurisprudencia del TS, tras recordar que únicamente pueden considerarse auténticas pruebas que vinculen al tribunal encargado de dictar sentencia, las practicadas en el juicio oral, pues el procedimiento probatorio ha de tener lugar necesariamente en el debate contradictorio que en forma oral se desarrolla ante el mismo juez o tribunal sentenciador, recuerda que esta regla conoce excepciones que, de acuerdo

---

c) En cuanto a los principios de inmediación, concentración y publicidad, entiende MONTERO que son una manifestación del principio de oralidad, conforme a los siguientes argumentos:
1) La oralidad, implica inmediación, es decir, «la exigencia de que el juzgador se haya puesto en contacto directo con las demás personas que intervienen en el proceso, sin que exista entre ellos elemento alguno interpuesto», y añade que «esta exigencia es particularmente importante con relación a las pruebas, hasta el extremo de que normalmente se ha venido concibiendo la inmediación solamente como la exigencia de que el juez que ha de pronunciar la sentencia haya asistido a la práctica de las pruebas», siendo uno de los efectos de la inmediación, la imposibilidad de que se produzcan cambios en las personas físicas que componen el órgano jurisdiccional durante la tramitación de la causa, y en especial que solo pueden concurrir a dictar la sentencia los magistrados ante los que se ha desarrollado la audiencia oral en la que el juez o tribunal se pone en relación directa con las pruebas y con las partes».
2) En cuanto a la concentración, sostiene que «decir oralidad es decir concentración», siendo la «unidad de acto», el aspecto que caracteriza a este principio, el cual «aparece con toda claridad en la segunda fase del proceso penal español». De este modo, el art. 744 LECrim dice que «abierto el juicio oral, continuara durante todas las sesiones consecutivas que sean necesarias hasta su conclusión»
3) Finalmente, por lo que atañe al principio de publicidad, que al igual que el principio de oralidad, se encuentra reconocido por la CE, que dispone en su art. 120.1, que «las actuaciones judiciales serán públicas, con las excepciones que prevean las leyes de procedimiento», declara MONTERO, que «sin oralidad no hay publicidad», por cuanto «solo un proceso oral y concentrado permite la publicidad real y con ella la fiscalización popular del funcionamiento de la justicia». Vid. MONTERO AROCA, J., *Derecho Jurisdiccional I - Parte general*, Valencia, Tirant Lo Blanch, 2017, pp. 253-254 y 299-303.

[704] Vid. STS 96/2009, de 10 de marzo, FJ 3.º

con la doctrina del TC enunciada en la Sentencia de 18 de junio de 2001[705], se concretan en las siguientes categorías de requisitos en cuanto a las fuentes de prueba susceptibles de preconstitución:

«a) material: que versen sobre hechos que, por su fugacidad, no puedan ser reproducidos el día de la celebración del juicio oral;

b) subjetivo: que sean intervenidas por la única autoridad dotada de la suficiente independencia para generar actos de prueba, como es el juez de instrucción, sin perjuicio de que, por especiales razones de urgencia, también esté habilitada la Policía Judicial para realizar determinadas diligencias de constancia y recoger y custodiar los elementos del cuerpo del delito;

c) objetivo: que se garantice la contradicción, para lo cual, siempre que sea factible, se le ha de permitir a la defensa la posibilidad de comparecer en la ejecución de dicha prueba sumarial [...]; y, por último,

d) formal: que el régimen de ejecución de la prueba sumarial sea el mismo que el del juicio oral (diferenciándose de este modo de los correlativos actos de investigación en los que las preguntas de las partes han de formularse a través del juez de instrucción), así como que su objeto sea introducido en dicho juicio público mediante la lectura de documentos, la cual ha de posibilitar someter su contenido a la confrontación de las demás declaraciones de los intervinientes en el juicio oral»[706].

Con base en lo indicado anteriormente, la prueba preconstituida, entendida como aquella prueba anticipada en sentido amplio que tiene lugar ante el juez de instrucción, presenta dos modalidades, según la imposible o muy difícil repetición en el juicio oral lo sea por razón de la muy probable fugacidad de las fuentes de prueba o, en el segundo caso, por la propia naturaleza intrínseca de la prueba.

Previamente a ocuparnos de esta distinción, cabe señalar, de acuerdo con la opinión de JAMARDO LORENZO, que nos encontramos ante una figura jurídica muy compleja, tanto por la escasa regulación en la materia como por la propia dificultad de

[705] STC 141/2001, de 18 de junio, FJ 4.º

[706] Vid. STS 850/2009, de 28 de julio, FJ 1.º, que cita las SSTC 217/1989, de 21 de diciembre, FJ 3.º; 303/1993, de 25 de octubre, FJ 3.º; 36/1995, de 6 de febrero, FJ 2.º; 200/1996, de 3 de diciembre, FJ 2.º; 40/1997, de 27 de febrero, FJ 2.º; 153/1997, de 29 de septiembre, FJ 5.º; 49/1998, de 2 de marzo, FJ 2.º; 115/1998, de 1 de junio, FJ 2.º; y 97/1999, de 31 de mayo, FJ 5.º.

su estructura, lo cual genera la necesidad de acudir a las posiciones doctrinales y jurisprudenciales para la fijación de un concepto riguroso, opiniones respecto de las que no existe consenso[707].

Al primer supuesto (cuando sea imposible o muy difícil la reproducción de la prueba en el juicio oral), se le ha denominado de varios modos. Así se ha hablado de «prueba anticipada», sin distinguirla estrictamente de la prueba anticipada en sentido propio[708]; de «prueba anticipada en sentido impropio», término este que ha sido usado tanto doctrinal[709] como jurisprudencialmente[710]; y finalmente, como lo ha hecho GIMENO SENDRA, de «prueba instructora anticipada»[711], denominación que nos parece la más acertada, puesto que, sencillamente, la nota distintiva con la prueba anticipada en sentido propio, viene constituida únicamente por el órgano judicial que la práctica.

Por su parte, al segundo supuesto, (aquel en el que la imposible o muy difícil repetición en el juicio oral se debe a la propia esencia de la prueba), se le denomina prueba preconstituida en sentido propio. Realizaremos separadamente un breve análisis acerca de cada una de las modalidades.

3.3.2.1. Prueba instructora anticipada

Siguiendo a JAMARDO LORENZO, «prueba anticipada no es más que una prueba común que ha de anticipar en el tiempo su práctica debido a circunstancias ajenas al concreto medio de prueba, esto es, por la previsible imposibilidad de que se practique en el momento procesal oportuno»[712]. En efecto, cuando hablamos de prueba instructora anticipada, nos estamos refiriendo a una prueba común, y en este mismo sentido es en el que GIMENO SENDRA aclara que, a diferencia de la prueba preconstituida que siempre es «documental», la instructora anticipada «consiste en pruebas personales, tales como la prueba testifical y pericial»[713].

---

[707] JAMARDO LORENZO, A., «La preconstitución de la prueba en el proceso penal», *Diario La Ley - Sección Doctrina*, n.º 8906, 2017, p. 2.

[708] Vid. ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., pp. 259-261 y ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., pp. 284-285.

[709] MARCA MATUTE, J., «El imputado y el anticipo probatorio», en Abel Lluch, X., Richard González, M. (dirs.), *Estudios sobre prueba penal - Vol. III*, Las Rozas (Madrid), La Ley, 2013, p. 212.

[710] Vid. STS 374/2019, de 23 de julio, FJ 6.º

[711] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 315 y ss.

[712] JAMARDO LORENZO, A., «La preconstitución de la prueba en el proceso penal», cit., p. 4.

[713] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., pp. 315-316.

Esta modalidad de preconstitución de la prueba se encuentra regulada en la LECrim, tanto para el procedimiento ordinario como para el abreviado, respectivamente en los arts. 448 y 777.2, los cuales establecen de forma análoga, que en aquellos casos en los que hubiera razones por las que razonablemente un testigo o víctima no pudiese comparecer a prestar su declaración en el juicio oral, por razón de su residencia o por otro motivo entre los que se menciona el temor a su muerte, el juez de instrucción practicará inmediatamente la prueba testifical, asegurando en todo caso la posibilidad de contradicción de las partes.

En cuanto a la pericial, señala ARAGONESES MARTÍNEZ, que si bien el informe pericial tiene, en principio, el valor de diligencia sumarial, también cabe la posibilidad de que el mismo tenga el carácter de prueba anticipada, por no poder ser reproducida en el juicio oral, como así puede suceder en los casos en los que el objeto de la pericia tiene que ser destruido por completo o si son precisos medios técnicos propios de lugares distintos al local del órgano jurisdiccional de imposible traslado y, por experiencia común, de práctica temporalmente larga[714].

Por otro lado, GIMENO SENDRA, afirma que la pericial anticipada podría tener sentido al promulgarse la LECrim en 1882, habida cuenta de la ausencia en dicho año de técnicas de custodia del cuerpo del delito y de peritos en determinadas demarcaciones judiciales. Pero no existiendo tales carencias en la actualidad, señala que «dicha prueba sumarial carece de sentido, debiendo todos los peritos prestar su informe en el juicio oral»[715].

Compartimos esta opinión, en punto relativo a que una prueba pericial sumarial que no puede ser reproducida en el juicio oral —como en los casos en que el objeto de la pericia tenga que ser destruido por completo o si, como mencionamos anteriormente, son medios técnicos propios de lugares distintos al local del órgano jurisdiccional de

[714] Menciona esta autora algunos ejemplos, como el de la STS de 20 de octubre de 1986 - ROJ: STS 9603/1986, FJ 1.º, en el que en relación con un informe dactiloscópico emitido por el Gabinete Central de Identificación, se declaró que este no era susceptible de ser reproducido en el juicio oral «ya que por la esencia misma del peritaje, que exige la concentración en un solo organismo de todas las fichas dactiloscópicas procedentes de todo el territorio nacional y la posibilidad de disponer de todas las procedentes del servicio del DNI hace que los datos del peritaje —muestras y fichas indubitadas— se configuren como únicos». Vid. ARAGONESES MARTÍNEZ, S., «El Sumario (II)», en De la Oliva Santos, A. y otros, *Derecho Procesal Penal*, Madrid, Editorial Universitaria Ramón Areces, 2007, p. 359.

[715] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 318.

imposible traslado—, tendría el carácter de prueba preconstituida en sentido propio y no de prueba instructora anticipada.

Sin embargo, consideramos que la pericial como prueba instructora anticipada, cobra todo su sentido, conforme ha declarado el TS, «cuando la materia u objeto de la pericia puede desaparecer o transformarse de forma esencial», en cuyo caso sostiene el alto Tribunal que «la ley permite la intervención de las partes, al modo de una prueba anticipada, precisamente porque las operaciones de análisis o exámenes no podrán reiterarse, lo que podría originar un supuesto de preconstitución probatoria»[716]. Y asimismo, en aquellos casos en los que el perito que tuviera que prestar su informe en el juicio oral y someterse, con respeto del principio de contradicción, a las preguntas que le fuesen formuladas por las partes, siempre que, al igual que ocurre con los testigos, por razones de residencia tuviera que ausentarse del territorio español o se temiese por su vida, en los mismos términos y conforme a los mismos preceptos a los que nos hemos referido con anterioridad.

En cuanto al procedimiento para la práctica de la prueba instructora anticipada, de conformidad con el art. 777.2 LECrim, el juez de instrucción practicará inmediatamente la misma asegurando en todo caso la posibilidad de contradicción de las partes, debiéndose documentarse dicha diligencia en soporte apto para la grabación y reproducción del sonido y de la imagen o por medio de acta autorizada por el letrado de la Administración de Justicia con expresión de los intervinientes.

3.3.2.2. Prueba preconstituida en sentido propio

Al hablar de prueba preconstituida en sentido propio, o simplemente de prueba preconstituida, se han manejado diversos conceptos doctrinales, sin que, sin embargo, puedan apreciarse contradicciones entre los mismos.

Así, por ejemplo, ASENCIO MELLADO señala que la prueba preconstituida viene a definir «un complejo compuesto por aquellos actos de investigación de carácter material, no personal, normalmente objetivos e irrepetibles, que se practican con anterioridad al juicio oral por la policía, el Ministerio Fiscal o el juez de instrucción»[717].

[716] Vid. STS 1212/2003, de 9 de octubre, FJ 2.º

[717] ASENCIO MELLADO, J. M., «*Derecho Procesal Penal*», cit., pp. 257-258.

MORENO CATENA afirma que se trata de una «fuente de prueba que tiene como finalidad dejar constancia de la existencia de un hecho, acto, negocio o relación jurídica, y del modo que existió, para su utilización futura»[718] y aclara que «se trata, pues, de un elemento apto para dar a conocer algo que sucedió en el pasado (el ejemplo paradigmático es el documento)»[719].

ARMENTA DEU señala que con la prueba preconstituida se trata de «articular un remedio ante determinadas diligencias que siendo de imposible reproducción se han desarrollado en la etapa instructora y naturalmente sin observar muchas de las garantías de una actividad encaminada a enervar la presunción de inocencia; pero a diferencia de la prueba anticipada tales supuestos no resultan previstos legalmente, sino que surgen por la propia naturaleza, efímera, de la fuente probatoria»[720].

Finalmente, GIMENO SENDRA concreta que la prueba preconstituida «es una prueba documental, que puede practicar el juez de instrucción y su personal colaborador (policía judicial y Ministerio Fiscal) sobre hechos irrepetibles, que no pueden, a través de los medios de prueba ordinarios, ser trasladados al momento de realización de juicio oral»[721].

Quedan claras, por tanto, las diferencias con la prueba instructora anticipada, que podemos concretar definitivamente en las siguientes:

a) La prueba instructora anticipada se encuentra prevista legalmente, mientras que la prueba preconstituida es un producto jurisprudencial que nace como excepción a la regla general de la práctica de toda la prueba en el acto de juicio oral, dado que, encontrándose el proceso penal orientado a la búsqueda de la verdad material, es preciso asegurar que no se pierden datos o elementos de convicción, siempre con las debidas garantías para la defensa.

b) La prueba instructora anticipada está creada para la práctica de pruebas personales, mientras que la preconstituida constituye una prueba documental.

---

[718] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 432.
[719] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 432.
[720] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 285.
[721] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 363.

c) La prueba preconstituida puede ser obtenida por el juez de instrucción, Ministerio Fiscal o Policía Judicial, mientras que la prueba instructora anticipada requiere siempre la intervención del juez de instrucción.

Finalmente, con base en las anteriores definiciones doctrinales, y partiendo de la premisa de que la prueba preconstituida no se encuentra prevista legalmente, sino que es producto de la jurisprudencia, podemos destacar como notas esenciales de esta institución, la de venir dada por actos de investigación realizados por el juez de instrucción, Ministerio Fiscal o Policía Judicial, que se transforman en fuente de prueba documental, ante la imposibilidad de su reproducción en el juicio oral por la naturaleza efímera de la fuente.

3.3.3. Supuestos de prueba preconstituida en sentido propio

Siguiendo el esquema de GIMENO SENDRA, cabe distinguir entre los siguientes grupos de prueba preconstituida:

a) Prueba preconstituida de las diligencias policiales de prevención. En este grupo se incluyen los métodos alcoholimétricos, grabaciones de vídeo vigilancia y análisis de estupefacientes. Se trata de diligencias policiales que pueden ser acordadas por el Ministerio Fiscal en el ámbito de las Diligencias de Investigación (art. 773.2 LECrim)[722], o directamente por la Policía Judicial en virtud de la función que, para la averiguación de los delitos, le viene encomendada por el art. 282 LECrim, en relación con la recogida urgente de todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro.

b) Prueba preconstituida de la Policía Judicial con autorización y control judicial. Se produce en aquellos supuestos en los que la intromisión en determinados derechos fundamentales exige la autorización previa y el adecuado control judicial. Se trata de los casos de circulación y entrega vigilada de drogas, inspecciones e intervenciones corporales, entrada y registro domiciliario, intervención de las comunicaciones telefónicas y telemáticas, intervención de los datos electrónicos de

[722] En relación con las Diligencias de Investigación del Ministerio Fiscal, vid. FISCALÍA GENERAL DEL ESTADO, *Circular 4/2013, de 30 de diciembre, sobre las Diligencias de Investigación*, 2013, Consultado en https://www.fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/cir_inst_cons/circular_4_2013.pdf, el 19 de abril de 2020.

tráfico, captación y grabación de comunicaciones orales, geolocalización y registros informáticos.

c) Prueba preconstituida del juez de instrucción. Se trata de aquellas diligencias de investigación en las que, por su propia naturaleza, se hace necesaria la intervención del juez, como es el caso de la inspección ocular[723].

No obstante este amplio elenco de supuestos, que aspira a abarcar la totalidad de las posibilidades, hay que tener en cuenta, de acuerdo con lo afirmado por JAMARDO LORENZO, que «el enorme avance del mundo tecnológico dificulta la tarea de reseñar todas ellas, ya que los medios tecnológicos destinados a la investigación de los delitos van aumentando con el desarrollo de las nuevas tecnologías y surgen métodos novedosos y de mayor eficacia para la consecución de los objetivos investigadores, lo que propicia la aparición de nuevas posibilidades en relación a la preconstitución probatoria»[724].

3.3.4. El carácter de prueba preconstituida de los registros informáticos

Por lo que respecta a los registros informáticos, no cabe duda de que siempre nos encontraremos ante un supuesto de prueba preconstituida, dado que la volatilidad que caracteriza a la prueba digital, a lo que habría que añadir la muy probable destrucción del material incriminatorio por parte de los culpables, haría imposible o muy difícil su reproducción en el juicio oral.

En este sentido, con un registro informático nos encontraremos en un gran número de casos ante un supuesto de recogida de efectos, instrumentos o pruebas del delito, ya se produzca esta con intervención urgente de la Policía Judicial o el Ministerio Fiscal (arts. 282 y 588 sexies c.4 LECrim) o tras la correspondiente resolución del juez de instrucción (arts. 326, 588 bis a.1 y 588 sexies a y b LECrim).

Por otro lado, también tendrán el carácter de prueba preconstituida aquellos supuestos en los que el registro informático se practique para la intervención de las comunicaciones electrónicas.

---

[723] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., pp. 363-364, 374-375, 379 y 427 y ss.

[724] JAMARDO LORENZO, A., «La preconstitución de la prueba en el proceso penal», cit., p. 5.

Finalmente, cabe señalar que para que una diligencia de investigación acordada por el juez de instrucción o llevada a cabo bajo su control, adquiera el carácter de prueba preconstituida, será necesario que la correspondiente resolución judicial, sea respetuosa con los principios rectores de las diligencias de investigación tecnológica, en los términos ya estudiados[725].

3.3.5. Incorporación al proceso de la prueba preconstituida

En cuanto a la entrada en el proceso de la prueba preconstituida, ya sea una prueba instructora anticipada o una prueba preconstituida en sentido propio, el último párrafo del art. 777.2 LECrim dispone que «a efectos de su valoración como prueba en sentencia, la parte a quien interese deberá instar en el juicio oral la reproducción de la grabación o la lectura literal de la diligencia, en los términos del artículo 730».

Aunque el referido artículo se encuentre en sede del procedimiento abreviado, resulta aplicable igualmente al procedimiento ordinario por imperativo del propio art. 730 LECrim.

De acuerdo con este último precepto «podrán también leerse o reproducirse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral, y las declaraciones recibidas de conformidad con lo dispuesto en el artículo 448 durante la fase de investigación a las víctimas menores de edad y a las víctimas con discapacidad necesitadas de especial protección».

No obstante, de la lectura de las actuaciones sumariales conforme a lo establecido en el art. 730, nos ocuparemos más adelante en un apartado dentro del epígrafe dedicado a los medios de prueba.

III. La prueba ilícita

1. Introducción

De acuerdo con lo que pusimos de manifiesto en el capítulo I[726], debemos tener en cuenta en todo momento la distinción entre diligencias de investigación (también

[725] Vid. supra apdo. I del capítulo III, pp. 143-151.
[726] Vid. nota al pie n.º 5 y el texto relacionado con la misma en el apartado I del capítulo I, pp. 13-14.

denominadas actos instructorios o actos de investigación) de los actos de prueba. Las primeras, con carácter general, constituyen el cauce para facilitar a las partes la fundamentación fáctica de sus respectivos escritos de calificación o acusación, pero no permiten al juez o tribunal sentenciador extender sobre ellos su conocimiento en la declaración de hechos probados, no pudiendo por tanto fundamentar una sentencia de condena. Por su parte, los actos de prueba, sí están dirigidos única y exclusivamente a poder fundar, en su día la resolución definitiva.

Pues bien, el primer requisito para que las fuentes de investigación se conviertan en auténticos medios de prueba susceptibles de enervar la presunción de inocencia, se concreta en la necesidad de la licitud de la prueba, o, dicho de otro modo, en que la prueba obtenida tras una diligencia de investigación tecnológica, de conformidad con lo dispuesto en el art. 11.1 LOPJ, no sea tachada de ilícita por haberse violentado, directa o indirectamente, los derechos o libertades fundamentales.

El mandato contenido en esta norma, y muy especialmente la expresión «indirectamente», ha generado, como veremos, una gran controversia tanto en la doctrina procesal como en la jurisprudencia. Señala PICÓ I JUNOY que, habida cuenta de los intereses en conflicto, estamos ante uno de los temas más complejos y difíciles de resolver[727].

A día de hoy, y tras varias décadas de debate, sigue sin ser un tema pacífico, lo cual nos obliga a adoptar una posición, no sin antes ofrecer una explicación del problema en los siguientes apartados.

2. Apuntes históricos

En primer lugar, realizaremos un breve examen de su evolución histórica, que dividiremos en dos apartados relativos a la prueba ilícita propiamente dicha, es decir la obtenida directamente, y la prueba prohibida o teoría de los frutos del árbol envenenado. Estos apuntes relativos a la evolución nos permitirán, al mismo tiempo, estudiar con una mayor profundidad el concepto de la prueba ilícita directa e indirecta.

[727] PICÓ I JUNOY, J., «La denuncia de la prueba ilícita en el proceso penal», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, p. 317.

2.1. La prueba ilícita directa

En nuestro ordenamiento jurídico, ya con anterioridad a la promulgación de la CE de 1978, se planteó el debate en relación con la pugna entre la búsqueda material de la verdad y la defensa de los derechos fundamentales de los ciudadanos, respecto del cual, en dicha época pre-constitucional, se impuso el criterio de la admisibilidad procesal del material probatorio, sin perjuicio de depurar las responsabilidades derivadas por la obtención de la fuente de prueba ilícita[728].

Varias décadas atrás, esta misma discusión tuvo lugar en los Estados Unidos de América, donde tras las sentencias del Tribunal Supremo de dicho país, dictadas en el caso Boyd v. United States, de 1 de febrero de 1886 y en el caso Weeks v. United States, de 24 de febrero de 1914, se estableció la doctrina de la *evidence wrongfully obtained*, en virtud de la que, a su vez, se estableció la regla conocida como *exclusionary rule*, conforme a la que las pruebas obtenidas con vulneración de derechos fundamentales han de ser excluidas del proceso penal.

Sin embargo, ya en periodo post-constitucional, la oposición entre estos dos valores, cedió, por primera vez, en favor de los derechos de los ciudadanos. Este primer reconocimiento tuvo lugar con la STC 114/1984, de 29 de noviembre, FJ 2.º, la que, aun cuando señaló que «lo cierto es que no existe un derecho fundamental autónomo a la no recepción jurisdiccional de las pruebas de posible origen antijurídico», declaró en su FJ 5.º, que «constatada la inadmisibilidad de las pruebas obtenidas con violación de derechos fundamentales, su recepción procesal implica una ignorancia de las "garantías" propias al proceso (art. 24.2 de la Constitución) implicando también una inaceptable confirmación institucional de la desigualdad entre las partes en el juicio (art. 14 de la Constitución)».

Al mismo tiempo, esta importante resolución del TC, tras señalar en su FJ 4.º que en esta encrucijada de intereses, dentro de los que chocan la necesaria procuración de la

[728] Tal y como explica RIVES SEVA, la posición de España en el siglo pasado estuvo marcada por una sentencia dictada en 1952 por el Tribunal alemán de Basel-Land, que fue conocida en nuestro país, merced a un trabajo de Schönke publicado en 1955 en la Revista de Derecho Procesal con el título «Límites de la prueba en el Derecho Procesal», y que significó el triunfo de la tesis de James Goldschmidt, partidario de la doble valoración de la obtención ilegítima de material probatorio, que conduce a su admisibilidad procesal, sin perjuicio de depurar las responsabilidades derivadas de la ilicitud del acto adquisitivo de la fuente de prueba. Vid. RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 11-12.

verdad en el proceso con la garantía —por el ordenamiento en su conjunto— de las situaciones jurídicas subjetivas de los ciudadanos, declaró que «estas últimas acaso puedan ceder ante la primera exigencia cuando su base sea estrictamente infraconstitucional, pero no cuando se trate de derechos fundamentales que traen su causa, directa e inmediata, de la norma primera del ordenamiento», determinando a continuación que «en tal supuesto puede afirmarse la exigencia prioritaria de atender a su plena efectividad, relegando a un segundo término los intereses públicos ligados a la fase probatoria del proceso».

De este modo, y en virtud de la diferenciación entre la prueba obtenida con vulneración de derechos fundamentales y aquella que se obtuviese con vulneración de derechos no fundamentales o la ley ordinaria, se acuñaron doctrinalmente los conceptos de prueba ilícita y prueba prohibida[729].

A este respecto, GIMENO SENDRA, ha señalado que «aunque ambos términos, prueba ilícita y prueba prohibida, suelan utilizarse indistintamente, en realidad, entrañan conceptos diferentes»[730] dado que, «la prueba ilícita es la que infringe cualquier Ley (no sólo la Fundamental, sino también la legislación ordinaria), en tanto que la prueba prohibida es la que surge como consecuencia de la violación, en su adopción o en su ejecución, de las normas constitucionales tuteladoras de los derechos fundamentales»[731].

La STC 114/1984, fue el detonante para que, con la promulgación de la nueva LOPJ, concretamente la LO 6/1985, de 1 de julio, del Poder Judicial, se reconociese legalmente la prohibición de la prueba obtenida con violación de los derechos fundamentales, dado que, su art. 11.1, tras establecer que «en todo tipo de procedimientos se respetarán las reglas de la buena fe», dispone en su inciso segundo

[729] El TS, se ha pronunciado en relación con esta distinción entre prueba obtenida con vulneración de derechos fundamentales y la que se obtuviese con vulneración de la ley ordinaria. Así, la STS 999/2004, de 19 de septiembre, FJ 1.º, al examinar un caso en el que se invocó la vulneración del derecho al secreto de las comunicaciones, ha declarado que si las infracciones cometidas tuvieren un mero carácter procesal, «la consecuencia alcanzará tan sólo al valor probatorio de los productos de la interceptación de las comunicaciones, pero manteniendo aún su valor como instrumento de investigación y fuente de otras pruebas de ella derivadas», respecto de lo cual, la STS 115/2015, de 5 de marzo, FJ 1.º, ha aclarado que lo que se haya conocido con la prueba irregular, «puede ser introducido en el juicio oral como elemento de convicción a través de otros medios de prueba que acrediten su contenido», añadiendo que «desde luego lo conocido puede ser objeto de posterior investigación y prueba por otros medios que legítimamente accedan al juicio oral».

[730] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 578.

[731] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 578.

que «no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales».

Ahora bien, tal y como explica ASENCIO MELLADO, el camino que hubo de seguirse hasta este pronunciamiento del TC del año 1984, no fue fácil ni pacífico. Así, el ATC 289/1984, de 16 de mayo, rechazó la pretensión de aplicación de la teoría de la prueba ilícita en atención a dos argumentos bien especificados: uno, la falta de apoyo de una petición así en norma alguna del derecho positivo o en la Constitución; otro, la de no ser un principio general del derecho admitido por la jurisprudencia, sino una mera aspiración *de lege ferenda* por lo que, entendía el TC en aquel momento, no existía norma alguna que prohibiera al juez o tribunal valorar pruebas cualquiera que fuera su origen[732].

Finalmente la referida STC 114/1984, conforme expone ASENCIO MELLADO, sentó las bases de la prueba ilícita, en los siguientes postulados:

1.º Inexistencia de un derecho fundamental autónomo cuyo contenido comporte la inadmisión de una prueba ilícita. No obstante, aunque no se reconozca tal derecho, la imposibilidad de estimación procesal existe como expresión de una garantía objetiva e implícita en el sistema de los derechos fundamentales, cuya vigencia y posición preferente en el ordenamiento puede requerir desestimar toda prueba obtenida con lesión de los mismos.

2.º Distinción entre actos contrarios a derechos fundamentales reconocidos en la CE y actos que atenten a otras normas del ordenamiento. De este modo, la inadmisión solo opera respecto de las pruebas obtenidas de forma antijurídica cuando se vulneren derechos fundamentales, por el lugar preferente que estos ocupan dentro del ordenamiento jurídico.

3.º La admisión en el proceso de una prueba ilícitamente obtenida implicará infracción del derecho a un proceso con todas las garantías proclamado en el art. 24.2 CE[733].

[732] ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., p. 78.
[733] ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., p. 78.

2.2. El efecto reflejo de la prueba ilícitamente obtenida

Nos hemos referido en el apartado anterior a la denominación dada a la prueba irregularmente obtenida, según esta se produjese vulnerando derechos fundamentales o la ley ordinaria. A este respecto, y en nuestra opinión de una forma más correcta, RIVES SEVA distingue entre prueba irregular, prueba ilícita y prueba prohibida, al señalar que «prueba irregular es la generada contraviniendo las normas de rango ordinario que regulan su obtención y practica; prueba ilícita la que en su origen o desarrollo se ha vulnerado un derecho o libertad fundamental; y prueba prohibida seria la consecuencia de la prueba ilícita, esto es, aquella que no puede ser traída al proceso puesto que deriva de otra producida con vulneración de derechos fundamentales»[734]. De este modo, estaríamos ante una prueba prohibida cuando «la prueba ha sido obtenida en forma lícita, pero se ha llegado a ella gracias a conocimientos conseguidos en forma ilícita»[735].

La prueba ilícita, como ya dijimos, tuvo su reconocimiento jurisprudencial con la STC 114/1984, siendo esta el detonante para su incorporación a nuestra legislación, mediante el art. 11.1 LOPJ, el cual incluyó el término «indirectamente». Posteriormente, en numerosas resoluciones, el TS se ha pronunciado sin fisuras en favor de la nulidad de la prueba ilícita.

Cabe destacar el ATS de 18 de junio de 1992, que, partiendo del postulado conforme al que «no se puede obtener la verdad real a cualquier precio», así como que «no todo es lícito en el descubrimiento de la verdad», sino «solo aquello que es compatible con la defensa del elemento nuclear de los derechos fundamentales, así la dignidad, la intimidad, etc., dentro de los parámetros fijados en la Ley», declaró, al referirse a la prueba refleja, que no podrán practicarse los medios de prueba que sean consecuencia de la prueba ilícitamente obtenida «pues sólo así se produce el efecto querido por la Ley cuando de nulidades radicales se trata, cabiendo sólo, por tanto, respecto de las acusaciones, utilizar pruebas, si estiman que disponen de ellas, distintas de aquellas que se declaran nulas, sin que, obviamente y por tanto, puedan tampoco

[734] RIVES SEVA, A. P., «Reflexiones sobre el efecto reflejo de la prueba ilícita», *Noticias jurídicas*, 2010, p. 1, Consultado en http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4605-reflexiones-sobre-el-efecto-reflejo-de-la-prueba-ilicita/, el 7 de febrero de 2020.
[735] LÓPEZ BARJA DE QUIROGA, J., «*Tratado de Derecho Procesal Penal*», cit., p. 879.

servir como apoyo de sus pretensiones, directa o indirectamente, las pruebas cuya nulidad radical se declara (artículos 11.1, 238 y 240 LOPJ)»[736].

Sin embargo, no fue hasta 1994 cuando por el TC se dio un paso todavía más proteccionista, confirmando la expansión imparable de la teoría de la prueba prohibida desde su reconocimiento constitucional en 1984 y legal en 1985[737], al admitir jurisprudencialmente el efecto reflejo de la prueba contaminada.

Previamente a referirnos a esta importante decisión de nuestro TC, debe decirse que el adverbio «indirectamente» en la redacción del art. 11.1 LOPJ, ha dado lugar a un amplio debate jurisprudencial y doctrinal, que perdura hasta nuestros días, en relación a la magnitud y trascendencia con la que ha de ser interpretado dicho vocablo. Con él, se vino a implantar legalmente en nuestro sistema, la doctrina de origen norteamericano de los frutos del árbol envenenado —*the fruit of the poisonous tree doctrine*—. En virtud de ella, las pruebas obtenidas una vez producida la indebida injerencia en el derecho fundamental[738], adquieren el mismo rango de invalidez que la obtenida directamente, sin que sea posible el acceso al proceso por ninguno de los medios legales de incorporación de la prueba obtenida, incluso por la testifical del agente que llevó a cabo la medida de investigación vulneradora del derecho fundamental.

El primer reconocimiento de esta doctrina tiene lugar con la Sentencia del Tribunal Supremo de los Estados Unidos de América, dictada en el caso Nardone v. United States, de 11 de diciembre de 1939, la cual declaró que «prohibir el uso directo de los métodos ilegales, pero no poner freno al indirecto, constituiría una incitación a estas mismas artimañas, tenidas por incompatibles con los standards éticos, y destructoras de la libertad personal».

En España, esta teoría fue acogida con la STC 85/1994, de 14 de marzo, FJ 4.º, conforme a la que «la imposibilidad de admitir en el proceso una prueba obtenida violentando un derecho fundamental no sólo deriva directamente de la nulidad de todo

[736] Vid. ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992, FFJJ 1.º y 9.º

[737] Vid. GÓMEZ COLOMER, J. L., «Prueba admisible y prueba prohibida: Cambios en el garantismo judicial motivados por la lucha contra el crimen organizado en la realidad jurisprudencial española actual», *Doctrina y Jurisprudencia Penal*, n.º 22, 2015, p. 13.

[738] Así, por ejemplo, la aprehensión de un alijo de droga, en el que el lugar donde será depositada se ha conocido con la interceptación de un correo electrónico, tras un registro informático llevado a cabo sin la debida autorización judicial y sin que quedasen acreditadas razones de urgencia.

acto violatorio de los derechos reconocidos en el capítulo II del título I CE, y de la necesidad de no confirmar, reconociéndolas efectivas, las contravenciones de los mismos (STC 114/1984), sino ahora también en el plano de la legalidad en virtud de lo dispuesto en el art. 11.1 LOPJ».

La doctrina de los frutos del árbol envenenado se aplicó, tras esta resolución, en diversas ocasiones por el TC resolviendo recursos de amparo. Puede mencionarse la STC 86/1995, de 6 de junio, FJ 3.º, que excluyó la prueba indirectamente obtenida, al declarar que «para este Tribunal el hecho de que el contenido de la conversación telefónica interceptada se extendiese al lugar en el que había de verificarse la entrega de la droga, que los interlocutores se refiriesen al vehículo en el que se realizaría el traslado y la circunstancia cierta de que la intervención policial se produjese a las pocas horas de detectarse la llamada telefónica permite suponer, lógica y razonablemente, que éste fue el medio que permitió a los agentes tomar conocimiento de los datos necesarios para conseguir la detención del sospechoso y la ocupación de los efectos del delito».

También el TS, en diversas sentencias, declaró que «el reflejo invalidante de las pruebas obtenidas violentando los derechos o las libertades fundamentales, se extiende a todas aquellas que traigan su causa, directa o indirectamente, de la prueba contaminada», añadiendo que «así lo establece tajantemente el art. 11.1 LOPJ sin dejar opciones a otras alternativas encaminadas a sanar los vicios originarios de la prueba matriz»[739], así como que «la prohibición alcanza tanto a la prueba en cuya obtención se haya vulnerado un derecho fundamental como a aquellas otras que, habiéndose obtenido lícitamente, se basan, apoyan o deriven de la anterior, (directa o indirectamente), pues sólo de este modo se asegura que la prueba ilícita inicial no surta efecto alguno en el proceso. Prohibir el uso directo de estos medios probatorios y tolerar su aprovechamiento indirecto constituiría una proclamación vacía de contenido efectivo, e incluso una incitación a la utilización de procedimientos inconstitucionales que, indirectamente, surtirían efecto. Los frutos del árbol envenenado deben estar, y están (art. 11.1 de la L.O.P.J.), jurídicamente contaminados»[740].

[739] Vid. SSTS de 23 de enero de 1995 – ROJ: STS 11600/1995; ROJ: STS 6977/1995; y ROJ: STS 198/1995, FJ 1.º

[740] Vid. SSTS 448/1997, de 4 de marzo, FJ 2.º; 472/1997, de 14 de abril, FJ 6.º; 538/1997, de 23 de abril, FJ 8.º;

La eficacia refleja de la prueba contaminada se mantuvo vigente hasta la igualmente importante y, a nuestro juicio, trascendental STC 81/1998, de 2 de abril, que vino a establecer la doctrina de la conexión de antijuridicidad, de la que más adelante nos ocuparemos, como una corrección al principio de la prueba prohibida, y respecto de la que puede afirmarse que constituye la tesis imperante en este momento, no obstante existir muchas opiniones discrepantes.

3. Fundamento

En cuanto al fundamento de la prueba prohibida, FERNÁNDEZ ENTRALGO ha señalado que «el argumento tópico, sobre el que se sustenta la inadmisibilidad de la prueba obtenida ilegítimamente, se centra en el propósito de disuadir al aparato policial de acudir a tales métodos investigadores prohibidos, so pena de ver condenados al fracaso sus esfuerzos, y al margen las responsabilidades (civiles, penales o administrativas) en que puedan incurrir los funcionarios que hicieron uso de aquéllos»[741]. Este es el razonamiento que sustentó la doctrina norteamericana, el denominado *deterrent efect* o efecto disuasorio, respecto del que MIRANDA ESTRAMPES afirma que se trata de un sistema «que no descartaría la aplicación de otros remedios alternativos (por ejemplo, sanciones penales o disciplinarias) en cuanto demostrasen su mayor eficacia para el logro de esa finalidad disuasoria»[742].

En nuestro ordenamiento jurídico, el TC fundamentó la nulidad de la prueba ilícita, no en el referido efecto disuasorio, sino en el valor preferente que los derechos fundamentales y las libertades públicas tienen en nuestro ordenamiento jurídico, al declarar en el FJ 2.º de la meritada STC 114/1984, la imposibilidad de estimación procesal de la prueba obtenida con violación de derechos fundamentales, «pero no en virtud de un derecho fundamental que pueda considerarse originariamente afectado, sino como expresión de una garantía objetiva e implícita en el sistema de los derechos fundamentales, cuya vigencia y posición preferente en el ordenamiento puede requerir desestimar toda prueba obtenida con lesión de los mismos».

---

[741] FERNÁNDEZ ENTRALGO, J., «Las reglas del juego. Prohibido hacer trampas: la prueba ilegítimamente obtenida», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, p. 76, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[742] MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», *Revista Catalana de Seguridad Pública*, n.º 22, 2010, p. 134.

Por ello, y con base en tal justificación, tal como dijimos anteriormente, cabe calificar como prueba ilícita, aquella obtenida con vulneración de derechos fundamentales, pero no así respecto de derechos de carácter infraconstitucional, que denominamos prueba irregular. Como dice PICÓ I JUNOY, los derechos fundamentales constituyen los pilares básicos sobre los que se asienta el ordenamiento jurídico, estableciendo una distinción entre este concepto y el de pruebas obtenidas con infracción de ley, las cuales han de ser admitidas por dos razonamientos: el primero por el imperativo del art. 11.1 LOPJ, que se refiere únicamente a derechos fundamentales, y el segundo por la configuración del derecho a la prueba como fundamental en el art. 24.2 CE[743].

Autores como MIRANDA ESTRAMPES, mantienen que, como consecuencia de las excepciones a la regla de exclusión de la prueba prohibida —de las que más adelante nos ocuparemos—, el TC, «aun sin llegar a un modelo de desconstitucionalización plena de la regla de exclusión, ha ido introduciendo en su discurso argumental referencias a las necesidades de disuasión limitando su ámbito de aplicación mediante el reconocimiento de excepciones inspiradas en gran medida en la jurisprudencia norteamericana»[744]. Del mismo modo, siguiendo al referido autor, MUÑOZ CARRASCO ha matizado que «las múltiples referencias a las necesidades de disuasión como límite al ámbito de aplicación de la regla de exclusión, han conducido a que nuestro sistema se acerque más a los principios inspiradores de la doctrina norteamericana del *"deterrent effect"* que a los de prevalencia de las garantías constitucionales en que se sustentan los sistemas europeos, incluido el nuestro»[745].

Sin embargo, autores como ASENCIO MELLADO, tras resaltar la importancia de determinar cuál sea el fundamento, constitucional o meramente legal de la prueba ilícita, por cuanto «del fundamento asignado derivan consecuencias inevitables y lógicas que afectan al entendimiento de la prueba ilícita y a la amplitud de la supresión de sus efectos en el proceso»[746], afirma que la prueba ilícita mantiene un doble fundamento constitucional, uno de carácter inmediato y otro mediato. En este sentido afirma que

[743] PICÓ I JUNOY, J., «La denuncia de la prueba ilícita en el proceso penal», cit., pp. 319-320.

[744] MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», cit., p. 136.

[745] MUÑOZ CARRASCO, P., «Análisis del estado actual de la prueba ilícitamente obtenida en el proceso penal español», *Revista Aranzadi Doctrinal*, n.º 1, 2019, p. 4.

[746] ASENCIO MELLADO, J. M., «Prueba ilícita: Declaración y efectos», *Revista General de Derecho Procesal*, n.º 26, 2012, p. 8.

constituye tal fundamento, «por una parte, inmediatamente, el derecho vulnerado, la necesidad de preservar su eficacia ante agresiones inadmisibles; por otra parte, mediatamente, el derecho a un proceso con todas las garantías o los demás en su caso si la infracción se produce al momento de admisión o valoración del medio por el que la prueba se aporta e incide en la condena»[747].

Por nuestra parte, en lo que se refiere al fundamento, compartimos la opinión de GÓMEZ COLOMER, cuando sitúa el fundamento tanto en la protección superior de los derechos fundamentales como en el efecto disuasorio, al señalar que con el reconocimiento legal y jurisprudencial de la prueba prohibida se alcanzan dos efectos trascendentales, «por un lado el efecto garantista, ya que una correcta teoría sobre la prueba prohibida contribuye eficazmente a una mejor protección de los derechos fundamentales del imputado o acusado garantizados por la Constitución que ordena esa democracia; y por otro lado y no en último lugar, el efecto disuasorio, por el que se asegura que las conductas de las autoridades de persecución penal, sobre todo durante la investigación del crimen y particularmente las realizadas por la policía, serán ajustadas a la misma Constitución»[748].

En este sentido, estimamos que el hecho de se hayan producido correcciones a la teoría de los frutos del árbol envenenado, no es causa suficiente para que este fundamento del respeto al valor superior de los derechos fundamentales, ceda en favor de forma exclusiva en el efecto disuasorio, entendiendo que ambos fundamentos son totalmente compatibles, aun con aquellos criterios correctores. Desde un punto de vista ontológico, conforme a nuestro sistema constitucional de derechos fundamentales, el respeto a estos debe y ha de ser en todo caso el primer fundamento de la prueba prohibida, porque precisamente por ese motivo se prohíbe, lo cual no impide que como anejo inseparable a dicho fundamento exista otro de carácter disuasorio.

---

[747] Afirma este autor que «el fundamento, pues, de la prueba ilícita, en tanto deriva de la posición preferente que ocupan los derechos en el ordenamiento jurídico, no puede ser otro, que la preservación del contenido esencial de cada derecho afectado por la injerencia ilegítima, pues la eficacia del derecho exige, aunque paralelamente se verifiquen otros fines accesorios de carácter disuasorio, la ineficacia de las pruebas obtenidas mediante agresiones inconstitucionales». Pero, a su vez, añade, «el TC español, ha fundamentado la prueba ilícita en el derecho al proceso con todas las garantías y, en ocasiones, en el derecho a la prueba pertinente e, incluso a la presunción de inocencia». Vid. ASENCIO MELLADO, J. M., «Prueba ilícita: Declaración y efectos», *Revista General de Derecho Procesal*, n.º 26, 2012, p. 17-18.

[748] GÓMEZ COLOMER, J. L., «Prueba admisible y prueba prohibida: Cambios en el garantismo judicial motivados por la lucha contra el crimen organizado en la realidad jurisprudencial española actual», cit., p. 7.

4. La prueba ilícita obtenida por particulares

En el supuesto en el que la prueba haya sido obtenida por un particular, el TS ha sentado doctrina de que la prueba sería considerada ilícita, no pudiendo tener entrada en el proceso, solo en aquellos casos en los que el propósito del particular hubiera estado encaminado a utilizarla como prueba. Consecuentemente, de haber sido otros los motivos por los que se obtuvo la fuente incriminatoria, aun violentando derechos fundamentales, pero alejados de la intención del particular de que la misma sirviera de prueba en un proceso, o dicho de otro modo, si la prueba hubiese sido obtenida «con absoluta desconexión de toda actividad del Estado en la investigación de hechos ilícitos»[749] no le sería de aplicación el art. 11.1 LOPJ y, por tanto, podría ser válidamente incorporada a las actuaciones.

Este criterio lo estableció la STS 116/2017, de 23 de febrero, FJ 7.º, que resolvió un caso en el que, con ocasión de un registro llevado a cabo en el domicilio de un particular por las autoridades francesas, fue intervenida, en formato digital, información relativa a personas que eran titulares de activos en una entidad bancaria suiza.

Esta información fue conseguida ilícitamente por un ingeniero informático que trabajaba para una entidad bancaria, con la finalidad de poder lucrarse con la venta de los datos de clientes de diferentes bancos suizos. Por las autoridades francesas, como quiera que, de la investigación realizada, pudiera quedar acreditada la comisión de delitos contra la Hacienda Pública, se acordó la entrega de la información obtenida, a los países afectados, entre los que se encontraba España. Con base en ello, en nuestro país se inició un procedimiento penal por un posible delito del art. 305 CP contra la Hacienda Pública.

La referida STS 116/2017, resolvió el recurso de casación que finalmente se interpuso en dicho proceso, y tras señalar que «las reglas de exclusión probatoria se distancian de su verdadero sentido cuando no tienen relación con la finalidad que está en el origen mismo de su formulación», declaró que «la decisión sobre la exclusión probatoria adquiere una dimensión especial si quien ha hecho posible que las pruebas controvertidas afloren, nunca actuó en el marco de una actividad de respaldo a los

[749] MARCHENA GÓMEZ, M., «La "Sentencia Falciani": ¿hacia un nuevo concepto de prueba ilícita entre particulares?», *Revista del Ministerio Fiscal*, n.º 3, 2017, p. 8.

órganos del Estado llamados a la persecución del delito», añadiendo que «este dato resulta decisivo».

Asimismo, cabe mencionar la STS 287/2017, de 19 de abril, FJ 2.º, que resuelve un caso en el que una madre entrega a las FCSE un ordenador familiar en el que se recogen imágenes acreditativas de abusos sexuales cometidos por el padre sobre una de sus hijas, declarando que «se trata de una prueba proporcionada por un particular a los agentes de la autoridad sin que esa entrega haya sido concebida como un mecanismo de elusión de las garantías que el sistema constitucional reconoce para la protección de los derechos».

Esta doctrina, establecida por la STS 116/2017, ha sido objeto de algunas críticas. Así, por ejemplo, ZARAGOZA TEJADA y GUTIERREZ AZANZA afirman que «abre una puerta que puede desencadenar […] importantes y peligrosas consecuencias»[750]. La principal radicaría en la circunstancia de que este criterio «puede provocar que los organismos estatales tengan la tentación de contactar con estos particulares a fin de que procedan ellos mismos a recopilar pruebas incriminatorias (realizando actos que supongan una afectación a derechos fundamentales) sin necesidad de esperar, como de hecho ocurre en la actualidad, al dictado de una resolución judicial habilitante»[751].

También otros autores, como ASENCIO MELLADO, critican de forma parecida esta posición, señalando que «reducir la prohibición a los casos en que el particular suplanta al Estado, limitaría la interdicción de admisión de la prueba a los supuestos extremos en los que el Estado se valiera arteramente de particulares para obtener pruebas ilegítimas»[752], añadiendo que estas consecuencias «no son admisibles por romper con la armonía del sistema»[753].

---

[750] ZARAGOZA TEJADA, J. I.; GUTIERREZ AZANZA, D. A., «La prueba ilícita. Una reflexión tras la STS del 23 de febrero del 2017», *Revista Aranzadi de Derecho y Proceso Penal - Parte Jurisprudencia*, n.º 47, 2017, p. 11.

[751] ZARAGOZA TEJADA, J. I.; GUTIERREZ AZANZA, D. A., «La prueba ilícita. Una reflexión tras la STS del 23 de febrero del 2017», *Revista Aranzadi de Derecho y Proceso Penal - Parte Jurisprudencia*, n.º 47, 2017, p. 11.

[752] ASENCIO MELLADO, J. M., «La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita», *Diario La Ley - Sección Tribuna*, n.º 9499, 2019, p. 5.

[753] ASENCIO MELLADO, J. M., «La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita», *Diario La Ley - Sección Tribuna*, n.º 9499, 2019, p. 5.

En cualquier caso, ha de significarse que la reciente STC 97/2019, de 16 de julio, vino a desestimar la demanda de amparo que se interpuso contra la meritada STS 116/2017, declarando en su FJ 5.º que «desde el punto de vista de la garantía contenida en el art. 24.2 CE, que es el único que atañe a este Tribunal, resulta plenamente compatible con dicho precepto constitucional la interpretación efectuada por el Tribunal Supremo del art. 11.1 LOPJ». De modo que, la interpretación del referido precepto efectuada por el TS, continua la referida resolución, «no merece, por tanto, ninguna censura desde el punto de vista del derecho a un proceso con todas las garantías (art. 24.2 CE)».

Sin embargo, el TC no ha ratificado la doctrina establecida por el TS en su Sentencia 116/2017, a la que anteriormente nos hemos referido, procediendo, de forma paralela, a llevar a cabo un análisis acerca de si el concreto juicio ponderativo realizado por el TS, y la consiguiente admisión como prueba de los elementos de convicción controvertidos, se ajusta a las exigencias constitucionales del derecho a un proceso con todas las garantías, llegando a las siguientes conclusiones:

a) El hecho de que la vulneración originaria del derecho sustantivo fuera cometida por un particular no altera, en absoluto, el canon de constitucionalidad aplicable desde la óptica del derecho a un proceso con todas las garantías. La exclusión de los elementos probatorios obtenidos ha de ser, también en este tipo de supuestos, el punto de partida o regla general, si bien, en cada caso concreto, el órgano judicial puede apreciar, con arreglo a los parámetros que ya han sido expuestos, la ausencia de necesidades de tutela procesal en relación con la vulneración consumada, incorporando, en esos casos excepcionales, los elementos controvertidos al acervo probatorio.

b) Desde un punto de vista interno, considera que, teniendo en cuenta que los datos controvertidos son, exclusivamente, la existencia de la cuenta bancaria y el importe ingresado en la misma, el resultado de la intromisión en la intimidad no es, por tanto, de tal intensidad que exija, por sí mismo, extender las necesidades de tutela del derecho sustantivo al ámbito del proceso penal, teniendo en cuenta, además, que los datos obtenidos se refieren a aspectos periféricos e inocuos, dado que no se introdujeron en el proceso datos, como podrían ser los concretos movimientos de cuentas, que puedan revelar o que permitan deducir los comportamientos o hábitos de vida del interesado.

c) Finalmente, de otro lado, y desde el punto de vista externo, señala el TC que tampoco existe un riesgo cierto de propiciar, con la admisión de la prueba controvertida,

prácticas que comprometan pro futuro la efectividad del derecho fundamental en juego en el ordenamiento jurídico español, ya que, a diferencia de las circunstancias que pueden determinar una respuesta distinta en otro ordenamiento jurídico, en España no existen prácticas de opacidad bancaria amparadas por el poder público que puedan dar lugar a la proliferación de comportamientos de intromisión ilícita entre particulares como el que, en este caso, ha resultado discutido. Por ello, concluye que no se advierte, tampoco desde un punto de vista externo, que exista una necesidad jurídica de extender al proceso penal la tutela del derecho a la intimidad.

De estas consideraciones, como podrá comprobarse más adelante cuando aclaremos el significado de la teoría de la conexión de antijuridicidad, el TC ha llevado un análisis del caso, teniendo en cuenta los parámetros que su misma doctrina fijó para determinar si se produce la referida conexión antijurídica, llevando a cabo un estudio de sus perspectivas interna y externa.

Esta resolución ha sido igualmente objeto de críticas doctrinales. Así, por ejemplo, ZARAGOZA TEJADA Y GUTIERREZ AZANZA afirman que, «en definitiva, la sentencia del Tribunal Constitucional ahonda en el progresivo abandono de la exclusión de la prueba ilícita fundamentada en la tutela del derecho fundamental lesionado»[754] y consideran que «se observa una progresiva aproximación a teorías más "utilitaristas" sobre la prueba ilícita, al estilo norteamericano»[755]. También ASENCIO MELLADO se ha referido a esta sentencia de una forma muy crítica, al señalar que el TC «ha optado por derivar o depreciar los derechos fundamentales y subordinarlos a criterios de seguridad o justicia sumamente peligrosos»[756].

Por nuestra parte, nos parece sumamente correcta la teoría que formuló el TS, en la Sentencia 116/2017, por cuanto la acción de un particular que, como dice la propia resolución en su FJ 6.º, «sin vinculación alguna con el ejercicio del *ius puniendi*», obtiene una prueba «ilícita» con desconocimiento de que la misma podría convertirse más tarde en fuente de prueba con posibilidad de desvirtuar la presunción de inocencia,

[754] ZARAGOZA TEJADA, J. I.; GUTIÉRREZ AZANZA, D. A., «La exclusión de la prueba ilícita tras la sentencia del Tribunal Constitucional de 16 de julio de 2019 sobre la "Lista Falciani"», *Revista Aranzadi de Derecho y Proceso Penal - Parte Jurisprudencia*, n.º 56, 2019, p. 8.

[755] ZARAGOZA TEJADA, J. I.; GUTIÉRREZ AZANZA, D. A., «La exclusión de la prueba ilícita tras la sentencia del Tribunal Constitucional de 16 de julio de 2019 sobre la "Lista Falciani"», cit., p. 8.

[756] ASENCIO MELLADO, J. M., «La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita», cit., p. 20.

no puede equipararse, en cuanto a sus consecuencias jurídicas, como igualmente se declara, «con la acción vulneradora del agente de la autoridad que personifica el interés del Estado en el castigo de las infracciones criminales».

Esta doctrina, no ha sido desautorizada por el TC, no obstante las consideraciones llevadas a cabo en su Sentencia 97/2019, anteriormente referidas. Estimamos que, como declaró la STS 116/2017, resulta decisiva la circunstancia relativa a la actuación del particular de forma absolutamente ajena a la actuación de los órganos del Estado encargados de la persecución del delito.

Sin embargo, adhiriéndonos a la opinión formulada por MARCHENA GÓMEZ, «la conclusión acerca de la necesidad de no valorar con arreglo a los mismos parámetros situaciones que merecen ser diferenciadas, no puede convertirse, sin más, en una afirmación axiomática, conforme a la cual el Estado no debería adentrarse en el examen de la forma de obtención de un material probatorio por el particular»[757]. Se impone, por tanto, dice el mencionado autor, «una llamada a la necesidad de ponderar, en función del caso concreto, las circunstancias en las que esa fuente de prueba ha sido obtenida y, al propio tiempo, la intensidad de la afectación del derecho fundamental que ha podido verse erosionado»[758].

En definitiva, tal y como expresa la STS 116/2017, FJ 7.º, tan decisivos resultan el alcance y la intensidad de la afectación del derecho menoscabado, como la necesidad de atender al significado de la actividad del particular, lo que exigirá una valoración según el caso concreto, que deberá ofrecer una solución respetuosa con los valores implicados. De este modo la regla de exclusión no correrá el riesgo de apartarse de su genuino fundamento.

5. Procedimiento y fase procesal para la exclusión de la prueba ilícita

Como quiera que la LECrim no establece el procedimiento en virtud del que la prueba ilícita ha de ser excluida del proceso, se hace necesario el análisis de cuál ha de ser el mismo, dado que, de acuerdo con lo señalado por ASENCIO MELLADO, «es una cuestión esencial, no baladí, la determinación del procedimiento a través del cual se ha

[757] MARCHENA GÓMEZ, M., «La "Sentencia Falciani": ¿hacia un nuevo concepto de prueba ilícita entre particulares?», cit., p. 56.
[758] MARCHENA GÓMEZ, M., «La "Sentencia Falciani": ¿hacia un nuevo concepto de prueba ilícita entre particulares?», cit., p. 56.

declarar la ilicitud de una prueba obtenida con vulneración de derechos fundamentales, por cuanto de la opción que se escoja van a derivarse consecuencias muy serias, tanto que pueden suponer la degradación efectiva de los derechos, situándolos en el ámbito del proceso por debajo de la apreciación de las nulidades procesales decretadas ante irregularidades legales»[759].

En cuanto al concreto procedimiento, habida cuenta de que, a salvo de lo dispuesto en el art. 786.2 LECrim para el procedimiento abreviado —que permite en una audiencia previa al inicio de las sesiones la posibilidad de denunciar la vulneración de algún derecho fundamental[760]—, no existe en la LECrim un trámite específico, es por lo que algunos autores defienden la aplicación supletoria (art. 4 LEC) del art. 287 de la LEC, que establece un breve trámite previo a la declaración de la ilicitud de la prueba por vulneración de derechos fundamentales en el proceso civil[761].

Así, por ejemplo, DE URBANO CASTRILLO Y TORRES MORATO afirman que —teniendo en cuenta aspectos tales como que puede ser planteada tan pronto como se tuviera conocimiento de la misma por las partes, como de oficio por el órgano judicial, exigiéndose la contradicción y estableciéndose la posibilidad de proponer pruebas—, «con la excepción de la limitación de las vías de reconsideración, porque en el proceso penal, existe, además, otro momento crucial, que es el del inicio de la vista oral, el resto

[759] ASENCIO MELLADO, J. M., «La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales», cit., p. 6.

[760] El art. 786.2 LECrim dispone, *in fine*, que «el juez resolverá en el mismo acto lo procedente sobre las cuestiones planteadas» y concluye estableciendo que «frente a la decisión adoptada no cabrá recurso alguno, sin perjuicio de la pertinente protesta y de que la cuestión pueda ser reproducida, en su caso, en el recurso frente a la sentencia». De acuerdo con ello, entendemos que en la mayoría de los casos, ante la dificultad que puede plantear la decisión acerca de la expulsión de una prueba ilícita en el acto, lo normal será que se desestime la petición por el juez y que definitivamente resuelva en sentencia.

[761] Bajo la rúbrica «ilicitud de la prueba», el art. 287 LEC dispone lo siguiente:

«1. Cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes.

Sobre esta cuestión, que también podrá ser suscitada de oficio por el tribunal, se resolverá en el acto del juicio o, si se tratase de juicios verbales, al comienzo de la vista, antes de que dé comienzo la práctica de la prueba. A tal efecto, se oirá a las partes y, en su caso, se practicarán las pruebas pertinentes y útiles que se propongan en el acto sobre el concreto extremo de la referida ilicitud.

2. Contra la resolución a que se refiere el apartado anterior sólo cabrá recurso de reposición, que se interpondrá, sustanciará y resolverá en el mismo acto del juicio o vista, quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en la apelación contra la sentencia definitiva».

de la regulación es perfectamente extrapolable a los procedimientos penales»[762]. También DEL MORAL GARCÍA, interpreta que no existe objeción alguna y si muchas ventajas en la aplicación supletoria del art. 287 LEC al proceso penal[763].

Estimamos, sin embargo, que no obstante estas apreciaciones, así como que, en efecto, no parece existir impedimento para la aplicación del art. 287 LEC, sería conveniente el establecimiento de un trámite específico para el proceso penal en una materia de esta envergadura. Esta reforma, como no podría ser de otro modo, debe llevarse a cabo conjuntamente con la regulación de la prueba ilícita en la LECrim, desarrollando así el art. 11.1 LOPJ, tal y como propondremos al final de este epígrafe.

Pero, al margen del procedimiento a emplear para expulsar la prueba ilícita, el cual, a la vista de lo indicado anteriormente, no pensamos que constituiría una cuestión excesivamente compleja, la problemática se ha planteado en relación con la fase del proceso penal en la que se debería proceder a declarar la ilicitud de dicha prueba. A este respecto, doctrinalmente se ha defendido que la exclusión se ha de producir en fase de instrucción, mientras que, frente a esta postura, existen opiniones que mantienen que la exclusión únicamente puede producirse en la fase de juicio oral[764].

---

[762] DE URBANO CASTRILLO, E.; TORRES MORATO, M. A., *La prueba ilícita penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2012, p. 70.

[763] DEL MORAL GARCÍA, A., «Tratamiento procesal de la prueba ilícita por vulneración de derechos fundamentales», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2001, pp. 171-173, Consultado en http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 22 de marzo de 2020.

[764] Sobre esta cuestión es conocido el debate mantenido entre los profesores GIMENO SENDRA Y ASENCIO MELLADO. El primero de ellos puso de manifiesto en un artículo doctrinal que la exclusión de la prueba ilícita ha de verificarse por el órgano enjuiciador sin que tal acuerdo deba adoptarse por el juez instructor, mientras que por el segundo se ha defendido que la declaración de ilicitud y consecuente expulsión de proceso debe realizarse tan pronto como se tenga conocimiento de ella, pudiendo llevarse a efecto por el juez instructor. Se trata de unos artículos doctrinales de conveniente lectura, dado que, además de ponerse de manifiesto por estos dos eminentes profesores la justificación de su opinión sobre esta cuestión, sirven igualmente para profundizar sobre la teoría de la prueba ilícita. Estos trabajos, por orden cronológico, son los siguientes:

1. GIMENO SENDRA, J. V., «Corrupción y propuestas de reforma», *Diario La Ley*, n.º 7990, 2012.

2. ASENCIO MELLADO, J. M., «La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales», *Diario La Ley - Sección Doctrina*, n.º 8009, 2013.

3. GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación al artículo del Prof . Asencio)», *Diario La Ley - Sección Tribuna*, n.º 8021, 2013.

4. ASENCIO MELLADO, J. M., «Otra vez sobre la exclusión de las pruebas ilícitas en fase de instrucción penal: respuesta al Prof. Gimeno Sendra», *Diario La Ley - Sección Doctrina*, n.º 8026, 2013.

En defensa de la exclusión de la prueba ilícita en fase de instrucción, ASENCIO MELLADO ha argumentado, con cita de las SSTC 184/2003, de 23 de octubre, 49/1996, de 26 de marzo y 149/2001, de 27 de junio, que no obstante declarar el TC en las referidas resoluciones que la labor de enjuiciar corresponde al tribunal competente y que es éste el que debe valorar si es procedente la condena a la luz de las pruebas aportadas, al mismo tiempo ordena, tras constatar la ilicitud de algunas que fundamentaron la condena objeto de recurso, la retrotracción de las actuaciones al momento anterior a la formulación de la acusación y la proposición de prueba para, que una vez excluidas las pruebas ilícitas, la acusación, sin contar con ellas, valore si puede o no acusar. Con base en ello, llega a la conclusión de que, en relación con las pruebas ilícitas, las citadas sentencias del TC «ponen el acento en la necesidad de que se excluyan con anterioridad a la formulación de la acusación y de la proposición de prueba para que las partes acusadoras la confeccionen a la vista exclusiva de las pruebas válidas y, con ello, para que la defensa pueda, por un lado, en su caso, no verse sujeta a un juicio si no hay pruebas para su celebración y, si las hay, que articulen su posición solo en atención a lo que posea valor probatorio»[765].

Asimismo, por otro lado, el mismo autor señala que, como quiera que el TC acuerda la retroacción de las actuaciones, al momento anterior a la presentación de los escritos de acusación, debe entenderse que «cuando se retrotrae es porque se aprecia una nulidad en el momento mismo al que se remiten las actuaciones o, lo que es igual, que el juez de instrucción incurrió en el defecto de no excluir lo que debió»[766].

Por lo que respecta a la posición defensora de la exclusión de la prueba ilícita en fase de juicio oral, GIMENO SENDRA afirma que «la misión de la instrucción no consiste en la declaración de la ilegalidad de los medios de prueba, sino la investigación y determinación del hecho punible y la responsabilidad de su autor»[767], añadiendo que «es ésta una competencia del órgano jurisdiccional decisor, quien, bien en la comparecencia

---

5. GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación a la réplica del Prof. Asencio)», *Diario La Ley - Sección Tribuna*, n.º 8027, 2013.

[765] ASENCIO MELLADO, J. M., «La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales», cit., p. 12.

[766] ASENCIO MELLADO, J. M., «Otra vez sobre la exclusión de las pruebas ilícitas en fase de instrucción penal: respuesta al Prof. Gimeno Sendra», cit., p. 11.

[767] GIMENO SENDRA, J. V., «Corrupción y propuestas de reforma», cit., p. 9.

previa, bien en la sentencia, podrá declarar la inconstitucionalidad de tales pruebas, así como la extensión de sus efectos»[768].

Y en la misma línea, el referido autor ha señalado que ningún precepto de la LECrim autoriza al juez de instrucción «a declarar nulidades derivadas de una supuesta prueba ilícita, ya que de ser así, se le otorgaría al juez de instrucción un poder omnímodo, que sustraería la legítima competencia del órgano de enjuiciamiento sobre la valoración de la prueba»[769].

Existen opiniones en ambos sentidos, como por ejemplo la de autores como DÍAZ CABALIE Y MARTÍN MORALES, quienes defienden que la exclusión de la prueba se produzca en fase de instrucción, proponiendo la incorporación a la LECrim de un trámite incidental a tal efecto[770]. En sentido contrario se pronuncia DEL MORAL GARCÍA, quien considera preferible sustraer del juez de instrucción esa resolución formal sobre la ilicitud de la prueba, afirmando que «es más acertado concentrar ambas facultades en el mismo órgano, única forma de evitar discrepancias de criterio que no ofrecerían fácil solución»[771].

Nuestra perspectiva, sin embargo, se alinea con posiciones más conciliadoras, en relación con la fuerte controversia referida, considerando la posibilidad de una postura ecléctica con base en las siguientes consideraciones:

- De excluirse la prueba ilícita en fase de instrucción, y no obstante continuar el procedimiento por la existencia de otros actos de investigación que puedan acreditar la culpabilidad del investigado, las partes acusadoras podrán interponer recurso de apelación para ante la audiencia correspondiente (arts. 220 y 766.3 LECrim), que incluso podrá ser susceptible de recurso de amparo por posible vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE) y a un proceso con todas las garantías (art. 24.2 CE). Lo mismo puede predicarse en el caso de dictarse un auto de sobreseimiento

[768] GIMENO SENDRA, J. V., «Corrupción y propuestas de reforma», cit., p. 9.

[769] GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación a la réplica del Prof. Asencio)», cit., p. 2.

[770] DÍAZ CABIALE, J. A.; MARTÍN MORALES, R., *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, Madrid, Civitas, 2001, p. 120.

[771] DEL MORAL GARCÍA, A., «¿Cuándo debe declarar la inutilizabilidad de un medio de prueba por vulneración de derechos fundamentales?», *Revista de Jurisprudencia - El Derecho*, n.º 2, Marzo, 2017, p. 9.

provisional[772]. Por tanto, la resolución que se dicte por el Juzgado de Instrucción no estará exenta de las debidas garantías.

- Del mismo modo, si como consecuencia de la exclusión de la prueba ilícita, se dictase auto de sobreseimiento libre, cabe contra el mismo recurso de casación, dado que, de conformidad con lo dispuesto en el art. 848 LECrim «podrán ser recurridos en casación, únicamente por infracción de ley, […] los autos definitivos dictados en primera instancia y en apelación por las Audiencias Provinciales o por la Sala de lo Penal de la Audiencia Nacional cuando supongan la finalización del proceso por falta de jurisdicción o sobreseimiento libre y la causa se haya dirigido contra el encausado mediante una resolución judicial que suponga una imputación fundada». Asimismo y al igual que en el caso planteado en el supuesto anterior, el auto dictado por el TS al resolver el recurso de casación, podrá ser susceptible de recurso de amparo ante la posibilidad de vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE) y a un proceso con todas las garantías (art. 24.2 CE).

- Finalmente, si la exclusión probatoria no se resuelve por el juez de instrucción, circunstancia que puede producirse por lo general por tratarse de una posible ilicitud no manifestada de forma notoria, no existe problema alguno, porque como señala GIMENO SENDRA, *de lege lata*, «ciertamente ha de convenirse que todo lo referente a la valoración de la prueba constituye una competencia del órgano de enjuiciamiento, quien, bien en la comparecencia previa en sede del procedimiento abreviado (art. 786.2 LECrim), bien en su sentencia con carácter general, habrá de decidir sobre la exclusión de su ámbito decisorio de la prueba inconstitucionalmente obtenida, así como de la extensión de sus efectos»[773].

Por todo ello, nos adherimos a opiniones como la de LÓPEZ BARJA DE QUIROGA, quien, desde una perspectiva conciliadora, escribe que «cabe defender que si la prueba se refiere a alguna cuestión relevante, debe, en cualquier caso, admitirse reservando para un momento posterior, que sería el de la sentencia, la decisión sobre la apreciabilidad de esa prueba»[774], pero aclara que, sin embargo, «cualquiera que sea la etapa procesal en

[772] La STC 39/2017, de 24 de abril, estima un recurso de amparo por vulneración del derecho a la tutela judicial efectiva, en relación con un auto de sobreseimiento provisional dictado por un juzgado de instrucción y resuelto en apelación con el carácter de firme por la correspondiente audiencia provincial.

[773] GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación a la réplica del Prof. Asencio)», cit., p. 2.

[774] LÓPEZ BARJA DE QUIROGA, J., «*Tratado de Derecho Procesal Penal*», cit., p. 909.

que se encuentre el proceso, una vez que se ha puesto de manifiesto que se trata de una prueba prohibida o que ha sido ilícitamente obtenida, debe procederse inmediatamente a su exclusión, bien por considerarla impertinente, bien porque su permanencia en los autos atenta contra las garantías del proceso»[775].

También desde una posición más moderada se pronuncia PAZ RUBIO, al escribir que, aun cuando no corresponde al juez instructor resolver en la fase de investigación o instrucción la cuestión relativa a la licitud o ilicitud de las pruebas, por exceder de su competencia objetiva y porque no es posible hacer tal análisis cuando los medios de investigación presuntamente ilícitos aún no han adquirido la categoría de prueba ni han sido valoradas como tales, «ello no significa, en absoluto, que al juez instructor no le vincule la prohibición constitucional de admitir pruebas —mejor, medios de investigación— obtenidos con violación de derechos fundamentales, puesto que las garantías constitucionales del proceso también se extienden a la fase sumarial»[776]. De este modo, tras dejar sentado que es indudable que el juez de instrucción puede rechazar la práctica de determinados actos de investigación o decretar de oficio o a instancia de parte la nulidad, si constata que las diligencias sumariales se pretenden obtener o han sido obtenidas de forma manifiestamente ilegal, afirma en una opinión que compartimos, que «sería absurdo que el instructor estuviera siempre obligado a ordenar o a proseguir la instrucción, aun con la certeza de la ilicitud total o parcial de la misma, y esperar hasta la fase de juicio oral, o a la sentencia, para que el juez o tribunal sentenciador repare la manifiesta infracción de los derechos fundamentales»[777].

En virtud de lo expuesto, consideramos que la prueba ilícita ha de excluirse del procedimiento, tan pronto como se tenga conocimiento de la misma. Como refuerzo a esta opinión, es conveniente traer a colación la Circular 1/2013 de la FGE, en la que se concluye que «consecuentemente deberán los Sres. Fiscales tanto en su función investigadora, como en su actuación inspectora durante la fase de instrucción, tener

[775] Matiza este autor que «evidentemente; si sólo durante el juicio oral queda acreditada la ilicitud de la prueba, entonces será en la sentencia en donde teniendo en cuenta ese extremo, no se aprovechará o apreciará la prueba ilícitamente obtenida». Vid. LÓPEZ BARJA DE QUIROGA, J., «*Tratado de Derecho Procesal Penal*», cit., p. 909.

[776] PAZ RUBIO, J. M., «La prueba en el proceso penal», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 1, 1992, p. 232.

[777] PAZ RUBIO, J. M., «La prueba en el proceso penal», cit., pp. 232-233.

siempre presente la máxima contenida en el ATS de 18 de junio de 1992: no todo es lícito en el descubrimiento de la verdad»[778].

Finalmente, es preciso hacer constar que el Anteproyecto de LECrim de 2013, se ocupó de este tema, ajustándose a la solución que nos parece más correcta, al disponer en el apdo. 4 del art. 13 que «en cualquier momento en que se constate la existencia de la infracción del derecho fundamental afectado las informaciones o fuentes de prueba o resultados de las pruebas han de ser excluidos del proceso, sin perjuicio de que, rechazada la exclusión, las partes puedan reproducir con posterioridad la petición de declaración de nulidad de la prueba». Se trata de una breve pero efectiva solución a este problema, que en nuestra opinión debería incorporarse con prontitud, de forma definitiva, a nuestra legislación procesal penal.

6. Correcciones al principio de la prueba prohibida

Desde la adopción de la doctrina de los frutos del árbol envenenado o del efecto reflejo de la prueba ilícita, puede afirmarse con rotundidad que, en nuestro ordenamiento jurídico, únicamente aquella verdad alcanzada con el debido respeto a los principios esenciales que conforman los derechos fundamentales puede considerarse admisible jurídicamente. Esta doctrina tiene plena vigencia por imperativo del art. 11.1 LOPJ, el cual sigue sin ser objeto de la que ya consideramos algo más que una necesaria reforma legislativa, tal y como expondremos más adelante.

Ahora bien, en la actualidad, esta prohibición de valoración probatoria, de acuerdo con reiterada jurisprudencia del TS y del TC, no rige de forma absoluta, dado que para que se produzca la expulsión del proceso de la prueba indirectamente obtenida, y por tanto se admita su efecto reflejo, será necesario que no resulte de aplicación a la misma alguna de las teorías correctoras que se han venido imponiendo jurisprudencialmente.

[778] La Circular 1/2013 cita de lo dispuesto en el punto 28 de la Recomendación (2000)19 del Comité de Ministros del Consejo de Europa sobre el papel del Ministerio Fiscal en el sistema de justicia penal, que dispone que «los Fiscales no deben presentar pruebas respecto de las que sepan o crean sobre bases razonables que fueron obtenidas mediante métodos contrarios a la Ley» así como que «en caso de duda el Ministerio Fiscal debe pedir al Tribunal que se pronuncie sobre la admisibilidad de tal prueba». Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*», cit., p. 7.

En efecto, a partir de la segunda mitad de la década de los noventa del siglo pasado, comienzan a surgir determinadas excepciones jurisprudenciales a los excesos que podría suponer la aplicación sin límites de la referida doctrina prohibitiva del efecto indirecto de la prueba ilícitamente obtenida. Estas excepciones encuentran su justificación en la circunstancia de que la expulsión de una prueba ilícita no impide que sean valoradas otras pruebas cuya proveniencia sea independiente de la prueba corrompida.

De este modo, como recientemente ha declarado la STS 423/2019, de 19 de septiembre, FJ 3.º, recordando la doctrina del TC[779], la ilicitud constitucional se extiende también a las pruebas derivadas o reflejas si entre ellas y las anuladas existe una conexión natural o causal, lo cual constituye el presupuesto para poder hablar de prueba derivada de otra ilícitamente obtenida. Por tanto, la regla es que todo elemento probatorio que pretenda deducirse a partir de un hecho vulnerador del derecho fundamental se halla también incurso en la prohibición.

Pero no obstante ser esta la regla general, en supuestos excepcionales, se ha venido admitiendo que estas pruebas que, en principio pudieran considerarse causalmente derivadas de la medida vulneradora del derecho fundamental, son jurídicamente independientes de dicha injerencia indebida, habiéndose reconocido como válidas y aptas para enervar el principio de presunción de inocencia[780]. En este sentido, señala la STS 963/2013, de 18 de diciembre, FJ 1.º, que «allí donde la prueba se hubiera obtenido de todos modos, sin necesidad de recurrir a otra anterior, faltará la conexión de antijuricidad, es decir, la relación causal de la primera con la segunda» y añade con otras

[779] Doctrina que se desarrolla en las SSTC 81/1998, de 2 de abril, FJ 4.º; 49/1999, de 5 de abril FJ 14.º ; 94/1999, de 31 de mayo, FJ 6.º; 171/1999, de 27 de septiembre FJ 4.º; 136/2000, de 29 de mayo, FJ 6.º; 28/2002, de 11 de febrero, FJ 4.º; 167/2002, de 18 de septiembre, FJ 6.º; 261/2005, de 24 de octubre, FJ 5.º; y 66/2009, de 9 de marzo, FJ 4.º

[780] Vid. STS 423/2019, de 19 de septiembre, FJ 3.º, que se refiere a la STS 86/2018, de 19 de febrero, que en su FJ 3.º no obstante declarar que la regla general es que todo elemento probatorio que pretenda deducirse a partir de un hecho vulnerador del derecho fundamental se halla también incurso en la prohibición de valoración, aclara que, «en supuestos excepcionales, se ha venido admitiendo que estas pruebas son jurídicamente independientes de dicha vulneración, habiéndose reconocido como válidas y aptas para enervar el principio de presunción de inocencia», y añade que «para establecer si se está ante un supuesto en que debe aplicarse la regla general que se ha referido o, por el contrario, nos encontramos ante alguna de las hipótesis que permiten excepcionarla, habrá que delimitar si estas pruebas están vinculadas de modo directo a las que vulneraron el derecho fundamental sustantivo, es decir, habrá que establecer si existe o no una conexión de antijuridicidad entre la prueba originaria y las derivadas».

palabras «todo resultado que se hubiera producido aunque una de sus condiciones no se hubiera producido, no es el resultado de esa condición».

En definitiva, afirma RIVES SEVA, «el TS ha advertido de los abusos a que puede conducir la doctrina del árbol podrido que todo lo contamina, pues de aceptarse al pie de la letra ese principio nos encontraríamos constantemente con situaciones de verdadera impunidad, que chocarían con la lógica de la realidad y con el respeto que ha de tenerse a conseguir una verdadera Justicia material»[781].

En relación con los criterios correctores que permiten estimar que existe una desconexión entre la prueba ilícita y la prueba derivada, todos los cuales, como dice ARMENTA DEU, conviven con la doctrina de la conexión de antijuridicidad, surgida a partir de la STC 81/1998, de 2 de abril[782], la jurisprudencia del TS ha declarado reiteradamente que «en la jurisprudencia de esta Sala se acostumbran a citar como criterios idóneos para excluir la conexión de antijuridicidad y validar por tanto las pruebas reflejas o derivadas los siguientes: el descubrimiento inevitable, el vínculo atenuado entre la prueba ilícita y la refleja, el hallazgo casual, la fuente independiente, la ponderación de intereses, la autoincriminación del imputado en el plenario, y alguna otra (SSTS 320/2011 de 22 de abril; 811/2012 de 30 de octubre; 69/2013 de 31 de enero; 912/2013 de 4 de diciembre; 963/2013 de 18 de diciembre; 1273/2014 de 12 de marzo; y 511/2015 de 17 de julio)»[783].

Teniendo en cuenta, que las excepciones al efecto reflejo convergen en la doctrina de la conexión de antijuridicidad[784], con carácter previo a ofrecer una explicación de esta, realizaremos unas consideraciones acerca de los criterios que consideramos más relevantes, dado que, en definitiva y al igual que en los supuestos de desconexión de antijuridicidad, todos suponen una desconexión de la prueba indirecta de la inicialmente obtenida de forma ilícita, y ello por cuanto, como señala ARMENTA DEU,

[781] RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., pp. 27-28.

[782] ARMENTA DEU, T., «*Lecciones de Derecho Procesal Penal*», cit., p. 296.

[783] Vid. SSTS 423/2019, de 19 de septiembre, FJ 3.º; 651/2018, de 14 de diciembre, FJ 2.º; 259/2018, de 30 de mayo, FJ 3.º; o 2/2018, de 9 de enero, FJ 6.º; entre otras.

[784] A este respecto, afirma ARMENTA DEU que «la esencia de la teoría de la conexión de la antijuridicidad encuentra su "talón de Aquiles" en supuestos semejantes a aquellos que han conducido a recurrir a las doctrinas acabadas de citar». Vid. ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», *Revista del Poder Judicial*, n.º especial XIX, 2006, p. 10.

«la jurisprudencia ha ido sentando una serie de parámetros que sirven para definir la existencia o no de la referida conexión de antijuridicidad»[785].

Estos criterios, cuyo estudio estimamos que será suficiente para la comprensión del problema así como para exponer a continuación la doctrina de la conexión de antijuridicidad y exponer nuestra opinión sobre el tema, siguiendo a MIRANDA ESTRAMPES, se concretan en la excepción de la fuente independiente, la del descubrimiento inevitable y la del nexo causal atenuado[786].

6.1. La fuente independiente

Al referirnos a la fuente independiente, como su propio nombre indica, en realidad no podemos hablar de una excepción, ya que, de ser auténticamente independiente, no podrá traer causa de la prueba prohibida al no tener conexión causal con la misma. En este sentido, como señala MIRANDA ESTRAMPES, «obviamente si la prueba utilizada no guarda ningún tipo de conexión con la prueba ilícita inicial, no se cumple el presupuesto esencial determinante del reconocimiento de eficacia refleja»[787]. En la misma línea, dice GARCÍA SAN MARTÍN que con esta excepción se excluye la aplicación del efecto reflejo, dado que «no queda constatada la vinculación directa entre la diligencia de prueba ilícita y la diligencia o diligencias posteriores; desvinculación que se entiende real y no meramente potencial»[788].

Por tanto, nos encontraremos con una fuente independiente de la inicialmente obtenida vulnerando derechos fundamentales, no por existir una desconexión jurídica, sino una desconexión causal natural, y en este sentido, de acuerdo con lo expresado por ARMENTA DEU, «la doctrina de la fuente independiente impide aplicar la doctrina de los

---

[785] ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», *Revista del Poder Judicial*, n.º especial XIX, 2006, p. 14.

[786] MIRANDA ESTRAMPES cataloga estos criterios correctores como los más relevantes, habida cuenta de su reconocimiento por la jurisprudencia norteamericana, reconocimiento a partir del que estas excepciones se han ido reconociendo también en otras legislaciones y ordenamientos jurídicos, como manifestación de un fenómeno de progresiva norteamericanización de la regla de exclusión. Vid. MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», cit., p. 142.

[787] MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», cit., p. 143.

[788] GARCÍA SAN MARTÍN, J., «La prueba penal ilícita y la prueba penal refleja: Hacia una restrictiva aplicación de la doctrina de los frutos del árbol envenenado», *Tirant Online, Documento TOL2.249.759*, 2011, p. 7.

frutos del árbol envenenado cuando no existe una vinculación directa entre la práctica de una diligencia de forma ilícita y la/s diligencia/s posterior/es»[789].

Este criterio corrector tiene su origen en la Sentencia del Tribunal Supremo de Estados Unidos, dictada en el caso Bynum v. United States, de 7 de enero de 1960[790], y fue acogida por el TC con la STC 86/1995, de 6 de junio, en la que no obstante haberse llevado a cabo una intervención telefónica sin autorización judicial, uno de los investigados confesó los hechos, llegando el TC a la conclusión de que el reconocimiento de los hechos era una prueba jurídicamente independiente de la intervención ilícita, permitiendo su incorporación al acervo probatorio y su posterior valoración[791].

A la STC 86/1995, siguieron otras resoluciones con las que quedó definitivamente consolidada esta doctrina, respecto de la que puede afirmarse que constituye el primer antecedente de la teoría de la conexión de antijuridicidad[792]. Entre ellas, cabe mencionar la STC 54/1996, de 26 de marzo, FJ 9.º, en la que no obstante declarar contaminadas varias pruebas testificales por considerar que tenían relación directa con la prueba ilícitamente obtenida, no lo hizo así con una concreta prueba testifical y la declaración del acusado, las cuales declaró jurídicamente independientes de la prueba ilícita.

Del mismo modo, se ha consolidado la jurisprudencia del TS con numerosas sentencias en las que (si bien ha matizado que no hay que confundir «prueba diferente» —pero derivada—, con «prueba independiente» —sin conexión causal—, en el entendimiento de que estas últimas sí que pueden valorarse, mientras que las primeras, en la medida en que indirectamente incorporan el conocimiento obtenido a través de una vulneración constitucional, no pueden surtir efecto alguno en el proceso por expreso mandato legal), ha declarado que es indiscutible la incorporación válida al proceso y la

[789] ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», cit., p. 12.

[790] En este caso el TS de Estados Unidos, determinó que no obstante ser ilegal la prueba de la huella dactilar tomada al investigado, dado que esta procedía de un arresto ilegal, el uso por parte de la fiscalía, con fines de comparación, de una huella más antigua del mismo investigado obrante en los archivos de la Oficina Federal de Investigaciones, de ninguna manera relacionada con el arresto ilegal, determinó la correspondencia de esta última huella con la obtenida en la escena del crimen.

[791] Vid. STC 86/1995, de 6 de junio, FFJJ 3.º y 4.º

[792] Vid. SSTC 171/1999, de 27 de septiembre, FJ 4.º; 239/1999, de 20 de diciembre, FJ 9.º; 8/2000, de 17 de enero, FJ 2.º; y 138/2001, de 18 de junio, FJ 8.º

posibilidad de que sea enervada la presunción de inocencia, en relación con las fuentes de prueba incriminatorias, siempre que tuvieran una causa real diferente y totalmente ajena a la vulneración del derecho fundamental[793].

6.2. El descubrimiento inevitable

De acuerdo con esta doctrina, el efecto reflejo de la prueba ilícita queda anulado, cuando tras una previsión *ex ante* puede justificarse que, aun cuando la prueba ilícita inicialmente obtenida tenga conexión causal con el hallazgo de una determinada fuente de prueba incriminatoria, el descubrimiento se hubiera producido igualmente por el curso de los acontecimientos consecuencia de la investigación.

Este criterio corrector, tiene su origen en la Sentencia del Tribunal Supremo de los EEUU dictada en el caso Nix v. Williams, de 11 de junio de 1984, que resolvió un caso en el que, tras un interrogatorio ilegal, el investigado confesó el lugar donde había enterrado a la víctima, si bien el tribunal interpretó que tal emplazamiento habría sido descubierto indefectiblemente, habida cuenta de la búsqueda que estaba teniendo lugar en la misma zona por un numeroso grupo de voluntarios.

Al igual que con la excepción de la prueba jurídicamente independiente, analizada en el apartado anterior, la jurisprudencia admitió esta teoría del descubrimiento inevitable, un poco antes del establecimiento de la doctrina de la conexión de antijuridicidad. Concretamente fue la STS 974/1997, de 4 de julio, FJ 4.º, la que declaró que estaba acreditado, a través de la prueba testifical debidamente practicada en el acto del juicio oral, que la acusada era objeto de un proceso de vigilancia y seguimiento como consecuencia de informaciones referentes a su dedicación habitual a la transmisión y venta de heroína a terceros, proceso de vigilancia que habría conducido, en cualquier caso, a la reunión en una cafetería donde se realizaría la entrega, y señala que «inevitablemente y por métodos regulares, ya había cauces en marcha que habrían desembocado de todos modos en el descubrimiento…».

[793] Vid. SSTS, 550/2001, de 3 de abril, FJ 4.º; 1203/2002, de 18 de julio FFJJ 2.º y 3.º; y 498/2003, de 24 de abril, FJ 4.º; entre muchas otras. Estas son sentencias dictadas poco después de darse a conocer las doctrinas correctoras, si bien el TS sigue pronunciándose del mismo modo en sentencias más recientes, tal y como dijimos en el apartado anterior al referirnos a los criterios correctores a la expansión del efecto reflejo de la prueba ilícita. Allí mencionamos las SSTS 423/2019, de 19 de septiembre, FJ 3.º; 651/2018, de 14 de diciembre, FJ 2.º; 259/2018, de 30 de mayo, FJ 3.º; o 2/2018, de 9 de enero, FJ 6.º; entre otras.

Cabe señalar que la referida resolución declaró que «el descubrimiento inevitable» ha de ceñirse a los supuestos de actuaciones policiales realizadas de «buena fe», puntualizando que esta limitación se ha de establecer «para evitar que se propicien actuaciones que tiendan a "acelerar" por vías no constitucionales la obtención de pruebas que se obtendrían indefectiblemente por otras vías, pero más tardíamente». No obstante deja claro que en el caso enjuiciado la buena fe concurre, dado que se contaba con una autorización judicial aunque con una motivación insuficiente.

Posteriormente a la referida STS 974/1997, el TS ha reconocido la excepción del descubrimiento inevitable en numerosas sentencias[794].

El TC no se ha ocupado expresamente de la teoría del descubrimiento inevitable, habida cuenta de que poco después del reconocimiento de esta excepción por el TS, estableció en la STC 81/1998, de 2 de abril, la doctrina de la conexión de antijuridicidad, en la que admitió el descubrimiento inevitable como uno de los factores que podía dar lugar a la desconexión entre la prueba inicial y la prueba refleja[795].

6.3. El nexo causal atenuado

Ya hemos dicho que para que tenga lugar el efecto reflejo, ha de existir un nexo causal entre la prueba ilícita inicialmente obtenida y la fuente de prueba obtenida indirectamente. Una vez que nos encontramos ante dicha causalidad natural, la jurisprudencia ha negado el efecto reflejo de la nulidad de la prueba ilícita, en aquellos casos en los que tal nexo causal no opere con total intensidad.

Al igual que las excepciones de la fuente independiente y el descubrimiento inevitable, esta teoría tiene su origen en los Estados Unidos de América, concretamente en la Sentencia del Tribunal Supremo de dicho país dictada en el caso Wong Sun v. United States, de 14 de enero de 1963[796].

---

[794] Cabe mencionar las SSTS 69/2013, de 31 de enero, FJ 4.º; 912/2013, de 4 de diciembre, FJ 3.º; 963/2013, de 18 de diciembre, FJ 3.º; y más recientemente la 259/2018, de 30 de mayo, FJ 4.º

[795] En la STC 238/1999, de 20 de diciembre, el Ministerio Fiscal invocó la excepción del descubrimiento inevitable, aunque el TC declara que no existe ilicitud probatoria por existir una desconexión de antijuridicidad. Vid. antecedente de hecho 8.º y FFJJ 2.º a 4.º de dicha resolución.

[796] Esta sentencia del alto Tribunal norteamericano, resolvió un caso en el que se decretó la ilicitud de una entrada y registro en un domicilio, en la cual uno de los ocupantes acusó a una segunda persona, que tras declarar acusó a su vez a una tercera como responsable de un delito de tráfico de drogas. Esta tercera persona, una vez puesta en libertad tras su detención y transcurridos unos días, se personó voluntariamente

La excepción del nexo causal atenuado, como así ocurre en el precedente norteamericano que acabamos de mencionar, se produce especialmente en los supuestos en los que se produzca una confesión de los hechos, formulada voluntariamente por el investigado con posterioridad a la intervención ilícita. En relación con esta confesión la STC 161/1999, de 27 de septiembre, FJ 4.º, declaró que su validez «no puede hacerse depender de los motivos internos del confesante, sino de las condiciones externas y objetivas de su obtención»[797]. Por tanto, si la confesión es prestada con las debidas garantías procesales, encontrándose el encausado debidamente asistido de Letrado, siendo conocedor de la trascendencia de sus declaraciones en el sentido de que pueden constituir prueba de cargo y realizadas las declaraciones sin coacción de ningún tipo, puede afirmarse que la declaración ha sido espontánea y voluntaria y, por tanto, que se ha producido la ruptura del nexo causal o su atenuación.

MIRANDA ESTRAMPES afirma que «esta excepción es, en realidad, una variante de la excepción de la fuente independiente»[798]. Aun siendo ello cierto, estimamos que no hay que confundir ambos criterios correctores, dado que una fuente de prueba jurídicamente independiente se produce cuando se rompe el nexo causal, mientras que, como su propio nombre indica, la teoría del nexo causal atenuado supone la existencia de algún elemento que debilita la relación de causalidad de tal forma, que permite la valoración de la prueba.

Llegados a este punto, debe señalarse que el transcurso de un dilatado periodo de tiempo ha sido causa de desconexión entre la prueba directa e indirecta[799]. Por ello, el

---

en las dependencias policiales, confesando voluntariamente con previa información de sus derechos, por lo que el Tribunal estimó que esta confesión suponía una atenuación del nexo causal que permitía la valoración de esta confesión como prueba válida.

[797] La STC 161/1999 declaró asimismo que «de lo que se trata es de garantizar que una prueba como es la confesión, que por su propia naturaleza es independiente de cualquier otra circunstancia del proceso ya que su contenido es disponible por el acusado y depende únicamente de su voluntad, no responda a un acto de compulsión, inducción fraudulenta o intimidación. Estos riesgos concurren en mayor medida cuando el derecho fundamental cuya lesión se aduce es alguno de los que, al regular las condiciones en que la declaración debe ser prestada, constituyen garantías frente a la autoincriminación (declarar sin Letrado, en situación de privación de libertad, o sin previa advertencia de la posibilidad de callar), pero no es éste el supuesto que aquí abordamos».

[798] MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», cit., p. 146.

[799] La STC 66/2009, de 9 de marzo, declaró en su FJ 5.º que el largo periodo de tiempo transcurrido entre la producción procesal de las intervenciones telefónicas (prueba ilícita directa) y la entrada y registro (prueba derivada de la anterior), sus distintos elementos internos y sobre todo el cauce diverso

mayor o menor lapso temporal entre una y otra podrá determinar la ruptura del nexo causal o en su caso la atenuación del mismo.

Finalmente, a diferencia de la excepción de la prueba independiente la excepción del nexo causal atenuado se adopta por la jurisprudencia con posterioridad a la doctrina de la conexión de antijuridicidad. Puede destacarse, además de la STC 161/1999, de 27 de septiembre, anteriormente mencionada, la STC 239/1999, de 20 de diciembre, FJ 9.º, de acuerdo con la que «la voluntariedad de las declaraciones autoinculpatorias del demandante de amparo, efectuadas con todas las garantías, y su fundamento en hechos no contaminados por la ilicitud constitucional del registro domiciliario que está en el origen del proceso penal en cuestión, han roto la conexión antijurídica que pudiera vincularlas, más allá de lo puramente causal, al mencionado registro y a las pruebas que de él se derivaron, que hemos dicho resultan prohibidas».

También el TS pronto se ocupó de tratar esta excepción. Así, por todas, puede mencionarse la STS 431/2001, de 19 de marzo, FJ 3.º, que tras referirse al reconocimiento del acusado de la tenencia de la droga, declaró que tal declaración constituye «una actuación que hemos de considerar eficaz como prueba de cargo por hallarse jurídicamente desconectada de esas posibles vulneraciones constitucionales».

Por tanto, puede apreciarse en las referidas resoluciones que, a diferencia de la prueba jurídica independiente y la del descubrimiento inevitable, la teoría del nexo causal atenuado se adopta, más que como una excepción independiente al efecto reflejo de la prueba ilícita, como uno de los factores que permiten apreciar si existe o no conexión de antijuridicidad.

7. La conexión de antijuridicidad

Íntimamente relacionada con las correcciones al principio de la prueba prohibida o efecto reflejo de la prueba ilícita, examinadas anteriormente, con la STC 81/1998, de 2 de abril, se configuró en nuestro sistema una doctrina, denominada «la conexión de antijuridicidad» que vino a aunar con un planteamiento abstracto, no casuístico, todas

(documental) de acceso al proceso del sustrato material probatorio (datos sobre la ubicación del domicilio registrado, distinto de las intervenciones telefónicas), «nos llevan a concluir el carácter jurídicamente independiente de la entrada y registro». Y añadió que «otro tanto podemos afirmar, a la luz de nuestra doctrina, respecto de las declaraciones del recurrente en instrucción, de las declaraciones de los coacusados en el plenario, y de las testificales…».

aquellos criterios correctores, construyéndose así una teoría, absolutamente consolidada en nuestra jurisprudencia, aunque no exenta de durísimas críticas doctrinales, a las que más adelante nos referiremos.

Con esta teoría, que inicialmente tuvo como principal finalidad la limitación de la eficacia indirecta de las fuentes de prueba obtenidas ilícitamente, se parte del postulado en virtud del que, si una prueba tiene causa en una intervención llevada cabo con violación de derechos fundamentales, se pondrá en marcha el efecto reflejo de la prueba ilícita proclamado en el art. 11.1 LOPJ, no siendo posible, en consecuencia, la valoración de dicha fuente probatoria, debiendo ser excluida del proceso.

En consecuencia, dicho de otro modo, para que se produzca la eficacia refleja de la prueba vulneradora de derechos fundamentales, será necesaria la existencia de una relación o conexión causal-natural entre la prueba originaria ilícita y la prueba derivada, o, en sentido contrario, puede afirmarse que si no existe un nexo causal natural entre la fuente probatoria indirecta y la directa, aquella será considerada jurídicamente independiente y por ello válida para enervar la presunción de inocencia.

Ahora bien, en determinados supuestos no será suficiente con dicha conexión natural para que se produzca la eficacia refleja de la prueba ilícita, sino que, además, será necesaria, tal y como se expone en el FJ 4.º de la STC 81/1998, de 2 de abril, la existencia de «un nexo entre unas y otras que permita afirmar que la ilegitimidad constitucional de las primeras se extiende también a las segundas», nexo al que denomina «conexión de antijuridicidad».

Por tanto, de acuerdo con lo expuesto y con lo señalado por la STC 66/2009, de 9 de marzo, FJ 4.º, «la valoración en juicio de pruebas que pudieran estar conectadas con otras obtenidas con vulneración de derechos fundamentales sustantivos requiere un análisis a dos niveles: en primer lugar, ha de analizarse si existe o no conexión causal entre ambas pruebas, conexión que constituye el presupuesto para poder hablar de prueba derivada» y «solo si existiera dicha conexión procedería el análisis de la conexión de antijuridicidad»[800].

[800] La indicada STC 66/2009, de 9 de marzo, menciona a continuación una serie de supuestos, con cita de distintas sentencias donde estos han sido aplicados, en virtud de los que ha declarado tal desconexión de antijuridicidad, al señalar que «por otra parte hemos mantenido la desconexión de antijuridicidad, por gozar de independencia jurídica, en supuestos de declaración autoincriminatoria, no sólo de acusado en plenario (SSTC 136/2006, de 8 de mayo, FFJJ 6 y 7, y 49/2007, de 12 de marzo, FJ 2), sino incluso de

Para tratar de determinar si esa conexión de antijuridicidad existe o no, continúa la STC 81/1998, creadora de esta doctrina, ha de analizarse, «en primer término la índole y características de la vulneración del derecho al secreto de las comunicaciones materializadas en la prueba originaria, así como su resultado, con el fin de determinar si, desde un punto de vista interno, su inconstitucionalidad se transmite o no a la prueba obtenida por derivación de aquélla», pero además ha de considerarse «desde una perspectiva que pudiéramos denominar externa, las necesidades esenciales de tutela que la realidad y efectividad del derecho al secreto de las comunicaciones exige», señalando asimismo que «estas dos perspectivas son complementarias, pues sólo si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo cabrá entender que su efectiva apreciación es constitucionalmente legítima, al no incidir negativamente sobre ninguno de los aspectos que configuran el contenido del derecho fundamental sustantivo».

Por tanto, como aclara ARMENTA DEU, la aplicación de esta teoría se supedita al resultado de dos análisis que debe efectuar el órgano judicial caso a caso. Un análisis desde un punto de vista interno «que se encamina a dilucidar si la antijuridicidad de una prueba se transmite o no a las consiguientes [...] al margen de la relación de causalidad entre ambas». Y un análisis desde una perspectiva externa que «examinará la magnitud de la vulneración del derecho procesal de que se trata en cuanto a las "necesidades esenciales de tutela que la realidad y efectividad del mismo exigen"»[801].

Es decir, continúa explicando la referida autora, «con el primer análisis se acomete la relevancia, desde el punto de vista de la causalidad, entre la vulneración del derecho fundamental y los efectos que conlleva directa e indirectamente. A partir de ahí,

---

imputado en instrucción (SSTC 167/2002, de 18 de septiembre, FJ 8; 184/2003, de 23 de octubre, FJ 2), y entre la declaración de imputado y la entrada y registro (STC 136/2000, de 29 de mayo, FJ 8) "en atención a", y porque "la admisión voluntaria de los hechos no puede considerarse un aprovechamiento de la lesión del derecho fundamental" (SSTC 161/1999, de 27 de septiembre, FJ 4; 8/2000, de 17 de enero, FJ 3; 136/2000, de 29 de mayo, FJ 8). E igualmente hemos mantenido la posible independencia y validez de la diligencia de entrada y registro, y de las evidencias obtenidas en ella, respecto de las intervenciones telefónicas ilícitas si la misma se pudiere haber obtenido de un modo lícito por el órgano judicial, de haberse conocido por este la circunstancia de la lesividad de un derecho fundamental (STC 22/2003, de 10 de febrero, FFJJ 10 y 11, con cita en el FJ 10 de la STC 49/1999, de 5 de abril, FJ 5, o 171/1999, de 27 de septiembre, FJ 4), o "examinando la valoración individualizada de las pruebas efectuada por el Tribunal penal" para condenar (STC 87/2001, de 2 de abril, FJ 4)».

[801] ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», cit., p. 13.

el análisis externo atiende a la perspectiva del examen de las necesidades de tutela del propio derecho fundamental (secreto de las comunicaciones, inviolabilidad del domicilio, etc.) de manera que exceptuar la regla general de exclusión de las pruebas obtenidas a partir del conocimiento que tiene origen en otra contraria al derecho fundamental en cuestión, no signifique, en modo alguno, incentivar la comisión de infracciones del repetido derecho fundamental, privándole así de una garantía indispensable para su efectividad»[802].

Más recientemente, el TS ha declarado lo siguiente:

«En cuanto a la perspectiva interna, es fundamental ponderar la gravedad del menoscabo del derecho constitucional en liza y su ámbito de repercusión en el caso concreto con respecto a las pruebas reflejas. Ha de considerarse, en primer término, cuál de las garantías de la injerencia en el derecho al secreto de las comunicaciones telefónicas (presupuestos materiales, intervención y control judicial, proporcionalidad, expresión de todas y cada una de las exigencias constitucionales) ha sido efectivamente menoscabada y en qué forma (STC 81/1998).

En lo que atañe a la perspectiva externa, ha de atenderse a la necesidad de tutela del derecho fundamental menoscabado según las circunstancias del caso concreto, ponderando si la conducta de los órganos encargados de la investigación penal se hallaba encaminada a vulnerar el derecho al secreto de las comunicaciones u otro derecho fundamental. A tal efecto, se procurará constatar si se está ante una vulneración intencionada, gravemente negligente o simplemente errónea, datos indiciarios que se consideran especialmente significativos para sopesar las necesidad de activar el efecto disuasorio por estimarlo indispensable para tutelar de cara al futuro la eficacia del

[802] Señala asimismo ARMENTA DEU que «este análisis se reconduce, en definitiva, a la correcta aplicación de las garantías de la limitación del derecho fundamental. Si se considera que se vulneraron frontalmente tales garantías (ausencia de resolución judicial, resolución carente por completo de motivación, por ejemplo) deberá estimarse que la apreciación de la prueba basada indirectamente en fuente ilícitamente obtenida, contribuye a enervar la necesidad de tutela del derecho fundamental. Si, por el contrario, no existe tal vulneración, sino una simple irregularidad (ausencia en el auto que permite la intervención telefónica de datos objetivos, más allá de las simples sospechas, por ejemplo) la necesidad de tutela del derecho fundamental (en este caso, el secreto de las comunicaciones) se entenderá suficientemente satisfecha con la prohibición de valoración de la prueba originada directamente por la intervención, aquélla directamente constitutiva de la lesión, sin necesidad de extender la prohibición a las pruebas derivadas». Vid. ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», cit. pp. 13-14.

derecho fundamental menoscabado, a cuyo fin debe procederse a la anulación de las pruebas derivadas»[803].

Ciertamente la aplicación de esta doctrina no está exenta de complejidad, por lo que, a fin de ofrecer una explicación que facilite su comprensión, expondremos dos de los casos resueltos por el TC.

a) La STC 81/1998, de 2 de abril, que como hemos indicado anteriormente fue la precursora de esta teoría, resolvió un recurso de amparo en el que, como consecuencia de la intervención ilícita, se obtuvo un dato neutro como es el de que el entonces sospechoso «iba a efectuar una visita».

Con base en este dato, la sentencia entra a valorar en primer lugar la índole y características de la vulneración del derecho y su resultado, a fin de determinar si desde un punto de vista interno se ha transmitido la inconstitucionalidad de la prueba originaria a la derivada. Con ello, el TC plantea en primer lugar cuál de las garantías de la injerencia en el derecho al secreto de las comunicaciones telefónicas (presupuestos materiales, intervención y control judicial, proporcionalidad, expresión de todas y cada una de las exigencias constitucionales) ha resultado vulnerada, aclarando que, en este caso, la infracción constitucional radicaba en la falta de expresión parcial del presupuesto legitimador de la injerencia en el derecho fundamental.

De este modo, el TC, manteniendo el argumento establecido por el TS en la sentencia recurrida, declara que el conocimiento derivado de la injerencia en el derecho fundamental contraria a la Constitución no fue indispensable ni determinante por sí sólo de la ocupación de la droga o, lo que es lo mismo, que esa ocupación se hubiera obtenido, también, razonablemente, sin la vulneración del derecho.

Sin embargo, para que, definitivamente, la prueba derivada no tenga conexión antijurídica con la inicial, han de examinarse, desde un punto de vista externo, las necesidades de tutela del derecho vulnerado. En el caso concreto, el TC estima que no consta en los hechos probados que la actuación de los agentes se hallase encaminada a vulnerar el derecho fundamental, dado que la inconstitucionalidad de la intervención se produjo por falta de expresión de datos objetivos en la resolución judicial más allá de las simples sospechas. Por ello queda excluida tanto la intencionalidad como la negligencia

[803] Vid. STS 423/2019, de 19 de septiembre, FJ 3.º

grave, situándonos en el ámbito del error, frente al que las necesidades de disuasión no pueden reputarse indispensables desde la perspectiva de la tutela del derecho fundamental[804].

b) La STC 161/1999, de 27 de septiembre, FJ 4.º, en un asunto en el que finalmente se estimó que la confesión voluntaria del acusado daba lugar a la desconexión de antijuridicidad, anulando el efecto reflejo de la prueba contaminada y permitiendo en consecuencia la validez de la misma, declaró lo siguiente:

Por un lado que «la libre decisión del acusado de declarar sobre los hechos que se le imputan permite, desde una perspectiva interna, dar por rota, jurídicamente, cualquier conexión causal con el inicial acto ilícito».

Y, a su vez, desde una perspectiva externa, que «esta separación entre el acto ilícito y la voluntaria declaración por efecto de la libre decisión del acusado atenúa, hasta su desaparición, las necesidades de tutela del derecho fundamental material que justificarían su exclusión probatoria, ya que la admisión voluntaria de los hechos no puede ser considerada un aprovechamiento de la lesión del derecho fundamental».

Finalmente, cabe referirse a la STS 113/2014, de 17 de febrero, FJ 11.º, dado que realiza una declaración que contribuye a una mejor comprensión de esta teoría. Propone esta resolución que —teniendo en cuenta que el análisis de la excepcional concurrencia de un supuesto de desconexión exige un examen complejo y preciso de cada supuesto que va más allá de la mera relación de causalidad natural— en primer lugar se realice el análisis desde una perspectiva externa, partiendo del examen de las necesidades esenciales de tutela del derecho fundamental afectado.

Para llegar a esta conclusión aclara que «cuando la necesidad de tutela de un derecho fundamental es especialmente intensa, como sucede por ejemplo en los supuestos de tortura o en los de vulneración del derecho al secreto de las comunicaciones telefónicas sin ningún tipo de autorización judicial, excepcionar la regla general de exclusión de las pruebas obtenidas a partir del conocimiento que tiene su origen en la violación de dichos derechos puede incentivar la comisión de infracciones y privarles de una garantía indispensable para su efectividad». Por tal circunstancia estima

[804] Vid. FFJJ 5.º y 6.º de la STC 81/1998, de 2 de abril.

que, en estos supuestos, «no cabe admitir excepción alguna, y el examen debe concluir en esta perspectiva externa».

Y continúa señalando que «solo cuando nos encontramos ante una injerencia llevada a cabo con intervención judicial, pero con motivación insuficiente o con un vicio procedimental, puede pasarse al análisis interno de la eventual concurrencia de un supuesto de ruptura de la conexión de antijuridicidad, pues en estos supuestos el TC estima que la necesidad de tutela inherente al derecho fundamental puede quedar satisfecha con la prohibición de valoración de la prueba directamente constitutiva de la lesión, sin que resulte necesario extender ilimitadamente dicha prohibición a las pruebas derivadas».

8. A modo de conclusión: Críticas a la teoría de la conexión de antijuridicidad y toma de posición

La doctrina de la conexión de antijuridicidad ha sido objeto de muy duras críticas doctrinales. Así, por ejemplo, por citar algunas de ellas, LÓPEZ BARJA DE QUIROGA se refiere a la misma como «una doctrina trampa en la que se utilizan criterios ajenos a lo que se pretende resolver»[805], añadiendo que se trata de «un sistema de argumentar no fiable y escasamente convincente»[806]. Por su parte GARCÍA SAN MARTÍN califica la tarea de determinación de la conexión o desconexión de antijuridicidad como «fatigosa y ardua»[807], produciéndose con la misma una «desnaturalización del sistema de prueba ilícita y la inoperatividad de las garantías constitucionales»[808]. Finalmente ASENCIO MELLADO ha señalado que esta doctrina supone «una auténtica alteración del orden constitucional diseñado en nuestro texto legal superior»[809].

[805] LÓPEZ BARJA DE QUIROGA, J., «*Tratado de Derecho Procesal Penal*», cit., p. 937.

[806] LÓPEZ BARJA DE QUIROGA, J., «*Tratado de Derecho Procesal Penal*», cit., p. 937.

[807] GARCÍA SAN MARTÍN, J., «La prueba penal ilícita y la prueba penal refleja: Hacia una restrictiva aplicación de la doctrina de los frutos del árbol envenenado», cit., p. 6.

[808] GARCÍA SAN MARTÍN, J., «Consideraciones en torno 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», cit., p. 6.

[809] Afirma ASENCIO MELLADO que «La conocida teoría conocida como conexión de antijuridicidad, ideada por el TC para servir de cauce de valoración de los efectos de las pruebas obtenidas indirectamente de otras atentatorias a los derechos fundamentales, ha significado, por su falta de fundamento constitucional adecuado, por la combinación de elementos que comporta pertenecientes a diferentes modelos jurídicos y por el fin que con ella se pretendió, que no ha permanecido oculto, cual es el de minorar los efectos de los derechos fundamentales y su subordinación a los de seguridad, una auténtica alteración del orden constitucional diseñado en nuestro texto legal superior, interpretado por el mismo TC

También jurisprudencialmente, no obstante tratarse de doctrina consolidada del TC, han existido críticas a la misma. Así, por ejemplo, en la STS 1/2006, de 9 de enero, el voto particular emitido en la misma[810] declaró que «es claro que la llamada teoría de la conexión de antijuridicidad supone una reformulación del art. 11.1 LOPJ» y que por tanto, «la regla legal pasa a ser excepción jurisprudencial», lo cual «según los cánones ordinarios de interpretación es rigurosamente inaceptable», añadiendo asimismo que «no es posible operar en este terreno con una artificiosa distinción de dos planos y otros tantos cursos causales, el jurídico y el natural o real».

Sin embargo, en relación con los pronunciamientos jurisprudenciales contrarios y críticos con la conexión de antijuridicidad, existe jurisprudencia que, al admitir la conexión de antijuridicidad, también ha criticado las posturas contrarias a la misma. Así lo hace la STS 515/2015 de 21 de julio, FJ 13.º, cuando al proponer que era conveniente un análisis en primer lugar desde la perspectiva externa, para determinar el grado de vulneración alcanzado con la intervención ilícita, señala que «esta relevante aportación de nuestra doctrina constitucional ha sido ignorada, por lo general, en los análisis doctrinales referidos a esta materia, que suelen realizar un análisis crítico muy superficial de la doctrina de la conexión de antijuridicidad, y postular planteamientos maximalistas, que no son aplicados en ninguno de los países de nuestro entorno y que, por lo general, prescinden o desconocen el matiz diferencial introducido por la doctrina de la conexión de antijuridicidad en relación a los supuestos en que no cabe admitir excepción alguna, y el examen debe concluir en la perspectiva externa».

Nos encontramos ante una discusión que, no obstante el carácter provechoso y constructivo del debate jurídico, se encuentra en un punto donde probablemente no se pueden predicar estas cualidades de aquellas posturas tan extremadamente controvertidas. Se hace necesaria, en nuestra opinión, la búsqueda de una solución ecléctica, que consideramos ha sido bien conseguida con la teoría de la conexión de antijuridicidad, aunque no por ello debamos dejar de decir que sería necesaria una simplificación de la misma, habida cuenta de su complejidad.

---

de manera acertada hasta la STC 81/1998, de 2 de abril y la relegación del art. 11.1 LOPJ a norma meramente formal, ya que no sólo ha perdido su plena eficacia con esta creación jurisprudencial, sino que, derechamente, se actúa de forma contraria a sus disposiciones». Vid. ASENCIO MELLADO, J. M., «Prueba ilícita: Declaración y efectos», cit., p. 47.

[810] Voto particular del magistrado D. Perfecto Andrés Ibáñez.

Una opinión de este tipo fue puesta de manifiesto por DE URBANO CASTRILLO, con anterioridad al establecimiento de la meritada doctrina, al señalar que, teniendo en cuenta los intereses plurales que laten en la decisión de admitir o no un material probatorio, esto es, la elección entre los derechos del ciudadano o los intereses de la sociedad en la persecución y castigo del culpable, «las posturas absolutas y maximalistas en este tema se han ido decantando hacia posiciones más matizadas y más casuísticas tratando de hallar un equilibrio entre la disyuntiva apuntada que, como acabamos de ver no es sino las dos caras de una misma cuestión: el derecho y ejercicio de la tutela judicial efectiva dentro de un Estado de Derecho»[811].

En nuestra opinión, partiendo en todo caso del máximo respeto a nuestro sistema de derechos fundamentales y su posición de preeminencia dentro del ordenamiento jurídico, consideramos oportuno realizar una reflexión valorando posiciones situadas en extremos opuestos. Surge así la pregunta acerca de la posibilidad de conseguir una solución justa situada en una posición intermedia, a partir de la quepa realizar un juicio de valor acerca de si una prueba indirecta violenta inexorablemente un derecho fundamental y por tanto ha de ser excluida del acervo probatorio, o si por el contrario existen otros factores distintos, en virtud de los que, con independencia de la prueba ilícita directa, se hubiera, igualmente, obtenido aquella.

Creemos que esta solución ha sido conseguida con la teoría de la conexión de antijuridicidad, por más que se tache a la misma de irrespetuosa con los derechos fundamentales, y, por tanto, consideramos que debe ser aceptada. Ello no obsta a que, como decíamos, la misma pueda ser simplificada, tarea que, llegados a este punto, indudablemente corresponde al legislador.

No debe olvidarse que la justicia se constituye en unos de los valores superiores de nuestro ordenamiento jurídico (art. 1.1 CE), así como que los derechos fundamentales no están exentos de los límites que encuentran en otros derechos fundamentales, teniendo en cuenta, además, que, tal y como fue señalado por la STC 114/1984, no existe un derecho fundamental autónomo a la no recepción jurisdiccional de las pruebas de posible origen antijurídico. En este sentido, se declara en la citada resolución que «la imposibilidad de estimación procesal puede existir en algunos casos, pero no en virtud de un derecho fundamental que pueda considerarse originariamente

[811] DE URBANO CASTRILLO, E., «Prueba ilícita en particular», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, p. 238.

afectado, sino como expresión de una garantía objetiva e implícita en el sistema de los derechos fundamentales […] conviene por ello dejar claro que la hipotética recepción de una prueba antijurídicamente lograda, no implica necesariamente la lesión de un derecho fundamental»[812].

El art. 11.1 LOPJ prohíbe que surtan efecto las pruebas obtenidas «indirectamente» violentando los derechos o libertades fundamentales, pero, ¿cuándo ha de entenderse que se ha producido tal vulneración de modo indirecto? A nuestro modo de ver, necesariamente, cuando no existiera otra posibilidad de obtención de la denominada prueba indirecta. Con los supuestos de desconexión que se utilizan por la jurisprudencia, en muchos casos la prueba indirecta se hubiera obtenido de otro modo y, por ello —sin perjuicio del análisis de cada caso concreto—, desde un punto de vista externo la necesidad de tutela del derecho infringido no exigirá el rechazo de la prueba derivada y, con ello, desde una perspectiva interna, la antijuridicidad no se transmitirá a la misma.

Con base en ello, si tomamos en consideración tres factores como son: a) uno de los criterios de desconexión, por ejemplo el «descubrimiento inevitable»; b) el valor «Justicia» consagrado en el art. 1.1 CE, y c) que no existe un derecho autónomo a la no recepción jurisdiccional de las pruebas de posible origen antijurídico; y, en atención a los mismos, se realiza una reflexión sobre las consecuencias de que en el enjuiciamiento de un delito grave, quedase acreditado que incluso cuando se hubiera descubierto el cuerpo del delito como consecuencia de una información que pudiera entenderse derivada de una intervención ilícita, tal descubrimiento se hubiera producido de forma segura e inevitable por otras circunstancias, y aun así los delincuentes quedaran absueltos, definitivamente el valor «Justicia» quedaría gravemente dañado.

Entendemos, en consecuencia, que algunas de las durísimas críticas realizadas en contra de esta doctrina son totalmente injustas, estimando, por el contrario, que aun cuando pueda resultar necesaria una simplificación de la misma, debe ser aplaudido el esfuerzo que la jurisprudencia, tanto del TC como del TS, ha llevado a cabo para conseguir resoluciones más justas, que de ningún modo pueden ser juzgadas como contrarias a nuestra legalidad, sin perjuicio de que deba llevarse a cabo una regulación

[812] Vid. STC 114/1984, de 29 de noviembre, FJ 2.º

que fortalezca en este punto el principio constitucional de seguridad jurídica (art. 9.3 CE).

No podría ceder la vulneración de los derechos fundamentales a favor del valor «Justicia», consagrado, no olvidemos, como «superior en nuestro ordenamiento jurídico», en aquellos casos de flagrantes injerencias indebidas en los derechos fundamentales, ya fuesen de forma directa o indirecta (sin posibilidad de desconexión por ninguna excepción), como así podría ocurrir en un supuesto de tortura, violación domiciliaria sin justa causa o autorización judicial o vulneración del derecho al secreto de las comunicaciones telefónicas sin ningún tipo de autorización judicial. En estos casos la justicia se encontraría ínsita en el propio derecho sin que pudiera segregarse del mismo, pero no así, cuando una de las excepciones que ya han sido mencionadas, atenuase o incluso vaciase la necesidad de tutela del derecho fundamental.

Opina del mismo modo RIVES SEVA, cuando tras señalar que «está doctrinalmente aceptado que el artículo 11.1 de la LOPJ consagra, en el plano de la legalidad ordinaria, una garantía que es implicación necesaria del contenido del artículo 24.2 de la Constitución: el derecho del presunto inocente a no ser condenado si no es en virtud de prueba válidamente obtenida»[813], afirma que «no podemos detenernos ahí, pues la Constitución proporciona otro elemento interpretativo de mayor relevancia, el valor Justicia proclamado en su artículo primero, que lleva a considerar legítimas desde la perspectiva constitucional las excepciones reconocidas en la jurisprudencia: la doctrina del hallazgo inevitable, o la conexión de antijuridicidad; que autorizan en algunos casos, el aprovechamiento de la noticia proporcionada por la prueba ilícita, limitando las consecuencias extremas de aquella rígida y literal interpretación del artículo 11.1 de la Ley Orgánica, que ha conducido en muchos casos a absoluciones que no se avienen con la razón, con el interés social y la Justicia»[814].

Acaso sea relevante, poner de manifiesto la STEDH dictada en el caso Schenk v. Switzerland, de 12 de julio de 1988, que en su apdo. 46 declaró que «aunque el Convenio garantiza en su artículo 6 el derecho a un proceso justo, no regula por ello la admisibilidad de las pruebas como tal, materia que, por tanto, corresponde ante todo al Derecho interno» y añadió que «el Tribunal no puede, por consiguiente, excluir en principio y en abstracto que se admita una prueba conseguida ilegalmente, como la de

[813] RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., p. 38.
[814] RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., p. 38-39.

que se trata. Sólo le corresponde averiguar si el proceso del señor Schenk, considerado en su conjunto, fue un proceso justo».

Llegados a un punto como este, en el que se trata de conseguir una solución equilibrada ante un problema tan controvertido, se hace necesario un breve estudio del Derecho comparado.

a) Portugal lleva a cabo una regulación con rango constitucional al incorporar en el art. 32.6 de su Constitución la regla de exclusión de la prueba ilícita, disponiendo que «serán nulas todas las pruebas obtenidas mediante tortura, coacción, atentado a la integridad física o moral de la persona o intromisión abusiva en la vida privada, en el domicilio, en la correspondencia o en las telecomunicaciones», sin referirse al efecto indirecto o *efeito-a-distancia*, el cual, según señala la STS 811/2012, de 30 de octubre, FJ 10.º, se encuentra matizado por la singularidad del caso, el tipo de prohibición de prueba vulnerado, la naturaleza e importancia del derecho en conflicto, el bien jurídico o interés sacrificado o el sujeto pasivo de la vulneración[815].

b) En Italia, el art. 191.1 del «Códice di Procedura Penale de 1988» dispone que «las pruebas adquiridas con violación de prohibiciones establecidas por las leyes no pueden ser utilizadas», sin que tampoco se efectúe ninguna mención al efecto reflejo, señalando la referida STS 811/2012 que en la jurisprudencia de este país se dan soluciones muy variadas como consecuencia de la ausencia normativa específica sobre propagación de la nulidad.

c) Por lo que respecta a Francia, su práctica procesal sigue «el principio de lealtad en la aportación de la prueba», señalando RIVES SEVA que, «a tenor del art. 172.2 del Código de Procedimiento Penal, el Tribunal decide si la anulación de actos lesivos de determinados principios fundamentales o del derecho de defensa, se limita al acto viciado, se extiende a todo o parte del procedimiento ulterior; entendiendo la doctrina que la exclusión no afecta a las pruebas descubiertas merced a la fuente espuria»[816].

d) En cuanto a Alemania, se aplica la «teoría de la ponderación de intereses», por la que la vulneración de una prohibición probatoria no conlleva necesariamente la

[815] Comienza declarando el FJ 10.º de la STS 811/2012, de 30 de octubre, que «es fácil constatar que en los países de nuestro entorno la eficacia indirecta de la prueba ilícita no se aplica de forma absoluta o ilimitada, sino en una forma matizada muy próxima a la doctrina de nuestro Tribunal Constitucional».
[816] RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., p. 40.

prohibición de utilización de la prueba derivada, en función de la gravedad del hecho y el peso de la infracción procesal concreta.

e) En Holanda, la ilicitud probatoria se establece en el art. 359 del Código de Procedimiento Procesal, de acuerdo con el que la calificación de una prueba como derivada de otra prueba ilícita no acarrea necesariamente la aplicación de una regla de exclusión, aplicándose los principios de proporcionalidad y subsidiariedad.

f) En Estados Unidos de América, señala la STS 811/2012 que, aun siendo este país pionero en la teoría de los frutos del árbol envenenado, es indudable que resoluciones como la de los casos Michigan v. DeFillippo[817] o Herring v. United States[818], han atenuado mucho los efectos de la *exclusionary rule*.

g) En cuanto a Canadá, el art. 24.2 de su Constitución de 1982 dispone que «cuando un Tribunal llegue a la conclusión de que una prueba fue obtenida de manera que infrinja o niegue derechos o libertades garantizados por esta Carta, la prueba será excluida si se establece que, teniendo en cuenta todas las circunstancias, su admisión en el procedimiento produciría un desprestigio a la Administración de Justicia». Por lo que se refiere a la valoración de tal desprestigio, FERNÁNDEZ ENTRALGO se refiere una sentencia de dicho país, en la que se consideró que «la pérdida de prestigio se produciría "…por la convalidación de conductas inaceptables de las instancias investigadora y

[817] En la Sentencia del Tribunal Supremo de los Estados Unidos de América, dictada en el caso Michigan v. DeFillippo, de 25 de junio de 1979, se resolvió un caso en el que un ciudadano fue arrestado por violación de una ordenanza de Detroit, en virtud de la que un oficial de policía puede detener e interrogar a un individuo si tiene una causa razonable para creer que el comportamiento del individuo justifica una mayor investigación. Como consecuencia de dicho arresto siguió un registro en el que se comprobó que portaba drogas, por lo que fue procesado por tráfico de estupefacientes. El Tribunal de Apelación de Michigan sostuvo que la ordenanza de Detroit era contraria a la Constitución por su vaguedad, y por ello tanto el arresto como el registro no eran válidos. Sin embargo, el Tribunal Supremo estimó finalmente que el arresto del demandado era válido, dado que había sido realizado de buena fe al no ser inconstitucional la ordenanza de Detroit en aquel momento, con independencia de la determinación posterior de su inconstitucionalidad. Por ello, la prueba del hallazgo de las drogas no debería haber sido suprimida.

[818] En la Sentencia dictada en el caso Herring v. United States, de 14 de enero de 2009, se dirimió un caso en el que se llevó a efecto un registro en virtud de una orden de un condado vecino, la cual se comprobó posteriormente que había sido retirada. Como consecuencia del registro fueron halladas armas y drogas, por lo que por el investigado se invocó la violación de la Cuarta Enmienda. Sin embargo, el Tribunal Supremo estimó que cuando los errores policiales que conducen a una búsqueda ilegal son el resultado de una negligencia aislada atenuada de la búsqueda en lugar del error sistémico o el desprecio imprudente de los requisitos constitucionales, la regla de exclusión no se aplica. Por tanto, consideró válido el registro.

acusadora...", proponiendo la adopción de un punto de vista de una persona razonable, a la hora de hacer una valoración más ética que pragmática»[819].

h) En el Reino Unido, la *Police and Criminal Evidence Act* de 1984 establece que «el Tribunal podrá rechazar una prueba de cargo cuando teniendo en cuenta todas las circunstancias, incluidas aquellas en que fue obtenida, su admisión produciría un efecto tan negativo sobre la limpieza del procedimiento, que el Tribunal no debería admitirla». Destaca RIVES SEVA, que «en este país la Corte de apelación ha tenido especial cuidado en no proporcionar guía alguna sobre como ejercitar el poder de inadmisión conferido a los Tribunales»[820].

i) Finalmente, en Australia, la jurisprudencia dominante, conforme ha puesto de manifiesto FERNÁNDEZ ENTRALGO, tiene declarado que «hay que valorar equilibradamente los intereses de la sociedad en la aprehensión de los culpables y en su persecución y condena, por una parte, y, por otra, el repudio de cualquier conducta o subterfugio procesal que sean contrarios al juego limpio (*unfair*) o ilegales en el sentido de llevar consigo una naturaleza tal que ofenda los conceptos que importan a la decencia democrática (*relevant concepts of democratic decency*)...»[821].

Con base en el resumen realizado, acerca de los efectos indirectos de la prueba ilícita en otros sistemas procesales, concluye la STS 811/2012, de 30 de octubre, FJ 10.º, que «la aplicación absolutamente ilimitada de la regla de la contaminación de los frutos del árbol prohibido carece en el sistema procesal penal actual de referentes en el Derecho Comparado, por lo que la aplicación de la doctrina matizada del Tribunal Constitucional a través de la teoría de la conexión de antijuridicidad resulta lo más coherente con el modelo procesal penal vigente en los países de nuestro entorno».

Resulta notorio que nos encontramos ante una aseveración totalmente cierta, dado que, como puede apreciarse, en ninguno de los estados que hemos mencionado se aplica de forma estricta la teoría de los frutos del árbol envenenado. Asimismo, no podría afirmarse que alguno de los países citados no posea un sistema democrático consolidado y respetuoso con los derechos fundamentales. Y, finalmente, de forma

[819] FERNÁNDEZ ENTRALGO, J., «Las reglas del juego. Prohibido hacer trampas: la prueba ilegítimamente obtenida», cit., pp. 68-69.
[820] RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., p. 41.
[821] FERNÁNDEZ ENTRALGO, J., «Las reglas del juego. Prohibido hacer trampas: la prueba ilegítimamente obtenida», cit., p. 68.

definitiva, no podemos admitir que la doctrina de la conexión de antijuridicidad sea irrespetuosa con los derechos fundamentales, sino que, muy al contrario, con ella y con el esfuerzo realizado, se ha conseguido, de una forma que estimamos correcta, la conciliación entre aquella pugna entre la búsqueda material de la verdad y la defensa de los derechos fundamentales de los ciudadanos, así como una adecuada armonización del valor superior de nuestro ordenamiento jurídico denominado «Justicia» y el derecho fundamental a un proceso con todas las garantías.

Consideramos por ello, como ya hemos venido adelantando, totalmente injustificadas las severas críticas realizadas contra la teoría de la conexión de antijuridicidad. Ahora bien, no por ello hemos de admitir la inactividad del legislador, manteniendo esta compleja amalgama de opiniones y, con ello, un inflexible debate que, podemos afirmar, ha girado en torno a un solo vocablo, como es el adverbio «indirectamente» que, a todas luces, se ha mostrado insuficiente y necesitado de desarrollo.

A este respecto, apunta GONZÁLEZ-MONTES SÁNCHEZ que «no sería descabellado, o bien ir pensando en una posible reforma, o bien pedir el esfuerzo del TC para establecer un catálogo de excepciones, en la medida de lo posible cerrado (aunque ciertamente los supuestos reales puedan superar la norma), que venga a conjugar y equilibrar los dos posibles extremos: de una parte, el respeto a los derechos fundamentales en sus dos vertientes, y de otra el fin del proceso y, en especial, del proceso penal donde los intereses que se tutelan son de naturaleza pública y donde, por ese motivo, pueden caber excepciones a la intangibilidad de aquellos derechos»[822].

Nos quedamos, sin duda, con la primera opción, dado que, por un lado, el catálogo cerrado de excepciones puede considerarse conseguido con la copiosa jurisprudencia del TC y del TS, mientras que, por otro, consideramos que a estas alturas es necesaria y urgente la regulación de la materia.

Algunos autores han propuesto que el artículo 11.1 LOPJ sencillamente debería disponer «no surtirán efecto las pruebas obtenidas violentando los derechos o libertades fundamentales»[823]. Sin embargo, consideramos que sería preferible mantener el referido precepto con su redacción actual, aunque procediendo de forma urgente al desarrollo del

[822] GONZÁLEZ-MONTES SÁNCHEZ, J. L., «La prueba ilícita», *Persona y Derecho*, n.º 54, 2006, p. 378.
[823] Vid. RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», cit., p. 41.

mismo, mediante el tratamiento procesal de la prueba ilícita y prueba prohibida en la LECrim.

Un correcto desarrollo del art. 11.1 LOPJ, y su consecuente tratamiento procesal, se consiguió en el Anteproyecto de LECrim de 2013, en el que se llevó a cabo una regulación que nos merece una opinión muy favorable[824].

Con ella, se ofrece una solución que se aproxima a la doctrina de la conexión de antijuridicidad, ya que con excepción de aquellas pruebas obtenidas como consecuencia de un acto de tortura[825], recoge dos excepciones fundamentales al efecto reflejo de la prueba ilícita, como son la del descubrimiento inevitable y de la confesión incriminatoria por parte del encausado.

---

[824] Concretamente el artículo 13 del Anteproyecto de LECrim de 2013, bajo la rúbrica «exclusión de la prueba prohibida», dispuso lo siguiente:
«1. No surtirán efecto en el proceso las informaciones o fuentes de prueba obtenidas, directa o indirectamente, con vulneración de derechos fundamentales o las pruebas en cuya práctica se lesionen los mismos. Tales pruebas serán de valoración prohibida.
2. Como excepción a la disposición establecida en el apartado anterior, podrán ser utilizadas y valoradas las pruebas que, sin estar conectadas con un acto de tortura, sean:
a) favorables al encausado; o
b) consecuencia indirecta de la vulneración de un derecho fundamental si, con independencia de la existencia del nexo causal entre la infracción del derecho fundamental y la fuente de prueba, en atención a las concretas circunstancias del caso, se llega a la certeza de que, conforme al curso ordinario de la investigación, la fuente de prueba hubiera sido descubierta en todo caso; o
c) consecuencia de la vulneración de un derecho fundamental exclusivamente atribuible a un particular que haya actuado sin ánimo de obtener pruebas.
3. La declaración autoincriminatoria del encausado, prestada en el plenario en términos que permitan afirmar su voluntariedad, se entenderá desconectada causalmente de la prueba declarada nula.
4. En cualquier momento en que se constate la existencia de la infracción del derecho fundamental afectado las informaciones o fuentes de prueba o resultados de las pruebas han de ser excluidos del proceso, sin perjuicio de que, rechazada la exclusión, las partes puedan reproducir con posterioridad la petición de declaración de nulidad de la prueba».

[825] La STC 97/2019, de 16 de julio, ha declarado en su FJ 2.º que «en los casos en los que existe una prohibición constitucional singular como es la de la tortura o tratos inhumanos o degradantes, supuesto en el cual, aun cuando la vulneración del art. 15 CE carezca de relación de medio fin con el proceso, no puede admitirse la recepción probatoria de los materiales resultantes». Y ha puesto de manifiesto igualmente que «como ha señalado el TEDH, los elementos de cargo (ya sean confesiones o pruebas materiales) obtenidos por medio de actos de violencia o brutalidad u otras formas de trato que puedan calificarse como actos de tortura, no deben nunca servir para probar la culpabilidad de la víctima (STEDH de 11 de julio de 2006, asunto Jalloh c. Alemania, § 99, y, en el mismo sentido, SSTEDH de 17 de octubre de 2006, asunto Göcmen c. Turquía, § 74 y de 28 de junio de 2007, asunto Harutyunyan c. Armenia, § 63).

De este modo, con una regulación de este tipo se contribuye, no solo al fortalecimiento de la seguridad jurídica, sino a una mejora en el funcionamiento de la Administración de Justicia.

IV. La cadena de custodia

1. Concepto

En el proceso penal, lo normal es que entre la recogida de los vestigios o fuentes de prueba y el momento de la celebración del juicio oral transcurra un amplio lapso de tiempo, en el que han de adoptarse las medidas de aseguramiento oportunas para garantizar que el material ocupado no sufra ninguna alteración o manipulación que pueda impedir su plena eficacia probatoria en el momento procesal oportuno.

A este proceso de aprehensión, custodia, y, en su caso, análisis pericial, llevado a cabo con la finalidad de obtener aquella virtualidad probatoria, se le denomina «cadena de custodia». Designa (y de ahí su denominación de «cadena») «una sucesión de fases procedimentales que deben estar interconexionadas entre sí»[826], siendo esencial «la necesaria concatenación de actuaciones, de tal modo que cada una de ellas arranca de la precedente y concluye en la siguiente, sin que pueda interrumpirse, por motivo alguno, esa vinculación interna»[827].

En este sentido, la STS 167/2020, de 19 de mayo, ha declarado en su FJ 7.º, que «la integridad de la cadena de custodia garantiza que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del Tribunal no sufre alteración alguna», por lo que «la regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza o elemento de convicción intervenido; se asegura de esa forma que lo que se analiza es justamente lo ocupado y que no ha sufrido alteración alguna».

[826] MESTRE DELGADO, E., «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, p. 69.
[827] MESTRE DELGADO, E., «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», cit., p. 69.

Nos encontramos ante un concepto que no se encuentra regulado legalmente, sino que ha sido la jurisprudencia la encargada de desarrollar los aspectos de esta institución, tanto desde un punto de vista conceptual como procedimental, así como las consecuencias de su incumplimiento.

El TS, en diversas resoluciones, ha definido la cadena de custodia como «el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba»[828].

También doctrinalmente se han ofrecido numerosas definiciones. Así, por ejemplo, FIGUEROA NAVARRO afirma que la cadena de custodia, a la que se la podría llamar «hoja de ruta de la prueba», puede ser definida como «un procedimiento, oportunamente documentado, que permite constatar la identidad, integridad y autenticidad de los vestigios o indicios delictivos, desde que son encontrados hasta que se aportan al proceso como pruebas»[829]. RICHARD GONZÁLEZ la define como «el conjunto de actos que tienen por objeto la recogida, el traslado y la custodia de las evidencias obtenidas en el curso de una investigación criminal que tienen por finalidad garantizar la autenticidad, inalterabilidad e indemnidad de la prueba»[830]. Finalmente, GUTIÉRREZ SANZ elabora el concepto de cadena de custodia desde una doble perspectiva[831]: a) Por un lado, como el conjunto de prácticas de carácter material que tienen como finalidad recoger vestigios o efectos materiales dejados en el lugar del delito, custodiarlos, analizarlos y garantizar su mismidad; b) y, por otro, como instrumento procesal imprescindible para otorgar verosimilitud a la prueba pericial y por tanto determinante en su valoración.

---

[828] Vid. SSTS 208/2014, de 10 de marzo, FJ 1.º; 147/2015, de 17 de marzo, FJ 1.º; 775/2015, de 3 de diciembre, FJ 2.º; y 157/2016, de 26 de febrero, FJ 1.º

[829] FIGUEROA NAVARRO, C., «El aseguramiento de las pruebas y la cadena de custodia», *La Ley Penal - Sección Estudios*, n.º 84, 2011, p. 4.

[830] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», *Diario La Ley - Sección Tribuna*, n.º 8187, 2013, p. 4.

[831] GUTIÉRREZ SANZ, M. R., *La cadena de custodia en el proceso penal español*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, p. 25.

2. Regulación

Como acabamos de decir, la cadena de custodia no se encuentra regulada legalmente de forma sistemática, aunque existen determinados artículos en la LECrim que hacen referencia a la misma. Se trata de las normas dedicadas a la aprehensión o incautación del cuerpo del delito, en el capítulo II del título V del libro II, en las que se ordena que con la recogida de los efectos se garantice la integridad de los mismos.

El primero de los preceptos de este capítulo, el art. 334 LECrim, establece que «el juez instructor ordenará recoger en los primeros momentos las armas, instrumentos o efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida», y añade que, «el Secretario judicial[832] extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren, describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo».

En coherencia con lo anterior, el art. 282 LECrim atribuye a la Policía Judicial, entre otras funciones, la de «recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial».

El art. 338 LECrim dispone que, «sin perjuicio de lo establecido en el capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el juez acordará su retención, conservación o envío al organismo adecuado para su depósito».

Además de estas reglas, existen otras que, de forma aislada, también se ocupan del aseguramiento de efectos, como así ocurre con la recogida de libros y papeles, respecto de la que el art. 574 LECrim, tras disponer que el juez ordenará recoger los libros y papeles que resulten necesarios para el sumario, establece que serán foliados, sellados y rubricados en todas sus hojas por el letrado de la Administración de Justicia.

---

[832] De conformidad con la Disposición Adicional Primera de la LO 7/2015, de 21 de julio, por la que se modifica la LO 6/1985, de 1 de julio, del Poder Judicial, a partir de su entrada en vigor, todas las referencias que se contengan en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, así como en otras normas jurídicas, a secretarios judiciales o secretarios sustitutos profesionales, deberán entenderse hechas, respectivamente, a letrados de la Administración de Justicia y letrados de la Administración de Justicia suplentes.

En el ámbito del procedimiento abreviado, el art. 770.3ª LECrim atribuye a la Policía Judicial la función de custodiar en todo caso los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, para ponerlos a disposición de la autoridad judicial, mientras que, de conformidad con el art. 778.3 LECrim, el juez podrá acordar, cuando lo considere necesario, que por el médico forense u otro perito se proceda a la obtención de muestras o vestigios, cuyo análisis pudiera facilitar a mejor calificación del hecho, acreditándose en las diligencias su remisión al laboratorio correspondiente.

Finalmente, el art. 796.1.7.ª realiza la única alusión en la LECrim al término «cadena de custodia» al disponer, en referencia a la práctica de pruebas para detectar la presencia de drogas tóxicas, estupefacientes y sustancias psicotrópicas en los conductores de vehículos a motor y ciclomotores, que la saliva que se facilite por el conductor, será analizada en laboratorios homologados, garantizándose la cadena de custodia.

A nivel reglamentario, la Orden JUS/1291/2010, de 13 de mayo, por la que se aprueban las normas para la preparación y remisión de muestras objeto de análisis por el Instituto Nacional de Toxicología y Ciencias Forenses, establece formularios para la remisión de muestras que presenten con claridad todos los datos necesarios para identificar, de forma inequívoca, los paquetes y las muestras, encauzar correctamente los análisis, asegurar el mantenimiento de la cadena de custodia, así como facilitar el control de las muestras y la devolución o destrucción cuando finalice el procedimiento correspondiente.

Ha de tenerse en cuenta, asimismo, el Acuerdo marco de colaboración entre el CGPJ, la Fiscalía General del Estado, el Ministerio de Justicia, el Ministerio de Hacienda y Administraciones públicas, el Ministerio del Interior, y la Agencia Española de Medicamentos y Productos Sanitarios, de 3 de octubre de 2012, que establece el protocolo a seguir en la aprehensión, análisis, custodia y destrucción de drogas tóxicas, estupefacientes o sustancias psicotrópicas, en el que, de acuerdo con su exposición de motivos, se establecen reglas para que, a fin de evitar riesgos para la salud pública, se proceda a la pronta destrucción de las drogas tóxicas intervenidas cuando no sea necesaria su conservación, así como para garantizar la cadena de custodia, fijándose

unas pautas de actuación con el fin de solucionar la disparidad de criterios existente en la materia[833].

Finalmente, en materia de incautación de drogas tóxicas, ha de tenerse igualmente en consideración la Recomendación del Consejo de la Unión Europea de 30 de marzo de 2004, sobre directrices para la toma de muestras de drogas incautadas (2004/C 86/04), que, en su octavo «considerando», señala como una de las finalidades de la recomendación, el establecimiento de unas directrices para preservar la cadena de custodia de las muestras enviadas, para incorporar, en la medida de lo posible, su admisibilidad como pruebas en acciones judiciales por delitos relacionados con la droga[834].

---

[833] Se puede acceder al citado Convenio en la web del CGPJ http://www.poderjudicial.es/cgpj/es/Temas/Relaciones_institucionales/Convenios/Acuerdo_Marco_de_colaboracion_entre_el_Consejo_General_del_Poder_Judicial__la_Fiscalia_General_del_Estado__el_Ministerio_de_Justicia__el_Ministerio_de_Hacienda_y_Administraciones_Publicas__el_Ministerio_de_Interior__y_la_Agencia_Estatal__Agencia_Espanola_de_Medicamentos_y_productos_Sanitarios__por_el_que_se_establece_el_Protocolo_a_seguir_en_la_aprehension__analisis__custodia_y_destruccion_de_drogas_toxicas__estupefacientes_o_sustancias_psicotropicas. Consultado el 22 de junio de 2020.

[834] Además de las mencionadas, las demás normas vigentes que regulan algún aspecto relativo a la cadena de custodia, son las siguientes:

- La Ley 17/1967, de 8 de abril, sobre Estupefacientes. De acuerdo con su art. 21 la posesión de sustancias estupefacientes, incluso por el propio Servicio de Control de Estupefacientes, implica la obligación de la más rigurosa custodia, de modo que se evite cualquier posibilidad de sustracción y de dedicación a usos indebidos. En el artículo 31 se establece que las sustancias estupefacientes decomisadas a los delincuentes e infractores de contrabando serán entregadas al Servicio de Control de Estupefacientes.
- El Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas, en el que en diversos preceptos se hace mención a la custodia de las armas que sean intervenidas. En los apartados 1 y 4 de su art. 166 dispone respectivamente que «toda autoridad o agente de la misma que, en uso de sus facultades, decomise o intervenga armas de fuego, deberá dar cuenta a la Guardia Civil, depositándolas en la Intervención de Armas correspondiente» y «…si los Juzgados y Tribunales estimasen que no pueden ser custodiadas las armas en sus locales con las debidas condiciones de seguridad, podrán remitirlas bajo recibo a la Intervención de Armas de la Guardia Civil, donde permanecerán a disposición de aquéllos hasta que surtan sus efectos en los correspondientes procedimientos».
- El Real Decreto 467/2006, de 21 de abril, por el que se regulan los depósitos y consignaciones judiciales, de acuerdo con el que se consignarán en la cuenta judicial, la moneda metálica, billetes de banco, cheques bancarios o valores realizables, intervenidos, aprehendidos o incautados por las FCSE, por Vigilancia Aduanera o cualquier otro funcionario público, poniéndose de este modo a disposición de la autoridad judicial competente.
- El Real Decreto 32/2009, de 16 de enero, por el que se aprueba el Protocolo nacional de actuación Médico Forense y de Policía Científica en sucesos con víctimas múltiples, que establece un protocolo de aplicación obligatoria por el Instituto Nacional de Toxicología y Ciencias Forenses y el de Medicina Legal así como por las unidades de Policía Judicial orgánicamente dependientes del Ministerio del Interior, estableciendo en su art. 19 una un control de calidad consistente en comprobar que se han completado

Sin embargo, doctrinalmente se estima que las normas reglamentarias son insuficientes, en tanto que regulan parcialmente la materia. En este sentido, RICHARD GONZÁLEZ afirma que «la Orden JUS de 2010 únicamente regula el modo de recoger y conservar las muestras para la remisión al laboratorio, mientras que el Acuerdo Marco Interministerial de 2012 y la Recomendación del Consejo de Europa se refieren específicamente a las sustancias estupefacientes»[835]. Por su parte, GUTIERREZ SANZ estima que aunque el Acuerdo Marco Interministerial de 2012 «ha tenido efectos beneficiosos, no por ello se ha logrado uniformidad en el tratamiento de las sustancias incautadas y, además, el acuerdo se ciñe exclusivamente al ámbito de drogas tóxicas, estupefacientes o sustancias psicotrópicas»[836].

Son numerosas las críticas a la falta de regulación legal. Así, EIRANOVA ENCINAS afirma que esta ausencia legislativa «hace que el conjunto de la regulación presente serias deficiencias»[837]. De forma similar, RICHARD GONZÁLEZ señala que las normas de recogida, custodia y análisis de evidencias «se regulan de un modo impreciso y deficiente debido a las múltiples modificaciones de la Ley, que han conducido a un sistema en el que se entremezclan las competencias del juez y de la Policía de un modo difícil de entender y mucho más de gestionar en el día a día de la investigación criminal»[838].

---

todas las operaciones, que se han recogido y documentado las muestras y objetos personales y se ha observado la cadena de custodia.

[835] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», cit., p. 9.

[836] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 53.

[837] Señala el referido autor las siguientes deficiencias:

«1. Existe un tratamiento separado de la «recogida» y «custodia» de datos y piezas de convicción, de las previsiones legales respecto de la prueba pericial («análisis»).

2. Falta de regulación del procedimiento de la «recogida» y «custodia» de las piezas de convicción. No existen previsiones sobre precintos, sellos y cualesquiera mecanismos que posibiliten el aislamiento y la no contaminación de la pieza de convicción. Simplemente se prevé la actividad de abrir diligencias informativas sobre lo que va sucediendo en la «recogida», «custodia» y «análisis» del elemento de convicción.

3. La garantía de «autenticidad» se hace recaer en diferentes sujetos que intervienen en la investigación (policía, juez, secretario judicial, perito), sin tener en muchos casos en cuenta al perito forense. Todo ello produce al menos dos disfunciones importantes: la primera, que cuando se custodia una pieza de convicción se pueda hacer sin atender a las normas forenses sobre el cuidado de la misma; la segunda, que en la recogida de elementos de convicción tenga distinto valor probatorio si éstos lo son por el juez (prueba anticipada) que por la Policía Judicial (diligencia de investigación)». Vid. EIRANOVA ENCINAS, E., «Cadena de custodia y prueba de cargo», *Diario La Ley - Sección Doctrina*, n.º 6863, 2008, p. 2.

[838] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», cit., p. 6.

De este modo, aunque esta falta de regulación se ha suplido por la actividad jurisprudencial, doctrinalmente se viene reclamando una regulación de las pautas de la cadena de custodia, de tal forma que, con el cumplimiento de las mismas, se asegure la autenticidad e integridad de las pruebas, evitando de este modo la exclusión de la prueba del acervo probatorio.

RICHARD GONZÁLEZ estima que, en definitiva, «no cabe duda de la necesidad de regular la cadena de custodia en la LECrim al tratarse de una materia esencial para la validez de la prueba»[839], mientras que FIGUEROA NAVARRO considera necesaria la regulación, «con el fin de garantizar la corrección procesal en la obtención y aseguramiento de aquellas fuentes de pruebas que, tras ser analizadas, accederán al plenario mediante el informe pericial correspondiente»[840]. Con ello «se otorgaría mayor confianza a la labor policial en la investigación de los delitos, se reforzaría el derecho a un proceso con todas las garantías, y aumentaría, aún más si cabe, el valor probatorio que viene otorgando la jurisprudencia a las pruebas periciales realizadas por los laboratorios oficiales»[841].

3. Procedimiento de custodia

De acuerdo con lo declarado por la jurisprudencia menor, la relevancia de la garantía de la «cadena de custodia» ha ido evolucionando legislativa y jurisprudencialmente no solo a la par del concepto de proceso debido en Derecho, sino paralelamente a la trascendencia que la prueba pericial posee en el proceso penal moderno, (fruto del nacimiento de nuevas formas de delincuencia y del avance de las técnicas de investigación)[842].

Asimismo, ha declarado que, aun cuando no existe una normativa reguladora expresa de las exigencias mínimas garantizadoras formalmente de la indemnidad de la «cadena de custodia», las nueva reformas normativas, la doctrina y la jurisprudencia han construido un «corpus jurídico» que es asumido como vinculante por la comunidad

[839] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal españoL», cit., p. 9.
[840] FIGUEROA NAVARRO, C., «El aseguramiento de las pruebas y la cadena de custodia», cit., p. 9.
[841] FIGUEROA NAVARRO, C., «El aseguramiento de las pruebas y la cadena de custodia», cit., p. 9.
[842] Vid. SAP 132/2009, Sección 2.ª de Barcelona, de 25 de febrero, FJ 2.º.

jurídica y respetado, desde luego, por las fuerzas policiales[843], que se adapta a lo establecido en la Recomendación del Consejo de la Unión Europea de 30 de marzo de 2004 sobre directrices para la toma de muestras de drogas incautadas, anteriormente mencionada, donde se establecen las pautas que deben regir la cadena de custodia, como son: a) informe detallado (descripción, numeración, pesaje, embalaje, origen, características externas, apariencia, fotos, etc.) de la incautación por parte de las fuerzas del orden destinado a la policía científica y a los tribunales; b) técnica de muestreo conforme a criterios predeterminados; y c) adoptar las medidas oportunas para garantizar la cadena de custodia en la transmisión de la sustancia o muestras[844].

No obstante lo anterior, lo cierto es que con el Anteproyecto de LECrim de 2011 se produjo un intento de dotar de carácter legal a las principales directrices del procedimiento y fases conformadoras de la cadena de custodia, dado que, conforme señala GUTIÉRREZ SANZ «el legislador pareció darse cuenta de la necesidad de regular de forma expresa la cadena de custodia en el seno de la LECrim»[845].

En este anteproyecto se trató la materia en un capítulo independiente con cuatro artículos[846]. En ellos —tras disponer que todas las fuentes de prueba obtenidas durante la investigación de los hechos delictivos serán debidamente custodiadas, a fin de asegurar su disponibilidad en el acto del juicio oral, así como la obligación de todos cuantos tengan relación con la fuente de prueba, fueren funcionarios públicos o particulares, de

---

[843] Vid. SSAP 430/2009, Sección 3.ª de Almería, de 21 de diciembre, FJ 2.º; 541/2012, Sección 8.ª de Barcelona, de 3 de septiembre, FJ 2.º; 550/2014, Sección 6.ª de Madrid, de 28 de julio; y 90/2018, Sección 2.ª de Barcelona, de 8 de febrero, FJ 2.º

[844] FIGUEROA NAVARRO Y DEL AMO RODRÍGUEZ se refieren al protocolo seguido por la Policía Científica para un adecuado sistema de cadena de custodia. Afirman estos autores en la p. 325 de su trabajo que «cuando analizamos la evolución de las normas internas y protocolos de actuación en el área de Policía Científica, nos tenemos que remontar al año 1995, año en el que se crea el primer Manual de normas de procedimientos para todas las áreas de Policía Científica que, en aquella época, se trabajaban». Vid. FIGUEROA NAVARRO, C.; DEL AMO RODRÍGUEZ, A., «La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica», en *Policía científica - 100 Años de Ciencia al Servicio de la Justicia*, Madrid, 2011, pp. 315-330. Consultado en http://www.interior.gob.es/documents/642317/1203227/Policía+Científica+-100+años+de+Ciencia+al+servicio+de+la+justicia+%28NIPO+126-11-081-7%29.pdf/b983385f-ec1c-48c0-a6fe-98ede304c2fc, el 13 de julio de 2019. En cuanto a los protocolos seguidos por los organismos oficiales puede consultarse RODRÍGUEZ JIMÉNEZ, E. Y OTROS, «La cadena de custodia en los laboratorios oficiales de criminalística y ciencias forenses de España», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015.

[845] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 57.

[846] Concretamente los arts. 357 a 360.

constituir, aplicar y mantener la cadena de custodia, garantizando la inalterabilidad de aquella—, estableció un procedimiento de gestión y custodia que debería ser desarrollado reglamentariamente. En todo caso, de acuerdo con el anteproyecto, era preciso dejar constancia documental en las actuaciones de los siguientes particulares:

a) La persona y el lugar en el que se localizó la muestra y la documentación del hallazgo.

b) Todas las personas que la hayan tenido a su cargo y los lugares en los que haya estado guardada, depositada o almacenada.

c) El tiempo que haya estado en poder de cada persona o depositada en un determinado lugar.

d) El motivo por el que la fuente de prueba ha sido enviada a otro lugar o ha pasado a manos de otras personas.

e) Las personas que han accedido a las fuentes de prueba, detallando en su caso las técnicas científicas aplicadas y el estado inicial y final de las muestras.

Por último, en el Anteproyecto de LECrim de 2011, se estableció que el quebrantamiento de la cadena de custodia fuese valorado por el tribunal a los efectos de determinar la fiabilidad de la fuente de prueba.

Sin embargo, en línea con lo afirmado por GUTIÉRREZ SANZ, quien señala que «resulta un tanto inexplicable es que estas previsiones desaparecieran»[847], estimamos incomprensibles los cambios de criterio del legislador, cuando de un asunto tan relevante se trata, en el que por la doctrina se viene reclamando unánimemente una regulación legal. Lo cierto es que, no obstante existir alguna mención, tales previsiones no se incluyeron en el Anteproyecto de LECrim de 2013. Si bien este último anteproyecto tampoco llegó al trámite parlamentario, el legislador tuvo la oportunidad, con la LO 13/2015, de incorporar a nuestra vigente LECrim una regulación sistemática de la cadena de custodia similar a la del Anteproyecto de 2011.

En este punto, como apunta PERALS CALLEJA, no debe olvidarse que, aunque las quejas relativas a la infracción de la cadena de custodia no son esencialmente impugnaciones que afecten de forma directa a los derechos fundamentales, puede darse

[847] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 59.

el caso de que en recurso de casación se alegue la vulneración de la presunción de inocencia por valorarse una prueba que ha llegado al juicio de una manera irregular y dicha irregularidad afecte al derecho de defensa[848].

Por tanto, seguimos sin la regulación de una materia que puede afectar a la validez o fiabilidad de la prueba pertinente para la defensa de las partes en el proceso, y, con ello, como ha señalado la jurisprudencia del TS, verse comprometidos los derechos fundamentales a un proceso con todas las garantías y a la presunción de inocencia (art. 24.2 CE)[849].

4. El quebrantamiento de la cadena de custodia

La inexistencia de una regulación sistemática de la cadena de custodia no permite que se pueda llevar a cabo un tratamiento con carácter general y sistemático de los supuestos de quebrantamiento, por lo que el análisis de los mismos se ha de realizar desde un punto de vista casuístico, con base en los numerosos casos resueltos por la jurisprudencia del TS, a la que hay que añadir los de la jurisprudencia menor de las AP. A este respecto, dice GUTIERREZ SANZ que la mencionada ausencia de una normativa única reguladora, tanto de los aspectos técnicos como de los jurídicos, «sitúa el examen de las irregularidades en la cadena de custodia en un plano un tanto confuso y en ocasiones cambiante»[850].

De acuerdo con lo señalado por DEL POZO PÉREZ «la importancia de la cadena de custodia es crucial y viene dada porque se encamina a obtener la certeza jurídica,

---

[848] PERALS CALLEJA, J., «La cadena de custodia. Problemas probatorios», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2014, p. 12, Consultado en http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 25 de junio de 2020.

[849] La STS 587/2014, de 18 de julio, ha declarado en su FJ 1.º que «es cierto que la ruptura de la cadena de custodia puede tener una indudable influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia. Resulta imprescindible descartar la posibilidad de que la falta de control administrativo o jurisdiccional sobre las piezas de convicción del delito pueda generar un equívoco acerca de qué fue lo realmente analizado. Lo contrario podría implicar una más que visible quiebra de los principios que definen el derecho a un proceso con todas las garantías». Y la STS 545/2012, de 22 de junio, señaló en su FJ 2.º que «la vulneración de la cadena de custodia puede tener un significado casacional, pero no como mera constatación de la supuesta infracción de normas administrativas, sino por su hipotética incidencia en el derecho a la presunción de inocencia del art. 24.2 de la CE».

[850] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 107.

asegura la identidad entre lo recogido y lo analizado»[851]. En relación con este aspecto, «la identidad entre lo recogido y lo analizado» o, como ha dicho la jurisprudencia «la mismidad de la prueba»[852], en caso de no quedar acreditado que el material analizado no es exactamente el mismo que el inicialmente incautado, se podría declarar la invalidez de la prueba, excluyéndose la misma del acervo probatorio.

Pero esta invalidez no se produce por infracciones de menor entidad en la cadena de custodia, en cuyo caso nos encontraríamos ante una irregularidad que no siempre implicaría la exclusión de la prueba, pudiendo ser subsanada. Como reiteradamente ha declarado el TS, «estamos ante un problema no tanto de validez como de fiabilidad»[853]. No se pueden confundir los dos planos, «irregularidad en los protocolos establecidos como garantía para la cadena de custodia no equivale a nulidad»[854]. Por ello, «habrá que valorar si esa irregularidad (no mención de alguno de los datos que es obligado consignar; ausencia de documentación exacta de alguno de los pasos...) es idónea para despertar dudas sobre la autenticidad o indemnidad de la fuente de prueba»[855].

De este modo, dependiendo de la entidad de la infracción, nos encontraríamos ante una falta subsanable o, en su caso, ante un vicio que pondría en duda la autenticidad de la fuente de prueba, impidiendo su valoración. Como dice RICHARD GONZÁLEZ, «una infracción menor de la cadena de custodia supondría una irregularidad que no determinará, necesariamente, el "apartamiento" del proceso de la prueba que podría ser valorada; mientras que una infracción mayor tendría por consecuencia la invalidez de la prueba que no podrá ser valorada al existir dudas sobre la autenticidad de la fuente de prueba»[856].

4.1. Supuestos de invalidez

Tal y como acabamos de indicar, y como también ha declarado el TS, «solo si las deficiencias formales despiertan serias dudas racionales, debería prescindirse de la

[851] DEL POZO PÉREZ, M., «La cadena de custodia: Tratamiento jurisprudencial», *Revista General de Derecho Procesal*, n.º 30, 2013, p. 11.
[852] Son numerosas las resoluciones del TS en las que se menciona este término. Vid. SSTS 777/2013, de 7 de octubre, FJ 7.º; 676/2016, de 22 de julio, FJ 2.º; y 513/2018, de 30 de octubre, FJ 6.º.
[853] Vid. STS 298/2020, de 11 de junio, FJ 9.º
[854] Vid. STS 1072/2012, de 11 de diciembre, FJ 4.º
[855] Vid. STS 339/2013, de 20 de marzo, FJ 9.º
[856] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», cit., p. 11.

fuente de prueba, no por el incumplimiento de algún trámite o diligencia establecida en el protocolo de recepción de muestras y su custodia, sino por quedar cuestionada su autenticidad», por lo que «habrá que sopesar si esa irregularidad es capaz de despertar dudas sobre la autenticidad o indemnidad de la fuente de prueba»[857].

El TC ha tenido la oportunidad de pronunciarse en relación con la materia que nos ocupa. Concretamente, la STC 170/2003, de 29 de septiembre, estimó un recurso de amparo declarando vulnerado el derecho a un proceso con todas las garantías[858], en la medida en que fueron valorados los informes periciales efectuados sobre un material informático que se incorporó sin que quedara acreditado el cumplimiento de las debidas garantías de custodia policial y control judicial sobre su identidad e integridad.

El TC acuerda la nulidad de la sentencia recurrida y la retroacción de las actuaciones, a fin de que se dicte una nueva resolución con exclusión de la prueba impugnada, y ello por entender que los soportes informáticos no sólo no fueron debidamente identificados, sino que tampoco se procedió a su correcto sellado y precintando, a lo que debe unirse el hecho objetivo, también destacado en vía judicial, de la existencia de una significativa discordancia numérica entre los CD intervenidos.

Concluye el TC «que se ha producido una deficiente custodia policial y control judicial de dicho material, que no estaba debidamente precintado y a salvo de eventuales manipulaciones externas tanto de carácter cuantitativo (número de las piezas de convicción halladas en los registros) como cualitativo (contenido de aquellos soportes que admitieran una manipulación por su carácter regrabable o simplemente por su naturaleza virgen en el momento de su incautación, e incluso su sustitución por otros), lo que impide que pueda afirmarse que la incorporación al proceso penal de los soportes informáticos se diera con el cumplimiento de las exigencias necesarias para garantizar una identidad plena e integridad en su contenido con lo intervenido y, consecuentemente, que los resultados de las pruebas periciales se realizaran sobre los mismos soportes intervenidos o que éstos no hubieran podido ser manipulados en cuanto a su contenido»[859].

---

[857] Vid. STS 129/2015, de 4 de marzo, FJ 1.º

[858] El TC indica que no cabe realizar pronunciamiento alguno en relación con la vulneración del derecho a la presunción de inocencia, en tanto que de la lectura de la sentencia de apelación se acredita que se motivó la declaración de responsabilidad de los recurrentes en una pluralidad de pruebas que no estaban afectadas por la vulneración declarada. Vid. STC 170/2003, de 29 de septiembre, FJ 4.º

[859] Vid. STC 170/2003, de 29 de septiembre, FJ 3.º

Por tanto, la invalidez de la prueba y su exclusión del acervo probatorio procederá en aquellos casos en los que se han producido infracciones graves que cuestionan seriamente la credibilidad del elemento probatorio y también, como dice RICHARD GONZÁLEZ, «ante la existencia de numerosas irregularidades que por sí solas no serían determinantes de la invalidez, pero que juntas determinan esa consecuencia»[860].

De acuerdo con lo expuesto, no resulta fácil establecer una relación de casos en los que resultaría infringida la cadena de custodia, dando lugar a la exclusión probatoria, sino que habrá que estar a cada caso concreto con el examen de precedentes de iguales o similares características, teniendo presente que sobre estos aspectos no existe una jurisprudencia uniforme. Así se entiende doctrinalmente, y, en este sentido, GUTIERREZ SANZ aporta, a título ejemplificativo, cuatro grupos de supuestos, en los que los tribunales han excluido la fuente de prueba[861]. Son los siguientes:

a) Vicios en la identificación, conservación y depósito de los elementos.

Se refiere a este supuesto la mencionada STC 170/2003, de 29 de septiembre, pudiendo mencionarse igualmente la SAP 52/2009, Sección Bis de Las Palmas de Gran Canaria, de 29 de julio, FJ 2.º, en la que se concluyó que, no constando que la droga incautada fuese trasladada al laboratorio oficial, se había roto la cadena de custodia, siendo imposible tener por probado que la droga analizada fuese la aprehendida en el mismo procedimiento, dictando finalmente sentencia absolutoria.

Asimismo, la SAP 4/2017, Sección 2.ª de Toledo, de 1 de febrero, FJ 1.º, declara que la ruptura de la cadena de custodia se ha producido al existir una diferencia notable (más del doble) entre el peso consignado en el oficio de la prisión donde se intervino la droga, y el que se refleja en el acta.

b) Intervalo de tiempo excesivo y sin justificar entre la aprehensión y la puesta a disposición judicial del efecto ocupado.

Se plantea esta infracción en el caso resuelto por la SAP 34/2015, Sección 9.ª de Málaga, de 29 de enero, FJ 1.º, que declaró que se había producido una fractura de la cadena de custodia que impedía la valoración de la prueba, al existir un amplio margen

[860] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal españoL», cit., p. 17.
[861] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., pp. 124-132.

de hasta dos meses y veintidós días, en el que no consta en la causa el paradero de la sustancia luego analizada, de modo que solo efectuando una presunción contra reo, imposible en causa penal, podría asegurarse que la sustancia ocupada por la Policía es la misma que se recibió para su análisis.

En la misma línea, la SAP 82/2010, Sección 3.ª de Barcelona, de 25 de enero, FJ 1.º, concluye que se ha producido una ruptura de la cadena de custodia de la sustancia intervenida a los acusados, toda vez que la sustancia se recibió en el laboratorio tres meses más tarde, sin que se especifique en ningún momento la persona encargada de la entrega, ni el lugar donde fue custodiada, por lo que existe una duda más que razonable sobre la identidad existente entre la sustancia analizada y la intervenida a los acusados.

c) Ausencia de custodia de los efectos dando lugar a una posible manipulación.

En el caso resuelto por la SAP 11/2011, Sección 29.ª de Madrid, de 27 de enero, se absolvió a los acusados, dado que, conforme se expone en su FJ 2.º, una vez abierto el paquete en la Aduana, no resultó acreditada su custodia y preservación con garantías de no quedar al acceso de terceros, encontrándose abierto el mismo durante uno o dos días en desconocidas condiciones.

d) Ausencia de documentación

La SAP 319/2008, Sección 3.ª de Almería, de 1 de octubre, FJ 1.º, tras señalar que no consta incorporada a las actuaciones el acta de aprehensión que debió firmar y sellar la Dependencia de Sanidad de Almería, con indicación del peso bruto y neto de las sustancias recepcionadas, habiendo manifestado las dos peritos que concurrieron al juicio que no reconocían la citada fotocopia del acta de aprehensión al no figurar la firma y el sello de su Servicio, estima que existe un claro y acreditado quebranto de la cadena de custodia, absolviendo a los acusados.

4.2. Supuestos de irregularidad que no determinan la exclusión probatoria

Tal y como apunta PERALS CALLEJA, «en los últimos tiempos se está produciendo una expansión desmesurada de los problemas relativos a la cadena de custodia, planteándose numerosas cuestiones en el terreno práctico desde el punto de

vista constitucional de la prueba, alegándose que la vulneración de los trámites de la cadena de custodia afectan a los derechos fundamentales del acusado»[862].

Este notable incremento de los recursos interpuestos invocando la irregularidad de la cadena de custodia, consideramos que trae causa de la ausencia de una regulación de la misma. Con ello, se están produciendo contradicciones entre distintas resoluciones en lo que respecta al tratamiento casuístico, planteándose una dificultosa delimitación entre los supuestos de invalidez y de mera irregularidad.

En general, la doctrina del TS es reacia a considerar quebrantada la cadena de custodia, teniéndose que producir, como ya dijimos anteriormente, infracciones muy graves o, en su caso, una acumulación de infracciones que, decididamente, ponga en seria dudas la mismidad de la prueba[863].

Como consecuencia de lo expuesto anteriormente y del mismo modo que indicamos para los casos de invalidez, resultaría muy dificultoso establecer un catálogo de supuestos que engloben las irregularidades de la cadena de custodia no invalidantes de la fuente de prueba[864], por lo que citaremos algunos que consideramos más relevantes.

a) La STS 339/2013, de 20 de marzo, FJ 9.º, ante la denuncia por parte del recurrente de irregularidades tales como que la sustancia intervenida no fuese precintada, que no constase quién transportó las sustancias ni cuando se realizó el traslado, no constando que quedasen a disposición policial ni judicial, declara que estas supuestas deficiencias «ni incrementan la posibilidad de que haya acaecido alguna de

---

[862] PERALS CALLEJA, J., «La cadena de custodia. Problemas probatorios», cit., pp. 13-14.

[863] Así, la Sala 2.ª del TS ha dejado claro esta posición en pronunciamientos como los de la STS 629/2011, de 23 de junio, en la que en su FJ 22.º declaró que «a pesar de la comisión de algún posible error, ello no supone, por sí solo, sustento racional y suficiente para sospechar siquiera que la analizada no fuera aquella sustancia originaria, ni para negar el valor probatorio de los análisis y sus posteriores resultados, debidamente documentados»; o de la STS 277/2016, de 6 de abril, en la que en su FJ 3.º señala que «la cadena de custodia no es una especie de liturgia formalizada en la que cualquier falla abocaría a la pérdida de toda eficacia».

[864] Una relación de casos de irregularidad no invalidantes puede consultarse en los siguientes trabajos:
- RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», cit., pp. 14-17.
- PERALS CALLEJA, J., «La cadena de custodia. Problemas probatorios», cit., pp. 13-42.
- LEAL MEDINA, J., «Ruptura de la cadena de custodia y desconexión con las fuentes de prueba. Supuestos concretos. Reflexiones que plantea», *Diario La Ley - Sección Doctrina*, n.º 8846, 2016.
- GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., pp. 109-123.

esas manipulaciones, ni disminuyen las posibilidades de descubrirlas, ni desde luego convierte en algo pausible [sic][865] lo que por nadie es pensable».

b) En cuanto al tiempo transcurrido entre la aprehensión de la prueba y su remisión al laboratorio correspondiente, la STS 383/2016, de 5 de mayo, FJ 5.º, señala que, aun cuando se recibieran las sustancias en Sanidad cinco meses más tarde de su aprehensión, no ha de entenderse rota la cadena de custodia y, haciendo suyos los argumentos de la sentencia de instancia, declara que «es lamentable, sin duda, que no existan más medios en dicho Ministerio a fin de agilizar los procedimientos, si bien no es suficiente motivo para no dar por buenos los análisis realizados y tirar por tierra la "cadena de custodia"».

c) Y respecto a la ausencia de documentación, la STS 545/2012, de 22 de junio, FJ 2.º, tras declarar que la vulneración de la cadena de custodia tiene significado casacional, por su posible incidencia en el derecho a la presunción de inocencia, pero no como mera constatación de la supuesta infracción de normas administrativas[866], señala que «el énfasis de la defensa, centrado en la ausencia de alguno de los documentos a los que se refiere la normativa citada[867], no tiene por qué conllevar una quiebra de alcance constitucional», concluyendo que «a efectos de tipicidad es suficiente con que la sustancia fuera intervenida a personas perfectamente identificadas y que el dictamen pericial que fijó su composición química, fuera sometido a contradicción en los debates del plenario».

d) Finalmente, también ha sido impugnada la cadena de custodia por no comparecer los funcionarios intervinientes en el proceso de custodia a ratificar sus informes en el juicio oral. La STS 303/2014, de 4 de abril, FJ 2.º, zanjó esta cuestión declarando que «se aparta de la lógica de lo razonable que todos los pasos que se den con la sustancia estupefaciente por los diferentes funcionarios y servicios concernidos deban ser ratificados en el juicio oral, diligenciamiento que solo se hace en la práctica, lógicamente, cuando alguna de las partes impugna la autenticidad de las firmas o de los sellos oficiales o cuando las diligencias presentan algún punto oscuro, expresan datos

[865] Resulta obvio que se trata de un error de transcripción, debiéndose haber consignado el vocablo «posible» en lugar de «pausible».
[866] Vid. nota al pie n.º 849, p. 409.
[867] Se refiere a la Orden JUS/1291/2010, de 13 de mayo, por la que se aprueban las normas para la preparación y remisión de muestras objeto de análisis por el Instituto Nacional de Toxicología y Ciencias Forenses.

contradictorios o muestran cualquier clase de signo que den pie para cuestionar la fiabilidad de la conservación de la fuente de prueba».

5. La impugnación de la cadena de custodia

Para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia, se hace necesaria una impugnación formal de la misma, la cual no deberá limitarse a plantear dudas de carácter genérico, sino que deberá estar sostenida con un razonamiento suficiente.

Esta impugnación plantea dos cuestiones que deben ser analizadas, como son: el momento procesal en el que ha interponerse la misma y tema de la carga probatoria del quebrantamiento de la cadena de custodia.

5.1. Momento procesal para la impugnación

Para que se produzca la impugnación de la cadena de custodia, previamente debe haberse solicitado por la acusación o acusaciones la incorporación de la documental acreditativa, lo cual deberá producirse en los escritos de calificación en el procedimiento ordinario y en los escritos de acusación en el procedimiento abreviado[868].

Así pues, señala PERALS CALLEJA, «en el caso de que conste unido a actuaciones un "documento de custodia", o diversos documentos que acrediten el camino que han seguido los efectos ocupados, deberá proponerse en el escrito de acusación, como prueba documental, tales actas o diligencias sin perjuicio de que haya que proponer como prueba testifical en determinados supuestos a los funcionarios que han manejado los efectos […] en el caso de que tal declaración sea necesaria para acreditar otros extremos o se haya impugnado la autenticidad de la cadena de custodia»[869].

Una vez propuesta la documental, lo normal es que la impugnación se produzca con la presentación del escrito de calificación por la defensa en el procedimiento

[868] Dispone el art. 656.1 LECrim, en sede del Procedimiento Ordinario, que «el Ministerio Fiscal y las partes manifestarán en sus respectivos escritos de calificación las pruebas de que intenten valerse, presentando listas de peritos y testigos que hayan de declarar a su instancia», mientras que tratándose del Procedimiento Abreviado, de conformidad con el art. 781.1-II, en el escrito de acusación «se propondrán las pruebas cuya práctica se interese en el juicio oral, expresando si la reclamación de documentos o las citaciones de peritos y testigos deben realizarse por medio de la oficina judicial».

[869] PERALS CALLEJA, J., «La cadena de custodia. Problemas probatorios», cit., p. 9.

ordinario o el escrito de defensa en el procedimiento abreviado[870], aunque en este último consideramos que la denuncia también puede formularse en el trámite de cuestiones previas, habida cuenta de la posibilidad, prevista por el art. 786.2 LECrim, de que las partes puedan, en dicho trámite, exponer lo que estimen oportuno acerca de cuestiones como la vulneración de algún derecho fundamental o nulidad de actuaciones.

Sin embargo, como así ocurre con todas las infracciones procesales, la parte afectada deberá denunciar la posible irregularidad tan pronto como tenga conocimiento de la misma. Así lo pone de manifiesto RICHARD GONZÁLEZ, señalando que «de otro modo es probable que la impugnación no sea atendida por entender el tribunal *ad quem* en vía de recurso que la parte se aquietó con la cuestión»[871].

Lo que en todo caso es necesario es que se dé a la contraparte la oportunidad de contradecir la impugnación, por lo que no es admisible que la misma se produzca en el informe final sin que se haya podido someter a debate la cuestión en los interrogatorios del juicio oral. De este modo, como ha declarado reiteradamente la jurisprudencia, «habrá de plantearse en momento procesalmente hábil para que las acusaciones, si a su derecho interesa, puedan contradecir eficazmente las objeciones planteadas»[872].

5.2. Carga probatoria del quebrantamiento de la cadena de custodia

En diversas resoluciones el TS ha declarado que no resulta aceptable la admisión de una impugnación de la cadena de custodia en la que se invoque la simple posibilidad de la manipulación de la fuente de prueba, en tanto que existe la presunción de que lo recabado por el juez, el perito o la Policía se corresponde con lo presentado el día del juicio como prueba, salvo que existan sospechas razonables, por lo que debe exigirse a la parte impugnante la prueba de manipulación efectiva[873].

EIRANOVA ENCINAS no comparte esta opinión, ya que estima que exigir al acusado que pruebe una manipulación real para hacer posible las consecuencias de la rotura de la cadena de custodia, pone a la defensa en una tesitura imposible, estimando

[870] En relación con el escrito de defensa en el Procedimiento Abreviado, vid. art. 784.1 LECrim.
[871] RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», cit., p. 14.
[872] Vid. SSTS 990/2016, de 12 de enero de 2017, FJ 13.º; 726/2017, de 8 de noviembre FJ 2.º; y 541/2018, de 8 de noviembre, FJ 3.º
[873] Vid. SSTS 714/2016, de 26 de septiembre, FJ 5.º; 787/2017, de 5 de diciembre, FJ 2.º; y 513/2018, de 30 de octubre, FJ 6.º

que «en el proceso penal este juego de la prueba es totalmente incorrecto, ya que se obligaría a la defensa a probar hechos constitutivos, no bastando con la prueba de los hechos impeditivos»[874].

En una línea similar, LADRÓN TABUENCA considera que esta práctica «resulta contraria al principio de normalidad probatoria o de mayor facilidad de acceso a la fuente de prueba», estimando que estos principios «deberían llevar como consecuencia necesaria, la inversión de la carga de la prueba, en el sentido de que fueran los organismos encargados de la práctica de la prueba pericial quienes hubieran de acreditar su actuación con pleno respeto a la *lex artis* y a los específicos protocolos de actuación, tanto puramente orgánicos como científicos»[875].

Asimismo, en alguna resolución de los tribunales se estima que corresponde a la acusación «acreditar que la cadena de custodia había sido correctamente realizada, no siendo carga de la prueba de la defensa el probar lo contrario»[876].

Sin embargo, autores como GUTIERREZ SANZ, afirman que «a lo que el principio de presunción de inocencia obliga es a presumir que una persona es inocente mientras no concurran pruebas que acrediten su culpabilidad, pero en ningún caso, puede equivaler a la presunción de que todas las pruebas son inutilizables hasta que no se acredite su licitud»[877].

Así lo pone de manifiesto igualmente TORRES-DULCE LIFANTE, aclarando que «según la opinión dominante, este instituto no se aplica a la comprobación de fallos o defectos en el procedimiento: quien los alega debe probarlos, puesto que se presume que los órganos encargados de la justicia penal respetan el derecho procesal»[878].

En cualquier caso, este criterio jurisprudencial se encuentra consolidado, dado que, de forma reiterada, el TS ha declarado que ni el derecho a la presunción de

[874] EIRANOVA ENCINAS, E., «Cadena de custodia y prueba de cargo», cit., p. 12.

[875] Vid. LADRÓN TABUENCA, P., «La regulación de la cadena de custodia en España: previsiones legales y desarrollos jurisprudenciales sobre la cadena de custodia de las fuentes de prueba», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, p. 25.

[876] Vid. SSAP 1074/2012, Sección 17.ª de Madrid, de 27 de julio, FJ 2.º y 34/2015, Sección 9.ª de Málaga, de 29 de enero, FJ 1.º

[877] GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 104.

[878] TORRES DULCE LIFANTE, E., «Prólogo», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, p. 8.

inocencia, ni el principio «in dubio pro reo», pueden llegar a significar, salvo que se acredite lo contrario, que las actuaciones de las autoridades son, en principio, ilícitas e ilegitimas, ya que ello supondría la paradoja de que, mientras tratándose de los acusados ha de presumirse siempre su inocencia en tanto no se prueba su culpabilidad, a los jueces y tribunales, en el mismo marco procesal, ha de presumírseles una actuación contraria a la Constitución y las leyes, en tanto no se prueba que han actuado conforme a Derecho, señalando que el principio de presunción de inocencia no puede extender su eficacia hasta esos absurdos extremos[879].

No obstante, consideramos que no se trata de que, de forma determinante, se deba probar que ha existido manipulación, lo que devendría imposible en muchos casos para la defensa, pudiendo situarla en una situación de indefensión[880], sino que exista un principio de prueba formado con base en unas alegaciones fundadas, que pueda enervar la presunción de veracidad. En este sentido, la jurisprudencia ha declarado de forma reiterada que «para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia no es suficiente con el planteamiento de dudas de carácter genérico, es necesario que el recurrente precise en qué momentos, a causa de qué actuaciones y en qué medida se ha producido tal interrupción, pudiendo, en su caso, la defensa, proponer en la instancia las pruebas encaminadas a su acreditación»[881]. Por otra parte, en caso de impugnación, será lo normal que la acusación proponga la declaración de todos los agentes o funcionarios intervinientes en el proceso de custodia.

Del mismo modo que, como veremos más adelante en el apartado dedicado a la impugnación de la prueba digital —respecto del que ya adelantamos nuestra opinión relativa a la necesidad de que la parte impugnante que ponga en duda la autenticidad e integridad de la fuente probatoria razone debidamente su solicitud con argumentos que de forma efectiva pongan en entredicho la verosimilitud de la misma—, estimamos que el que ponga en duda la cadena de custodia deberá acreditarlo con una argumentación

[879] Vid. SSTS 187/2009, de 3 de marzo, FJ 1.º; 6/2010, de 27 de enero, FJ 2.º; y 147/2015, de 17 de marzo, FJ 1.º

[880] Afirma a este respecto GUTIERREZ SANZ que «mantener la presunción de regularidad frente a la alegación de irregularidades importantes, aun cuando no se pueda demostrar la alteración real de la fuente de prueba, coloca en algunos casos a la parte en una situación de indefensión». Vid. GUTIÉRREZ SANZ, M. R., «*La cadena de custodia en el proceso penal español*», cit., p. 106.

[881] Vid. SSTS 990/2016, de 12 de enero de 2017, FJ 13.º; 250/2017, de 5 de abril, FJ 7.º; 726/2017, de 8 de noviembre, FJ 2.º; 469/2019, de 14 de octubre, FJ 4.º; y 649/2019, de 20 de diciembre, FJ 4.º

suficiente, sin que se limite a una impugnación genérica, de tal modo que el tribunal quede obligado a dar una respuesta motivada.

De este modo, el acusado no tendría la carga —a nuestro juicio desproporcionada— de tener que probar de forma efectiva que se ha producido una manipulación, pero si la de argumentar debidamente su impugnación, con una mención expresa de los aspectos vulnerados dentro del protocolo y, si lo considera oportuno, proponer la prueba que considere procedente, consiguiendo así generar una sospecha bastante para desvirtuar la presunción de veracidad que debe regir sobre las distintas fases de la cadena de custodia.

6. La cadena de custodia de la prueba digital obtenida con los registros informáticos

Como ya hemos visto, la cadena de custodia no se encuentra regulada legalmente de forma sistemática, aunque existen determinados artículos en la LECrim que, con carácter general, hacen referencia a la misma. Por lo que respecta a la cadena de custodia de la prueba digital, tampoco existe regulación legal expresa, ni siquiera a nivel reglamentario.

La reforma operada por la LO 13/2015, aun cuando el legislador tiene en cuenta la facilidad con la que la prueba digital podría alterarse o destruirse, no ha profundizado en la materia. En lo concerniente a los registros informáticos ha establecido unas reglas en orden al aseguramiento de la misma y de los propios equipos. Así, el art. 588 sexies c.1 LECrim, en relación con los registros de dispositivos de almacenamiento masivo de información, dispone que el juez podrá autorizar la realización de copias de los datos informáticos y fijará las condiciones necesarias para asegurar su integridad, así como las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial. De forma similar, en lo que respecta a los registros remotos de equipos informáticos, de conformidad con los apartados d) y e) del art. 588 septies a.2 LECrim, la resolución judicial que autorice el registro deberá especificar la autorización, en su caso, para la realización y conservación de copias de los datos informáticos, así como las medidas precisas para la preservación de la integridad de los datos almacenados.

En esta regulación, en las dos modalidades de registros informáticos, el legislador deja a discreción de la autoridad judicial el establecimiento de las condiciones necesarias para garantizar la identidad de los datos almacenados. Por tanto, no

existiendo regulación expresa sobre la materia, deberá aplicarse lo dispuesto en el art. 334 LECrim, en el sentido de que, por el letrado de la Administración de Justicia, se extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren los efectos, describiendo los mismos. Sin embargo, no será posible, de acuerdo con lo establecido en el art. 338 LECrim, el envío al organismo adecuado para su depósito, al no existir el mismo.

Por otra parte, no ha tenido en cuenta el legislador las peculiaridades de los equipos informáticos y la prueba digital, dado que, como señala MESTRE DELGADO, en estos casos «el problema se complica en la medida en que, por su propia configuración de uso, estos instrumentos contienen o transmiten datos por esencia vinculados a los derechos fundamentales a la intimidad o al secreto de las comunicaciones»[882], siendo este «uno de los elementos diferenciales de la cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos, respecto de las cadenas de custodia de otros elementos probatorios, ya que, en aquellos, las Fuerzas y Cuerpos de Seguridad, salvo contadas excepciones, no pueden acceder a los vestigios de manera directa y sin autorización judicial»[883 y 884].

Por ello, teniendo en cuenta la volatilidad que caracteriza a las fuentes de prueba digitales, y considerando que, al igual que ocurre con las sustancias estupefacientes, aquellas requieren un tratamiento distinto al que tradicionalmente se ha dado a las fuentes de prueba convencionales o, en general, al resto de los efectos del delito, estimamos que hubiera sido necesaria una regulación de las medidas para la conservación y depósito de los dispositivos informáticos o de las fuentes de prueba digitales en general[885], estableciendo un organismo adecuado para el depósito de las

[882] MESTRE DELGADO, E., «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», cit., p. 50.

[883] MESTRE DELGADO, E., «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», cit., p. 50.

[884] VELASCO NUÑEZ afirma que las pericias informáticas tienen la peculiaridad frente a las que versan sobre corporeidades no reproducibles (cadáveres, máquinas, droga, armas, etc.) de que una vez entregada la copia "espejo" al perito, por quedar el original guardado por el secretario judicial, no se ven afectadas por las consideraciones sobre la cadena de custodia, pues la reproducción o copia garantiza fielmente que el objeto de la pericia (cuerpo del delito o pieza de convicción) es el mismo que el aprehendido y analizado. Vid. VELASCO NÚÑEZ, E., *Delitos cometidos a través de internet. Cuestiones procesales*, Las Rozas (Madrid), La Ley, 2010, p. 232.

[885] Así lo entiende DELGADO MARTÍN, quien señala que, aun cuando cabe valorar positivamente que el art. 588 sexies c.1 LECrim ha previsto la posibilidad de autorizar copias de los datos informáticos para

mismas, en el que serían custodiados con las debidas garantías. De ello nos ocuparemos en el último apartado de este epígrafe.

Finalmente, debe señalarse que para el estudio de la cadena de custodia de la prueba obtenida tras los registros informáticos, resulta aplicable lo expuesto en los anteriores apartados. No obstante, existen algunas cuestiones propias de estas fuentes de prueba, como son las relativas al proceso de copia de los datos intervenidos y las referentes al depósito de los efectos en un organismo adecuado, que examinamos a continuación.

6.1. La copia de los datos

De conformidad con lo dispuesto en el art. 588 sexies c.2 LECrim, 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 en condiciones que garanticen la autenticidad e integridad de los datos. Esta regla tendrá lugar, dispone el referido precepto, salvo que los dispositivos constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen.

Por ello, aunque en muchas ocasiones, principalmente cuando se traten de localizar datos concretos, no será necesaria la realización de copias, siendo suficiente con el registro del dispositivo, en los registros de dispositivos de almacenamiento masivo de información, lo más normal será el copiado de los datos; al igual que, obviamente por su propia naturaleza, con los registros remotos de equipos informáticos, salvo en aquellos casos en los que por la naturaleza del delito o por constituir el equipo informático el objeto o instrumento del delito, sea necesaria y así se acuerde la incautación.

Tal y como señala BENITEZ IGLESIAS, existen diferentes técnicas para realizar el copiado de datos de un equipo informático, como son: clonado, imagen y copia

---

preservar su integridad, «habría resultado más conveniente que la propia ley estableciera los elementos básicos para garantizar la autenticidad e integridad de los datos, no solamente para hacer posible un dictamen pericial, sino también para preservar la cadena de custodia». DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 390.

selectiva[886]. Siguiendo a este autor realizaremos unas consideraciones sobre estas modalidades de copia.

- En cuanto al clonado, también denominado «volcado», se trata de un proceso de copiado de la información contenida en un dispositivo, duplicándola bit a bit, por lo que supone la creación de una copia idéntica a la del dispositivo original, sin que este se vea alterado. Es el procedimiento ideal en los casos en los que se ha de practicar una pericial posterior, si bien presenta el inconveniente de tener que disponer de un dispositivo de, al menos, la misma capacidad, por cada dispositivo clonado, lo que supone un alto coste.

- La creación de una imagen es un proceso en el que también se procede al copiado íntegro de los datos, diferenciándose del clonado en la forma de almacenamiento de la información. Mientras en el clonado encontraríamos una estructura idéntica de archivos y carpetas, en la imagen se localizaría un único archivo que contendría, de forma comprimida, toda esa estructura de archivos y carpetas.

Este procedimiento tiene algunas ventajas respecto del clonado. La posibilidad de compresión conlleva que el dispositivo puede ser de menor capacidad que el de origen, así como que el archivo creado puede ser troceado e incluso almacenarlo en varios dispositivos de menor capacidad como DVD, lo que reduce los costes. Otra ventaja radica en la circunstancia de que cuando se realiza una imagen, se genera un archivo «log», que recoge información de los procesos realizados, el cual se almacena con la propia imagen, por lo que en todo momento se dispondrá de datos como los relativos a la herramienta, ya sea de software o hardware, que ha generado la imagen, identificación del dispositivo origen, identificación del dispositivo destino, tiempo que ha durado el procedimiento, etc.

- Finalmente, la copia selectiva supone duplicar únicamente la información que pudiera ser relevante para la investigación o la causa. Este procedimiento puede resultar necesario en casos en los que se tenga un tiempo limitado (un clonado o imagen puede durar horas e incluso días dependiendo del volumen y herramientas de las que se

[886] BENITEZ IGLESIAS, J. F., «La cadena de custodia: fuente de prueba de dispositivos informáticos y electrónicos», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2014, pp. 15-18, Consultadoen http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 25 de junio de 2020.

disponga); se encuentren dañados los equipos no pudiendo acceder a toda la información; o cuando existe un requerimiento judicial específico de acceder a determinados datos.

Aun cuando la copia selectiva tiene la ventaja de la economía en cuanto al tiempo empleado y la capacidad de almacenamiento de los dispositivos, presenta como inconvenientes la pérdida del resto de información, siendo muy probable que en caso de necesidad sobrevenida ya no fuera posible obtenerla.

Por lo que respecta a la forma de asegurar el material intervenido, de acuerdo con lo señalado por SANZ-GADEA GÓMEZ, «no basta con hacer el volcado, sino que es necesario verificar que el mismo se ha realizado con éxito, para lo cual existen métodos y procedimientos matemáticos que verifican que la información volcada en la copia es completa»[887]. Uno de estos procedimientos, que además preserva los datos ante posibles alteraciones, es la llamada «función *hash*»[888], la cual consiste en la obtención, mediante un programa informático, de un código alfanumérico denominado «código *hash*», de tal modo que cualquier alteración de los datos copiados, por pequeña que fuese, supondría la modificación del código.

En relación con este procedimiento, afirma GUDÍN RODRÍGUEZ-MAGARIÑOS que permite la realización de un resumen de la información contenida en una cadena de dígitos, y posibilita con ello identificar probabilísticamente un gran conjunto de información, de tal modo que «el hashing viene a hacer la función que el cotejo visual entre original y copia en los documentos tradicionales»[889].

---

[887] SANZ-GADEA GÓMEZ, J. B., «Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita», *Tirant Online, Documento TOL5.638.931*, 2015, p. 5.

[888] Siguiendo a ANGUAS BALSERA, «una "función de hash" es una función matemática que a partir de una entrada genera un código alfanumérico llamado «resumen de integridad» o sucintamente "hash", de forma que cualquier alteración de la entrada genera cambios significativos en el resultado de dicha función». Vid. ANGUAS BALSERA, J., «La pericial informática», en Abel LLuch, X. (coord.), *Tratado pericial judicial*, Las Rozas (Madrid), La Ley, 2014, p. 321.

[889] Dice además este autor que «la ventaja de la identificación de la información electrónicamente almacenada en un soporte informático a través del hashing es doble: en primer lugar permite identificar el contenido efectivo de la información, posibilitando así el acceso indiscriminado a su contenido sin riesgo para el documento original, y de otra parte, da a la información obtenida el tratamiento de verdadero documento, esto es, produce su virtualidad por si misma sin necesidad de una valoración jurídica ulterior». Vid. GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «Incorporación al proceso del material informático intervenido durante la investigación penal», *Boletín del Ministerio de Justicia*, n.º 2163, 2014, p. 5.

La LECrim guarda silencio respecto de estas cuestiones, y, de acuerdo con lo dispuesto en los arts. 588 sexies c.1 y 588 septies a.2 LECrim, queda a discreción del juez competente la decisión sobre cuestiones técnicas como el copiado y el aseguramiento de material informático, aspectos que requieren conocimientos específicos y que, por lo tanto, cuando menos en sus aspectos básicos deberían estar previstos.

Por ello, compartimos opiniones como la de LÓPEZ-BARAJAS PEREA cuando señala que «aquí es donde la Ley adolece de mayores insuficiencias lo cual resulta paradójico, dado que se trata de una cuestión delicada desde un punto de vista técnico y de gran trascendencia para su eficacia procesal»[890]. Consecuentemente estimamos que deberían ser regulados legalmente los criterios mínimos configuradores de estas actuaciones.

6.2. Presencia del letrado de la Administración de Justicia en las operaciones de volcado de un ordenador

De conformidad con los arts. 440, 453.1 y 459.1 LOPJ, los Letrados de la Administración de Justicia son funcionarios públicos que constituyen un Cuerpo Superior Jurídico, dentro de cuyas funciones se incluye el ejercicio de la fe pública judicial, en virtud de la que «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», teniendo encomendado el «depósito de los bienes y objetos afectos a los expedientes judiciales, así como del de las piezas de convicción en las causas penales, en los locales dispuestos a tal fin». No obstante, no tendrán esta última responsabilidad de depósito de los efectos del delito, respecto de «las excepciones que puedan establecerse reglamentariamente en cuanto al destino que deba darse a éstos en supuestos especiales».

En consonancia con estas funciones, y de conformidad con el art. 334 LECrim, al que ya nos referimos anteriormente, el letrado de la Administración de Justicia extenderá diligencia expresiva del lugar, tiempo y ocasión en que se encontraren efectos de cualquiera clase que puedan tener relación con el delito y se hallen en el lugar en que éste se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida,

[890] LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», cit., pp. 159-160.

describiéndolos minuciosamente para que se pueda formar idea cabal de los mismos y de las circunstancias de su hallazgo.

Con base en estos preceptos, se ha planteado si este funcionario debe encontrarse presente en el acto de copia de datos, lo cual ha sido defendido por algunos autores. Así, por ejemplo, VELASCO NUÑEZ considera necesaria su intervención, «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»[891]. Lo entiende de igual modo CUADRADO SALINAS, quien afirma que «para garantizar lo que el Tribunal Constitucional denomina "ausencia de manipulación externa del objeto intervenido", durante la diligencia de registro (ocupación, precintado, etiquetado, etc.) ésta deberá realizarse [...], en presencia del Secretario Judicial»[892].

Sin embargo el TS, de forma reiterada, ha venido declarando que la presencia del letrado de la Administración de Justicia no podría aportar ninguna garantía durante la operación del volcado de datos, habida cuenta de que, en principio, el referido funcionario es un profano en cuestiones informáticas avanzadas y ninguna garantía podría aportar su presencia[893].

En definitiva, ha declarado la STS 342/2013, de 17 de abril, FJ 8.º, «la presencia del fedatario judicial en el acto del volcado de datos no actúa como presupuesto de validez de su práctica» y añade que «lo decisivo es que, ya sea mediante la intervención

[891] VELASCO NÚÑEZ, E., «*Delitos tecnológicos: definición, investigación y prueba en el proceso penal*», cit., p. 90.

[892] No obstante, esta autora matiza su opinión al señalar que es lógico concluir que no será necesaria su presencia durante todo el proceso de clonado de datos «cuando estemos en presencia de grandes cantidades de datos digitales que conlleven un tiempo considerable para su clonado y deba hacerse por ello en el laboratorio, que no en sede judicial, por la naturaleza científica de dicho análisis». Vid. CUADRADO SALINAS, C., «Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa», cit., p. 6.

[893] Esta doctrina se inicia con la STS 1599/1999, de 15 de noviembre, que en su FJ 2.º declaró 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», añadiendo que «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». Posteriormente se han dictado otras resoluciones en el mismo sentido, como la STS 256/2008, de 14 de mayo, en la que se afirma que la presencia del letrado de la Administración de Justicia, «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»; y la STS 480/2009, de 22 de mayo, que hace suyos los pronunciamientos de las dos resoluciones anteriores.

de aquél 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».

Por nuestra parte, estimamos que con arreglo a los preceptos anteriormente citados y demás concordantes de la LECrim, el letrado de la Administración de Justicia deberá dejar testimonio, mediante la oportuna diligencia, de los dispositivos informáticos intervenidos tras una entrada y registro domiciliario o los que fueran puestos a disposición del tribunal tras una intervención policial fuera del domicilio, todo ello con una descripción de los mismos, quedando de este modo una adecuada constancia en autos de la naturaleza y cantidad de los equipos o instrumentos informáticos[894].

Respecto de la presencia de este funcionario durante la práctica del volcado de datos, es cierto que, por ser un profano en cuestiones informáticas[895], no podría certificar de forma plena que mediante el proceso que ha presenciado se ha procedido a la copia exacta de los datos intervenidos, por lo que, a semejanza de las dudas que podrían plantearse respecto de los efectos del delito que se encontrasen en una entrada y registro domiciliario sin que dicha localización la hubiera presenciado el letrado de la Administración de Justicia, estas podrían suscitarse acerca de los datos volcados.

Pueden plantearse dos casos:

- El primero de ellos tendría lugar con el copiado de datos en el mismo momento de la diligencia de registro domiciliario en presencia de este fedatario público o cuando un dispositivo concreto se haya intervenido fuera del domicilio y puesto a disposición del juzgado, siempre que se trate de una copia selectiva de datos que no plantee mayor

[894] Señala la Circular 5/2019 de la FGE que «aunque la intervención del letrado de la Administración de Justicia no sea necesaria durante el proceso de copiado, en ocasiones será preciso que garantice la identidad e integridad de la prueba extendiendo acta en el momento de desprecinto del dispositivo y comienzo del clonado, así como de la conclusión del mismo». Vid. FISCALÍA GENERAL DEL ESTADO, «*Circular 5/2019, sobre registro de dispositivos y equipos informáticos*», cit., p. 27.

[895] Dice a este respecto ANGUAS BALSERA que «la actuación del fedatario público no está exenta de inconvenientes, puesto que a las dificultades que pudiera tener para evaluar la integridad de los medios, herramientas o sistemas empleados en la acción hay que añadir la posible complejidad de las acciones a realizar por el perito y la dificultad que puede tener su debida observación, verificación y estricta documentación». Vid. ANGUAS BALSERA, J., «La pericial informática», cit., p. 324.

dificultad, en el entendimiento de que tratándose de un sencillo sistema de copiado y pegado que es conocido por cualquier ciudadano de nivel cultural medio, no existiría problema alguno en que el letrado de la Administración de Justicia pudiera certificar que se han copiado los datos efectivamente interesados.

No obstante, y sin perjuicio del conocimiento de estas cuestiones básicas informáticas, nos adherimos a opiniones como la de VELASCO NUÑEZ, cuando señala que «dada la complejidad técnica de la aprehensión de los muy volátiles e intrusivos elementos de convicción y prueba de los delitos informáticos, es importante que la diligencia de entrada, registro y confiscación sea practicada en compañía de algún experto perito en la materia»[896].

En este sentido, consideramos que lo ideal es que este experto sea un funcionario de la Administración de Justicia perteneciente a un cuerpo a crear de informáticos forenses, que, de forma similar a los médicos forenses o a los facultativos del Instituto Nacional de Toxicología, dotaría estas actuaciones de un mayor grado de seguridad e imparcialidad.

- El segundo supuesto sería aquel en el que por el volumen de la información a copiar, el proceso de volcado puede prolongarse horas e incluso días, siendo necesario que se practique en unas dependencias adecuadas, en cuyo caso no es viable que el letrado de la Administración de Justicia se encuentre presente durante todo el proceso.

En este caso, cobra quizás más fuerza la propuesta anterior, relativa a que estas tareas se realicen por informáticos forenses pertenecientes a un cuerpo técnico de la Administración de Justicia, llevándose a cabo en laboratorios especializados. Lo que acabamos de decir no debe empecer la tarea llevada a cabo por las FCSE, que merece todo nuestro respeto y que, consideramos debe mantenerse a los fines de investigación.

Pero lo cierto es que, tratándose del auxilio a los tribunales de justicia en materia probatoria, nos encontramos ante un campo como la informática, en constante avance, que desde hace un tiempo viene reclamando, de forma muy especial para los informes periciales en relación con la prueba digital, esta autonomía y especialización, las cuales estimamos necesarias y consideramos que con el transcurso de cierto tiempo, nos encontraríamos ante una figura funcionarial con un prestigio consolidado.

[896] VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales (1ª Parte)», *Revista de Jurisprudencia - El Derecho*, n.º 4, Febrero, 2009, p. 4.

6.3. Presencia del interesado y su defensa durante el volcado de datos

Se ha planteado cierta controversia en relación con la necesidad de que tanto el interesado como su letrado defensor se encuentren presentes durante el acto de volcado de datos, habiéndose instado la nulidad de la prueba en algún caso por no haber sido citados para dicho acto.

Resulta notorio que, cuando el registro se practique durante el transcurso de una diligencia de entrada y registro, en la mayoría de los casos se encontrará presente el investigado[897], pudiendo presenciar el proceso de copiado y pegado de los datos en otro soporte.

Pero no ocurre lo mismo en aquellos casos en los que resultase necesario un volcado completo de los datos una vez concluido el registro domiciliario, por no ser posible, por su complejidad y duración, realizarlo durante la diligencia de entrada y registro, debiéndose intervenir los dispositivos para la práctica del volcado en dependencias policiales o judiciales tras la aprehensión de los mismos.

Algunos autores, como FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, consideran que, partiendo de la no procedencia de la aplicación analógica de las normas de la LECrim para la detención y apertura de la correspondencia, que exigen la citación del interesado, «la presencia del investigado en la diligencia de volcado, en cuanto que no se toma ni aparta nada, sino que consiste meramente en la realización de la copia, no

[897] Debe tenerse en cuenta que de conformidad con el art. 569 LECrim, el registro se hará a presencia del interesado, o de la persona que legítimamente le represente, estableciendo que si no fuere habido o no quisiere concurrir, se practicará a presencia de un familiar mayor de edad, y en su defecto a presencia de dos testigos, disponiendo finalmente que la resistencia del interesado, de su representante, de los individuos de la familia y de los testigos, producirá la responsabilidad declarada en el CP a los reos del delito de desobediencia.
La jurisprudencia del TS ha declarado en relación con este precepto que «el imputado o la 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» y añade que «por ello es por lo que «la ley autoriza a prescindir del interesado "cuando no fuere habido"», señalando finalmente que «cuando el interesado está detenido su presencia es absolutamente necesaria». Vid. STS 284/2016, de 6 de abril, FJ 2.º

se justifica en dotar de mayor garantía a la operación de volcado»[898], añadiendo que «tampoco puede aducirse que exista el derecho de designar perito para tal diligencia», si bien otra cuestión es «el derecho de la parte a interesar que un perito de su elección analice posteriormente el contenido del dispositivo y realice una pericia»[899].

También el TS se ha pronunciado de forma similar sobre este particular, señalando que no es necesaria la presencia del interesado ni de su letrado, argumentando que la actividad de volcado no consiste en seleccionar archivos concretos, sino en realizar una copia, por lo que «la presencia del imputado, 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…»[900].

Sin embargo, hemos de mostrarnos críticos con estas opiniones, ya que consideramos que no se puede afirmar de forma concluyente que en la diligencia de volcado «no se toma ni aparta nada», por cuanto cabría la posibilidad de alterar algún archivo obrante en los dispositivos de almacenamiento, habida cuenta de que el letrado de la Administración de Justicia carece de conocimientos informáticos así como que tampoco interviene la figura de un funcionario del pretendido cuerpo de informáticos forenses.

Además, en nuestra opinión, sí que existe analogía con la detención y apertura de la correspondencia[901], ya que lo único que cambia es el tipo de soporte: papel o documento electrónico. Por tanto, disponiendo el art. 584 LECrim, que «para la apertura y registro de la correspondencia postal será citado el interesado» y que «este o la persona que designe podrá presenciar la operación», estimamos que, aunque el legislador no haya previsto dicho ofrecimiento al investigado, debería citarse al mismo para que, pueda presenciar la operación asistido de su letrado o un perito informático.

Por estas razones, nos parecen mucho más acertadas opiniones doctrinales como la de BONILLA CORREA, quien considera que aunque la presencia del interesado no sea

---

[898] FERNÁNDEZ-GALLARDO FERNÁNDEZ GALLARDO, J. Á., «Registro de dispositivos de almacenamiento masivo de información», *Dereito - Revista xurídica da Universidade de Santiago de Compostela*, vol. 25, 2016, p. 45.

[899] FERNÁNDEZ-GALLARDO FERNÁNDEZ GALLARDO, J. Á., «Registro de dispositivos de almacenamiento masivo de información», cit., p. 45

[900] Vid. ATS 425/2016, de 4 de febrero, FJ 1.º

[901] Vid. Arts. 579, 584 y 586 LECrim.

necesaria, este tiene derecho a participar en ella si lo desea, bien personalmente o a través de su letrado o un técnico, en la medida en que sea factible[902].

6.4. La necesidad de un órgano adecuado, encargado del depósito, custodia y análisis de los dispositivos electrónicos

Actualmente, como regla general, las piezas de convicción, incluidos los equipos y dispositivos informáticos, se custodian en las propias dependencias judiciales, normalmente en los propios archivos judiciales, los cuales se encuentran en muchos casos hacinados, careciendo de las medidas de seguridad necesarias para su adecuada conservación[903].

Como dice ANGUAS BALSERA, «la informática forense constituye un conjunto de técnicas orientadas a la adquisición, preservación y análisis de elementos indiciarios informáticos de una forma verificable y sólida, de manera que puedan ser introducidos en un procedimiento reglado de resolución de conflictos»[904]. Por tanto, la informática forense, además de la recogida y el análisis de las fuentes de prueba digitales, tiene por objeto su preservación y por ello se hace necesaria la adopción de medidas de seguridad para la protección y seguridad de la prueba digital y consecuentemente de los equipos informáticos. Así, por ejemplo, en relación con los teléfonos móviles, expertos informáticos, como RUBIO ALAMILLO, ponen de manifiesto la necesidad de aislarlos debidamente introduciéndolos en «bolsas especiales denominadas jaulas de Faraday»[905]. Este mismo autor, afirma en otro trabajo que «cualquier conexión que se produzca a un

[902] BONILLA CORREA, J. A., «Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio», *Diario La Ley - Sección Doctrina*, n.º 8522, 2015, p. 10.

[903] Cabe señalar que en los partidos judiciales de Madrid, Barcelona, Bilbao, Sevilla, Valencia y Zaragoza, por Real Decreto 2783/1976, de 15 de octubre y por Orden de 14 de julio de 1983, se crearon depósitos judiciales únicos con el fin de conservar de modo unificado las piezas de convicción.

[904] ANGUAS BALSERA, J., «La pericial informática», cit., p. 322.

[905] RUBIO ALAMILLO, J., «Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales», *Diario La Ley - Sección Ciberderecho*, n.º 22, 2018, p. 2. En la misma línea, afirma este autor en otro lugar que «para evitar esta contaminación, es necesario el uso de bloqueadoras de escritura, que son dispositivos que actúan como puente entre el disco duro o memoria y el ordenador, de tal forma que el disco o memoria nunca se conectan directamente al ordenador, sino a la bloqueadora, siendo ésta la que se conecta finalmente a la máquina. Así pues, la conservación de la cadena de custodia en discos duros y otros dispositivos de almacenamiento masivo es una tarea que debe realizarse con material forense especializado, capaz de clonar (que no copiar, que es un concepto distinto en Informática Forense), los discos duros de forma rápida y proporcionar un código hash al investigador, calculado a partir de un algoritmo de cifrado estándar». Vid. RUBIO ALAMILLO, J., «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Tribuna*, n.º 8662, 2015, p. 7.

ordenador de la evidencia (disco duro, memoria USB, dispositivo móvil, etc.), sin tomar las debidas precauciones, la contaminará de forma irremediable»[906].

Por otro lado, como señala SANZ-GADEA GÓMEZ para mantener la pureza del procedimiento forense y dado que la esterilidad de los medios y sistemas empleados en la técnica forense debe entenderse como una condición esencial para el inicio de cualquier procedimiento de análisis, «los medios técnicos a utilizar por los forenses informáticos deben estar certificados, de tal manera que no hayan sido expuestos a variaciones magnéticas, ópticas (laser) o similares, para evitar que las copias de las evidencias obtenidas puedas estar contaminadas […] un instrumental contaminado puede ser causa de una interpretación o análisis erróneo de una supuesta evidencia »[907].

Como podemos apreciar, son muchos los casos que justifican que el depósito y posterior análisis de los dispositivos informáticos contenedores de prueba digital se verifique en un organismo adecuado que asegure, con los medios apropiados, la integridad de las fuentes de prueba, así como la imparcialidad en el ejercicio de tales funciones.

Dijimos en el anterior apartado que el art. 459 LOPJ encomienda a los letrados de la Administración de Justicia el depósito de los efectos del delito. Sin embargo exceptúa los de aquellos en los que se disponga reglamentariamente la remisión al organismo competente.

En este sentido, consideramos que, por todas las razones expuestas, se hace necesaria la creación de una entidad a semejanza de los Institutos de Medicina Legal y Toxicología —aun con las evidentes diferencias—, que podría denominarse Instituto de Informática Forense, donde, sin perjuicio de las tareas llevadas a cabo en materia de investigación por la Policía Científica, se ejercerían las tareas de auxilio a los tribunales propias de la informática forense.

Como ya hemos señalado en alguna ocasión, la jurisprudencia ha señalado y el legislador así lo ha reconocido, al referirse en el apartado IV del preámbulo de la LO

[906] Dice este autor que «conectar a un ordenador la prueba sin precauciones, sería el equivalente a tomar el arma homicida del ejemplo anterior sin guantes». Vid. RUBIO ALAMILLO, J., «Conservación de la cadena de custodia de una evidencia informática», *Diario La Ley - Sección Doctrina*, n.º 8859, 2016, p. 2.

[907] SANZ-GADEA GÓMEZ, J. B., «Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita», cit., pp. 5-6.

13/2015 a los equipos informáticos, que «esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción» (efectivamente es así por el contenido que pueden albergar, de gran incidencia en los derechos fundamentales a la vida privada), pese a lo cual no se han establecido mecanismos que los aseguren debidamente.

Por ello, en atención a todo lo expuesto, estimamos que con la necesaria regulación que debería llevarse a cabo de la cadena de custodia, debería incluirse la creación de un organismo adecuado con la finalidad de auxiliar a los tribunales en las funciones jurisdiccionales de recogida, depósito y preservación de los equipos electrónicos y la prueba digital, como sería un Instituto de Informática Forense que se encontraría servido por un cuerpo de informáticos forenses, teniendo en cuenta principalmente que, aun cuando la prueba digital no tenga menos importancia que cualquier pieza de convicción que no se encuentre bajo la impronta de las TIC, existe un peligro de pérdida de la misma que no puede predicarse de otros efectos relacionados el delito.

V. Medios de prueba válidos para la incorporación al juicio oral de la prueba obtenida con los registros informáticos

1. Requisitos previos

Previamente a ocuparnos de los medios de prueba mediante los que podrá tener entrada la prueba digital en el proceso, hemos de referirnos a los requisitos previos para que el material intervenido pueda ser valorado por el tribunal. Estos presupuestos, se concretan en la puesta a disposición del tribunal del material intervenido y la proposición de prueba efectuada por la parte interesada, quien deberá indicar el medio probatorio mediante el que se procederá a su introducción en el juicio oral.

1.1. Puesta a disposición del tribunal del material intervenido

El material intervenido ha de ser puesto a disposición del tribunal, lo cual se verificará por la Policía Judicial, una vez realizadas las copias o el volcado de datos —aunque, como ya hemos indicado anteriormente, no existiría ningún obstáculo a que

dicha puesta a disposición tuviera lugar por el sugerido en este trabajo «Instituto de Informática Forense» con carácter previo a la celebración del juicio oral—[908].

Ha de tenerse en cuenta, de acuerdo con lo declarado por el TS, que, aunque en los autos de intervención telefónica se establece que el disco magnético u óptico original se pondrá a disposición judicial una vez finalizada la intervención o cuando se complete su capacidad, «ello no significa que el disco duro deba entregarse materialmente al Juzgado, sino que como medio de investigación judicial que ejecuta la policía, tales grabaciones permanecen en el disco duro hasta que la autoridad judicial ordene su borrado…», por lo que será suficiente con la entrega de una copia[909].

Se entregarán los soportes digitales como discos ópticos, discos duros, pen-drives, etc., aunque en aquellos casos en los que con el registro informático se hayan intervenido comunicaciones, ya sea por correo electrónico, programas de mensajería, redes sociales o una conversación grabada, habrá que estar a lo dispuesto en el art. 588 ter f) LECrim, donde se establece que la Policía Judicial pondrá a disposición del juez la transcripción de los pasajes que este considere de interés y las grabaciones íntegras realizadas, así como el art. 588 ter i), que establece las reglas para la incorporación a la causa de las grabaciones y transcripciones que se estimen procedentes y su traslado a las partes para que por estas se pueda interesar la inclusión de las comunicaciones que entienda relevantes y hubiesen sido excluidas, así como las referentes a la notificación a las personas intervinientes en las comunicaciones interceptadas[910].

---

[908] Vid. supra apdo. IV.6.4 de este capítulo, pp. 431-433.

[909] Vid. STS 492/2016, de 8 de junio, FJ 8.º, que añade a modo aclaratorio que «en cualquier momento del proceso es posible la verificación de la integridad de los contenidos volcados a los soportes CD/DVD entregados en el juzgado, mediante su contraste con los que quedan registrados en el Servidor Central del SITEL a disposición de la autoridad judicial. Contraste que puede realizar el juzgado en los correspondientes terminales para acreditar su identidad con la "matriz" del servidor central».

[910] El art. 588 ter i) LECrim, bajo la rúbrica «Acceso de las partes a las grabaciones», dispone lo siguiente:

1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso.

2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

1.2. Proposición de prueba

Atendiendo a la regla general inserta dentro del principio acusatorio que rige nuestro sistema procesal penal, y de acuerdo con lo establecido en el art. 728 LECrim, que dispone que «no podrán practicarse otras diligencias de pruebas que las propuestas por las partes…», se hace necesario que por las partes se proponga la prueba que estimen procedente. A este respecto, si bien el art. 729.2 LECrim dispone que se exceptúan de lo dispuesto en el artículo anterior «las diligencias de prueba no propuestas por ninguna de las partes, que el Tribunal considere necesarias para la comprobación de cualquiera de los hechos que hayan sido objeto de los escritos de calificación», se trata, como ha señalado la jurisprudencia del TS, de una norma que «constituye una excepción a la regla general y por ello de siempre se ha estimado que no puede ser objeto de interpretación extensiva por los Tribunales…»[911].

De tal modo que, de acuerdo con lo afirmado por RICHARD GONZÁLEZ, la prueba se practicará a instancia de parte, de modo que si las partes no la solicitaran, dando por buena la actuación policial, no será necesaria y no se practicará[912], señalando asimismo este autor que «del mismo modo corresponde al acusado impugnar cualquier circunstancia derivada de la actuación [...] poniéndolo de manifiesto tan pronto sea

---

3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia.

[911] Vid. SSTS 328/2001, de 6 de marzo, FJ 3.º y 881/2016, de 23 de noviembre, FJ 2º. Cabe señalar que el art. 729.2 ha sido objeto de una fuerte controversia doctrinal, siendo objeto de debate si el hecho de concederse la facultad al Tribunal de poder traer alguna prueba al proceso que no haya sido propuesta por las partes, estaría en contra del principio acusatorio y de un juez imparcial. Como quiera que se trata de un tema que no es objeto de nuestro trabajo, nos limitaremos a mantener su carácter excepcional conforme a lo declarado en las dos SSTS indicadas anteriormente, y en la misma línea, siguiendo a TOMÉ GARCÍA, estimamos que, como quiera que el art. 729.2 alude a la posibilidad excepcional de que el Tribunal acuerde de oficio pruebas para la comprobación de hechos ya introducidos por las partes en sus escritos de calificación provisional —por lo que el Tribunal no tiene potestad alguna en materia de aportación fáctica—, la utilización de dicha facultad no vulnera, en nuestra opinión, el principio acusatorio. Vid. TOMÉ GARCÍA, J. A., «Fase decisoria (II). La prueba», en De la Oliva Santos, A. y otros, *Derecho Procesal Penal*, Madrid, Editorial Universitaria Ramón Areces, 2007, p. 507.

[912] RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 297.

posible y como máximo al solicitar la práctica de prueba en el escrito de calificación (incluso cabría una alegación de esta clase al inicio del juicio oral)»[913].

La proposición ha de efectuarse en el proceso ordinario con la presentación del escrito de calificación provisional (art. 656 LECrim), y con la presentación de los escritos de acusación y defensa en el procedimiento abreviado, (arts. 781.1, II y III, y 784.1 y 2 LECrim), mientras que en el procedimiento para el enjuiciamiento de delitos leves la proposición se efectúa en el mismo trámite del juicio (art. 969 LECrim)[914].

Finalmente, la proposición de prueba, deberá realizarse con indicación del medio probatorio mediante el que se procederá a su práctica, lo que nos lleva al examen de los distintos medios de prueba.

2. Los medios de prueba

El art. 24.2 CE convirtió en un derecho fundamental el de utilizar los medios de prueba pertinentes en cualquier tipo de proceso en que el ciudadano se vea involucrado. En relación con el mismo, la jurisprudencia constitucional ha declarado que «este derecho fundamental, inseparable del derecho mismo a la defensa, consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el juez o Tribunal y, al haber sido constitucionalizado, impone una nueva perspectiva y una sensibilidad mayor

---

913 RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 297.

914 Afirma BARONA VILAR que esta regla general, en relación con los momentos procesales para la proposición de prueba, no es absoluta, sino que se han establecido diversas excepciones a la misma, diferentes según el procedimiento de que se trate. Así:

«a) Tanto en el procedimiento ordinario como en el abreviado el rigor preclusivo de proposición se ve mermado en la práctica de careos, en las pruebas de oficio, e incluso en la admisión de pruebas en el acto del juicio oral ofrecidas por las partes, cuando las considere admisibles el juzgador y siempre que puedan servir a los efectos de acreditar alguna circunstancia influyente en el valor probatorio de la declaración de un testigo (supuestos del art. 729). Excepción también se halla cuando aparecen nuevos hechos o nuevos elementos de prueba que requieren la suspensión de la vista y la apertura de una sumaria instrucción complementaria (art. 746.6). Finalmente, la petición en la vista de la lectura de la documentación de las diligencias de investigación que ampara el art. 730 también comportaría una excepción a la preclusión de la proposición de pruebas.

b) Con carácter específico, en el procedimiento abreviado, es posible, al inicio de la vista, solicitar la práctica de cualquier medio de prueba que se propongan para practicarse en el acto (art. 786.2). Es posible también que se solicite nueva prueba por la defensa en los supuestos de cambio de tipificación penal de los hechos o apreciación de mayor grado de participación o de ejecución de circunstancias de agravación de la pena, en las conclusiones definitivas (art. 788.4)». Vid. BARONA VILAR, S., «La prueba (I y II)», cit., p. 386.

en relación con las normas procesales atinentes a ello, de suerte que deben los Tribunales de Justicia proveer a la satisfacción de tal derecho, sin desconocerlo ni obstaculizarlo, siendo preferible en tal materia incurrir en un posible exceso en la admisión de pruebas que en su denegación»[915].

No obstante, adentrándonos en el tema que nos interesa, y siguiendo a FUENTES SORIANO, para dar acceso al proceso a las pruebas obtenidas de contenido digital a fin de examinar si pueden tener valor probatorio y, en tal caso, qué valor probatorio pueden alcanzar, valor «resultará imprescindible traer al ámbito de la tecnología digital la clásica distinción entre fuentes y medios de prueba»[916].

Esta distinción la realizó CARNELUTTI, llamando medio de prueba «a la actividad del juez mediante la cual busca la verdad del hecho a probar», mientras que denomina fuente de prueba «al hecho del cual se sirve para deducir la propia verdad»[917].

Por su parte, MONTERO AROCA escribe que con la expresión fuente de prueba nos estamos refiriendo a un concepto extrajurídico, a una realidad anterior al proceso, mientras que los medios de prueba aluden a conceptos jurídicos, y sólo existen en el proceso, en cuanto en él nacen y se desarrollan, de tal modo que «la fuente es anterior al proceso y existe independientemente de él; el medio se forma durante el proceso y pertenece a él»[918].

En este sentido, afirma FUENTES SORIANO, la fuente de prueba vendrá constituida por una información ajena al proceso, mientras que el medio de prueba será el mecanismo, instrumento o procedimiento, específicamente arbitrado por el ordenamiento para introducir válidamente dicha información en el proceso[919]. Por tanto, se hace necesario distinguir entre la información que proporcionarán las fuentes de prueba digitales obtenidas como consecuencia de un registro informático, y el procedimiento establecido para la válida incorporación de dichas fuentes de prueba al proceso.

---

[915] Vid. STC 30/1986, de 20 de febrero, FJ 8.º

[916] FUENTES SORIANO, O., «Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías», *Revista General de Derecho Procesal*, n.º 44, 2018, p. 18.

[917] CARNELUTTI, F., *La prueba civil*, (Trad. ALCALÁ ZAMORA Y CASTILLO) Buenos Aires, Ediciones Depalma, 1982, pp. 70-71.

[918] MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», cit., p. 45.

[919] FUENTES SORIANO, O., «Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías», cit., p. 18.

Cualquiera de los medios probatorios establecidos en la LECrim, son apropiados para la válida incorporación de la prueba digital. Por tanto, los datos obtenidos tras un registro informático, podrán incorporarse a través del interrogatorio del acusado, la testifical, la pericial, la documental y el reconocimiento judicial[920]. A ellos hay que añadir, de acuerdo con lo previsto en el art. 299.2 LEC, de aplicación supletoria al proceso penal, la reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

Una vez que, tras la proposición efectuada por una de las partes, hayan tenido entrada las fuentes de prueba en el proceso por alguno de estos medios y, siendo admitidas por el tribunal, se practiquen en el juicio oral con respeto a los principios de contradicción, oralidad, inmediación, concentración y publicidad, nos encontraremos ante un auténtico acto de prueba con virtualidad para enervar la presunción de inocencia. Realizaremos algunas consideraciones en relación con los medios de prueba citados.

2.1. El interrogatorio del acusado

Dice MORENO CATENA que «la declaración del acusado en el juicio oral no es propiamente un verdadero interrogatorio, sino, como dijo acertadamente hace muchos años GÓMEZ ORBANEJA, un medio de defensa, que permite a los acusados tomar posición frente a la acusación y a las pruebas de que ésta se valga»[921], añadiendo que, «por eso, el nombre adecuado a este medio de prueba es el de declaración, en cuanto no

[920] Estos medios de prueba se mencionan en el título III del libro III, dedicado al Juicio Oral (arts. 688 a 727). En relación con los mismos, afirma GIMENO SENDRA que nos encontramos ante una regulación parcial y deficiente, habiéndose de integrar sus preceptos con las normas relativas a los correspondientes actos de investigación, que se contienen en su libro II («del sumario»). Así, continúa el citado autor, las declaraciones del acusado se encuentran huérfanas de regulación legal en esta sede del juicio oral, debiéndose de aplicar directamente las normas relativas a las declaraciones indagatorias y lo mismo acontece con el reconocimiento judicial, al que la LECrim le dedica un solo precepto (art. 727). La prueba documental se despacha con dos preceptos (los arts. 726 y 730) y la pericial con tres (los arts. 723-725), por lo que también hay que suplir esta laguna con las disposiciones pertinentes de la fase instructora. El único medio de prueba, que ostenta alguna exhaustividad es la testifical (arts. 701-722), si bien también son muchos los preceptos relativos a las declaraciones de testigos en la instrucción, cuya aplicación también resulta reclamable en el juicio oral. Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 581.

[921] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 450.

se trata con él de fijar la verdad de los hechos, sino de dar la posibilidad al acusado de posicionarse en el juicio»[922].

Afirma, además, el citado autor que «es evidente, en este sentido, que la declaración del acusado en el juicio oral ni reúne las características propias de verdadero medio de prueba, ni tiene nada que ver con la confesión que regula la LECrim en los arts. 688 y ss.; estas normas hacen referencia a la confesión del acusado bien de los hechos objeto de acusación, bien a las penas solicitadas, regulando la conformidad; se trata [...] de una cierta manifestación del poder de disposición del acusado sobre el objeto del proceso penal»[923].

Una mención parecida la realiza JIMÉNEZ CONDE, quien, tras señalar que la LECrim no regula este medio de prueba en el juicio oral, ya que solo alude, en los arts. 688 a 700 LECrim, a «la confesión de los procesados» —con la circunstancia de que la conformidad del acusado no es operativa en el proceso ordinario, previsto para penas superiores a nueve años de prisión—, matiza que «esta censurable omisión de la LECrim se ha suplido por la práctica forense con la aplicación supletoria las normas del sumario relativas a "las declaraciones de los procesados" (arts. 385 y ss.), pero respetando los principios propios del juicio oral»[924].

No obstante lo anterior, de acuerdo con lo apuntado por TOMÉ GARCÍA, «a pesar de la laguna existente, tanto la doctrina como nuestros Tribunales vienen considerando la declaración o interrogatorio del acusado como primera prueba a practicar»[925].

En este sentido, entendemos que, tal y como ha declarado el TS —que desestimó un recurso de casación interpuesto por el acusado condenado, dado que el mismo declaró ante la policía y ante el Juzgado con el más absoluto laconismo—, «aunque es verdad que nuestra Constitución ha elevado a derechos fundamentales del inculpado el

---

[922] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 450.

[923] Aclara igualmente este autor que «la declaración del acusado propiamente dicha es una manifestación de ciencia y de voluntad cuyo fin es posicionarse en el propio juicio: en primer lugar, puede negarse a prestar declaración si lo considera oportuno, en el ejercicio de su derecho fundamental (art. 24.2 CE), sin que esta opción pueda acarrearle consecuencia perjudicial alguna; en segundo lugar, puede declarar o responder sólo a las preguntas que entienda convenirle, utilizando ese momento esencialmente como un mecanismo de defensa, es decir, aportando la información que considere favorable a su posición procesal». Vid. MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 450.

[924] JIMÉNEZ CONDE, F., «*Introducción al Derecho Procesal Penal*», cit., p. 131.

[925] TOMÉ GARCÍA, J. A., «Fase decisoria (II). La prueba», en De la Oliva Santos, A. y otros, *Derecho Procesal Penal*, Madrid, Editorial Universitaria Ramón Areces, 2007, p. 491.

de guardar silencio, es decir no declarar, a no declararse o confesarse culpable a no prestar juramento y en definitiva a defenderse mintiendo», no es menos cierto que, «cuando ya existe la prueba objetiva contra él, su silencio, omitiendo dar convincentes explicaciones de su comportamiento, pueden privar al Tribunal de los elementos precisas para reinstaurar la presunción de inocencia que había desaparecido»[926].

En efecto, esta doctrina encaja perfectamente en el contexto en el que nos encontramos, dado que, una vez obtenidos los datos tras la ejecución de un registro informático, existe un principio de prueba objetiva contra el acusado, que no podrá ser anulado por el silencio o respuestas evasivas del acusado.

Han de plantearse asimismo en este punto, aquellos casos en los que hay varios acusados, y uno de ellos reconoce los hechos, mientras que otro u otros no lo hacen, o en su caso, incriminan a cualquiera de los demás en su declaración. En relación con este tema, el TC no ha mantenido un criterio firme. Así, en un primer momento, admitió las declaraciones de los coimputados equiparándolas a la prueba testifical y, por tanto, constituyendo «un dato a tener en cuenta por el tribunal al ponderar la credibilidad que le merezca»[927]. Posteriormente declaró de forma reiterada que «las declaraciones de los coimputados carecen de consistencia plena como prueba de cargo cuando, siendo únicas, no resultan mínimamente corroboradas por otras»[928]. Y finalmente admitió la declaración de un coimputado al entender que la misma quedaba corroborada, no por otras pruebas, sino por la declaración de otro coimputado avalada por datos periféricos[929].

Se trata de una cuestión controvertida en la que existen diversas opiniones doctrinales[930], habiéndose instado por autores partidarios de la necesaria corroboración

---

[926] Vid. STS de 21 de junio de 1985 - ROJ: STS 1180/1985, Considerando 3.º

[927] Vid. STC 137/1988, de 7 de julio, FJ 4.º

[928] Vid. por todas SSTC 34/2006, de 13 de febrero, FJ 2.º; 230/2007, de 5 de noviembre, FJ 3.º; y 102/2008, de 28 de julio, FJ 3.º

[929] Vid. STC 56/2009, de 9 de marzo, FJ 3.º. Cabe destacar que en esta resolución se dictó un voto particular considerando que la declaración del coimputado no se encontraba debidamente corroborada por otras pruebas de conformidad con la doctrina anterior del TC.

[930] En relación con las declaraciones contradictorias de los coimputados y su valoración probatoria pueden consultarse las siguientes obras: DÍAZ PITA, M. P., *El coimputado*, Valencia, Tirant Lo Blanch, 2000; DE LA ROSA CORTINA, J. M., *Confesiones. Declaraciones de imputados y acusados. Coimputados, testigos imputados y testigos condenados*, Cizur Menor (Navarra), Editorial Aranzadi, 2012; SÁNCHEZ YLLERA, I., «Dudas razonables: la declaración de los coimputados», *Revista Xurídica Galega*, n.º 50, 2006; y

de la declaración del coimputado por otras fuentes de prueba, que «el legislador plasme con claridad esta regla probatoria partiendo del principio de la insuficiencia de la declaración del coimputado salvo que la misma venga corroborada en cuanto al aspecto específico de la participación en los hechos por otras fuentes probatorias autónomas»[931].

En todo caso, por lo que a la prueba digital se refiere, consideramos que la misma quedará válidamente incorporada al acervo probatorio con el reconocimiento por el acusado o cualquiera de los acusados, una vez preguntado o preguntados en el acto de juicio oral, de la veracidad de los datos electrónicos obtenidos.

De este modo, con este reconocimiento y la incorporación de la prueba digital mediante la documental —o los medios de reproducción de la palabra, el sonido, la imagen e instrumentos de archivo, a los que más adelante nos referiremos—, consideramos, sin perjuicio de la libre valoración de la prueba por el Tribunal, que nos encontraríamos ante una fuente de prueba debidamente introducida en el juicio oral, con virtualidad para enervar la presunción de inocencia.

2.2. La testifical

De acuerdo con la terminología empleada por la LECrim, la prueba de examen de los testigos, se encuentra regulada de los arts. 701 a 722 de dicho texto legal, en los que se regula detalladamente el procedimiento a seguir, para la práctica de las testificales en el juicio oral, estableciendo unas reglas independientes de las establecidas para las declaraciones de los testigos en fase de instrucción (arts. 410-450 LECrim).

Siguiendo a GIMENO SENDRA, por prueba testifical ha de entenderse «la declaración de conocimiento efectuada por personas físicas que, sin participar en él, conocen de la comisión del hecho punible, bien directamente (testigos directos) o por referencias (testigos indirectos)»[932].

MIRANDA ESTRAMPES, M., «La declaración del coimputado como prueba de cargo suficiente: análisis desde la perspectiva de la doctrina del TC. (Radiografía de un giro constitucional involucionista)», *Revista Xurídica Galega*, n.º 58, 2008.

[931] MIRANDA ESTRAMPES, M., «La declaración del coimputado como prueba de cargo suficiente: análisis desde la perspectiva de la doctrina del TC. (Radiografía de un giro constitucional involucionista)», cit., p. 24.

[932] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 583.

En este sentido, las personas que hayan tenido contacto con el material intervenido o que por cualquier otra circunstancia tengan conocimiento del contenido del mismo, deberán someterse a las preguntas que, con respeto al principio de contradicción, le sean formuladas por las partes, siempre que sean propuestos como testigos por cualquiera de ellas.

Cabe señalar que, en determinadas ocasiones, será necesaria la declaración como testigos de los agentes de la Policía Judicial que intervinieron en el registro informático, a fin de corroborar de forma adicional la existencia de datos o archivos electrónicos incriminatorios, especialmente en los supuestos de registros remotos de equipos informáticos en los que la testifical de los agentes, entendemos que resulta indispensable para el esclarecimiento de los hechos, así como para ilustrar al tribunal enjuiciador, sobre cualquier aclaración que resulte necesaria en cuanto a la forma de acceso a los equipos, aprehensión de los datos y el software mediante el que se ejecutó el control de la información [art. 588 septies a.2 b) LECrim].

Finalmente, aunque lo normal es que la testifical sirva como prueba complementaria, podría darse el caso de que la prueba testifical sea el único medio para demostrar la existencia de la prueba digital, lo cual puede ocurrir en caso de que la prueba digital obtenida se extraviase o desapareciese, situación en la que la que sería fundamental la declaración de los agentes de la Policía Judicial u otras personas que conociesen su contenido.

2.3. Los medios de reproducción de la palabra, el sonido, la imagen e instrumentos de archivo.

Dice VELASCO NUÑEZ que si un correo electrónico (aquí lo hacemos extensivo a cualquier prueba digital) se introduce en el juicio oral mediante una testifical, nos encontramos con el inconveniente «de generar un grado de convicción menor, seguramente, que si se tuviese delante el soporte original»[933].

Ya hemos dicho anteriormente que, sin perjuicio de que en casos excepcionales la testifical sirva con exclusividad para la introducción de la prueba digital en el juicio oral, lo normal es que esta se use con carácter suplementario y, en este sentido, no es

[933] VELASCO NÚÑEZ, E., «Correo electrónico, SMS y virus troyanos: aspectos procesales penales», cit., pp. 26-27.

difícil advertir que la reproducción en el acto de juicio oral de la palabra, el sonido, la imagen e instrumentos de archivo, es el medio de prueba genuino para que la prueba digital tenga entrada en el proceso, logrando con el mismo un mayor grado de convencimiento del tribunal sobre la verdad material que con cualquier otra fuente de prueba.

No cabe duda de que, con la reproducción en el acto del juicio de las fotografías, audios o vídeos que hubieran sido intervenidos, el principio de inmediación judicial cobrará su máxima expresión, por cuanto no existe otro modo más fiable de que el tribunal tenga un contacto directo con la prueba que la reproducción en el juicio de los documentos electrónicos.

En este punto, resulta de gran interés la opinión de BUJOSA VADELL, quien señala, refiriéndose a la prueba videográfica (aplicable igualmente al audio y la imagen), que coincidiendo con la reproducción en el juicio oral, «aparte de las consideraciones de adecuación técnica pertinentes, son importantes las consideraciones que las partes quieran exponer acerca de la regularidad de esta prueba […], irregularidades o manipulaciones que puedan impedir, limitar o condicionar la valoración probatoria, o incluso de presentar interpretaciones que se puedan derivar de las imágenes que se emiten, con el fin de influir en esa valoración»[934].

Sin embargo, nuestra LECrim, por razones obvias si se tiene en cuenta el estado de la técnica a finales del siglo XIX, nada establece en cuanto a la posibilidad de la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo en el acto del juicio oral, por lo que es necesario acudir a la legislación supletoria, como es la LEC, que tras fijar en art. 299.1 los medios de prueba de los que se podrá hacer uso en juicio, dispone en su art. 299.2 que «también se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

Esta lógica omisión del legislador decimonónico no es óbice para que, ya en el siglo XXI, teniendo en cuenta las modificaciones de las que ha sido objeto la LECrim, y muy especialmente la operada por la LO 13/2015, de 5 de octubre, de modificación de la

[934] BUJOSA VADELL, L. M., «Tecnologías de la imagen y valoración de la prueba», cit., p. 229.

Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, se hubiera incluido en la Ley procesal una regulación en cuanto a la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo. Por otro lado, no resulta comprensible que habiéndose abordado este tema en el Anteproyecto de LECrim de 2013 —donde se establecía un procedimiento para que, si era instado por las partes se procediese a la audición o el visionado del contenido de soportes de datos que no se limitasen a almacenar información escrita—[935], el legislador no lo tuviese finalmente en consideración con la reforma de 2015.

Asimismo, ha de tenerse en cuenta que la LO 7/2015, de 21 de julio, por la que se modifica la LO 6/1985, del Poder Judicial, vino a dar una nueva redacción al art. 230 LOPJ, y en su apartado 1.º, donde decía que «los Juzgados y Tribunales y las fiscalías podrán utilizar…» pasó a disponer que «… 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».

Esta carencia legislativa viene provocando que, en numerosas ocasiones, como consecuencia de la ingente carga de trabajo que sufren nuestros tribunales, y la escasez de medios electrónicos que permitan la simultánea grabación del acto de juicio y la reproducción de imagen, audio y video, se opte por la incorporación al juicio mediante

[935] Concretamente el art. 462 del Anteproyecto de LECrim de 2013, disponía en su apartado segundo que «a petición del Fiscal o de cualquiera de las partes, los documentos y efectos a que se refiere el apartado precedente podrán ser exhibidos durante el interrogatorio de los testigos y del encausado o en el transcurso del informe pericial. Del mismo modo, podrá procederse a la lectura, visionado o audición de cualesquiera otras fuentes de prueba». Y el art. 463, bajo la rúbrica «alegaciones de las partes sobre los documentos y las piezas de convicción y petición de reproducción de sonidos o imágenes», establecía que: «1. Concluida la práctica de las pruebas personales de la acusación, el Magistrado o Presidente del Tribunal preguntará a las partes acusadoras si desean formular alguna alegación sobre los documentos, soportes de datos y demás fuentes de prueba designados como prueba de cargo y que consideren relevantes para respaldar sus pretensiones, concediéndoles, en su caso, un breve turno de intervención, en el que las partes acusadoras podrán solicitar la audición o el visionado del contenido de soportes de datos que no se limiten a almacenar información escrita.
2. Concluida la práctica de las pruebas personales de la defensa se procederá respecto a las partes pasivamente legitimadas del mismo modo previsto por el apartado anterior respecto a la prueba de descargo».

otros medios de prueba que, aun cuando son totalmente válidos, no son tan determinantes para el convencimiento del tribunal como la reproducción en juicio.

Por ello, estimamos que, *de lege ferenda*, debería llevarse a cabo una minuciosa regulación para el proceso penal, del medio de prueba consistente en la reproducción de la imagen, el audio y el video que, en todo caso, hiciese necesaria la incorporación de la prueba digital por este medio, al menos cuando así lo solicitase alguna de las partes.

2.4. La documental

La prueba documental se encuentra prevista en la LECrim en un solo precepto, el art. 726, De acuerdo con él, «el Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad».

Siguiendo a ASENCIO MELLADO, se entiende por documento «toda representación realizada por cualquier medio -escrito, hablado, visionado etc.-, de la realidad y que preexiste al proceso y es independiente de él, de manera que se aporta al mismo con fines esencialmente probatorios»[936], definición que comprende al documento electrónico, al que ya nos referimos al ocuparnos de la prueba digital[937].

Del mismo modo que para la prueba documental en general, para la prueba digital, la documental puede ser pública o privada.

Nos encontraremos ante una documental pública cuando los archivos de imagen, audio o video se incorporen a un soporte electrónico como un disco duro, pen drive o DVD, bajo la fe pública de un notario o del letrado de la Administración de Justicia, o asimismo cuando se proceda a la impresión en papel de documentos electrónicos como un correo electrónico, conversación de whatsapp, imagen, o se transcriba un archivo de audio, debidamente cotejados bajo la misma fe pública.

La documental será privada cuando el documento sea aportado por un particular y, tal y como señala VELASCO NUÑEZ, en tal caso «ante la inexistencia de intervención de fedatario público en su adquisición, el mero texto y datos deberán ser adverados por su conseguidor, que deberá, caso de duda o negación, declarar contradictoriamente sobre

[936] ASENCIO MELLADO, J. M., «*Derecho Procesal Penal*», cit., p. 155.
[937] Vid. supra apdo. II.2.3 de este capítulo, pp. 339-341.

este extremo en el acto de la vista oral, convirtiendo la prueba en una mezcla de documental y testifical»[938].

En todo caso, en el proceso penal, como veremos en el último epígrafe de este capítulo dedicado a la impugnación y valoración de la prueba, y a diferencia del proceso civil donde la documental pública tiene el carácter de prueba tasada[939], rige el principio de libre valoración de la prueba tanto para la documental pública como para la privada.

Ahora bien, sin perjuicio de lo anterior, resulta relevante en el contexto que nos ocupa la distinción entre los documentos que se incorporan como actos de investigación al procedimiento instructor (sumario o diligencias previas) y los que son aportados o reclamados a alguna entidad pública o privada en fase de juicio oral.

El primer supuesto será la práctica habitual cuando se lleve a cabo una diligencia de registros informáticos, en cuyo caso nos encontraremos ante una prueba preconstituida del juez de instrucción[940] que, generalmente, será incorporada al proceso mediante la lectura de las diligencias sumariales prevista en el art. 730 LECrim.

El segundo supuesto se produce frecuentemente cuando en los escritos de acusación o defensa, por alguna de las partes, se aporta algún documento (ya sea en papel o electrónico) o se solicita que se reclame por medio de la oficina judicial (art. 781.1.II LECrim); pero también pueden introducirse al inicio de las sesiones del juicio oral (art. 786.2 LECrim)[941] e incluso dentro del juicio oral, tal y como indica el art.

---

[938] VELASCO NÚÑEZ, E., «Correo electrónico, SMS y virus troyanos: aspectos procesales penales», cit., p. 26.

[939] No está de más recordar que cuando hablamos de «prueba tasada» también denominada «prueba legal» nos estamos refiriendo a un sistema de valoración de la prueba que consiste en vincular al juzgador a una valoración preestablecida, es decir, a un efecto que ya está determinado para un concreto medio probatorio. En el proceso civil, la documental pública es prueba tasada de acuerdo con lo establecido en el art. 319.1 LEC, que bajo la rúbrica «fuerza probatoria de los documentos públicos» dispone que «con los requisitos y en los casos de los artículos siguientes, los documentos públicos comprendidos en los números 1.º a 6.º del artículo 317 harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella».

[940] Vid. supra apdos. II.3.3.3 y II.3.3.4 de este capítulo, pp. 352-354.

[941] Afirma GIMENO SENDRA que la la aportación de algún documento al inicio de las sesiones del juicio oral de acuerdo con el artículo 786.2 LECrim, aunque se refiere al procedimiento abreviado, «en la práctica forense, se ha generalizado a todos los procedimientos». Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 588.

729.3.º LECrim, «para acreditar alguna circunstancia que pueda influir en el valor probatorio de la declaración de un testigo».

Finalmente, tal y como señala MORENO CATENA, «la prueba documental, por su propia naturaleza, no requiere de la oralidad para transmitir al juzgador la información que la fuente de prueba contiene»[942], dado que de conformidad con el art. 726 LECrim deberá examinarla por sí mismo, rigiendo por tanto la regla del «examen de oficio»[943]. En cualquier caso «la garantía de la práctica de este medio de prueba es la inmediación, por supuesto, y la contradicción, de modo que será necesario dentro del juicio oral abrir el debate procesal sobre estas fuentes de prueba»[944].

2.5. La lectura de las diligencias sumariales del art. 730

Como ya hemos tenido oportunidad de comentar anteriormente, rige en el proceso penal el principio proclamado en el art. 741 LECrim, conforme al que las pruebas han de practicarse en el juicio oral. Sin embargo, el art. 730 establece una excepción al mismo, al disponer que «podrán también leerse o reproducirse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independientes de la voluntad de aquéllas, no puedan ser reproducidas en el juicio oral, y las declaraciones recibidas de conformidad con lo dispuesto en el artículo 448 durante la fase de investigación a las víctimas menores de edad y a las víctimas con discapacidad necesitadas de especial protección».

Con este precepto se da cobertura a la doctrina de la prueba instructora anticipada y a la prueba preconstituida. Por tanto, en aquellos casos de «imposible o muy difícil práctica» en el acto del juicio oral, podrán constituir prueba de cargo tanto las diligencias de investigación practicadas en la instrucción, como las declaraciones de testigos o peritos que, en los términos ya estudiados[945], se hubieran llevado a cabo como prueba instructora anticipada.

No obstante, en todo caso, para que dichas actuaciones adquieran fuerza probatoria, no será válida la fórmula de «tener por reproducidas» las mismas, sino tal y como reza el art. 730 LECrim, deberán leerse o reproducirse (en caso de que se trate de

---

[942] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 471.
[943] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 588.
[944] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 471.
[945] Vid. supra apdo. II.3.3.2.1 de este capítulo, pp. 348-350.

imagen, audio o video) en el acto de juicio oral, respetando el principio de contradicción.

En cuanto al fundamento de la lectura, afirma ASENCIO MELLADO que «se halla en la necesidad de que el proceso penal como tal alcance sus fines propios de descubrimiento y sanción en su caso de los hechos delictivos, así como igualmente, y en este mismo marco, el allegar al Tribunal sentenciador todo el material y datos accesibles que le permitan formarse una convicción completa y no sesgada»[946].

Centrándonos en el tema de los registros informáticos, es frecuente con los mismos la intervención de archivos de imagen, audio o video, pero también documentos de texto como, por ejemplo, un mensaje de correo electrónico. Asimismo, en numerosas ocasiones se procede a la impresión de pantallazos de mensajes emitidos o recibidos a través de las redes sociales con programas como «Whatsapp, Facebook, Twiter, etc.», que se aportan como documental, o incluso a la transcripción de pasajes concretos de archivos de audio, en ambos supuestos cotejados bajo la fe pública del letrado de la Administración de Justicia, y que, de acuerdo con lo ya estudiado, se convierten en prueba documental preconstituida.

Por otro lado, puede darse el caso de que la descripción de la intervención, así como el contenido de mensajes o audios —siempre que hubieran sido obtenidos conforme a resolución judicial dictada de acuerdo con los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad—, sean plasmados por la Policía Judicial en el atestado policial.

A este respecto, ha de tenerse en cuenta, siguiendo la puntualización de RODRÍGUEZ FERNÁNDEZ, que «el art. 730 se refiere únicamente a "las diligencias practicadas en el sumario", y no, por tanto, a las realizadas ante la Policía en el atestado»[947]. Por tal razón, señala que «las declaraciones obrantes en el atestado, no ratificadas ante el juez instructor, de imposible reproducción en el juicio oral, no pueden ser leídas al amparo del art. 730»[948], para concluir que «la única forma de introducir tales declaraciones como material probatorio valorable por el Tribunal sentenciador sería

[946] ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., pp. 177-178.

[947] RODRÍGUEZ FERNÁNDEZ, R., «Prueba preconstituida y prueba anticipada. Análisis jurisprudencial», *Diario La Ley - Sección Doctrina*, n.º 8487, 2015, p. 8.

[948] RODRÍGUEZ FERNÁNDEZ, R., «Prueba preconstituida y prueba anticipada. Análisis jurisprudencial», cit., p. 8.

mediante la declaración, en el juicio oral, como testigo de referencia del agente de policía que tomó la declaración»[949].

Con base en lo indicado anteriormente, aun cuando la reproducción de la imagen, el audio y el vídeo en el acto del juicio oral, es la forma idónea para introducir la prueba digital en el proceso penal, también es cierto, como igualmente hemos dicho, que ante la ingente carga de trabajo que sufren nuestros tribunales, y la escasez de medios electrónicos que permitan la simultánea grabación del acto de juicio y la reproducción de imagen, audio y video, se opte en numerosos casos por la incorporación al juicio mediante la lectura de documentos, como así se produce, tal y como acabamos de exponer, con los resultados de determinados registros informáticos.

En estos casos opera plenamente el art. 730 LECrim y, por tanto, siempre que se respete lo establecido en este precepto, los documentos impresos podrán constituir prueba válidamente incorporada al proceso y fundar una sentencia condenatoria. Cabe señalar que la jurisprudencia del TS, en relación con la transcripción de las intervenciones telefónicas —aplicable a los documentos electrónicos en general, ya sean de texto, imagen, audio o video— ha declarado que «…como medio de prueba plena en el juicio deberá ser introducido en el mismo regularmente, bien mediante la audición directa del contenido de las cintas por el Tribunal, fuente original de la prueba, mediante la lectura en el juicio de las transcripciones, diligencia sumarial documentada, previamente cotejadas por el Secretario con sus originales, e incluso por testimonio directo de los agentes encargados de las escuchas»[950].

Ahora bien, reiteramos para concluir, que la lectura de los documentos en el juicio oral deberá realizarse con respeto a los principios de publicidad, oralidad, inmediación, contradicción y concentración, y en tal sentido se verificará, de acuerdo con lo expresado por MUERZA ESPARZA, «no como una simple fórmula retórica y de estilo, sino en condiciones que permitan a las partes someterlas a contradicción evitando formalismos de frecuente uso forense, todo ello con el fin, precisamente, de permitir a la

[949] En relación con esta afirmación, cita el autor la STC 217/1989, de 21 de diciembre. Vid. RODRÍGUEZ FERNÁNDEZ, R., «Prueba preconstituida y prueba anticipada. Análisis jurisprudencial», cit., p. 8.

[950] Vid. SSTS 363/2008, de 23 de junio, FJ 2.º, en la que se citan las SSTS 807/2001, de 11 de mayo; 1778/2001, de 3 de octubre; 112/2002, de 17 de junio; y 1070/2003, de 22 de julio.

defensa del acusado someter las actuaciones sumariales a una efectiva contradicción en el acto de la vista»[951].

2.6. La inspección ocular

Como medio de prueba, la LECrim se refiere a la inspección ocular en el art. 727, que establece las reglas procedimentales, distinguiendo si el objeto del reconocimiento se encontrase en el lugar del juicio[952] o fuera de él, y estableciendo que, en el primer caso, «se constituirá el Tribunal con las partes, y el Secretario extenderá diligencia expresiva del lugar o cosa inspeccionada, haciendo constar en ella las observaciones de las partes y demás incidentes que ocurran», mientras que si el lugar estuviese fuera del lugar del juicio «se constituirá en él con las partes el individuo del Tribunal que el Presidente designe, practicándose las diligencias en la forma establecida en el párrafo anterior».

Sin embargo el art. 727 LECrim, remite para todo lo demás, a lo dispuesto en el título V, capítulo I, del libro II, es decir a los arts. 326 a 333, dedicados a la inspección ocular en fase de instrucción dentro de las diligencias de comprobación del delito y averiguación del delincuente.

Siguiendo a GÓMEZ COLOMER, «la inspección ocular es en el proceso penal lo que el reconocimiento judicial es en el proceso civil[953] […] mediante este acto de investigación, el juez realiza una comprobación personal del lugar de los hechos, observando lo ocurrido y describiéndolo, además de recoger los vestigios, restos y huellas del delito»[954]. Por su parte, JIMÉNEZ CONDE se refiere a la inspección ocular como el «reconocimiento por los miembros del Tribunal a través de sus sentidos de

[951] El referido autor cita al pie, para su confrontación, las SSTC 51/1995, de 23 febrero; 280/2005, de 7 noviembre, así como la STS 480/2009, de 22 de mayo. Vid. MUERZA ESPARZA, J. J., «Sobre el valor de la prueba preconstituida en el proceso penal», en Jimeno Bulnes, M., Pérez Gil, J. (coords.), *Nuevos horizontes del derecho procesal*, Barcelona, Bosch Editor, 2016, p. 775.

[952] La LECrim, dado que en el momento de su promulgación no existían los Juzgados de lo Penal, celebrándose los juicios penales en las Audiencias Provinciales, utiliza para referirse al lugar del juicio el término «la capital», vocablo que, obviamente, hemos de interpretarlo como el lugar del juicio.

[953] El art. 353.1 LEC dispone que «el reconocimiento judicial se acordará cuando para el esclarecimiento y apreciación de los hechos sea necesario o conveniente que el tribunal examine por sí mismo algún lugar, objeto o persona».

[954] GÓMEZ COLOMER, J. L., «Los actos de investigación no garantizados», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, p. 212.

cualquier objeto o lugar que guarde relación con los hechos […], a la que resulta más apropiado llamar prueba de "reconocimiento judicial"»[955].

Prescindiendo de todas las particularidades propias de la inspección ocular, que no son objeto de este trabajo, y pasando a ocuparnos de la aplicación de la misma a los registros informáticos, debe ponerse de manifiesto que (si bien la función inicial de esta diligencia de investigación y medio de prueba, iba dirigida a la recogida de vestigios o pruebas materiales, tales como documentos, armas o muestras de sangre, así como a diligencias tales como el levantamiento de cadáver o inspecciones corporales), con la irrupción de las TIC, esta actuación procesal ha de extenderse a la comprobación de cualquier documento electrónico, ya sea de texto, imagen, audio o video. En este sentido, señala ABEL LLUCH que «el reconocimiento judicial es un medio apto para incorporar la evidencia electrónica y, particularmente, para la percepción judicial directa de datos de prueba del entorno digital»[956].

No obstante, no será lo normal que se produzca un reconocimiento judicial por parte del tribunal enjuiciador, habida cuenta de la posibilidad de preconstitución de la prueba sin su intervención, mediante el cotejo por parte del letrado de la Administración de Justicia. En cualquier caso, se trata de una posibilidad existente tanto en fase de juicio oral como en fase de instrucción.

En el juicio oral, expone MARTÍNEZ JIMÉNEZ, con cita de abundante jurisprudencia, que «su práctica o no en este segundo momento dependerá de que el Tribunal disponga de elementos suficientes para formar un juicio y conforme a ello, que resulte necesario o inútil, debiéndose indicar que, en general, resulta inútil una vez concluso el sumario y transcurridos varios meses, pues no cabe ya recoger huellas o vestigios que puedan poner de relieve la forma de comisión, por vía de hipótesis, los hechos objeto de acusación»[957]. Aun así, afirma este autor, «no cabe decir que esta prueba no pueda practicarse en el juicio oral»[958], citando a este respecto la STS 1244/2001, de 25 de junio, que reconoce que puede ser necesario para el juicio examinar

[955] JIMÉNEZ CONDE, F., «*Introducción al Derecho Procesal Penal*», cit., p. 136.

[956] ABEL LLUCH, X.; PICÓ I JUNOY, J.; SERRANO MOLINA, A., «Preguntas con respuesta: la prueba a consulta», *Diario La Ley - Sección Práctica Forense*, n.º 7564, 2011, p. 7.

[957] MARTÍNEZ JIMÉNEZ, J., «El reconocimiento judicial», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo I*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, pp. 341-347.

[958] MARTÍNEZ JIMÉNEZ, J., «El reconocimiento judicial», cit., p. 344.

el lugar de los hechos, siempre que pueda existir alguna circunstancia relevante que no haya desaparecido, debiendo, quien proponga esta prueba, decir con precisión cuál es el dato que tiene que ser apreciado por el tribunal[959].

En todo caso, teniendo en consideración las peculiaridades de la prueba digital, el tribunal podrá acordar el reconocimiento judicial o inspección ocular, bien de acuerdo con el art. 726 LECrim, conforme al que debe examinar por sí mismo los libros, documentos, papeles y demás piezas de convicción, o mediante la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo, de acuerdo con lo ya estudiado anteriormente.

Por lo que respecta a la fase de instrucción, el juez de instrucción podrá proceder a la inspección ocular de los dispositivos de almacenamiento y al examen por el mismo de los archivos de texto, imagen, audio o video, con asistencia de las partes y la intervención del letrado de la Administración de Justicia que extenderá la correspondiente acta, con la consiguiente preconstitución de la prueba.

2.7. La pericial

La LECrim dedica a la pericial como medio de prueba los arts. 723 a 725, en los que únicamente trata cuestiones formales relativas a la práctica de la prueba en el acto

[959] La referida STS 1244/2001, de 25 de junio, declara en su FJ 2.º, lo siguiente:
«No cabe decir que esta prueba debe practicarse durante la instrucción. Lo normal es que se lleve a cabo en el sumario o en las diligencias previas como prueba preconstituida con validez para el juicio oral por haberse practicado con intervención de las partes, precisamente porque de ordinario lo que se pretende es precisar datos que el tiempo puede borrar. Pero esto no impide que pueda ser necesario para el juicio examinar el lugar de los hechos por existir alguna circunstancia relevante que no haya desaparecido. Pero en estos casos la parte que propone esta prueba debe decir con precisión cuál es el dato concreto que tiene que ser apreciado por el Tribunal, para que pueda resolverse sobre su necesidad. Aunque siempre debe tenerse en cuenta que la práctica de una inspección ocular, que ha de hacerse fuera de la sala donde se celebra el juicio, lleva consigo una ruptura de la concentración y publicidad de las sesiones y unos trastornos por la necesaria constitución de todos (Tribunal, partes, incluso testigos pidió el recurrente en este caso) en un lugar diferente. Es conocida la doctrina de esta sala que habla del carácter excepcional de esta prueba de inspección ocular en el juicio oral, pues choca con los mencionados principios (concentración y publicidad), de modo tal que sólo debe practicarse cuando las partes no dispongan de ninguna otra prueba para llevar al juicio los datos que se pretendan (Sentencias 26.3.91, 24.6.92 y 6.7.92, entre otras muchas). Desde luego, es imprescindible, para que pueda admitirse esta prueba para el juicio oral, que se precise por qué razón concreta tiene que ir el Tribunal al lugar de los hechos, que se diga qué circunstancia es la que tiene que percibir allí el Tribunal que pueda justificar el traslado fuera de la sala donde el juicio se ha de desarrollar. Y esto no lo dijo el escrito de proposición ni lo dice tampoco ahora la parte al formular el presente recurso. Ciertamente fue bien denegada la prueba».

de juicio oral, por lo que resultan aplicables para el estudio de la misma, los arts. 456 a 485 LECrim, que regulan los aspectos procesales del informe pericial como diligencia instructora.

Por ello, la prueba pericial constituye tanto un medio de prueba como un acto de investigación, y en tal sentido se ha pronunciado el TS al declarar que «en orden a la naturaleza y sentido de la pericia o informe pericial hemos de manifestar que, amén de estimarse medio de prueba en su función de averiguación en el juicio oral de la verdad material delimitada en las pretensiones penales que se ejercitan, en aquellos casos que se interesa y practica a instancias del instructor, constituye un acto de investigación o preprobatorio de auxilio judicial para suplir la ausencia de conocimientos científicos, artísticos o culturales del juez, teniendo como finalidad tal diligencia constatar una realidad no captable directamente por los sentidos, en contraste con la prueba testifical o inspección ocular»[960].

En efecto, de acuerdo con el art. 456 LECrim, «el juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fueren necesarios o convenientes conocimientos científicos o artísticos». Precisamente en tales conocimientos radica la diferencia fundamental del testigo con el perito, por lo que este, como señala ESCOBAR JIMÉNEZ, a diferencia del testigo, es sustituible, y por ello «lo que justifica su intervención es precisamente la razón de su ciencia, ocupando una posición activa en relación con el examen de lo que constituye el objeto de la pericia»[961], mientras que «el testigo declara sobre hechos pasados relacionados con el proceso y percibidos por él mismo personalmente, siendo por ello insustituible, teniendo una posición pasiva en cuanto es él mismo objeto de examen»[962].

Cabe destacar asimismo, que en el procedimiento ordinario todo reconocimiento pericial se hará por dos peritos, salvo que, conforme al art. 459 LECrim, no hubiese más de uno en el lugar y no fuere posible esperar la llegada de otro sin graves inconvenientes para el curso del sumario. Esta norma no rige en el procedimiento abreviado, en el que, de acuerdo con el art. 788.2-I LECrim, el informe pericial podrá ser presentado por un

[960] STS 1212/2003, de 9 de octubre, FJ 2.º

[961] ESCOBAR JIMÉNEZ, R., «La prueba de peritos», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo II*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, pp. 49-50.

[962] ESCOBAR JIMÉNEZ, R., «La prueba de peritos», cit., p. 50.

solo perito. No obstante, tal y como ha reiterado la jurisprudencia del TS, la duplicidad de peritos en el procedimiento ordinario se rellena con su realización por un laboratorio oficial, dado su carácter público y por estar integrado por diversos profesionales[963].

2.7.1. La pericial informática

2.7.1.1. Consideraciones previas

En relación con la pericial informática afirma RICHARD GONZÁLEZ que, tal y como resulta de su propio nombre, «se trata de una prueba pericial ordinaria que se distingue por su contenido que será el del análisis de programas, sistemas de comunicación, archivos informáticos de cualquier clase y, en general, todos aquellos hechos que se produzcan, transmitan o manifiesten en forma electrónica»[964], añadiendo este autor, en referencia al proceso penal, que «lo que se persigue con la prueba pericial informática es dar cuenta y acreditar hechos de esta naturaleza que traen causa del resultado de la investigación efectuada por la policía»[965].

De este modo, podemos afirmar que si la pericial es, en general, un medio para facilitar al juez conocimientos científicos necesarios para la acreditación de los hechos, la pericial informática es aquella modalidad de prueba pericial en la que la ciencia a aportar al juez se encuentra en las dudas que surgen en aspectos contenidos en las fuentes de prueba digitales o en los dispositivos electrónicos donde se encuentran estas.

De acuerdo con lo afirmado por ANGUAS BALSERA, «la pericial informática se distingue de otras periciales en que los elementos que trata no nos son en general accesibles directamente, precisando un medio tecnológico para su observación, llevando asociada una inherente intangibilidad y ausencia de significado propio»[966].

---

[963] Vid. STS 1302/2005, de 8 de noviembre, FJ 1.º, que con cita de otras resoluciones declara que «precisamente, por las condiciones de laboratorio público, dotado de la imparcialidad que caracteriza la función de la administración pública, y por la naturaleza oficial del laboratorio, que incorpora a varios profesionales que trabajan en el mismo, la jurisprudencia de esta Sala ya admitió que los informes periciales firmados por una persona, como responsable del laboratorio oficial, rellenaban la exigencia de pluralidad de peritos que exige el art. 459 para las causas tramitadas en el procedimiento ordinario por delitos».

[964] RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 329.

[965] RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 329.

[966] ANGUAS BALSERA, J., «La pericial informática», cit., p. 319.

Señala este mismo autor en otro estudio que «el peritaje en informática tendría una visión eminentemente probática de los indicios y no se quedaría en hechos simples sino que estaría en disposición de extraer hechos complejos y de alto nivel de las evidencias observadas, incluso cuando estos hechos de alto nivel requieren de una capacitación para su interpretación o valoración»[967].

Por otro lado, la pericial informática puede ser necesaria no solo en relación con los ciberdelitos[968] (en los que, en su gran mayoría, resultará imprescindible), sino en relación con cualquier tipología delictiva. En este sentido, tal y como afirma RUZ GUTIERREZ, la incautación de equipos informáticos o dispositivos de almacenamiento de datos, ocupa un papel decisivo, tanto en la investigación de delitos informáticos como en la de todo tipo de delitos[969].

2.7.1.2. Tipología de periciales informáticas

La primera cuestión a plantear, consiste en determinar en qué casos es necesaria una pericial informática. En este punto, siguiendo a MAGRO SERVET, podemos hablar de tres grandes campos en los que se puede practicar la pericial, como son los siguientes: pericias de autenticidad; pericias de contenido, funcionamiento y recuperación de datos; y pericias sobre Internet[970].

a) En cuanto a las pericias de autenticidad, se trata de determinar si un determinado contenido digital es auténtico o ha sido manipulado. Dicho en palabras de DE JORGE MESAS, «su finalidad es, por tanto, dejar sentada la integridad de la prueba, que constituye un elemento esencial del ineludible binomio autenticidad (la misma

---

[967] ANGUAS BALSERA, J., «El peritaje en informática en el marco de las disciplinas que le son afines. Puntos de contacto y perfil de la actividad», *Diario La Ley - Sección Práctica Forense*, n.º 7329, 2010, p. 2.

[968] En relación con el concepto y tipología de los ciberdelitos, vid. supra apdo. II.2 del capítulo I, pp. 20-22.

[969] RUZ GUTIÉRREZ, P. R., «La confección del dictamen pericial informático y su incorporación al proceso como medio de prueba objeto de valoración judicial», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009, p. 117, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[970] MAGRO SERVET, V., «La instrucción de los delitos informáticos», *Estudios de Derecho Judicial del Consejo General del Poder Judicial*, n.º 64, 2004, p. 31. En este punto, el autor cita la obra de FERNÁNDEZ, C.A., «Prueba Pericial Delitos y tecnología de la Información Características y valoración en el Proceso Penal Argentino», *Derecho Informático y de las Nuevas Tecnologías*, n.º 5, Boletín n.º 5, enero de 2003.

fuente de prueba) e integridad (ausencia de manipulación o alteración), que ha de quedar meridianamente acreditado en el proceso»[971].

En el ámbito de la investigación de los delitos en general, se trata de la modalidad de pericial que más se practicará, dado que en muchos casos será puesta en duda la autenticidad o integridad de la fuente de prueba digital, ya sea de texto, imagen, audio o video. Así, por ejemplo, podrá discutirse la veracidad de un mensaje de correo electrónico, la de la efectiva remisión de un audio a través de aplicación de whatsapp, o la autenticidad de unas imágenes encontradas en un dispositivo de almacenamiento.

b) En cuanto a las periciales sobre el contenido, funcionamiento y recuperación de datos, afirma MAGRO SERVET que abarcan tan diversos aspectos como «el almacenamiento de datos, el análisis y determinación de estructuras de diseño de sistemas, la [sic] medios de comunicación y transferencia de datos, métodos de entrada, acceso, procesamiento y salidas, etc.»[972]. Serán más susceptibles de ser practicadas en aquellos procesos en los que se investiguen delitos más concretos, como los delitos contra la propiedad intelectual e industrial, sin perjuicio de poder ser practicadas en relación con cualquier delito, incluidos los ciberdelitos.

En cuanto a la pericial sobre el contenido de datos, tal y como señala DE JORGE MESAS, «se trata de aquellas pericias en las que lo que se busca es el análisis de los contenidos para establecer si se trata de software auténtico o de una copia no autorizada con infracción de derechos de propiedad intelectual, las fechas de modificación o creación de los archivos, su origen o destino en caso de tratarse ele información enviada o recibida por correo electrónico, la existencia de daños en el software, etc.»[973].

La pericial de funcionamiento de datos, estará orientada al esclarecimiento de las dudas en relación a la ejecución informática de determinados archivos sin programa

---

[971] DE JORGE MESAS, L. F., «La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal (...más sobre las nuevas tecnologías)», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 2, 2007, p. 365, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[972] MAGRO SERVET, V., «La instrucción de los delitos informáticos», cit., p. 31. En relación con esta afirmación, el autor cita la obra de FERNÁNDEZ, C.A., «Prueba Pericial Delitos y tecnología de la Información Características y valoración en el Proceso Penal Argentino», *Derecho Informático y de las Nuevas Tecnologías*, n.º 5, Boletín n.º 5, enero de 2003.

[973] DE JORGE MESAS, L. F., «La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal (...más sobre las nuevas tecnologías)», cit., p. 365.

específico, análisis de virus, o análisis de programas y archivos usados para estafas informáticas.

Por lo que respecta a la pericial de recuperación de datos, tendrá lugar en aquellos casos en los que existan archivos encriptados o eliminados. De este modo, tal y como señala DE JORGE MESAS, el perito tendrá que «conseguir el acceso a los archivos que pueden estar ocultos, por el establecimiento de una contraseña que impide acceder a los mismos a quien no la conozca; o por medio de la utilización de procedimientos de cifrado o encriptado codificado de la información [...] la actividad del perito puede ir encaminada también a la recuperación de los archivos eliminados del equipo o dispositivo informático»[974].

c) Finalmente, en relación con las pericias sobre internet, será lo normal su práctica en la investigación de ciberdelitos, tales como delitos de acceso ilícito, interceptación ilícita, estafas informáticas, ciberacoso, amenazas a través de las redes sociales, difusión de archivos digitales de pornografía infantil, etc.

Así, por ejemplo, en determinadas ocasiones será necesario: determinar si la dirección IP desde la que se profirieron amenazas correspondía al ordenador del acusado; descifrar texto encriptado por la red; determinar la procedencia de un programa ilícito; verificar la fecha en la que se produjo la intromisión; etc.

No obstante, las pericias de internet también podrán darse en los procesos seguidos por cualquier tipología delictiva. Así, por ejemplo, teniendo en cuenta que la propia intervención en el acto del registro del dispositivo de almacenamiento masivo o en el registro remoto de un equipo informático constituye una actuación pericial, en aquellos supuestos legales en los que haya que extender el registro datos contenidos en otro sistema (arts. 588 sexies c.3 y 588 septies a.3 LECrim), ya se estará practicando una pericial relacionada con internet, teniendo que explicitar el perito o los peritos en el correspondiente informe emitido de conformidad con el art. 478 LECrim, la relación detallada de todas las operaciones practicadas y su resultado.

De igual modo, cualquier registro remoto de equipos informáticos ha de ser considerado como una pericia sobre internet, ya que toda intrusión remota, necesariamente ha de practicarse por la red y exige que por la autoridad judicial se

[974] DE JORGE MESAS, L. F., «La incorporacón de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal (...más sobre las nuevas tecnologías)», cit., p. 365.

especifique la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información (art. 588 septies a.1 c), por lo que necesariamente deberá emitirse un informe pericial por parte de los agentes intervinientes en la diligencia, acreditativo de tales particularidades.

2.7.1.3. Momento procesal para la práctica de la pericial informática

Habida cuenta de la división del proceso penal en dos fases, la instructora y la enjuiciadora, conforme hemos indicado anteriormente, el informe pericial es susceptible de ser efectuado en ambas fases.

En cuanto a la fase instructora, también hemos tenido oportunidad de comentar que la propia ejecución de un registro informático ya constituye una pericial, como así lo pone de manifiesto RICHARD GONZÁLEZ, quien señala que «la investigación consistente en el rastreo remoto de equipos informáticos, al igual que la intervención telemática o el registro de dispositivos masivos de almacenamiento siempre tendrán como elemento común la aportación al juicio de un informe pericial que será el elemento fundamental a efectos de prueba del resultado de la intervención, sin perjuicio de que, además, se puedan visionar u oír grabaciones de imagen y sonido de archivos que pudiera haberse aprehendido en la intervención»[975].

Este informe será practicado directamente por la Policía Judicial o por instrucción del Ministerio Fiscal en los supuestos de urgencia, o, con carácter general, en virtud de autorización judicial, por la Policía Judicial o por uno o dos peritos designados judicialmente.

Además de la práctica de la pericial como consecuencia de la medida de investigación, podrá proponerse por cualquiera de las partes, y acordarse por el juez de instrucción, la práctica de un informe pericial cuando lo considere oportuno para resolver sobre el procesamiento o en su caso sobreseimiento de la causa.

Pero, al mismo tiempo, cabe recordar que también es posible que para la práctica de un registro de dispositivos de almacenamiento masivo —no así en cuanto a los registros remotos que siempre exigirán un informe pericial—, de conformidad con lo

[975] RICHARD GONZÁLEZ, M., «*Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*», cit., p. 328.

dispuesto en el art. 588 sexies c.1 LECrim, el juez fije en la resolución que autorice el registro 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, que se practicaría a posteriori, por uno o dos peritos.

Por otro lado, también es posible la práctica de la prueba pericial informática en el plenario, bien como reproducción de la ya practicada en fase de instrucción, o como una nueva prueba que deberán solicitar las partes, al igual que el resto de pruebas, en los escritos de calificación en el procedimiento ordinario (art. 656 LECrim) y en los escritos de acusación y defensa en el procedimiento abreviado (arts. 781.1-II y 784.2 LECrim).

De un modo u otro, es decir, ya se presente en fase de instrucción o de juicio oral, conforme establece el art. 478 LECrim, el informe pericial comprenderá, si fuere posible:

1.º Descripción de la persona o cosa que sea objeto del mismo, en el estado o modo en que se halle.

2.º Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.

3.º Las conclusiones que en vista de tales datos formulen los peritos conforme a los principios y reglas de su ciencia o arte.

Finalmente los arts. 479-485 LECrim se ocupan de las particularidades del acto pericial, disponiendo el art. 480 que «las partes que asistieren a las operaciones o reconocimientos podrán someter a los peritos las observaciones que estimen convenientes haciéndose constar todas en la diligencia». Se trata de una regla dirigida a la fase de instrucción, resultando superflua para el juicio oral, si se tiene en cuenta que en el mismo rige de forma imperativa el principio de contradicción.

2.7.2. La preconstitución de la pericial informática

De acuerdo con el art. 477 LECrim, con carácter general el acto pericial será presidido por el juez instructor, asistiendo siempre el letrado de la Administración de Justicia que actúe en la causa.

Asimismo, el art. 476 LECrim establece la posibilidad de que puedan concurrir al acto pericial, el querellante, si lo hubiere, con su representación, y el procesado con la

suya aun cuando estuviere preso, siempre que se dé el caso del párrafo segundo del art. 467 LECrim, es decir, cuando la pericial no pudiere reproducirse en el juicio oral.

Este último precepto se ocupa de la recusación de los peritos, estableciendo que los peritos no podrán ser recusados por las partes cuando el informe pericial pudiere tener lugar de nuevo en el juicio oral, mientras que sí que habrá lugar a la recusación cuando no pudiere reproducirse en el juicio oral.

Lo que viene a expresar el art. 467 LECrim[976], es que en aquellos casos en los que el material sobre el que ha de emitirse el informe pericial no pueda conservarse hasta la celebración del juicio oral, se hace necesaria la preconstitución de la prueba, afirmando MORENO CATENA, que «este es el sentido de la recusación de los peritos durante la investigación y, tan es así, que el legislador sólo permite plantearla cuando el reconocimiento e informe no pudiera reproducirse en el juicio oral; en caso contrario, los peritos no podrán ser recusados por las partes»[977].

A este respecto, el TC ha declarado que «la eventual parcialidad de los peritos por su relación objetiva o subjetiva con el procedimiento sólo adquiere relevancia constitucional en los supuestos en que dicha pericial asuma las características de prueba preconstituida, y no cuando pueda reproducirse en la vista oral, ya que, en este último caso, el órgano judicial, con la superior garantía que implica la inmediación y la posibilidad de contradicción, podrá valorar todas las circunstancias del desarrollo de la misma y sopesar, en su caso, la influencia que en el desarrollo de la prueba pudiera tener un eventual interés del perito con el hecho y con las partes», adicionando que «ello es lo que justifica, en última instancia, que el art. 467 LECrim limite las posibilidades de recusación de peritos nombrados judicialmente a los casos en que la pericial no pudiera reproducirse en el juicio oral»[978].

Del conjunto de estos preceptos y doctrina del TC, puede afirmarse que (a diferencia de aquellos casos en los que la pericial sea aportada por una de las partes y

[976] Cabe reseñar que el Anteproyecto de LECrim de 2013, obvió lo previsto en el art. 467 LECrim, simplificando lo relativo a la recusación de los peritos, estableciendo escuetamente en el art. 395 que «1. Las partes podrán recusar al perito en el que concurra causa de abstención ante el Tribunal competente para el conocimiento de la causa, conforme a lo establecido en la Ley de Enjuiciamiento Civil. 2. La recusación de un perito no suspenderá la práctica de la diligencia».

[977] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 468.

[978] Vid. STC 196/2006, de 20 de junio, FJ 5.º

sea debatida en el acto de juicio oral) nos encontraremos ante una pericial preconstituida cuando esta sea acordada judicialmente en fase de instrucción, compareciendo al acto pericial las partes, en presencia del juez y bajo la fe pública judicial del letrado de la Administración de Justicia, no siendo en tal caso necesaria la reiteración de la misma en el juicio oral, procediéndose a su práctica mediante la lectura de documentos del art. 730 LECrim y el eventual interrogatorio del perito o los peritos que emitan el informe.

Lo que acabamos de señalar cobra especial importancia en lo que respecta a las periciales informáticas, habida cuenta del carácter volátil de los contenidos informáticos y el evidente peligro de pérdida de los mismos, por lo que, como señala MORENO CATENA, en estos casos en los que existe el riesgo de que el material no pueda conservarse hasta la celebración del juicio oral, «es evidente que los informes evacuados durante el sumario se han de convertir en un medio de prueba anticipada al juicio y, por ello, han de rodearse de todas las garantías en su realización, especialmente la imparcialidad de los peritos, logrando apartar, de lo que ahora es práctica de un verdadero medio probatorio, al perito sospechoso de parcialidad»[979].

En cualquier caso, aunque la prueba se haya preconstituido y ya no sea necesaria su reproducción en el juicio oral, lo normal será que el perito deba comparecer al mismo a fin de someterse a las observaciones que le formulen las partes (art. 480 LECrim) así como contestar a las preguntas y facilitar las aclaraciones que le sean solicitadas por el juez (art. 483 LECrim).

Ahora bien, como señala VELASCO NUÑEZ, distintos factores como «la escasez de peritos, su necesaria constante presencia en juicio, los costes por su desplazamiento en tiempo y dinero por toda la geografía nacional, la imparcialidad, objetividad, competencia técnica, desinterés en el caso concreto que suelen presentar, los altos niveles de especialización técnica, la necesidad de atender a imperativos de formación, la sofisticación y coste de las modernas pericias, etc., han llevado a matizar esta necesidad procesal en el caso de las realizadas por expertos policiales que no intervienen en las actividades operativas salvo para dar asesoramiento técnico»[980].

---

[979] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 468.

[980] VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales (2ª Parte)», *Revista de Jurisprudencia - El Derecho*, n.º 4, Abril, 2009, p. 5.

Así ocurre con los informes periciales informáticos emitidos por la Sección de Informática Forense de la Comisaría General de Policía Científica o por el Departamento de Ingeniería del Laboratorio de Criminalística de la Guardia Civil, o como también ocurriría con los informes que se emitiesen por el sugerido, en este trabajo, Instituto de Informática Forense[981].

De este modo, de forma consolidada, la jurisprudencia del TS vino excluyendo la necesidad de comparecencia de los peritos de los gabinetes y laboratorios oficiales, en atención a las garantías técnicas y de imparcialidad que ofrecen los mismos y que propician la validez, *prima facie,* de sus dictámenes e informes sin necesidad de su ratificación en el juicio oral, siempre que no hayan sido objeto de impugnación expresa en los escritos de conclusiones, en cuyo caso si deberían ser sometidos a contradicción en dicho acto como requisito de eficacia probatoria[982].

Esta jurisprudencia fue recogida por el legislador mediante la Disposición Adicional Tercera de la LO 9/2002, de 10 de diciembre, que añadió un nuevo párrafo al art. 788.2 LECrim, disponiendo que en el ámbito del procedimiento abreviado «tendrán carácter de prueba documental los informes emitidos por laboratorios oficiales sobre la naturaleza, cantidad y pureza de sustancias estupefacientes cuando en ellos conste que se han realizado siguiendo los protocolos científicos aprobados por las correspondientes normas».

---

[981] Vid. supra apdo. IV.6.4 de este capítulo, pp. 431-433.

[982] Vid. STS 806/1999, de 10 de junio, FJ 3.º con cita de diversas sentencias del mismo Tribunal. Puede destacarse asimismo la STS de 5 de mayo de 1995 - ROJ: STS 9679/1995, que en su FJ 4.º declara que «esta doctrina no cuestiona en absoluto, la doctrina general atinente a que la prueba hábil para desvirtuar la presunción de inocencia debe practicarse en el acto del juicio oral ni tampoco pretende, pues no podría hacerlo respetando la Constitución, invertir la carga probatoria sobre los hechos integradores de una infracción penal, sino únicamente aclara que los hechos que deben ser objeto de prueba son los controvertidos y si sobre una determinada cuestión técnica existe un dictamen técnico en las actuaciones, emitido por organismos oficiales fiables, que no es cuestionado por la defensa —por ejemplo, ésta no discute que la sustancia ocupada sea cocaína, y únicamente alega que el acusado la tenía para su propio consumo— la acusación puede legítimamente prescindir de llevar al juicio oral a los técnicos informantes, en evitación de los problemas prácticos que la reiteración de tales comparecencias conllevaría, sin que la defensa que no cuestionó el resultado de la pericia pueda en casación negar con éxito su valor probatorio, precisamente porque aceptó expresa o tácitamente su resultado. Tampoco puede servir esta doctrina, dirigida fundamentalmente a evitar el fraude que representa cuestionar en casación lo que se asumió en la instancia, de cómoda cobertura para prescindir, por sistema, de la práctica en el juicio oral de las pruebas periciales, que siempre que sea posible se deben realizar con las garantías de inmediación, contradicción y publicidad que sólo el juicio oral proporciona, conforme a la doctrina general sobre la práctica de la prueba en el proceso penal».

En todo caso, aun cuando este precepto se refiere al procedimiento abreviado y a los informes emitidos en relación con sustancias estupefacientes, consideramos que, por todas las razones expuestas anteriormente, los informes periciales informáticos emitidos por los equipos especializados de las FCSE, o en su caso los que pudieran ser emitidos por un Instituto de Informática Forense, tendrán el mismo carácter de prueba preconstituida y deberán ser incorporados al juicio oral mediante la lectura de documentos del art. 730 LECrim, sin perjuicio de su impugnación por la defensa.

No obstante, la impugnación no podrá ser formulada en cualquier momento, sino en el escrito de calificación provisional en el procedimiento ordinario o en el escrito de defensa en el procedimiento abreviado. De este modo, «cuando la parte acusada no expresa en su escrito de calificación provisional su oposición o discrepancia con el dictamen pericial practicado, ni solicita ampliación o aclaración alguna de ésta, debe entenderse que dicho informe oficial adquiere el carácter de prueba preconstituida, aceptada y consentida como tal de forma implícita»[983].

Se trata de una cuestión que ha sido avalada por la jurisprudencia del TC, que tras determinar que «resulta innegable la condición de prueba preconstituida que el certificado médico inicial y los posteriores forenses incorporan» ha declarado que «el único modo de desvirtuar la fuerza de convicción que pruebas preconstituidas periciales puedan tener es interrogar al Perito en el acto del juicio oral, para lo cual deberá ser reclamado por la parte que pretende o ratificar su dictamen o, como podía haber sido aquí el caso, impugnar el mismo, no haber puesto en duda la corrección científica del citado certificado lleva aparejado como consecuencia que, en tanto que prueba documentada, que no documental, el órgano judicial, tal como estatuye el art. 726 LECrim, haya examinado "por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a las más segura investigación de la verdad", no ha de olvidarse que este precepto encabeza la regulación de la prueba documental y de la inspección ocular y que, por tanto, de no efectuarse tacha alguna sobre los citados elementos, el Tribunal dispone libremente de ellos y puede formarse su pertinente convicción legítimamente»[984].

Asimismo, de forma muy expresiva, el TS ha dejado claro que en los casos en los que la defensa, conociendo que el Fiscal propone la comparecencia del perito salvo

[983] Vid. ESCOBAR JIMÉNEZ, R., «La prueba de peritos», cit., p. 75.
[984] Vid. STC 24/1991, de 11 de febrero, FJ 3.º

que el informe no fuese impugnado por la defensa, no contradice el mismo, está mostrando su conformidad implícita, de tal modo que, en el caso enjuiciado, si no se citó a juicio al perito fue como consecuencia de esa actitud de la defensa[985].

Con base en todo lo anterior y para concluir este apartado, diremos que la prueba pericial informática tendrá con carácter general, cuando esta se practique como consecuencia de un registro informático practicado como medida de investigación, el carácter de preconstituida, por lo que su incorporación al juicio tendrá lugar mediante la lectura de documentos prevista en el art. 730. Ello no impide que la misma pueda ser impugnada por la defensa o que por esta se pueda presentar una contrapericia, en cuyo caso será necesario el debate en el juicio oral la presencia del perito o los peritos, a fin de que con respeto del principio de contradicción, la prueba pueda quedar válidamente incorporada y así poder ser valorada por el tribunal.

VI. Eventual impugnación y valoración de la prueba digital

Una vez que la prueba digital obtenida como consecuencia de un registro informático acordado como diligencia de investigación ha tenido entrada en el juicio oral, por alguno de los medios de prueba anteriormente estudiados, comienza el proceso de valoración de la prueba o lo que es lo mismo se pone en marcha por el tribunal el proceso de análisis que relacionará el resultado final del juicio celebrado con la prueba practicada.

Si la prueba digital es objeto de impugnación, el tribunal deberá resolver sobre la procedencia de la misma. Si es estimada, la prueba impugnada no tendrá entrada definitiva en el proceso y, por tanto, no será objeto de valoración. Por consiguiente, adquiere especial relevancia la eventual impugnación de la prueba digital.

Ello hace necesario el tratamiento conjunto de la valoración de la prueba y los aspectos procesales de su eventual impugnación.

1. Eventual impugnación de la prueba digital

Si bien la LECrim no se ocupa de ello, cualquier prueba, en general, puede ser impugnada por la parte contraria a la que la ha propuesto, dado que, de no ser así, se vería gravemente comprometido el principio de contradicción. No obstante, la LEC, de

[985] Vid. STS 276/2013, de 18 de febrero, FJ 5.º

aplicación supletoria conforme a su art. 4, se ocupa en diversos apartados de la impugnación de las pruebas[986]. Se trata, una vez más, de una materia que, en nuestra opinión, por las particularidades propias del proceso penal, debería tener una regulación propia en la, futura, nueva LECrim.

En cuanto al documento electrónico, tal y como señala ORTUÑO NAVALÓN, al igual que ocurre con el documento en general, la impugnación puede versar sobre aspectos como su autenticidad —es decir, la concordancia entre el autor aparente y el real—, su exactitud o coincidencia entre el original y la copia, testimonio o certificación y su certeza; es decir, la concordancia entre las declaraciones o testimonios contenidos en el documento y la realidad. Por ello, el documento electrónico debe observar esas garantías, o sea: «a) integridad; es decir, que el soporte en el que se presenta no ha sido alterado; b) autenticidad, que supone constatar la realidad del sujeto al que se atribuye y del contenido que refleja; a las que cabe añadir: c) la licitud, es decir, que en su obtención no se hayan vulnerado derechos y libertades fundamentales»[987].

En este sentido, en lo que respecta a la prueba digital, quizás con más motivo por su carácter volátil, consideramos que será más probable su impugnación que otras pruebas. Ello no obstante, tal y como advierte ARRABAL PLATERO, «lo cierto es que la manipulación o creación *ex novo* de pruebas aportadas al proceso no es una circunstancia exclusivamente circunscrita a esta fuente probatoria [...] téngase presente, a modo de ejemplo, la habilidad con la que mienten los testigos, la facilidad con la que puede falsificarse una firma manuscrita, la habitual desconfianza en la objetividad de los peritos de parte o la duda que trasmiten muchos documentos privados sobre su originalidad»[988].

---

[986] La LEC se ocupa de la impugnación de pruebas en los siguientes preceptos:
1. El art. 287 regula la impugnación en caso de ilicitud probatoria, estableciendo que en este caso, la parte que la invoque deberá alegarlo de inmediato, con traslado a las demás partes.
2. El art. 289.2 se refiere a la impugnación de los dictámenes periciales.
3. El art. 303 establece la posibilidad de impugnar la admisibilidad de las preguntas formuladas en el interrogatorio de las partes.
4. El art. 320 se dedica al procedimiento a seguir en caso de impugnación de un documento público.
5. El art. 326 dispone que los documentos privados harán prueba plena en el proceso cuando su autenticidad no sea impugnada.
6. El art. 369 a la impugnación de las preguntas que se formulen a los testigos.

[987] ORTUÑO NAVALÓN, M. C., «*La prueba electrónica ante los tribunales*», cit., p. 110.

[988] ARRABAL PLATERO, P., *La Prueba Tecnológica: Aportación, Práctica y Valoración*, Valencia, Tirant Lo Blanch, 2019, p. 338. En relación con esta afirmación, la autora hace referencia a varias opiniones

Partiendo de las anteriores apreciaciones, para el examen de la impugnación de la prueba digital, se hace necesario el planteamiento de tres cuestiones fundamentales, como son: la pregunta relativa a si es posible la manipulación o alteración de la prueba digital; el momento del planteamiento de la impugnación y la necesidad de razonar la misma. Por último habrá que plantear el recurso a otros medios de prueba adicionales como corolario de la impugnación.

1.1. La posible la manipulación o alteración de la prueba digital

Se hace necesario el planteamiento de esta cuestión, dado que, aunque, *prima facie*, parece evidente la respuesta afirmativa a la misma, se trata de un asunto que no ha de verse de una forma tan clara, si tenemos en cuenta que la alteración de determinados elementos de prueba digital exige conocimientos técnicos que, aun cuando puedan ser conocidos por muchas personas legas en informática, requiere algún estudio de los aspectos necesarios para llevar a cabo tal fraude. En este sentido, estimamos que incluso puede resultar más fácil la falsificación de un documento en papel que la de un documento electrónico.

Aun así, determinadas alteraciones resultarán fáciles para cualquier usuario informático, como la modificación de contenidos mediante la edición de un documento con un programa de tratamiento de textos u hoja de cálculo. Sin embargo, acciones como la suplantación de identidad, tomar el control de la cuenta de otro en redes sociales, el acceso a sistemas informáticos ajenos, etc., requieren estudio y preparación, no siendo siempre posible por los sistemas de seguridad existentes —tanto a nivel particular en los dispositivos informáticos mediante programas de seguridad, como por las propias compañías titulares de redes sociales y de todo tipo de plataformas a las que se accede por los particulares para distintos fines a través de la red internet—.

No obstante, aunque la alteración no estará al alcance de todos, resulta evidente que, una vez adquiridos los conocimientos necesarios, la misma puede ser accesible a cualquier ciudadano que de forma habitual haga uso de las TIC. Por ello, resultando

---

doctrinales en el mismo sentido, pudiendo mencionar la que pone de manifiesto FUENTES SORIANO, quien destaca cómo la facilidad para fingir, crear o manipular las pruebas no tecnológicas es muy superior, con respecto a las tecnológicas, para la mayoría de los ciudadanos, profanos en cuestiones informáticas. Vid. FUENTES SORIANO, O., «La impugnación de la prueba digital», en Álvarez Alarcón, A., García Molina, P. (dirs.); Conde Fuentes, J., Arrabal Platero, P. (coords.), *Tendencias actuales del Derecho Procesal*, Albolote (Granada), Editorial Comares, 2019, p. 284.

muy posible especialmente para grupos y organizaciones criminales, el Derecho ha de contemplar esta eventualidad, exigiéndose, de acuerdo con lo señalado por el Dictamen 1/2016 de la Unidad de Criminalidad Informática de la FGE, tanto de los operadores jurídicos, como en particular del Ministerio Fiscal, «unas especiales cautelas en su valoración como medio de prueba»[989].

Esta posibilidad, aun no encontrándose expresamente contemplada en la LECrim, ha sido puesta de manifiesto por la jurisprudencia y, en este sentido, la STS 300/2015, de 19 de mayo, FJ 4.º, en relación con la posibilidad de manipulación de conversaciones mantenidas por redes sociales, ha puntualizado, como idea básica, que «la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas», añadiendo que «la posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas», y que «el anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo»[990].

En cualquier caso, de acuerdo con lo apuntado por ARRABAL PLATERO, «con indiferencia de la naturaleza —tecnológica o no— de la prueba, existen garantías suficientes en el proceso para la expulsión de aquellas que estuviesen adulteradas»[991], teniendo en cuenta, como asimismo afirma la referida autora, que «para los supuestos en los que no pueda probarse la falsedad de una prueba o su manipulación y, por ende,

---

[989] UNIDAD DE CRIMINALIDAD INFORMÁTICA DE LA FISCALÍA GENERAL DEL ESTADO, *Dictamen 1/2016 sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas*, 2016, p. 2, Consultado en https://www.fiscal.es/documents/20142/f1f4b75c-5a89-511d-cca5-ce94c544adf5, el 12 de junio de 2020.

[990] Asimismo, en similar sentido se ha pronunciado la STS 754/2015, de 27 de noviembre, que en relación con la invocación de falta de autenticidad del diálogo mantenido a través de un programa chino denominado «We Chat» utilizado como un modo de comunicación basado en mensajes bidireccionales cortos, tipo «Whatsapp», ha declarado en su FJ 3.º que «las posibilidades de manipulación son muy variadas y el órgano jurisdiccional tiene que ponerse en guardia con todas las cautelas que sean recomendables ante la posibilidad de una superchería». También, en relación con la aplicación «Whatsapp» reitera lo mismo, en su FJ 2.º, la STS 375/2018, de 19 de julio. Existe además numerosa jurisprudencia menor en el mismo sentido, pudiéndose citar, entre otras, las SSAP 99/2020, Sección 22.ª de Barcelona, de 26 de febrero; 283/2020, Sección 2.ª de Cáceres, de 23 de marzo; o 154/2020, Sección 5.ª de Valencia, de 24 de abril.

[991] ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., p. 338.

permanezcan en el proceso, los jueces cuentan con los instrumentos jurídicos que el ordenamiento les dota para valorar el conjunto probatorio con garantías de solvencia»[992].

1.2. Momento procesal para el planteamiento de la impugnación.

La impugnación de la prueba digital, como la de cualquier otra prueba, no puede tener lugar en cualquier momento, sino, como ya hemos indicado anteriormente, debe plantearse con el escrito de calificación provisional en el procedimiento ordinario o con el escrito de defensa en el procedimiento abreviado.

Así lo entiende la jurisprudencia del TS, al afirmar que «la verdadera y propia impugnación puede llevarse a cabo en el escrito de defensa con respecto a la prueba digital aportada por la acusación»[993], habiendo matizado la jurisprudencia menor, refiriéndose al procedimiento abreviado, que al articular una impugnación extemporáneamente, en el trámite de cuestiones previas del art. 786.2 LECrim, «ya no es posible pericial informática alguna, por no poderse practicar en el acto, no existiendo posibilidad procesal de más trámites»[994].

Finalmente, esta postura queda suficientemente avalada por lo declarado por la STS 276/2013, de 18 de febrero, que, acertadamente en su FJ 5.º, pone de manifiesto que «no parece muy próximo a la buena fe procesal guardar el más espeso de los silencios hasta los momentos finales del acto del juicio oral [...] para exteriorizar entonces, y solo entonces, una impugnación del informe pericial sobre la sustancia intervenida que parece obedecer más a razones de estrategia que a un real afán de contradicción».

1.3. Necesidad de razonar la impugnación.

Se ha planteado la cuestión acerca de la necesidad de razonar la impugnación de la prueba digital cuando esta sea formulada por el encausado, problema que no se encuentra previsto en las leyes procesales. Sin embargo, aunque en otras jurisdicciones como la civil o la laboral podría entenderse como un trámite natural a fin de que no se

[992] ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., p. 338-339.
[993] Vid. STS 332/2019, de 27 de junio, FJ 4º.
[994] Vid. SAP 291/2019, Sección 3.ª de Murcia, de 13 de septiembre, FJ º 1. Aclara esta resolución al final del texto mencionado que no existe la posibilidad de más trámites en el juicio oral, fuera de los supuestos de instrucción suplementaria, si bien no es el caso en el asunto enjuiciado.

vea comprometido el principio de igualdad de armas[995]; no resulta del todo claro que, con base en el principio de presunción de inocencia, recaiga sobre el encausado la carga procesal de tener que razonar o aportar un principio de prueba en relación con su impugnación, sin que su actuación se pueda limitar sencillamente a negar la autenticidad de un determinado documento electrónico, como por ejemplo la negación de la autoría de un correo electrónico.

No obstante, como ya hemos mencionado, de estimarse finalmente la impugnación, o lo que es lo mismo si se acreditase que el documento electrónico en cuestión no es auténtico, podría llevar consigo la exclusión de la concreta prueba digital del acervo probatorio. Por consiguiente, de acuerdo con el principio de igualdad de armas en el proceso y teniendo en cuenta que la impugnación puede suponer el desplazamiento de la carga de la prueba de acreditar la autenticidad del documento electrónico a la parte que propuso la prueba digital[996], estimamos que, cuando menos, será exigible que se exprese algún razonamiento que apoye la falta de autenticidad

[995] Siguiendo a MONTERO AROCA, el principio de igualdad en el proceso, con carácter general, «requiere conceder a las partes de un proceso los mismos derechos, posibilidades y cargas, de modo tal que no quepa la existencia de privilegios ni en favor ni en contra de alguna de ellas. Así entendido el principio no es sino consecuencia de aquel otro más general, enunciado en todas las constituciones, de la igualdad de los ciudadanos ante la ley» señalando asimismo que «la existencia del principio de contradicción se frustraría si en la propia ley se estableciera la desigualdad de las partes», dado que «el contradictorio tiene únicamente sentido cuando a !as partes se reconocen los mismos derechos, cargas y deberes procesales. MONTERO AROCA, J., «*Derecho Jurisdiccional I - Parte general*», cit., pp. 253-254. En cuanto al proceso penal, afirma GIMENO SENDRA que «el principio de igualdad de armas es una proyección del genérico principio de igualdad del art. 14 CE en el derecho a un proceso con todas las garantías del art. 24.2, el cual hay que estimarlo vulnerado cuando el legislador crea privilegios procesales carentes de fundamentación constitucional alguna […] o, bien el legislador, bien el propio órgano jurisdiccional crean posibilidades procesales que se le niegan a la parte contraria […] o la gravan indebidamente con cargas procesales desorbitadas (así, por ejemplo, si una presunción legal produjera una inversión de la carga de la prueba que obligara al investigado a la "*probatio diabólica*" de tener que acreditar su propia inocencia), sin que ambas posibilidades y cargas procesales alcancen justificación objetiva y razonable alguna», señalando asimismo que «el encuadramiento, por otra parte, del principio de igualdad de armas en el derecho a un "proceso con todas las garantías" ha de obligar al órgano jurisdiccional a ser absolutamente respetuoso con el cumplimiento del referido principio sobre todo en la administración de la prueba». Vid. GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., pp. 76-77.

[996] Tal y como dice DELGADO MARTÍN, «la existencia de alegaciones impugnatorias con suficiente seriedad puede producir en la práctica un efecto similar a un desplazamiento de la carga de la prueba. De esta forma, la carga recaerá sobre la parte que pretenda la validez probatoria del medio impugnado, quien deberá aportar medios probatorios para acreditar la integridad y/o autenticidad del documento impugnado, frecuentemente mediante pericial». Vid. DELGADO MARTÍN, J., «La prueba del whatsapp», *Diario La Ley - Sección Tribuna*, n.º 8605, 2015, p. 6.

invocada, dado que una impugnación no concretada, debería considerarse una actuación con fines estratégicos no ajustada a las exigencias de la buena fe[997].

En este sentido, doctrinalmente, diversos autores proponen como requisito para que la impugnación pueda ser valorada judicialmente, que se aporte un principio de prueba. Así, ante la posibilidad de que esta actitud procesal impugnatoria se convierta en una tónica general e inmediata, en la que, a cambio de nada y sin mayores justificaciones, se hace recaer sobre la parte que presentó la prueba la carga de probar su integridad, propiciando un desequilibrio entre las partes ciertamente considerable, FUENTES SORIANO estima que «con la finalidad de paliar el desequilibrio que las consecuencias de la impugnación provoca entre las partes, resultaría aconsejable que los Tribunales comenzaran a plantearse la necesidad de exigir un principio de prueba, para admitir a trámite la impugnación»[998].

De forma similar, BERTRÁN PARDO afirma que «las alegaciones que duden de las condiciones de autenticidad o de exactitud de la prueba en las que se fundamente la impugnación han de ser serias, claras y exhaustivas, es decir, han de tener la suficiente entidad para que se produzca el efecto del desplazamiento de la carga de la prueba y la misma recaiga en la parte que aportó al proceso esos documentos impugnados, quien deberá entonces proponer la prueba pericial»[999].

---

[997] Cabe recordar que el art. 247 LEC establece en su apartado 1.º que «los intervinientes en todo tipo de procesos deberán ajustarse en sus actuaciones a las reglas de la buena fe», mientras que en su apartado 2.º establece que «los tribunales rechazarán fundadamente las peticiones o incidentes que se formulen con manifiesto abuso de derecho o entrañen fraude de ley o procesal».

[998] Afirma FUENTES SORIANO que por «principio de prueba» no cabe entender «prueba», ya que «no es la prueba de la impugnación lo que se está requiriendo aportar para admitir a trámite la impugnación, sino tan sólo la presentación de algún elemento externo, indicio o argumento que la dote de una mínima credibilidad o sostenibilidad (v.gr., el dispositivo móvil que formó parte del proceso comunicador, unas claves de acceso para facilitar el rastreo, el disco duro en el que se contiene el e-mail aportado, etc.), citando en apoyo de dicha afirmación la doctrina del TS iniciada con la STS de 29 de noviembre de 1975 - ROJ: STS 1650/1975, que declaró que por principio de prueba cabe entender «todo elemento que, sin servir para formar de una manera plena la convicción del juez sobre la existencia de determinados hechos, induzca, sin embargo a una creencia racional de su certeza». Vid. FUENTES SORIANO, O., «Videos, comunicación electrónica y redes sociales: cuestiones probatorias», *Práctica de Tribunales*, n.º 135, 2018, p. 14.

[999] BERTRÁN PARDO, A. I., «Los contenidos de whatsapp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo», *Noticias jurídicas*, 2015, Consultado en http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgentes-por-delitos-de-violencia-contra-la-muje/, el 6 de junio de 2018.

Para apreciar si existe una impugnación con suficiente seriedad, señala DELGADO MARTÍN, que podrán tenerse en cuenta varios elementos, como son los siguientes:

«En primer lugar, la existencia de razones en las que se fundamente la concreta impugnación, porque en la práctica hay ocasiones en que concurre una mera manifestación impugnatoria sin respaldo alegatorio; así como el propio contenido de las mencionadas razones.

En segundo lugar, la propia diligencia de la parte impugnante al proponer medios probatorios que puedan menoscabar la integridad y/o autenticidad de la prueba digital propuesta de contrario, que ha de ser apreciada en relación con la postura procesal de la parte que propuso la prueba digital»[1000].

La jurisprudencia del TS ha exigido en determinadas ocasiones el razonamiento de la impugnación. Así, por ejemplo, la STS 358/2016, de 26 abril, FJ 1.º, en relación con la impugnación del contenido de unas escuchas telefónicas, ha declarado que «no basta una impugnación genérica como la que se realizó» así como que «no se ajusta a las exigencias de la buena fe procesal ese cuestionamiento puramente estratégico y no concretado»[1001].

Por su parte, la Unidad de Criminalidad Informática de la FGE también se ha pronunciado en relación con esta cuestión, dando por hecho que la impugnación ha de razonarse de una forma seria, al señalar que no siempre se producirá el desplazamiento de la carga de la prueba, sino que el mismo «vendrá determinado necesariamente por la propia razonabilidad y seriedad del planteamiento impugnatorio mismo, cuestión que habrá de valorarse en cada asunto en particular»[1002].

[1000] DELGADO MARTÍN, J., «La prueba del whatsapp», cit., p. 6.

[1001] Asimismo, la STS 409/2014, de 21 de mayo, en su FJ 2.º, en relación con una filmación videográfica, determina que la autenticidad de la misma no se cuestionó expresamente, ya que la defensa, en el trámite de cuestiones previas impugnó las grabaciones en tanto las mismas no fueran objeto de ratificación y reproducción, de tal modo que el TS estima que se trata de una alegación que no constituye una impugnación formal, ya que «no se apunta dato alguno que pueda servir de indicio de una supuesta alteración de la cinta incorporada a autos». Esta sentencia cita la STS 1336/1999, de 20 de septiembre, en la que se rechazó la nulidad del material videográfico, consistente en grabación efectuada por las cámaras de los accesos a una entidad bancaria, que se postulaba por el recurrente en aquel caso basándose en la mera posibilidad de su alteración sin que existiera dato alguno que lo avalara.

[1002] UNIDAD DE CRIMINALIDAD INFORMÁTICA DE LA FISCALÍA GENERAL DEL ESTADO, «*Dictamen 1/2016 sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas*», cit., p. 3.

En definitiva, tal y como dice ARRABAL PLATERO, resulta exigible «una cierta justificación de la impugnación de una prueba tecnológica que le dote de una mínima apariencia de verosimilitud que condicione su admisión»[1003], entendiendo que, *de lege ferenda*, debería regularse un trámite para la impugnación de la prueba en el proceso penal que contemplase esta particularidad, y por tanto, en el caso de impugnarse la prueba, por el impugnante se acreditase con un planteamiento razonado y serio, «que existen disfunciones entre la prueba aportada de contrario y la realidad»[1004].

1.4. El recurso a otros medios de prueba adicionales como corolario de la impugnación.

Como ya hemos dicho anteriormente, en caso de admitirse la impugnación de la prueba una vez formulada mediante un planteamiento serio, es decir, con la aportación de algún indicio o argumento que le atribuya cierta credibilidad, resulta doctrinal y jurisprudencialmente[1005] aceptado que, con carácter general, «se puede producir en la práctica un efecto similar a un desplazamiento de la carga de la prueba, que recaerá sobre la parte que pretenda la validez probatoria del medio impugnado, quien deberá aportar medios probatorios para acreditar la integridad y/o autenticidad del documento impugnado»[1006].

[1003] ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., p. 352.

[1004] ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., p. 352.

[1005] Son diversas las resoluciones del TS que sostienen esta tesis. Así, por ejemplo, las SSTS 499/2019, de 23 de octubre, FJ 3.º; 332/2019, de 27 de junio, FJ 4º; 169/2019, de 28 de marzo, FJ 2.º; y 300/2015, de 19 de mayo, FJ 4.º

[1006] Vid. DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 85. En relación con el desplazamiento de la carga de la prueba, compartimos la opinión de Arrabal Platero (aun cuando no será aplicable en los casos de registros informáticos acordados como diligencia de investigación, sino cuando la acusación impugne una prueba digital propuesta por el acusado), quien señala que este desplazamiento de la carga de la prueba se produce hacia cualquiera de las partes, ya sea acusación o defensa, y en este sentido, «no puede alegarse el derecho a la presunción de inocencia por el acusado para evitar su obligación de fundamentar la verosimilitud de la prueba aportada», dado que «no se trata de probar la inocencia o culpabilidad del acusado, que es aquello que protege el derecho a la presunción de inocencia, sino de exigir al acusado que, si tiene que valerse de una prueba cuya integridad ha sido puesta en duda, dé muestras de su fiabilidad», concluyendo que «el derecho fundamental a la presunción de inocencia del acusado que rige en el proceso penal le exime de probar que no ha cometido los hechos que se le imputan pero no le dispensa de practicar la prueba instrumental frente a la impugnación de contrario de los elementos negativos del delito». Vid. ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., pp. 353-354.

Lo normal en estos casos será la práctica de una prueba pericial que acredite la realidad de los aspectos controvertidos, como la autenticidad del documento electrónico, origen de la comunicación, identidad de los interlocutores, si se ha producido un acceso indebido a un determinado equipo informático, etc.

En este sentido, como por otro lado se desprende de todo lo dicho con anterioridad, estimamos que puede afirmarse, sin lugar a dudas, que la pericial se alza como el medio de prueba más relevante en lo que a la prueba digital se refiere, por cuanto en caso de ser esta impugnada, aun cuando el tribunal valorando otras pruebas en su conjunto podría llegar a un determinado convencimiento, en una mayoría de los casos será necesaria una nueva pericial para desvirtuar lo que se ha pretendido acreditar con la primera.

Ahora bien, no siempre será necesaria una pericial, como así ocurrió en el caso resuelto en casación por la STS 300/2015, de 19 de mayo, en el que tal y como declaró el TS concurrían otras circunstancias probatorias que excluían las dudas sobre la realidad de la conversación, como fueron la declaración de la víctima poniendo a disposición del tribunal la contraseña de su perfil en la red social, a fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial, y la declaración del testigo con el que la víctima mantuvo la conversación.

Este mismo criterio ha sido puesto de manifiesto en el Dictamen 1/2016 de la Unidad de Criminalidad Informática de la FGE, en el que se afirma que la pericial como prueba instrumental en los casos de impugnación de la prueba digital, «solo puede resultar inexcusable cuando no exista posibilidad de acreditar aquéllos extremos por otros medios, tales como la declaración de otros destinatarios de la comunicación, la aportación por el administrador de una red social, previa autorización judicial, del contenido cuestionado u otros»[1007].

Por tanto, tal y como dice FUENTES SORIANO, en virtud del principio de libre valoración de la prueba, pese a lo que a primera vista pudiera parecer, «ni la aportación de la prueba pericial se convierte en el único mecanismo posible para adverar el proceso

[1007] UNIDAD DE CRIMINALIDAD INFORMÁTICA DE LA FISCALÍA GENERAL DEL ESTADO, «*Dictamen 1/2016 sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas*», cit., p. 6.

comunicador cuestionado, ni toda impugnación supondrá el necesario desplazamiento de la carga de la prueba»[1008], de tal modo que «el convencimiento del juez sobre su fiabilidad o credibilidad puede venir apoyado en la corroboración de otros elementos probatorios como pudieran ser la declaración de testigos, las propias manifestaciones de las partes, la existencia de denuncias previas con la misma base, etc.»[1009].

Con base en todo lo anterior, el tribunal deberá tomar en consideración los razonamientos de ambas partes en relación con la prueba digital impugnada así como los demás elementos probatorios incorporados al proceso, para determinar si es necesaria una pericial contradictoria que garantice la autenticidad del documento electrónico o, en su caso, debe valorarse el documento electrónico objeto de prueba de forma conjunta con las demás pruebas, sin que aquella sea necesaria.

2. Valoración de la prueba

Una vez que se ha procedido a la práctica de la prueba, es decir, cuando las partes han finalizado la tarea de intentar convencer al tribunal acerca de la veracidad de los hechos puestos de manifiesto en sus respectivas alegaciones, comienza el proceso de valoración de la misma, entendida como el ejercicio intelectual a realizar por el juez o tribunal mediante el que, a la vista de las pruebas practicadas, decidirá lo procedente en cuanto a la fuerza de las mismas para dotar de verosimilitud tanto a los hechos que se invocan en la petición acusatoria como a las pretensiones de la defensa para excluir o minorar la culpabilidad del acusado o la antijuridicidad de los hechos.

Este proceso de valoración, comenzará con una valoración individual de cada medio de prueba para concluir con una valoración conjunta, proceso que, de acuerdo con DE URBANO CASTRILLO, recorrerá las siguientes etapas:

[1008] FUENTES SORIANO, O., «Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías», cit., pp. 24-25.

[1009] Afirma FUENTES SORIANO, citando a DELGADO MARTÍN, que la valoración judicial de la prueba electrónica conforme a las normas de la sana crítica «… excluye la existencia de regla alguna de distribución formal de la carga de la prueba en caso de impugnación…» ya que «…será el juez o Tribunal quien valore todas las circunstancias concurrentes (medios probatorios utilizados, valoración conjunta de la prueba, postura procesal de las partes) para atribuir o no eficacia probatoria a aquélla prueba». Vid. DELGADO MARTÍN, J., «La prueba del whatsapp», cit., p. 6 y FUENTES SORIANO, O., «Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías», cit., pp. 24-25.

1.ª) Admisión de las pruebas que cumplan las exigencias de pertinencia, licitud y necesidad, rechazándose las que no cumplan estos requisitos.

2.ª) Delimitación del acervo probatorio, es decir, de las distintas pruebas que han de ser valoradas, distinguiendo entre las pruebas de cargo y descargo, puesto que ambas han de ser objeto de valoración.

3.ª) Ponderación individualizada de cada prueba, atribuyendo mayor o menor peso a cada medio probatorio concreto, desde la perspectiva de la sana crítica, concediendo más o menos valor a una u otras pruebas y escasa o nula credibilidad a otras.

4.ª) Toma de decisión, en relación con el *factum*, presupuesto de los pronunciamientos o respuestas a las pretensiones debatidas, resultando relevante la debida motivación del *iter* discursivo empleado para la decisión[1010].

La teoría sobre la valoración de la prueba descansa sobre el método que se adopte para llevar a cabo la misma, por lo que nos referiremos a continuación a los sistemas de valoración existentes en nuestro Derecho Procesal.

2.1. Sistemas de valoración de la prueba

2.1.1. Sistemas vigentes en el Derecho Procesal español

Existen actualmente en nuestro sistema procesal dos métodos de valoración probatoria, como son los de libre valoración y prueba legal o tasada. Como se ha puesto de manifiesto doctrinalmente, «en el ordenamiento español no rige en exclusiva uno de los dos sistemas puros de valoración de la prueba, sino que se ha optado por un sistema mixto, en el que se han pretendido combinar armónicamente algunas reglas legales con la sana crítica»[1011].

La distinción entre ambos sistemas la explica TARUFFO señalando que «la técnica de la prueba legal consiste en la producción de reglas que predeterminan, de forma general y abstracta, el valor que debe atribuirse a cada tipo de prueba»[1012], mientras que

[1010] DE URBANO CASTRILLO, E., *La valoración de la prueba electrónica*, Valencia, Tirant Lo Blanch, 2009, pp. 29-30.
[1011] MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», cit., p. 61.
[1012] TARUFFO, M., *La prueba de los hechos*, Madrid, Editorial Trotta, 2005, p. 387.

«el principio opuesto, de la prueba libre o de la libre convicción, presupone la ausencia de aquellas reglas e implica que la eficacia de cada prueba para la determinación del hecho sea establecida caso a caso, siguiendo criterios no predeterminados, discrecionales y flexibles, basados esencialmente en presupuestos de la razón»[1013].

Es decir, el sistema de prueba tasada comporta un mandato legal al órgano judicial para que, con independencia de su apreciación y convencimiento personal, observe unas normas preestablecidas que le indicarán si un concreto hecho ha de considerarse probado. Se trata de un sistema sobre el que existen voces críticas, que postulan su completa desaparición del sistema, como la de NIEVA FENOLL, quien afirma que «el sistema de prueba legal es, en realidad, una anomalía histórica que ha durado demasiado tiempo»[1014].

El principio de libre valoración de la prueba, es el sistema que impera con carácter general en nuestro Derecho Procesal, de acuerdo con lo dispuesto en el art. 218.2 LEC[1015]. No obstante, en el proceso civil, como decíamos, rige un sistema mixto, ya que, de acuerdo con el art. 319.1 LEC[1016], la «documental pública» tiene el carácter de prueba legal o tasada[1017], circunstancia que no se da en el proceso penal, en el que no

---

[1013] TARUFFO, M., *La prueba de los hechos*, Madrid, Editorial Trotta, 2005, p. 387.

[1014] NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», *Ars Iuris Salmanticensis*, n.º 5, Junio, 2017, p. 59. En el resumen inicial de este trabajo NIEVA FENOLL expone lo siguiente: «El sistema de valoración legal de la prueba hace tiempo que está claramente marginado en el proceso civil, y es legalmente inexistente en el proceso penal. Sin embargo, la larga vigencia del mismo, más por el uso forense que por disposición legal, ha determinado que actualmente todavía se encuentren inexplicables manifestaciones del antiguo sistema que deben ser abolidas. Entre ellas se cuentan la valoración, todavía legal, de la prueba documental en el proceso civil, los juramentos y promesas, incomprensibles hoy en día, así como la propia concepción de la mismísima carga de la prueba, o incluso el estudio de las presunciones. Todo ello conserva a día de hoy un análisis impropio de un sistema en el que rige la libre valoración de la prueba, lo que impide el pleno desarrollo científico de este sistema, que afecta, lógicamente, a la práctica de los tribunales».

[1015] El art. 218.2 LEC, tras establecer que «las sentencias se motivarán expresando los razonamientos fácticos y jurídicos que conducen a la apreciación y valoración de las pruebas, así como a la aplicación e interpretación del derecho», determina la aplicación del principio de libre valoración al continuar disponiendo que «la motivación deberá incidir en los distintos elementos fácticos y jurídicos del pleito, considerados individualmente y en conjunto, ajustándose siempre a las reglas de la lógica y de la razón».

[1016] El art. 319.1 LEC establece que «con los requisitos y en los casos de los artículos siguientes, los documentos públicos comprendidos en los números 1.º a 6.º del artículo 317 harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella».

[1017] Siguiendo a GIMENO SENDRA, «la LEC tan solo conoce como prueba tasada a la documental pública, que hará "*prueba plena del hecho, acto o estado de cosas que documenten*", salvo que versen sobre

existe ninguna excepción legal al referido principio de libre valoración, resultando el mismo aplicable en relación con todas las pruebas practicadas.

Por tanto, como ya hemos indicado, en el derecho procesal penal rige con exclusividad el principio de libre valoración de la prueba proclamado en el art. 741.1 LECrim, de acuerdo con el que «el Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley».

2.1.2. La transición del sistema de prueba tasada al de libre valoración, pasando por el sistema de la íntima convicción

Aunque previamente no lo hemos mencionado, con anterioridad al establecimiento del sistema de libre valoración, obviando los antiguos sistemas de la prueba ordálica y apriorística[1018], subsistió durante un tiempo otro sistema de valoración denominado de la «íntima convicción»[1019], respecto del que estimamos necesarias unas

---

materia de usura en cuyo caso rige la libre valoración (art. 319.3). Rechaza este autor que la prueba de «interrogatorio de las partes» tenga el carácter de tasada, manteniendo que se trata de una prueba de libre valoración, dado que, «si bien es cierto que el juez habrá de tener como ciertos los hechos reconocidos y que sean perjudiciales para las partes, tampoco lo es menos que dicho valor privilegiado queda condicionado a que no lo contradiga "el resultado de las demás pruebas" (art. 316), lo que convierte a dicho interrogatorio en una prueba de valoración conjunta». Asimismo, «las demás pruebas han de ser valoradas con arreglo a las normas de la "sana crítica", es decir, según las máximas de la experiencia y de la lógica o, lo que es lo mismo, con arreglo al sistema de libre valoración; de este modo están sometidos a dicho criterio de las reglas de la sana crítica: los documentos privados (art. 334.1), el dictamen de peritos (art. 348), la prueba de testigos (art. 376) y las reproducciones de la palabra, imagen y sonido (art. 382.3)». Vid. GIMENO SENDRA, J. V., *Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*, Majadahonda (Madrid), Editorial Colex, 2007, pp. 49-50.

[1018] Para un breve y sin embargo completo resumen de lo que fueron las pruebas ordálica y apriorística, vid. MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», cit., pp. 54-56.

[1019] Algunos autores como ARRABAL PLATERO no consideran este método un auténtico sistema de valoración ya que «está basado en la intuición objetiva del juez y es huérfano de cualquier tipo de motivación». En este sentido, afirma esta autora que aun cuando algunos autores se refieren al principio de «libre valoración» como sistema de «valoración en conciencia o de íntima convicción (v. gr. MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 442), tal y como señala BUJOSA VADELL, no hay que interpretar literalmente estas cláusulas normativas de «apreciación en conciencia» o de «íntima convicción», dada la exigencia constitucional de motivación de las sentencias como manifestación de la tutela judicial efectiva de los Juzgados y Tribunales (BUJOSA VADELL, L. M., «La valoración de la prueba electrónica», en Bueno de Mata, F. (coord.), *Fodertics 3.0*, Albolote (Granada),

breves consideraciones, a fin de dejar constancia de las limitaciones que surgieron a este principio, llegando así al principio de libre valoración.

Dice GIMENO SENDRA que «el sistema de prueba legal responde, en sus primitivos orígenes, a un pensamiento mítico o supersticioso del antiguo Derecho germánico, con arreglo al cual determinados medios probatorios, realizados ante una supuesta intervención divina, debían causar "prueba plena"»[1020] añadiendo que este sistema «permaneció vigente a lo largo de toda la Edad Media, siendo potenciado en el proceso penal hasta límites de inhumanidad durante la hegemonía del absolutismo»[1021].

Otros autores, como NIEVA FENOLL, sitúan el origen de la prueba tasada en el Código de Hammurabi, donde se establecían normas muy precisas en relación con la prueba de testigos, dirigidas al juez sobre el modo de proceder probatorio para dictar su sentencia en el proceso, de tal modo que se creó la regla conforme a la que, para dar por probado un hecho, debía existir una pluralidad de testigos y no uno solo, regla que la encontramos en el Codex de Justiniano, en el que también se encuentran los primeros trasuntos del valor privilegiado de la prueba documental[1022].

Frente a este sistema, continúa GIMENO SENDRA, como una conquista del pensamiento liberal, surgió, hacia finales del S. XVIII y principios del S. XIX, el de la «libre valoración de la prueba», que aparece en la historia como una institución íntimamente ligada a la del Jurado, dado que no era posible exigir al pueblo el conocimiento de las complejas reglas de valoración de la prueba tasada, que desde la legislación de Partidas hasta la Novísima Recopilación, se habían mantenido, tanto en el proceso civil como en el penal, por lo que los autores de la Ilustración decidieron que el Jurado presenciara el juicio oral y emitiera su veredicto exclusivamente con arreglo a su «íntima convicción»[1023].

Editorial Comares, 2015, p. 81). Vid. ARRABAL PLATERO, P., «*La Prueba Tecnológica: Aportación, Práctica y Valoración*», cit., p. 393.

[1020] GIMENO SENDRA, J. V., «*Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*», cit., p. 46.

[1021] GIMENO SENDRA, J. V., «*Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*», cit., p. 46.

[1022] NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», cit., pp. 59-60.

[1023] Afirma GIMENO SENDRA que este sistema se reveló como mucho más perfecto que el de la prueba tasada, dando lugar, como consecuencia del conocimiento solo de los actos de prueba por el Jurado y consecuentemente el desconocimiento por el mismo de los actos de investigación, al fortalecimiento del sistema acusatorio, dado que las partes tenían la carga procesal de ser exhaustivas con la aportación del

De este modo, tal y como afirma NIEVA FENOLL, «con la introducción de la "íntima convicción" se cumplían las aspiraciones seculares de varios juristas que habían denunciado la absurdidad del sistema de valoración legal»[1024]. Sin embargo, este nuevo método de valoración no nace con la configuración actual, sino como un sistema intermedio entre la prueba tasada y el de libre valoración de la prueba, no identificado con este último, por cuanto la «íntima convicción» era un sistema propenso a transformar una pretendida discrecionalidad en arbitrariedad, y ello dado que, conforme señala MONTERO AROCA, este principio «se resolvía en dos postulados: 1) La valoración de la prueba no consiste en un ejercicio de la razón, sino en una declaración de voluntad, y 2) esa declaración no tiene que ser motivada»[1025].

Este método de apreciación en conciencia sin limitación alguna para el juzgador, tuvo su origen en Inglaterra, donde el sistema de la prueba legal se encontraba atemperado por el recurso al «*the best of their knowledge*», expresión coloquial que finalmente emergió con la «*intime conviction*», desarrollada conjuntamente con el jurado por la Constitución francesa de 1791.

Sin embargo, en línea con lo indicado anteriormente, no fueron pocas las dificultades para superar el sistema de prueba legal, expone NIEVA FENOLL, pues existían opiniones en favor del sistema de valoración legal, al entender que este ofrecía mayor seguridad jurídica que un uso difícilmente controlable de la «conciencia» de los juzgadores[1026].

Fue finalmente en Alemania, donde Savigny y otros, explicaron que «libre valoración no significa arbitrariedad y falta de motivación, sino todo lo contrario»[1027]. A partir de ahí se comienza a introducir en los Códigos europeos el sistema de libre

---

material de hecho y su prueba en juicio, de tal modo que el juicio oral dejó de ser un mero apéndice de la fase instructora para convertirse en un auténtico proceso. Vid. GIMENO SENDRA, J. V., «*Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*», cit., p. 47.

[1024] Vid. NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», cit., pp. 62-63.

[1025] Dice MONTERO AROCA que «por este camino de la íntima convicción se acaba en la arbitrariedad y en la irresponsabilidad, y lo más grave es que se descubrió inmediatamente que la íntima convicción no tenía porqué ser exclusiva del jurado y del proceso penal, sino que podía también referirse a los jueces técnicos y al proceso civil». Vid. MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», cit., pp. 58-59.

[1026] NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», cit., pp. 63-64.

[1027] NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», cit., p. 64.

valoración con la configuración actual, llegando a España con el Reglamento sobre el modo de proceder el Consejo Real en los negocios contenciosos de la Administración de 30 de diciembre de 1846, en cuyo art. 148 se introduce por primera vez el concepto «reglas de la sana crítica», incorporándose en la LEC de 1855 para la valoración de las declaraciones de los testigos y en la Ley de Enjuiciamiento Civil de 1881 con respecto a la prueba pericial[1028], siendo de reseñar igualmente que el art. 741.1 LECrim conserva en la actualidad su redacción original de 1882.

Así, aunque la «íntima convicción» siguió siendo aplicable a los jurados[1029], ya no era posible mantener este sistema para la resolución de los casos por los jueces profesionales, ante el surgimiento de las «reglas de la sana crítica» como un límite infranqueable al mismo, que finalmente, con la aplicación de dichas reglas, quedó convertido en el vigente principio de libre valoración de la prueba.

Sin embargo, no puede afirmarse que en lo que atañe al proceso penal se aplicasen estrictamente las reglas de la sana crítica, siendo ya tras la CE de 1978 cuando de forma definitiva ha quedado desterrado este sistema, interpretándose el término previsto en el art. 741 LECrim «apreciación en conciencia», de acuerdo con el sistema de libre valoración, como así se desprende de la copiosa jurisprudencia, tanto del TC[1030] como del TS[1031]. Ambos tribunales, con base en el derecho constitucional a la presunción

---

[1028] Vid. NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», cit., p. 64

[1029] No está de más señalar que la Ley del Jurado de 20 de abril de 1888 (publicada en la Gaceta de Madrid de 25 de abril de 1888 y que permaneció vigente hasta la suspensión de la misma por Decreto de 8 de septiembre de 1936) se refería a la «íntima convicción de los jurados» en su art. 72-II al disponer que «sin perjuicio de la cuestión de culpabilidad o inculpabilidad del agente, sobre la cual declaran los Jurados con libertad de conciencia…» y en el art. 84 donde se disponía que «la votación será nominal y en alta voz, contestando cada uno de los jurados según su conciencia bajo el juramento prestado, a cada una de las preguntas *sí* o *no*». Por su parte, la vigente LO 5/1995, de 22 de mayo, del Tribunal del Jurado, dice en el apartado II de su exposición de motivos, dedicado a «los ciudadanos jurados», que «la Ley tiene muy en cuenta que el juicio por Jurados constituye expresión plena de los principios básicos procesales de inmediación, prueba formada con fundamento en la libre convicción, exclusión de pruebas ilegales, publicidad y oralidad», por lo que, añade, «se han seleccionado aquellos delitos en los que la acción típica carece de excesiva complejidad o en los que los elementos normativos integrantes son especialmente aptos para su valoración por ciudadanos no profesionalizados en la función judicial».

[1030] Vid. SSTC 31/1981, de 28 de julio, FJ 3.º; 140/1985, de 21 de octubre, FJ 3.º; 150/1987, de 1 de octubre, FJ 2.º; y 94/1990, de 23 de mayo, FJ 2.º

[1031] Cabe destacar la STS de 9 de septiembre de 1992 - ROJ: STS 6715/1992, que en su FJ 1.º declaró que para condenar «no basta con la probabilidad de que el imputado sea el autor, ni con la convicción moral de que así ha sido», sino que «es imprescindible que por procedimientos legítimos se haya alcanzado la certeza jurídica, que no es, desde luego, certeza absoluta pero que, siendo convicción nacida de pruebas de

de inocencia, «pusieron coto a la práctica forense de entender que el juez estaba limitado solamente por su conciencia, sin necesidad de justificar su decisión»[1032].

2.2. El principio de libre valoración

Hablar de libre valoración tiene como condición la libertad del juez, por cuanto de existir prueba tasada, es decir, prueba cuyo resultado ya se encuentra prefijado por el legislador, no se podría hablar de tal libertad, y en tal sentido afirma CALVO CABELLO que «el juez ha de ser libre para valorar las pruebas […], sin esa libertad apreciativa, no hay valoración judicial […] habrá una fijación de hechos sometiéndose a las pautas impuestas por el legislador, pero no una valoración»[1033].

Ahora bien, en atención a todo lo expuesto en los apartados anteriores, esta libertad, de acuerdo con lo señalado por GÓMEZ ORBANEJA, no significa que el juez pueda seguir su capricho o entregarse a la conjetura o a la sospecha, sino que «supone una deducción racional, partiendo de unos datos fijados con certeza»[1034]. Por su parte, GIMENO SENDRA, en similar sentido, afirma que «apreciación en conciencia no significa libre arbitrio, sino que el Tribunal debe motivar su sentencia, lo que en el ámbito del proceso penal (en el que no existe ninguna prueba privilegiada que exonere al juez de dicho deber de motivación…), significa fundamentalmente razonar la prueba»[1035].

Del mismo modo, la jurisprudencia del TS ha dejado sentado en numerosas ocasiones que «la "estimación en conciencia" a que se refiere el art. 741 LECrim, no ha de entenderse o hacerse equivalente a cerrado e inabordable criterio personal e íntimo

---

signo acusatorio, es suficiente para legitimar, desde el punto de vista procesal y constitucional, una sentencia condenatoria», concluyendo que «el Derecho Procesal, que trae causa directa en nuestra Constitución, exige una certeza que derive de una evidencia, desde el punto de vista jurídico, en el sentido de que el proceso de reflexión judicial ha de tener su soporte en pruebas inequívocamente de cargo que, de alguna manera, con las inevitables posibilidades de error propias del intelecto humano, evidencian la realidad del hecho y de la participación […], nuestro derecho está construido sobre el principio "in dubio pro reo" de tal manera que, incluso si esa prueba de cargo está acompañada de otra de descargo o ella sola entraña una duda razonable, el Tribunal habrá de absolver o pronunciarse en el sentido más favorable al reo».

[1032] MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., «*Derecho Procesal Penal*», cit., p. 442.

[1033] CALVO CABELLO, J. L., «La valoración de la prueba en el juicio oral», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, p. 445, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[1034] GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., «*Derecho Procesal Civil, Vol. I*», cit., pp. 295-296.

[1035] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., pp. 95-96.

del juzgador, sino a una apreciación lógica de la prueba, no exenta de pautas o directrices de rango objetivo», señalando que entre estas reglas «se encuentran, desde luego, todas las que rigen el proceso penal y lo configuran como un proceso justo, con todas las garantías, las que inspiran el principio de presunción de inocencia y las reglas de la lógica y la experiencia conforme a las cuales han de realizarse la inferencias que permitan considerar un hecho como probado»[1036].

Asimismo, ha declarado el alto Tribunal que «la íntima convicción, la "conciencia" del Juez en la fijación de los hechos no puede conformarse al margen de las reglas de la experiencia y de la necesidad de exteriorización»[1037]. Así, a modo de ejemplo, pone de manifiesto que «el porqué se cree a un testigo o porqué [sic] se descarta un testimonio no puede convertirse en un ejercicio de decisionismo judicial no controlable…»[1038].

Estas pautas que han de observarse para llevar a cabo la tarea valorativa, quedando reflejadas en la sentencia mediante la oportuna motivación del tribunal, no son otras que las del respeto a la lógica, a las máximas de experiencia y a los conocimientos científicos, que conjuntamente conforman las ya mencionadas «reglas de la sana crítica», de las que nos ocupamos a continuación.

2.3. Las reglas de la sana crítica

De acuerdo con lo expuesto, en la actualidad, hablar de la «sana crítica» supone referirse a un criterio corrector de la «íntima convicción», mediante el que el juez o tribunal, ha de fundamentar su decisión explicitando los motivos de la misma, garantizando así la racionalidad del proceso de «libre valoración».

Se trata de un concepto que, históricamente, más que como un criterio corrector, ha sido considerado como un auténtico sistema de valoración. Así lo entiende COUTURE, quien afirma que «este concepto configura una categoría intermedia entre la prueba legal y la libre convicción»[1039], dado que «sin la excesiva rigidez de la primera y sin la

[1036] Vid. SSTS 555/2019, de 13 de noviembre, FJ 1.º; 216/2019, de 24 de abril, FJ 6.º; y 162/2019, de 26 de marzo, FJ 1.º

[1037] Vid. STS 364/2015, de 23 de junio, FJ 1.º

[1038] Vid. STS 364/2015, de 23 de junio, FJ 1.º

[1039] COUTURE, E. J., *Fundamentos del Derecho Procesal Civil*, Buenos Aires, Ediciones Depalma, 1958, p. 270.

excesiva incertidumbre de la última, configura una feliz fórmula, elogiada alguna vez por la doctrina, de regular la actividad intelectual del juez frente a la prueba»[1040].

Sin embargo, en la actualidad, de acuerdo con ASENCIO MELLADO, «la inmensa mayoría de la doctrina viene entendiendo que la sana crítica no constituye un tercer sistema valorativo, sino que por el contrario, se identifica con la libre valoración que, de este modo, es conceptuada como apreciación acorde con las reglas de la sana crítica»[1041].

En la LECrim no se menciona la valoración de la prueba conforme a las reglas de la sana crítica, refiriéndose al «criterio racional» (art. 717) y «apreciación según su conciencia» (arts. 741 y 973). Sin embargo, sí se ordena como tal en la LEC para la valoración de las distintas pruebas[1042]. Pero lo cierto es que no se concreta en ningún precepto de nuestro ordenamiento jurídico procesal[1043], cuáles son estas reglas de la sana crítica[1044].

Según apunta BARRIOS GONZÁLEZ, con motivo del debate de la LEC de 1855 «se intentó formularlas dos veces en la Comisión Codificadora […], mas hubo de desistirse de este propósito ante la imposibilidad de fijarlas de una manera taxativa y, por eso, no se hallan determinadas ni en ése ni en ningún otro texto legal»[1045].

El Diccionario del español jurídico de la RAE[1046] define la sana crítica como «criterio para la valoración de la prueba conforme a un raciocinio lógico». Por ello, teniendo en cuenta que las reglas de la sana crítica son, fundamentalmente, reglas de un justo entendimiento, tal y como ha declarado la jurisprudencia del TS, aunque las

---

[1040] COUTURE, E. J., «*Fundamentos del Derecho Procesal Civil*», cit., p. 270.

[1041] ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., p. 36.

[1042] Vid. arts. 316.2, 326.2, 334.1, 348, 350.4, 376, 382.3 y 384.3 de la LEC.

[1043] Sí que aparecen expresamente citadas, señala DE URBANO CASTRILLO, en los Códigos procesales de países de nuestra órbita cultural civiles, tales como Argentina, Chile, Colombia y Venezuela. Vid. DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 31.

[1044] En el Anteproyecto de LECrim de 2013, se dio un cierto impulso a este punto al disponer el art. 6.3 que «las pruebas serán libremente valoradas por el Tribunal, conforme a las reglas de la lógica, de la ciencia y las máximas de la experiencia».

[1045] En relación con esta mención de los debates parlamentarios de la LEC de 1855, BARRIOS GONZÁLEZ hace referencia a una cita de la obra AGUILERA DE PAZ, E.; RIVAS MARTÍ, F., *Derecho Judicial Español*, Madrid, Editorial Reus, 1920, pp. 846-847. Asimismo en la nota al pie n.º 4 se refiere a otras obras en las que se menciona este dato histórico. Vid. BARRIOS GONZÁLEZ, B., «Teoría de la sana crítica», *Opinión Jurídica: Publicación de la Facultad de Derecho de la Universidad de Medellín*, vol. 2, n.º 3, 2003, p. 101, Consultado en https://revistas.udem.edu.co/index.php/opinion/index, el 1 de junio de 2020.

[1046] Acceso a través de la web, https://dej.rae.es/.

concretas reglas de la sana crítica «no se hallan recogidas en precepto alguno», en definitiva, «están constituidas por las exigencias de la lógica, los conocimientos científicos, las máximas de la experiencia y, en último término, el sentido común»[1047].

Por tanto, la libre valoración de la prueba exige que la motivación de la decisión que se adopte finalmente en sentencia, no contradiga los principios de la lógica, de las máximas de experiencia y de los conocimientos científicos, sin que el juez o tribunal pueda, en ningún caso, hacer uso de su conocimiento privado de los hechos, salvo que se trate de hechos notorios, de acuerdo con lo dispuesto en el art. 281.4 de la LEC, que dispone que «no será necesario probar los hechos que gocen de notoriedad absoluta y general». No obstante, como dice GIMENO SENDRA, «solo los hechos notorios evidentes (es decir, aquellos de fama pública absoluta, tales como fechas históricas, lugares geográficos, etc.) excluyen la actividad probatoria»[1048].

2.3.1. Los principios de la lógica

Según el DRAE, el vocablo «lógico o lógica» tiene diversas acepciones, de las que nos interesan la cuarta y la quinta en las que respectivamente se define como un adjetivo del siguiente modo: «4. Dicho de una consecuencia: Natural y legítima. 5. Dicho de un suceso: Que tiene antecedentes que lo justifican».

En este sentido, algunas afirmaciones doctrinales como la de COLOMA CORREA Y AGÜERO SAN JUAN sostienen que las reglas de la lógica «instituyen los límites del ejercicio del razonamiento»[1049], y de forma similar otros autores como ZUBIRI DE SALINAS señalan que «la valoración de la prueba ha de hacerse conforme a las reglas de

[1047] Vid. SSTS 1103/2007, de 21 de diciembre, FJ 3.º; 1125/2011, de 2 de noviembre, FJ 8.º; y 19/2020, de 28 de enero, FJ 3.º

[1048] Por tanto, el concepto de notoriedad debe ser tratado con cautela, dado que, como puntualiza GIMENO SENDRA, «para que un hecho sea considerado como notorio es necesario que el mismo sea conocido y tenido por cierto por una generalidad de personas dotadas de una cultura media, en el lugar y tiempo en que se dicta la resolución». Por ello, continúa el citado autor «la notoriedad es, pues, un concepto indeterminado y relativo; no solo depende del lugar y del tiempo, sino también del nivel cultural de las personas» y también «de que sea conocida por el juez, ya que, en caso contrario, será necesaria su prueba». Vid. GIMENO SENDRA, J. V., «*Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*», cit., p. 400.

[1049] COLOMA CORREA Y AGÜERO SAN JUAN, realizan un amplio estudio de las reglas de la sana crítica. Vid. COLOMA CORREA, R.; AGÜERO SAN JUAN, C., «Lógica, ciencia y experiencia en la valoración de la prueba», *Revista Chilena de Derecho*, vol. 41, n.º 2, 2014, p. 682, Consultado en https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-34372014000200011&lng=en&nrm=iso&tlng=es, el 3 de junio de 2020.

la lógica, sin que los razonamientos del tribunal sean arbitrarios, incoherentes o contradictorios, o lleven al absurdo»[1050].

Las reglas de la lógica tienen especial incidencia en la valoración de las pruebas de interrogatorio del acusado, testifical y documental. Como dicen COLOMA CORREA Y AGÜERO SAN JUAN, la lógica se sitúa en un nivel diferente que los conocimientos científicos y las máximas de la experiencia, dado que, a diferencia de estos, «la lógica no regula la introducción de información al proceso de análisis del caso, sino que vela por la corrección comunicativa de lo que puede ser pensado o imaginado»[1051]. En este sentido, para mostrar la conexión entre las declaraciones vertidas en el juicio oral por acusados y testigos y las conclusiones a las que se llegue por el juez o tribunal, deberán establecerse motivadamente unos razonamientos, que resulten coherentes por las propias reglas de la lógica[1052].

Con base en lo anterior, podemos concluir que la valoración de la prueba no se ajustará a los principios de la lógica, cuando no exista corrección en la motivación, en el sentido de que las consecuencias obtenidas no sean naturales o legítimas o se aparten de forma irracional de los antecedentes que debieran justificarlas.

2.3.2. Las máximas de la experiencia

Siguiendo a STEIN cabe definir las máximas de la experiencia como «definiciones o juicios hipotéticos de contenido general, desligados de los hechos concretos que se juzgan en el proceso, procedentes de la experiencia, pero

[1050] ZUBIRI DE SALINAS, F., «¿Qué es la sana crítica? La valoración judicial del dictamen experto», *Jueces para la Democracia. Información y Debate*, n.º 50, 2004, p. 54.

[1051] COLOMA CORREA, R.; AGÜERO SAN JUAN, C., «Lógica, ciencia y experiencia en la valoración de la prueba», cit., p. 682.

[1052] Diversas sentencias de la jurisprudencia menor, han declarado que «la libertad de apreciación de las declaraciones testificales no quiere decir apreciación arbitraria del resultado de la prueba, sino operación crítica y lógica», añadiendo que si bien «la LEC prescinde de indicar circunstancias y formular reglas para esta apreciación, remitiéndose a la experiencia y buen sentido del juzgador, debiendo tenerse en cuenta las relaciones del testigo con las partes y con los hechos sobre los que declara, la razón de ciencia de sus contestaciones, las respuestas que da a las preguntas, desconocidas por el testigo hasta el momento que se le formulan, explicaciones que el juez puede pedirle para el esclarecimiento de los hechos, y resto de circunstancias concurrentes en el testigo, tanto por lo que se refiere a su conducta procesal, como respecto a los datos personales de él y demás elementos de referencia que servirán para determinar y valorar la certeza de los juicios emitidos por el testigo». Vid. SSAP 410/2016, Sección 1.ª de Pontevedra, de 8 de septiembre; y 695/1999, Sección 3.ª de Granada, de 10 de septiembre.

independientes de los casos particulares de cuya observancia se han deducido y que, por encima de esos casos, pretenden tener validez para otros nuevos»[1053].

ASENCIO MELLADO, afirma que de acuerdo con las máximas de la experiencia «se suele aceptar en la vida como verdadero aquello que se corresponde al uso habitual de las cosas y a su decurso natural»[1054].

En similar sentido, señala FERNÁNDEZ ENTRALGO, «las máximas de experiencia no son, en definitiva, más que la condensación de la observación empírica colectiva y sucesiva de hechos análogos, hasta formular una conclusión sobre "lo que suele ocurrir" *(id quod plerumque accidit)* dadas unas determinadas circunstancias»[1055].

En este sentido, podemos afirmar que se trata de reglas o consecuencias generales que, con base en el sentido común y en relación con determinados sucesos, son admitidas por todos. Su importancia es grande en la valoración de la prueba indiciaria y en aquellos casos en que un experto ilustra sobre la explicación de un hecho, existiendo numerosos pronunciamientos en los que son aplicadas en la prueba indiciaria[1056], dependiendo su credibilidad «del grado de excepciones que admita»[1057].

No obstante, las máximas de la experiencia tienen algunos inconvenientes, produciéndose, como ahora veremos, cierta colisión entre estas y los conocimientos científicos, dado que, como dice IGARTUA SALAVERRÍA, «las máximas de la experiencia son generalizaciones que están consteladas de excepciones; porque es variable su base empírica y la tasa de regularidad observada; porque las máximas no están recogidas en

---

[1053] STEIN, F., *El conocimiento privado del juez* (traducido por DE LA OLIVA SANTOS, A.), Madrid, Editorial Ramón Areces, 1990, p. 22.

[1054] En relación con este aserto, el autor cita a ROSENBERG, L., *Tratado de Derecho Procesal Civil. Tomo II*, Buenos Aires, Ediciones Jurídicas Europa-América, 1955, pp. 200-201. Vid. ASENCIO MELLADO, J. M., «*Prueba prohibida y prueba preconstituida*», cit., p. 16.

[1055] FERNÁNDEZ ENTRALGO, J., «Los conocimientos privados del juez en materia psicológica. Las posibilidades de introducirlos para argumentar su convicción», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 53, 2010, p. 22, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[1056] Así, por ejemplo, la STS de 12 de junio de 1991 - ROJ: STS 3181/1991, en su FJ único, ha considerado una máxima de la experiencia, el hecho de que una persona que no es drogadicta, que se encuentra en un bar y tiene en su poder drogas diversas, en cantidades superiores a lo acostumbrado, debe tener el propósito de —de alguna manera— entregarlas a otros. Asimismo, la STS 974/2012, de 5 de diciembre, en su FJ 9.º, ha estimado que es una máxima de la experiencia que un individuo que participa en un delito de blanqueo de capitales tiene la intención de lucrarse.

[1057] Vid. DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 33.

un texto ni se sabe quién las formuló (a diferencia de los conocimientos científicos); porque, ante un mismo caso, a menudo ocurre que sean utilizables máximas que conducen a resultados diferentes»[1058].

Finalmente, de acuerdo con lo apuntado por PEREDA GÁMEZ, «no cabe confundir las máximas de experiencia con los juicios de valor del tribunal recogidos a través de las presunciones judiciales, en tanto a través de las máximas de experiencia se sientan conclusiones razonables en un orden normal de las cosas […] mientras que la construcción de las presunciones parte de la constatación de un hecho base del que se trata de deducir un hecho consecuencia con respeto a las "reglas del criterio humano"»[1059].

Con base en todo lo anterior, podemos concluir que, del conjunto de toda la prueba practicada, el juez o tribunal podrá tener en consideración las máximas de la experiencia —con independencia de que sean técnicas, normativas, sociales, culturales— de las que tenga conocimiento, ya sea este último propio o aportado mediante una pericial, y ello, siempre que doten de un cierto valor de probabilidad a la inferencia final.

2.3.3. Los conocimientos científicos

A diferencia de las máximas de la experiencia, en las que las consecuencias se encuentran demostradas por la observación empírica de los hechos, los conocimientos científicamente afianzados se encuentran asociados con nociones avaladas por la ciencia, que no son conocidas por todos.

[1058] Por ello, continúa el referido autor, «habrá que prescindir de las "máximas" que contradigan algún conocimiento científico, o que sean incompatibles con otras máximas o que no sean reconocidas como tales en la comunidad de referencia», y por tanto «no habrá que absolutizar la máxima excluyendo cualquier excepción, ni atribuirle un grado de probabilidad que no le corresponde, ni preferirla frente a otra máxima de superior probabilidad, ni primarla frente a otra máxima más específica». Vid. IGARTUA SALAVERRÍA, J.; HERNÁNDEZ GARCÍA, J., «Valoración de la prueba», en Hernández Garcia, J. (dir.), *113 cuestiones básicas sobre la prueba en el proceso penal*, Madrid, Cuadernos Digitales de Formación del Consejo General del Poder Judicial, 2013, pp. 705-706, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

[1059] GASCÓN ABELLÁN, M. Y OTROS, «La motivación fáctica», en Hernández García, J. (dir.), *123 cuestiones básicas sobre la motivación de las resoluciones judiciales*, Madrid, Cuadernos Digitales de Formación del Consejo General del Poder Judicial, 2012, p. 279, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

Los conocimientos científicos se manifiestan en el proceso mediante la prueba pericial, mediante la que el perito deberá aportar, en palabras de ABELL LLUCH, unas máximas de la experiencia técnicas, distintas de las comunes, de las que el juez, en principio, carece[1060]. En este sentido, tal y como dice DE URBANO CASTRILLO, «las máximas de la experiencia tienen su punto flaco: no son verdades axiomáticas, salvo que hablemos de otra cosa, como el conocimiento científico…»[1061], por lo que como ya dijimos con anterioridad, siguiendo a IGARTUA SALAVERRÍA, «habrá que prescindir de las "máximas" que contradigan algún conocimiento científico…»[1062].

No obstante, con arreglo a lo que acabamos de decir, señala ABEL LLUCH que pudiera parecer, a priori, que una vez que se requieren conocimientos científicos que no pueden quedar acreditados por máximas de la experiencia, podrían confundirse las funciones del perito y del juez, atribuyéndose al perito una función que no le es propia. Sin embargo, aclara el referido autor, «al perito le corresponde ofrecer unos datos y al juez interpretar los datos en función de la hipótesis sujeta a controversia»[1063], de tal modo que «el perito aporta unas máximas de experiencia técnicas, y el juez declara o no probados unos hechos controvertidos, atendiendo a la valoración de la prueba pericial, conjuntamente con el resto de las pruebas practicadas»[1064].

Por tanto, el juez no queda vinculado por el informe pericial, pero debe aprehender la ciencia aportada por el perito y aplicar la misma al caso enjuiciado, aplicando de este modo los conocimientos adquiridos, como una regla de la sana crítica, para justificar si considera acreditados los hechos[1065].

[1060] ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», *Diario La Ley - Sección Tribuna*, n.º 8658, 2015, p. 9.

[1061] DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 34.

[1062] IGARTUA SALAVERRÍA, J.; HERNÁNDEZ GARCÍA, J., «Valoración de la prueba», cit., p. 706.

[1063] ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», cit., p. 9.

[1064] ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», cit., p. 9.

[1065] Para la incorporación de los conocimientos científicos al proceso y su valoración, según IGARTUA SALAVERRÍA, en primer lugar el juez decidirá si son relevantes o no (necesarios o no) los conocimientos científicos o técnicos de un experto para la solución del caso. Después, en conexión con lo anterior, dispondrá acerca de qué tipo de conocimientos han de retenerse como científicos. Más tarde, ya dentro de un tipo reconocido como especializado, habrá de discriminar los conocimientos válidos de lo que es basura o charlatanería. Por último, valorará el resultado probatorio que han rendido los conocimientos utilizados comparándolo con el estándar de prueba exigido en el proceso penal». Vid. IGARTUA SALAVERRÍA, J.; HERNÁNDEZ GARCÍA, J., «Valoración de la prueba», cit., p. 736.

Dice a este respecto TARUFFO que «el juez no tiene necesidad de poseer todas las nociones y las técnicas que necesita el científico para producir la prueba, sino que le basta, más bien, con disponer de los esquemas racionales que le permitan establecer el valor de la prueba científica a los efectos de la determinación del hecho»[1066]. No existe, por tanto, una equivalencia entre las tareas del juez y el perito, sino que, como indica ZUBIRI DE SALINAS, el juez lleva a cabo «un juicio sobre el juicio del experto, en la medida en que sea necesario justificar la decisión —especialmente [...] en supuestos en que el juez se aparte de las conclusiones del perito o existan informes contradictorios—»[1067].

Esto supone, de acuerdo con la opinión de LEDESMA IBÁÑEZ, que «el juez debe actuar como un guardián»[1068], y en tal sentido esta autora menciona la apreciación en este punto de HERNÁNDEZ GARCÍA, quien afirma que «el juez debe actuar de *gatekeeper*, admitiendo sólo aquella prueba científica cuya atendibilidad resulte metodológicamente segura [...] ha de distinguir la ciencia buena de lo que la doctrina norteamericana denomina *junk sciencie* (ciencia chatarra o basura)»[1069].

Finalmente, con base en las anteriores apreciaciones, es fácil plantearse la cuestión de si el juez puede, en relación con conocimientos científicos que no pueden ser considerados máximas de la experiencia comunes, introducir en la valoración el saber propio sobre aspectos técnicos o científicos, adquiridos como consecuencia de su propio estudio o experiencia profesional.

Nuestra respuesta a tal cuestión es negativa, mostrándonos de acuerdo con la opinión de autores como FERNÁNDEZ ENTRALGO, quien afirma que las máximas de la experiencia no pueden extenderse hasta comprender conocimientos que son propios de una ciencia extrajurídica, y en este sentido señala que «menos aún se puede aceptar que en las resoluciones judiciales se hagan consideraciones generales sobre conocimientos científicos extrajurídicos […] para aplicarlas a las circunstancias del caso litigioso sin

---

[1066] TARUFFO, M., «*La prueba de los hechos*», cit., p. 334.

[1067] ZUBIRI DE SALINAS, F., «¿Qué es la sana crítica? La valoración judicial del dictamen experto», cit., pp. 59-60.

[1068] GASCÓN ABELLÁN, M. Y OTROS, «La motivación fáctica», cit., p. 266.

[1069] HERNÁNDEZ GARCÍA, J., «Exigencias éticas y motivación», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 12, 2009, p. 23, Consultado en http://www.poderjudicial.es/abnetportal/abnetcl.exe/O7401/ID721744c3?ACC=101.

haber sido proporcionadas por el correspondiente perito examinado contradictoriamente en juicio»[1070].

De este modo, aunque los jueces, por su propio estudio o experiencia, tengan ciertos conocimientos sobre una determinada materia, la aportación de los mismos deberá realizarse mediante una prueba pericial y no de forma autónoma sin la intervención de peritos por la propia iniciativa del juzgador en atención a sus propios conocimientos.

Esta postura ha sido igualmente defendida por ZUBIRI DE SALINAS[1071], con base en los siguientes tres argumentos:

a) Ese conocimiento personal del juez no es, de entrada, científicamente contrastable, ya que el ejercicio de la jurisdicción sólo avala los conocimientos jurídicos del titular de ella, pero en modo alguno los posibles conocimientos que pueda tener de otras disciplinas.

b) Aunque pudiera ser objetivamente evaluable ese conocimiento, mediante la constancia en el proceso de la titulación habilitante que un determinado juez tuviera en su poder, el conocimiento personal del juez no habría venido al proceso aportado como prueba y no habría sido sometido a la necesaria contradicción procesal.

c) En caso de recurso, la Sala en su función revisora no tendría elementos de juicio para poder valorar ese conocimiento personal, aun en el caso de que el juez hubiese razonado ampliamente sobre el porqué de la decisión adoptada, justificándola, pues los componentes del tribunal de alzada no habrían de tener, necesariamente, los mismos conocimientos expertos que el juez que ha resuelto en primera instancia.

2.4. La valoración conjunta

La motivación llevada a cabo en los fundamentos jurídicos de la sentencia como consecuencia de la libre valoración de la prueba, exigirá, además de la determinación de la relevancia y fiabilidad individual de cada una de las pruebas, que se lleve a cabo una

[1070] FERNÁNDEZ ENTRALGO, J., «Los conocimientos privados del juez en materia psicológica. Las posibilidades de introducirlos para argumentar su convicción», cit., p. 25.
[1071] ZUBIRI DE SALINAS, F., «¿Qué es la sana crítica? La valoración judicial del dictamen experto», cit., p. 59.

valoración conjunta de todas ellas. Se trata de una doctrina jurisprudencial[1072], que ha sido incorporada a la legislación procesal mediante el art. 218.2 LEC, al disponer en su segundo inciso que «la motivación deberá incidir en los distintos elementos fácticos y jurídicos del pleito, considerados individualmente y en conjunto, ajustándose siempre a las reglas de la lógica y de la razón».

Según MONTERO AROCA la valoración conjunta es necesaria en aquellos casos en los que varios medios de prueba se complementan entre sí, como sucede cuando existen varios testigos que declaran sobre el mismo hecho y cuando existen pruebas cuyos resultados son contradictorios[1073]. En este sentido, tal y como afirma JIMÉNEZ CONDE, cada uno de los hechos «ha de ser producto de la certeza causada, bien por un medio de prueba concreto capaz por sí sólo de acreditarlo, bien, en el caso de que concurran varios medios de prueba sobre el mismo hecho, por la prevalencia que racionalmente se otorgue a uno respecto de otros, si se contradicen o por la fuerza probatoria que cada uno de ellos posea, si apuntan en una misma dirección, originándose indudablemente una certeza mayor al ser varios y no uno sólo»[1074].

No obstante, tanto la jurisprudencia del TC como del TS han declarado que la valoración conjunta es una potestad exclusiva del órgano judicial, que éste ejerce libremente con la sola obligación de razonar el resultado de dicha valoración[1075].

Sin embargo, la valoración conjunta cobra especial importancia en aquellos supuestos de pruebas contradictorias, en los que se torna imprescindible so pena de infringir el derecho constitucional a la presunción de inocencia, como así ha declarado la

---

[1072] Afirma GIMENO SENDRA que esta jurisprudencia no es ni mucho menos de nueva creación, ya que sus orígenes se remontan al nacimiento mismo de la LEC de 1881, cuando la jurisprudencia de la Sala de lo Civil del TS puso de manifiesto la inviabilidad del sistema tasado de valoración al ser superado por el carácter discrecional de la apreciación de la prueba, surgiendo con tal finalidad y la de justificar la inaplicación de las normas legales valorativas, la corriente jurisprudencial conocida como «la apreciación conjunta de los medios probatorios». Vid. GIMENO SENDRA, J. V., «*Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*», cit., p. 420.

[1073] MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», cit., p. 63.

[1074] JIMÉNEZ CONDE, F., *La apreciación de la prueba legal y su impugnación*, Salamanca, Universidad, Departamento de Derecho Procesal, 1978, p. 311.

[1075] Vid. SSTC 76/90, de 26 de abril, FJ 8.º; 120/1994, de 25 de abril, FJ 2.º; y 172/2005, de 20 de junio, FJ 4.º Asimismo las SSTS 149/2020, de 18 de mayo, FJ 5.º; 374/2009, de 28 de enero, FJ 10.º; y 133/1998, de 9 de febrero, FJ 3.º

jurisprudencia del TC, que ha establecido la necesidad de una valoración conjunta en caso de que existan pruebas contradictorias[1076].

Mediante la valoración conjunta de la prueba, el juez o tribunal, una vez determinadas las pruebas, tanto de cargo como de descargo, deberá realizar una ponderación individualizada de todas ellas, y, de acuerdo con las reglas de la sana crítica, otorgará mayor o menor eficacia a cada una[1077].

En todo caso, la valoración conjunta deberá realizarse una vez justificada cada prueba de forma individual, de tal modo que, el argumento de una la valoración conjunta no podrá eludir la referida ponderación individualizada, que, como dice DE URBANO CASTRILLO, se trata de una «tarea inexcusable en la que se excluirán de valoración las pruebas declaradas ilícitas, en las que otras se dirá que no arrojan ninguna luz al caso o que una concreta se considera decisiva, etc.»[1078].

Por ello, no será posible sustituir la ponderación individual de cada elemento de prueba «por el cómodo recurso a hacer un juicio global, sin más explicaciones, ya que este proceder no satisface las exigencias constitucionales de motivación del art. 120.3 CE, y habrá que reputarlo nulo»[1079].

2.5. Valoración de la prueba digital

La valoración de la prueba digital se ajustará, como cualquier otra prueba en el ámbito del proceso penal, al principio de libre valoración y por tanto a las ya

[1076] Vid. STC 125/2017, de 13 de noviembre, FJ 10.º que estima un recurso de amparo por no haber sido tenido en cuenta el testimonio del acusado, quien negó haber cometido la acción que se le imputaba. El alto Tribunal estima vulnerado el derecho a la presunción de inocencia al declarar que «se aprecia que, en la valoración conjunta de la actividad probatoria precisa para considerar acreditada no solo la falsedad de los hechos recogidos en el documento, sino la infracción objetiva del deber de cuidado que se le imputa al demandante, la ponderación de su propio testimonio, que negó haber cometido la acción imputada, y de otros adicionales sobre los hechos, era absolutamente esencial para poder inferir de manera concluyente su culpabilidad, habida cuenta de la ya señalada obligación de someter a valoración la versión o la prueba de descargo aportada por el acusado».

[1077] Así se hizo en el caso resuelto por la STS 466/2019, de 14 de octubre, que en su FJ 7.º dejó constancia de que «los hechos reflejados en el juicio histórico han sido acreditados mediante la valoración conjunta de una multiplicidad de pruebas y el razonamiento valorativo se ha exteriorizado de forma prolija en un extenso fundamento jurídico en el que se da cuenta de todas y cada una de las pruebas practicadas, de su resultado y de las consecuencias que se desprenden de su contenido».

[1078] DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 29.

[1079] DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 29.

examinadas reglas de la sana crítica, llevándose a cabo del mismo modo un examen individual, seguido, si procede según el juez o tribunal, de una apreciación conjunta y contrastada con el resto del material probatorio. La prueba digital tiene, sin embargo, algunas particularidades.

Una de ellas se plantea en cuanto que, dadas las especiales características de la prueba digital, el juez deberá atender especialmente a la autenticidad del origen y a la integridad del contenido, es decir a la coincidencia del autor y de los datos de los documentos electrónicos con los inicialmente obtenidos, dado que, como dice DELGADO MARTÍN, «si concurren dudas sobre la autenticidad y/o integridad de los datos, resultará muy probable que el juez deniegue fuerza o eficacia probatoria a la prueba»[1080]. En este punto, aun cuando rige el principio de libre valoración, tratándose de documento electrónico, tendrán mayor fiabilidad a los efectos de su autenticidad e integridad, y por tanto otorgarán un mayor nivel de credibilidad, los documentos firmados electrónicamente con arreglo a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica[1081], que aquellos que no tengan tal cualidad. Todo ello, sin perjuicio de que un documento con las garantías de la firma electrónica, también podría ser manipulado, en cuyo caso sería imprescindible una pericial para acreditar tal extremo.

De este modo, tendrá especial trascendencia en el ámbito de los registros informáticos la acreditación de una correcta cadena de custodia del material intervenido, así como las medidas de seguridad que sobre los documentos electrónicos obrantes en el mismo se hayan adoptado, como el establecimiento de un «código hash» tras la

[1080] DELGADO MARTÍN, J., «*Investigación tecnológica y prueba digital en todas las jurisdicciones*», cit., p. 81.

[1081] Disponen los apdos. 1, 2 y 3 del art. 3 de la Ley 59/2003, de 19 de diciembre:

1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Por su parte, el art. 11.1 de la misma Ley, dispone:

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

diligencia de volcado, del que se haya dejado constancia en la oportuna acta extendida por el letrado de la Administración de Justicia bajo el auxilio de un informático forense, conforme a lo ya estudiado en el apartado de la cadena de custodia[1082].

Asimismo, como ya hemos estudiado, en el ámbito de la prueba digital adquiere especial importancia la prueba pericial, principalmente en los supuestos de impugnación de la autenticidad o integridad de los documentos electrónicos, debiéndose proceder a su libre valoración de acuerdo con las reglas de la sana crítica, sin que los informes periciales sean vinculantes para el juez o tribunal, lo cual, como dice VELASCO NUÑEZ, «aleja el papel del juez del mero automatismo, aun cuando las pericias tengan mucho peso en ocasiones por su valor de convicción, muchas veces en consonancia con el carácter científico y cuasiaxiomático de las mismas»[1083].

Por otro lado, un sector doctrinal afirma que la valoración de la prueba digital se halla sujeta a una «sana crítica especialísima», en atención a la mención del art. 384.3 LEC que, en relación con la valoración de los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso, dispone que la misma se efectuará conforme a las reglas de la sana crítica aplicables a aquellos «según su naturaleza».

Dice a este respecto ABEL LLUCH, que «la cualificación de "especialísima" referida a la sana crítica es una apelación a una mayor sensibilidad judicial, a un *plus* —si se quiere expresar de este modo— puesto que la valoración de un hecho o una prueba electrónica puede demandar una especial atención o una mejor información sobre aspectos técnicos»[1084].

En el mismo sentido, DE URBANO CASTRILLO, resaltando la importancia del papel que desempeñan los defensores y los peritos en esta modalidad probatoria, afirma que «es preciso combinar las exigencias generales de racionalidad, flexibilidad, lógica y experiencia con una formación básica de los juristas implicados en su valoración, que no

[1082] Vid. supra apdos. IV.6.1 y IV.6.2 de este capítulo, pp. 422-429.

[1083] VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales (2ª Parte)», cit., p. 5.

[1084] A ello, dice el referido autor, «cabría añadir que la valoración de la prueba electrónica, especialmente cuando se ha impugnado su falta de autenticidad o integridad, puede precisar el auxilio de una prueba pericial, cuya libre valoración es incontrovertida». Vid. ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», cit., p. 15.

puede dejar en manos del "conocimiento privado del juez", a modo de aleas, la tutela judicial»[1085].

Sin embargo, como igualmente señala ABEL LLUCH, estimamos que la apostilla «según su naturaleza» del art. 384.3 LEC no aporta nada, especialmente en el proceso penal, dado que «las reglas de la sana crítica, por definición se refieren siempre a las circunstancias del caso concreto, y se trata de una simple redundancia, en la medida que la libre valoración supone tener en cuenta la naturaleza propia del medio que se aplica, llegándose a afirmar que se podría incluso haber prescindido de esta previsión legal»[1086].

2.6. Control casacional

La libre valoración de la prueba tiene una gran importancia, hasta tal punto que la misma es controlada por el tribunal de casación cuando en este recurso extraordinario es invocada la vulneración del derecho constitucional a la presunción de inocencia. Por ello, consideramos oportuno realizar unas breves consideraciones en relación con este control casacional de la valoración de la prueba, con el propósito de resaltar la gran importancia de este aspecto final del proceso penal declarativo.

Señalaremos en primer lugar, que una sentencia judicial cuyo fallo no se ajuste a criterios de «valoracion racional», es decir, que se dicte sin que se expresen en los «fundamentos de derecho» las razones que, mediante una argumentación lógica, llevan a la conclusión final, o lo que es lo mismo, que se infrinjan las reglas de la sana crítica, supondría que uno de los poderes públicos estaría incurriendo en arbitrariedad, circunstancia proscrita por en el inciso final del art. 9.3 CE, por lo que no cabe duda alguna del necesario control que tanto el TC como el TS —al resolver sobre las posibles vulneraciones del derecho a la presunción de inocencia—, han de llevar a cabo en sus resoluciones del respeto a esta tarea judicial.

Por tanto, explica GÓMEZ COLOMER, «la prueba debe ser valorada concretamente, pues es necesario que el acusado y demás partes sepan de dónde ha extraído el órgano jurisdiccional sus elementos de convicción»[1087]. Asimismo, como dice DE URBANO CASTRILLO, la decisión final «debe observar una metodología racional que

[1085] DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., pp. 120-121.

[1086] ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», cit., pp. 14-15.

[1087] GÓMEZ COLOMER, J. L., «La terminación del proceso penal», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, p. 432.

en una sociedad democrática ha de ser objeto de control, incluso por el tribunal de casación»[1088].

Ello quiere decir que, una vez verificada una lógica conexión entre las razones expuestas en la fundamentación jurídica y el fallo, ajustándose aquellas, en general, a las ya estudiadas reglas de la sana crítica, el control casacional habrá llevado a cabo su función, sin que proceda que lleve a cabo un juicio de conformidad con la valoración llevada a cabo por los tribunales *a quo*. Como dice GIMENO SENDRA, «el tribunal de instancia es, pues, con las anteriores limitaciones, soberano en la apreciación de la prueba, sin que pueda el TS, ni el TC sustituirlo en la función de valoración de la prueba, la cual, como exigencia del principio de inmediación, ha de corresponder exclusivamente a quien ha presenciado la actividad probatoria, esto es, al tribunal sentenciador»[1089].

Existe reiterada jurisprudencia, tanto del TC como del TS conforme a la que el control casacional incluye la posibilidad de verificar la racionalidad de las conclusiones obtenidas por el tribunal de instancia, explicitadas a través de la motivación, pudiendo rechazar la credibilidad que le concedió el tribunal sentenciador si sus conclusiones son contrarias a las máximas de la experiencia o incurren en arbitrariedad.

Así, por ejemplo, la STC 136/2006, de 8 de mayo, declaró en su FJ 3.º que nuestro sistema casacional no queda limitado al análisis de cuestiones jurídicas y formales, siendo posible, a través de la invocación del derecho a la presunción de inocencia del 24.2 CE, que «el Tribunal Supremo controle tanto la licitud de la prueba practicada en la que se fundamenta el fallo, como su suficiencia para desvirtuar la presunción de inocencia y la razonabilidad de las inferencias realizadas»[1090].

Por su parte, el TS en numerosas resoluciones[1091], ha dejado sentado que el control casacional se extiende, no solo a comprobar la existencia de prueba de contenido

---

[1088] DE URBANO CASTRILLO, E., «*La valoración de la prueba electrónica*», cit., p. 27.

[1089] GIMENO SENDRA, J. V., «*Manual de Derecho Procesal Penal*», cit., p. 577.

[1090] En el mismo sentido la STC 70/2002, de 3 de abril, FJ 7.º, declaró que el recurrente «tiene abierta una vía que permite al Tribunal Supremo la "revisión íntegra", entendida en el sentido de posibilidad de acceder no sólo a las cuestiones jurídicas, sino también a las fácticas en que se fundamenta la declaración de culpabilidad, a través del control de la aplicación de las reglas procesales y de valoración de la prueba».

[1091] Vid. SSTS 120/2003, de 28 de febrero, FJ 4.º; 23/2007, de 23 de enero, FJ 5.º; 1582/2002, de 30 de septiembre, FJ 1.º; y 951/1999, de 14 de junio, FJ 3.º

incriminatorio, si esta ha sido obtenida lícitamente y si ha sido practicada con regularidad procesal, sino que además, para demostrar que la misma es capaz de enervar la presunción de inocencia, deberá verificarse si la misma ha sido racionalmente valorada por el tribunal de instancia, es decir, si por este se atendió a las reglas de la lógica, los principios de la experiencia y conocimientos científicos, o, dicho de otro modo, que la valoración realizada no es irracional, manifiestamente errónea o arbitraria.

CONCLUSIONES

I

Con el inicio, a finales del siglo XX y principios del siglo XXI, de la llamada «era digital», proliferaron nuevas formas de delinquir, a través de las TIC y de internet, que pasaron a denominarse «ciberdelitos». La dificultad de su investigación hizo necesaria la progresiva especialización de la Policía Judicial y el uso de las propias TIC para combatir estas modalidades delicitivas, utilizando para ello diversas medidas de investigación tecnológica.

El uso de estas medidas, apoyándose en la casuística existente en relación con la ya existente medida de intervención de las comunicaciones telefónicas, se extendió a la investigación de cualquier modalidad delictiva.

Han sido numerosas las ocasiones en las que tanto la jurisprudencia del TEDH como la del TC instaron la necesaria regulación legal de estas medidas, que, finalmente, se produjo con la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

II

La regulación de las medidas de investigación tecnológica llevada a cabo por la LO 13/2015 merece una opinión favorable, dado que con la misma han quedado regulados de forma general todos los aspectos que venían siendo reclamados por la jurisprudencia del TEDH y TC.

Así, ha quedado satisfecho el requisito de la previsibilidad de la norma como un elemento necesario de la seguridad jurídica, al haberse regulado las particularidades de cada tipo de diligencia en un capítulo independiente para cada una de ellas y, sobre todo, con el capítulo dedicado a las disposiciones comunes a todas las medidas de investigación tecnológica, en el cual han quedado regladas cuestiones como la duración de la medida, su control judicial, afectación de terceras personas, la regulación de los supuestos en los que sea necesaria la utilización de la información obtenida en un procedimiento distinto, la de los hallazgos casuales o las circunstancias en las que se debe proceder a la destrucción de los registros obtenidos tras las intervenciones.

Es igualmente satisfactoria la inclusión del requisito de la jurisdiccionalidad de las medidas de investigación tecnológica en la LECrim, dado que han quedado

debidamente cubiertos los dos aspectos esenciales de este requisito, como son la exigencia de resolución judicial y su motivación, además de establecerse una relación de todos los aspectos que han de constar tanto en la solicitud de autorización judicial como en la propia resolución, tales como las razones que justifican la adopción de la medida, el hecho punible objeto de investigación y su calificación jurídica, los indicios racionales de criminalidad, identidad de los investigados, duración de la medida o finalidad perseguida con la misma.

Merece también una valoración positiva la inclusión, de acuerdo con la jurisprudencia constitucional consolidada, de los demás principios rectores, especialmente el de proporcionalidad, que contemplado desde un punto de vista amplio comprende los de idoneidad, necesidad y excepcionalidad.

No obstante, y sin perjuicio de una valoración global positiva, existen diversas cuestiones —nos referiremos a las más relevantes en otras conclusiones— que no han sido reguladas y otras que deben ser mejoradas. Esta revisión debe llevarse a efecto mediante la promulgación de una nueva LECrim, con una completa y nueva regulación que permita una justicia penal más acorde con las necesidades de nuestra sociedad, conforme a las exigencias de una inexorable realidad del siglo XXI, muy alejada de la que, de una forma sobresaliente fue recogida por el legislador del siglo XIX.

III

Sin perjuicio de que se trata de una realidad indiscutible, en mi opinión, no existe un derecho independiente al entorno virtual —como así se ha declarado en algunas sentencias del TS y por algún sector doctrinal—, dado que no consta un reconocimiento expreso por parte del legislador. El entorno virtual debe protegerse porque en él coexisten los derechos fundamentales a la vida privada. Pero ello no significa que podamos elevar a la categoría de derecho tal realidad, aun siendo cierto que todos los datos que se puedan localizar dentro de los dispositivos informáticos conjuntamente considerados podrían describir el perfil ideológico de cualquier persona. Finalmente, derivaría en una vulneración de la intimidad personal.

Con la LO 13/2015 no se ha configurado este pretendido derecho. El legislador se ha limitado a establecer la necesidad de que, por parte del juez competente, se lleve a cabo una ponderación de las razones que justifican el registro de un ordenador, otorgando un tratamiento unitario a esta amplia variedad de datos, ofreciendo, de este

modo, una mayor protección a los diferentes derechos fundamentales que pueden ser afectados, que no son otros que los derechos a la vida privada del art. 18 CE.

La necesidad de autorización judicial fijada con la reforma de la LECrim para la ejecución de un registro informático, con independencia de la entrada y registro domiciliario, no puede interpretarse en el sentido de que se reconozca la existencia de un nuevo derecho. Tal exigencia se impone por dos cuestiones independientes, como son:

1. Porque la posibilidad de intervenir tan variados y desconocidos datos que afectan a la vida privada, nunca podrá ser considerada una injerencia leve en el derecho a la intimidad, y por ello, tratándose siempre de una injerencia grave, será necesaria la autorización judicial, con excepción de los casos de urgencia en los que puedan intervenir directamente las FCSE.

2. El derecho al secreto de las comunicaciones podría verse vulnerado.

Por estas razones, de producirse una intromisión indebida en el entorno virtual en la que se desvelaran preferencias, ideología o, en definitiva, la manera de sentir, pensar o comportarse de un ciudadano, quedaría transgredido en todo caso su derecho a la intimidad, sin perjuicio de que, adicionalmente y dependiendo de cada caso concreto, quedasen vulnerados los derechos al secreto de las comunicaciones o el derecho a la protección de datos de carácter personal.

IV

La existencia de esta realidad, que no derecho, del entorno virtual, hace necesario un reconocimiento legal de la misma, que estimamos debería tener lugar mediante un adecuado desarrollo legal de derecho constitucional del art. 18.4 CE, que ordena al legislador que limite el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Se trata, al igual que en su día se hizo con la protección de datos de carácter personal, de cumplir tal mandato conforme a la realidad de la era digital, entendiendo que la expresión «limitará el uso de la informática» ha de entenderse como una expresión de una gran amplitud, dirigida al uso de la informática que hagamos todos, incluido por supuesto el Estado en el ámbito de la investigación del delito.

Por ello, *de lege ferenda*, proponemos un desarrollo legislativo del art. 18.4 CE, interpretado de conformidad con la realidad social del tiempo en que ha de ser aplicado atendiendo fundamentalmente a su espíritu y finalidad, regulando todos los aspectos del denominado entorno digital en aras de una mayor seguridad jurídica y respeto a los derechos fundamentales.

V

Los datos de tráfico o asociados constituyen, con carácter general, un elemento de la comunicación protegido por el secreto de las comunicaciones, por lo que la cesión de estos datos por las operadoras para los fines de investigación del delito, requerirá autorización judicial.

Sin embargo, una buena parte de estos no se encuentran amparados por el derecho al secreto de las comunicaciones sino por el derecho a la protección de datos de carácter personal, siendo esta una distinción relevante por el distinto alcance constitucional de los derechos del art. 18 CE, dado que existe un régimen más flexible para la intromisión en la intimidad y protección de datos que cuando se trata del derecho al secreto de las comunicaciones.

Existen, por tanto, dos modalidades de datos de tráfico: los que se encuentran vinculados a un proceso de comunicación y aquellos que no tienen tal atributo, quedando protegidos los primeros por el derecho al secreto de las comunicaciones y los segundos al derecho a la protección de datos de carácter personal.

El criterio diferenciador de la incardinación en uno u otro derecho ha sido establecido legalmente por el art. 588 ter j LECrim, encontrándose en la circunstancia de que el concreto dato de tráfico se encuentre vinculado o no a un proceso de comunicación.

Sin embargo, no se ha establecido ninguna regla que distinga cuando se produce esta vinculación a un proceso de comunicación y cuando no. Por ello, *de lege ferenda*, consideramos que, en aras de una mayor seguridad jurídica, es necesaria la plasmación de una forma clara, de los datos que dentro de la extensa relación del art. 3 de la Ley 25/2007, quedan vinculados a un proceso de comunicación. El acceso a estos exige, en todo caso, el requisito de la reserva jurisdiccional y, por tanto, su régimen jurídico quedaría diferenciado del relativo al de los datos que, por no encontrarse vinculados a un

proceso de comunicación, tendrían un régimen más flexible, pudiendo en casos de urgencia ser reclamados directamente por el Ministerio Fiscal o la Policía Judicial a las operadoras.

VI

No encontrándose establecido con carácter general para las medidas de investigación tecnológica limitativas de derechos fundamentales, y muy especialmente para las de registro de dispositivos de almacenamiento masivo de información, un catálogo de delitos en virtud de los cuales puedan acordarse las mismas, estas podrán llevarse a efecto cuando se investiguen delitos graves.

No obstante, cuando el delito no pueda ser calificado como grave según la pena a imponer, de acuerdo con los criterios establecidos en los arts. 13 y 33 del CP, se considerarán graves a estos efectos, aquellos que tengan una trascendencia social que exija la intervención. Asimismo, el uso de las tecnologías de la información, tanto para la perpetración del delito como para la obstrucción a su persecución se considera igualmente un criterio válido a la hora de entender que nos encontramos ante un delito grave a los efectos de legitimar la intervención.

Para la valoración de la trascendencia social determinante de la gravedad, se tendrán en cuenta aspectos como la propia naturaleza de los hechos investigados, su mecánica comisiva y las inevitables necesidades para su ulterior probanza. Asimismo, será un criterio que determine la gravedad del delito, la lucha contra la delincuencia que, a su vez, esté calificada como grave.

VII

Debe ampliarse, a mi entender, el plazo máximo de veinticuatro horas establecido en el art. 588 bis c.1 LECrim, para que el juez de instrucción dicte la resolución autorizando o denegando la medida de investigación tecnológica previamente solicitada por la Policía Judicial o el Ministerio Fiscal, habida cuenta de que, en determinados supuestos, bien por la complejidad del caso o por la elevada carga de trabajo del órgano judicial, no será posible el cumplimiento del mismo.

Con carácter general, sería más aconsejable la fijación de un plazo más generoso, que podría ser, por ejemplo, de tres días, que permitiría, sin el riesgo de que se

produzcan dilaciones indebidas, que el exigente ejercicio de la potestad jurisdiccional en un asunto de tan alta trascendencia como es la tutela de los derechos fundamentales, se llevase a cabo con un completo estudio y reflexión, garantizando de este modo el respeto a los mismos.

En cualquier caso, debería fijarse un plazo de veinticuatro horas para aquellas diligencias que por su propia naturaleza, o según las circunstancias de cada caso, exigiesen una intervención urgente, la cual debería ponerse de manifiesto en la solicitud, informando al juzgado de dicha circunstancia, a fin de ser examinada en el mismo día de su presentación por el juez de instrucción.

Asimismo, tras la reforma operada por la LO 13/2015, aun cuando la jurisprudencia del TS venía admitiendo que la resolución que acordase la medida de investigación se remitiese al oficio policial solicitando la misma, entiendo que no es admisible tal remisión, dado que el art. 588 bis c.3 LECrim establece en su apartado a) que la resolución deberá reflejar «el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que se funde la medida».

En actuaciones tan graves, como las que coartan el libre ejercicio de los derechos fundamentales, es necesario que la justificación de las mismas sea razonada a fin de que los destinatarios conozcan los motivos por los que se sacrificó el derecho. De este modo, no se pueden considerar reiteraciones innecesarias aquellas cuestiones que, cuando se restringen los derechos reconocidos por la Constitución, el juez competente extraiga de los argumentos plasmados en la solicitud policial, las cuales deberá hacer constar de forma debidamente motivada en la resolución judicial. En este sentido, en mi opinión, la jurisprudencia que, con anterioridad a la LO 13/2015, se mostraba permisiva con la motivación por remisión a la solicitud policial, no se ajusta a una correcta intepretación de la vigente LECrim.

VIII

De acuerdo con el art. 588 bis k LECrim, aplicable a todas las medidas de investigación tecnológica, una vez que se ponga término al procedimiento mediante resolución firme, se procederá al borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, procediéndose, además, a la destrucción de las copias conservadas cuando

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. Sin embargo, esta regla se exceptúa en aquellos casos en los que no fuera precisa la conservación a juicio del tribunal.

Estas excepciones no han de dejarse a discreción de los tribunales, debiendo establecerse legalmente los casos en los que las copias deban conservarse. De no ser así, el principio de seguridad jurídica sufriría cierto menoscabo al establecerse una fórmula tan intederminada como la ya mencionada: «…siempre que no fuera precisa su conservación a juicio del Tribunal».

Por ello, estimo que, *de lege ferenda*, en aras de la seguridad jurídica y en atención a los derechos fundamentales en juego —los derechos a la vida privada del art. 18 CE—, deben establecerse los supuestos en los que únicamente podrán conservarse las copias obtenidas como consecuencia de la diligencia de investigación tecnológica practicada, una vez que se dicte resolución firme que ponga fin al proceso, proponiendo los siguientes:

a) esclarecimiento de hechos delictivos distintos a los juzgados que guarden conexidad.

b) determinación de la participación en el hecho investigado de sospechosos no afectados por la resolución que al mismo le ha puesto fin.

c) continuación de las actuaciones respecto de otros investigados o acusados en los casos de sobreseimiento libre o sentencia absolutoria respecto de alguno de ellos.

d) necesidad de investigación de la posible comisión de un nuevo delito tras un hallazgo casual que no guardase conexidad.

IX

Resulta acertada la inclusión en la LECrim de una norma como el art. 588 octies, en virtud del que el Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión, con la obligación del requerido de prestar su colaboración y guardar secreto del

desarrollo de la diligencia, pudiendo incurrir, de no hacerlo, en un delito de desobediencia.

Sin embargo, el legislador no ha excluido de esta obligación a las personas dispensadas de la obligación de declarar por razón de parentesco conforme al art. 416.1 LECrim y a las que, de conformidad con el artículo 416.2 LECrim, no pueden declarar en virtud del secreto profesional, por lo que, *de lege ferenda*, en aras de una mayor seguridad jurídica y con la finalidad de evitar actuaciones desproporcionadas, debe incluirse por el legislador, en una próxima reforma, un segundo apartado del art. 588 octies LECrim, en el que se establezca la exención de la obligación de conservar los datos, de las personas citadas.

Asimismo, la orden de conservación no debe emitirse con una discrecionalidad incontrolada, debiéndose exigir una mínima justificación. Por ello, se propone la reforma del referido precepto en el sentido de exigirse la necesidad de resolución judicial para la orden de conservación de datos.

No existen mayores problemas en obtener una autorización judicial para esta medida de aseguramiento, para la que podría establecerse un plazo prudencial que permitiese un adecuado estudio por parte del juez competente, así como la apertura de un procedimiento judicial, lo que impediría cualquier vulneración del principio de especialidad, todo ello sin perjuicio de establecer unos determinados supuestos de urgencia en los que la Policía Judicial o Ministerio Fiscal podrían impartir la orden de conservación de datos.

Finalmente, dado que el art. 588 octies LECrim establece que la persona requerida deberá conservar los datos durante un periodo máximo de noventa días prorrogable por una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días, es necesario que este proceso se encuentre supervisado judicialmente, con el objetivo primordial de vigilar el correcto cumplimiento de los principios rectores que han de regir toda diligencia de investigación.

X

En una línea similar a la orden de conservación de datos, los arts. 588 sexies c.5 y 588 septies b.2 LECrim establecen respectivamente, en relación con los registros de dispositivos de almacenamiento masivo de información y con los registros remotos sobre equipos informáticos, un deber de colaboración de terceros. De acuerdo con estos

preceptos, cualquier persona que conozca el funcionamiento del sistema informático objeto de registro o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo, tendrá la obligación de facilitar la información que resulte necesaria para el buen fin de la diligencia —tanto a las autoridades como a los agentes encargados de la investigación—, pudiendo incurrir, de no facilitar la información, en delito de desobediencia.

Sin embargo, para los registros de dispositivos de almacenamiento masivo de información se exceptúa de dicha obligación aquellos casos en los que se derive una carga desproporcionada para el afectado.

Nos encontramos ante una situación en la que deberá valorarse la proporcionalidad de la obligación de colaborar, debiéndose justificar, por tanto, que el sacrificio de los derechos e intereses de la persona afectada no resulte superior al beneficio que, para el interés público y de terceros, resulte del cumplimiento de dicho deber.

Dicha valoración de la proporcionalidad exige una concreción legal de los casos en los que, por suponer una carga desproporcionada, no será posible exigir la información a terceras personas, quedando en tales casos supeditada la emisión de la orden al juicio de proporcionalidad que, motivadamente, deberá reflejar en la correspondiente resolución judicial el juez competente.

Por otra parte, resulta paradójico que la referida limitación del deber de colaboración, únicamente se establece para los registros de dispositivos de almacenamiento masivo en el art. 588 sexies c.5 LECrim, pero no así para los registros remotos de equipos informáticos en el art. 588 septies b.2 LECrim, en el que nada se expresa acerca de no ser posible la petición de información cuando de ello se derive una carga desproporcionada para el afectado. Por ello, sin perjuicio de que pueda aplicarse analógicamente lo dispuesto en relación con los dispositivos de almacenamiento masivo, a fin de evitar excesos en la investigación, debe incorporarse la misma mención para los registros remotos de equipos informáticos.

XI

El legislador, con la reforma de la LO 13/2015, ha establecido legalmente el criterio fijado por la doctrina constitucional, disponiendo, para la interceptación de las

comunicaciones telefónicas y telemáticas (art. 588 ter g LECrim) y para la utilización de dispositivos técnicos de seguimiento y localización (art. 588 quinquies c LECrim), que el cómputo se iniciará a partir de la fecha de la autorización judicial. Sin embargo, resulta sumamente criticable que no se haya efectuado una mención similar para el registro remoto de sistemas informáticos. Ello no debe obstar a que, ante tal laguna jurídica, se pueda recurrir a una autointegración analógica con base en las dos regulaciones referidas en diligencias de la misma naturaleza.

En cualquier caso, una mayor protección de los derechos fundamentales en juego así como las exigencias del principio de seguridad jurídica, aconsejan que el día y hora concreto en el que la medida deberá iniciarse, deba ser fijado en el auto acordando la práctica de la medida, así como, consecuentemente, el día y hora de su finalización.

Ello contribuiría a evitar el transcurso de plazos excesivos entre el acuerdo y la ejecución, impidiendo que en las diligencias en las que puedan verse comprometidos los derechos fundamentales la Policía Judicial tenga un excesivo margen de actuación, que no obstante ser conveniente en general para la investigación policial, no debe ser así cuando exista la posibilidad de restricción de derechos fundamentales, en cuyo caso ha de exigirse un estricto control judicial de la medida.

XII

Uno de los aspectos más relevantes dentro de las novedades de la LO 13/2015 es el relativo a la extensión o alcance de la medida de investigación tecnológica, importancia que se ve incrementada al tratarse de los registros informáticos, donde se presenta el fenómeno del entorno virtual como aquel en el que convergen los distintos derechos a la vida privada.

De acuerdo con esta previsión, el juez deberá especificar de forma motivada, la concreta información que se requiere para culminar una investigación, sin que proceda el acceso a más datos que los estrictamente necesarios —sin perjuicio de aquellos casos más complejos en los que motivadamente se acuerde el registro completo—, evitando, de este modo, cualquier intrusión improcedente en la privacidad de la persona afectada, lo que estaría en contra de los principios rectores de las medidas de investigación tecnológica.

El juez mediante una motivación respetuosa con estos principios (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad), deberá especificar los datos

que resultan necesarios para la investigación. De este modo, aun cuando sea necesaria la aprehensión de todo el material informático**,** una vez que se practique el volcado y posterior registro, este deberá contraerse únicamente a los archivos digitales (voz, imagen, texto, audio, video o en su caso datos que revelen el momento de emisión o recepción de un mensaje, datos bancarios, de ubicación, etc.), que se especifiquen por el juez en el auto acordando la intervención.

XIII

La LECrim no fija delitos concretos respecto de los que se pueda acordar la medida de registro de dispositivos de almacenamiento masivo de información, a diferencia de la de registro remoto de equipos informáticos, o la de intervención de las comunicaciones telefónicas y telemáticas, por lo que, legalmente, no existe impedimento para que pueda ser investigado cualquier delito con esta medida de investigación, incluso un delito leve.

Una primera aproximación en cuanto al grado de injerencia de una y otras intervenciones, nos lleva a la conclusión de que, por su carácter dinámico y clandestino, el registro remoto o la intervención de las comunicaciones son diligencias que pueden suponer una mayor intromisión en los derechos fundamentales. Sin embargo, el registro de dispositivos de almacenamiento masivo, normalmente será sorpresivo para el investigado, por lo que no siempre y en todo caso ha de ser menos invasivo en los derechos a la vida privada que el registro remoto, debiéndose tener en cuenta que el registro puede afectar igualmente al derecho al secreto de las comunicaciones.

Por ello, resulta necesaria una previsión legal que coadyuve al cumplimiento del principio de proporcionalidad, mediante el establecimiento de un catálogo de delitos, de cierta gravedad, que permitan la adopción de una investigación tan invasiva, sin perjuicio de la motivación de la resolución judicial en relación con la ponderación entre la gravedad del delito, derecho sacrificado y el beneficio obtenido para el conjunto de la sociedad.

XIV

La LECrim, tras la reforma operada por la LO 13/2015, en su art. 588 sexies c.4, permite la intervención policial sin necesidad de autorización judicial previa —aunque con la obligación de dar cuenta al juez competente en el plazo máximo de veinticuatro

horas— en relación con los registros de almacenamiento masivo de información —no así respecto de los registros remotos de equipos informáticos—, en los casos de urgencia en que se aprecie un interés constitucionalmente legítimo que haga imprescindible la medida.

Sin embargo, para dicha actuación urgente, es necesaria una precisa habilitación legal, sin que sea suficiente una mención genérica a razones de urgencia, por lo que resulta necesaria una mejora de la LECrim en este sentido, teniendo en cuenta, además, que, para la práctica de un registro informático no será necesario, en la mayoría de los casos, una actuación inmediata por parte de la Policía Judicial, pudiendo esperar sin ningún problema a la resolución del juez competente, que deberá contener una especial motivación en relación con los principios rectores de las medidas de investigación tecnológica.

Por tanto, *de lege ferenda*, encontrándose el concepto de «urgencia» establecido de forma muy difusa, debe restringirse el mismo acotando los casos en los que la Policía Judicial podría proceder a un registro informático sin necesidad de autorización judicial, únicamente a aquellos supuestos excepcionales en los que, ante la posibilidad del fracaso de la investigación, la intervención sea absolutamente inaplazable.

XV

Ha de valorarse positivamente la incorporación a la LECrim de la medida de registros remotos de equipos informáticos, por la importancia de la misma para la lucha contra el crimen organizado.

Es, sin embargo, una materia respecto de la que todavía no existe una doctrina jurisprudencial al no haberse llevado a la práctica lo suficiente no obstante el tiempo transcurrido desde la aprobación de la LO 13/2015.

Se trata de una compleja medida de investigación, no exenta de problemas técnicos para su ejecución, por lo que serán necesarias nuevas investigaciones en el campo de la informática que coadyuven a su perfeccionamiento, a fin de que su uso pueda extenderse a un mayor número de investigaciones penales.

XVI

Mediante un registro remoto informático, en general, es posible la intervención de determinadas comunicaciones telemáticas. Sin embargo, el legislador no ha previsto en el art. 588 septies LECrim, la posibilidad de la intervención de las comunicaciones mediante un registro remoto.

La intervención de las comunicaciones telemáticas, junto con la de las comunicaciones telefónicas, tienen una regulación específica en un capítulo independiente, con algunas diferencias de bastante relevancia en relación con los registros remotos, como son las siguientes:

a) La que se refiere al catálogo de delitos en virtud del que se pueden acordar ambas medidas.

b) La posibilidad de que la intervención de las comunicaciones sea ordenada por el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, en casos de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas, posibilidad que no se establece para los registros remotos.

c) La duración máxima de la medida. En los registros remotos puede ser de un mes, prorrogable por iguales periodos hasta un máximo de tres meses, mientras que para la intervención de las comunicaciones es de tres meses, prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Con estas diferencias, pudiera parecer que la pretensión del legislador ha sido no permitir la intervención de las comunicaciones mediante un registro remoto. Sin embargo, aunque el objeto inicial del registro remoto será la obtención de contenidos digitales, es posible la intervención de las comunicaciones telemáticas que el investigado mantenga a través de programas de mensajería o redes sociales, teniendo en cuenta la naturaleza de esta intervención, que, al igual que la de la de intervención de las comunicaciones, tiene carácter dinámico y se realiza sin conocimiento del afectado. Por otro lado, una intervención de comunicaciones telemáticas puede suponer una conexión remota para la que podrán utilizarse datos de identificación y códigos, o un software espía.

Por ello, atendiendo a la similitud entre ambas medidas, así como por la circunstancia de la exigencia en todo caso, a diferencia de los registros de dispositivos de almacenamiento masivo, de autorización judicial, no existe inconveniente en la intervención de las comunicaciones telemáticas, cuando se acordase un registro remoto de equipos informáticos.

XVII

De acuerdo con el catálogo de delitos establecidos, cuya investigación se constituye en presupuesto necesario para la ejecución de un registro remoto de equipos informáticos, parece clara la intención del legislador de delimitar el ámbito de esta medida a la persecución de infracciones criminales de especial gravedad.

Dentro de este catálogo ha sido incluida la posibilidad de acordar la medida para los «delitos cometidos a través de instrumentos informáticos o cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación», habiendo dado lugar esta incorporación a cierta controversia doctrinal, apoyándose las posturas más críticas en la circunstancia de que la medida podría ser acordada para delitos menos graves, incluso para delitos leves, considerándose por ello una previsión desproporcionada.

Sin embargo, la citada regla es del todo correcta, ya que la medida ha de considerarse proporcionada, más que por la pena eventualmente aplicable, por la propia naturaleza de los hechos investigados y de los aspectos y medios relacionados con su ejecución, teniendo en cuenta, además, la necesidad de una rápida intervención cuando se trata de delitos cometidos a través de las TIC para la preservación de la prueba, tan volátil en estos casos.

Además, no ha de olvidarse que el juez competente deberá justificar la proporcionalidad de la medida, así como los principios rectores de necesidad y excepcionalidad. En virtud de este último, no podrá acordarse la intervención cuando estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles para el esclarecimiento del hecho. Por su parte, en relación con el cumplimiento del principio de necesidad, difícilmente la investigación de determinados delitos menos graves o leves se vería dificultada sin el recurso a una diligencia tan lesiva como esta,

debiendo tener un carácter insustituible. Por ello, los principios de excepcionalidad y necesidad no permitirían siempre y en todo caso la intervención.

No obstante, lo dicho anteriormente no impide que, dado el tiempo transcurrido desde la reforma legal, pudiera matizarse el contenido de este apartado, delimitando, dentro de los delitos cometidos a través de medios tecnológicos, aquellos cuya investigación podría dar lugar a un registro remoto.

XVIII

En el catálogo de delitos establecido en la LECrim cuya investigación es presupuesto necesario para la intervención de las comunicaciones telefónicas y telemáticas, aunque coincide en algunos tipos con el establecido para los registros remotos, existen algunas diferencias relevantes, que pueden ser calificadas de incoherentes en atención a la similar naturaleza de ambas medidas.

En efecto, ambas intervenciones pueden llevarse a cabo para la investigación de delitos de terrorismo, los cometidos en el seno de organizaciones criminales y aquellos perpetrados a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación.

Sin embargo, el legislador ha regulado las dos medidas de investigación con las siguientes diferencias en el listado de tipos delictivos:

a) Para la intervención de las comunicaciones telefónicas y telemáticas se incluyen los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. Asimismo puede acordarse respecto de delitos cometidos en el seno de un grupo criminal. Para estas infracciones penales la LECrim no permite que sea acordado un registro remoto.

b) En sentido contrario, para los registros remotos se incluyen los delitos cometidos contra menores o personas con capacidad modificada judicialmente, los cometidos contra la Constitución, de traición y relativos a la defensa nacional. Para estos delitos, sin embargo, sí podrá acordarse una intervención de las comunicaciones, dado que se encuentran penados con pena con límite máximo de, al menos, tres años de prisión.

Nos encontramos ante una regulación cuando menos confusa, por lo que, *de lege ferenda*, debe establecerse una regulación similar para la intervención de las

comunicaciones telefónicas y telemáticas y los registros remotos, en el entendimiento de que no puede apreciarse un mayor grado de injerencia en los derechos fundamentales a la vida privada de una en relación con la otra.

El problema quedaría resuelto incluyendo en el catálogo de delitos establecidos para los registros remotos los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión y los delitos cometidos en el seno de grupos criminales.

XIX

De acuerdo con el art. 588 septies c LECrim, los registros remotos de equipos informáticos tendrán una duración máxima de un mes, prorrogable por iguales periodos hasta un máximo de tres meses. Se trata de una duración demasiado breve, si tenemos en consideración que esta medida será utilizada únicamente en casos especialmente graves en los que seguramente será necesaria una mayor duración de la investigación.

No obstante, sin perjuicio de la valoración que pueda tener este plazo de intervención, llama la atención la diferencia existente con el establecido para la interceptación de las comunicaciones telefónicas y telemáticas, respecto de las que el art. 588 ter g LECrim, dispone que será de tres meses, prorrogables por periodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Atendiendo a que el grado de injerencia de un registro remoto de equipos informáticos en los derechos fundamentales a la vida privada no necesariamente tiene que ser superior al que se produce con la intervención de las comunicaciones telefónicas y telemáticas, resulta excesiva una diferencia tan elevada en el plazo de duración, teniendo en cuenta, además, que ambas medidas únicamente pueden ser acordadas cuando se investiguen delitos de especial gravedad.

Aun cuando por las especiales características de los registros remotos, no esté justificado que se establezca para ellos el mismo plazo que para las intervenciones telefónicas y telemáticas, es aconsejable, *de lege ferenda*, un incremento prudencial del plazo inicial y sus posibles prórrogas, sin perjuicio de aquellos supuestos en los que se acordase una intervención de las comunicaciones telemáticas mediante un registro remoto, en cuyo caso será de aplicación de la normativa prevista para la interceptación de las comunicaciones telefónicas y telemáticas.

En cuanto al *dies a quo* para el inicio de la intervención, no se efectúa mención alguna en el art. 588 septies LECrim, a diferencia, nuevamente, de lo previsto para las comunicaciones telefónicas y telemáticas en el art. 588 ter g LECrim, así como para la medida de utilización de dispositivos técnicos de seguimiento y localización en el art. 588 quinquies c LECrim, en las que se establece que el plazo se computará desde la fecha de autorización judicial.

Para los registros remotos, no es posible computar el inicio de la intervención desde la resolución judicial, dado que, habida cuenta de la dificultad de su ejecución, será necesario un tiempo adicional para, en su caso, la instalación del software en en el equipo investigado, lo cual no ocurre en el caso de la intervención de las comunicaciones, en las que la interceptación es prácticamente inmediata una vez que se remite a oportuna comunicación a la operadora.

Sin embargo, por razones de seguridad jurídica y respeto a los derechos fundamentales, es necesario establecer legalmente un momento en el que se iniciará el cómputo de la medida, sin que este aspecto quede bajo la discrecionalidad de los jueces, por lo que es conveniente su regulación.

Para solucionar adecuadamente este problema, estimo que podría establecerse una preceptiva solicitud de autorización judicial por parte de la Policía Judicial para la instalación del software que permita la ejecución del registro remoto —sin perjuicio de los casos de intervención mediante datos de identificación y códigos, en cuyo caso la Policía Judicial tendrá a disposición los mismos con carácter previo a la solicitud de la autorización judicial—. Una vez verificada la instalación, deberá comunicarse inmediatamente al juez a fin de que pueda fijar la fecha de inicio, a partir de la que se computará el plazo de ejecución de la medida.

XX

El agente encubierto informático, ha sido incorporado por la LO 13/2015 de forma simultánea a la de las medidas de investigación tecnológica, con la finalidad de adaptar la LECrim a la sociedad digitalizada en la que nos encontramos inmersos.

No puede decirse que esta figura haya sido pensada para coadyuvar a la ejecución de la diligencia de registros remotos de equipos informáticos, dado que, de acuerdo con el art. 282 bis 6 LECrim, la finalidad de la creación del agente encubierto

informático es que el mismo pueda actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, así como intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

Sin embargo, existe una estrecha relación entre la intervención por registro remoto y el agente encubierto informático, dado que los canales cerrados de comunicación como foros, chats o grupos privados en redes sociales, pueden servir para obtener datos de identificación o códigos, y del mismo modo los mismos podrían ser la vía adecuada para la instalación de software espía en un equipo informático.

Por todo ello, es conveniente una regulación más minuciosa en la que se asocie la práctica de un registro remoto con la intervención de un agente encubierto informático, lo que supondría a su vez una especialización de los agentes policiales, que coadyuvaría a mejorar la seguridad jurídica y el respeto a los derechos fundamentales.

XXI

Al hablar de prueba anticipada y prueba preconstituida, nos referimos a dos modalidades probatorias realizadas antes del juicio oral. La primera se practica ante el propio tribunal sentenciador y la segunda ante el juez de instrucción.

La prueba preconstituida, entendida como aquella prueba anticipada, en sentido amplio, que tiene lugar ante el juez de instrucción, presenta dos modalidades, según la imposible o muy difícil repetición en el juicio oral, lo sea por razón de la muy probable fugacidad de las fuentes de prueba o, en el segundo caso, por la propia naturaleza intrínseca de la prueba.

Al primer supuesto (cuando sea imposible o muy difícil la reproducción de la prueba en el juicio oral), se le ha denominado de varios modos. Así se ha hablado de «prueba anticipada», sin distinguirla estrictamente de la prueba anticipada en sentido propio; de «prueba anticipada en sentido impropio»; y, finalmente, de «prueba instructora anticipada», siendo esta última, en mi opinión, la denominación más acertada, en atención a que la principal nota distintiva con la prueba anticipada viene constituida únicamente por el órgano judicial que la práctica. Por su parte, al segundo supuesto, (aquel en el que la imposible o muy difícil repetición en el juicio oral se debe

a la propia esencia de la prueba), se le denomina prueba preconstituida en sentido propio, o, sencillamente, prueba preconstituida.

Las diferencias entre ambas modalidades radican, fundamentalmente, en que la prueba instructora anticipada está creada para la práctica de pruebas personales, mientras que la preconstituida constituye una prueba documental. Además, la prueba preconstituida puede ser obtenida por el juez de instrucción, Ministerio Fiscal o Policía Judicial, mientras que la prueba instructora anticipada requiere siempre la intervención del juez de instrucción.

Por lo que respecta a los registros informáticos, no cabe duda de que siempre nos encontraremos ante un supuesto de prueba preconstituida en sentido propio, dado que la volatilidad que caracteriza a la prueba digital, a lo que habría que añadir la muy probable destrucción del material incriminatorio por parte de los culpables, haría imposible o muy difícil su reproducción en el juicio oral.

Asimismo, la preconstitución podrá tener lugar como prueba instructora anticipada, en aquellos casos en los que la habiéndose practicado una pericial como consecuencia de un registro informático, cualquiera de los peritos intervinientes tuviera que prestar su informe en el juicio oral y someterse, con respeto del principio de contradicción, a las preguntas que le fuesen formuladas por las partes, siempre que, al igual que ocurre con los testigos, se temiese por su vida o, por razones de residencia, tuviera que ausentarse del territorio español.

XXII

Con la teoría de la conexión de antijuridicidad desarrollada por el TC, a pesar de las fuertes críticas doctrinales, se ha dado una eficaz solución a la pugna entre la búsqueda material de la verdad y la defensa de los derechos fundamentales de los ciudadanos. Asimismo se ha conseguido la armonización entre la defensa del valor superior de nuestro ordenamiento jurídico, denominado «Justicia», y el derecho fundamental a un proceso con todas las garantías.

Dicho con otras palabras, se ha conseguido una solución justa respecto del efecto reflejo de la prueba ilícita o doctrina de los frutos del árbol envenenado, de tal modo que, las pruebas obtenidas indirectamente una vez producida la indebida injerencia en el derecho fundamental, no necesariamente adquieren el mismo rango de invalidez que la

obtenida directamente, siempre que existan otros factores distintos en virtud de los que, con independencia de la prueba ilícita directa, se hubieran igualmente obtenido las fuentes de prueba incriminatorias.

La justicia se constituye en unos de los valores superiores de nuestro ordenamiento jurídico (art. 1.1 CE) y, por otro lado, los derechos fundamentales no están exentos de los límites que encuentran en otros derechos fundamentales, además de que, como señaló la STC 114/1984, no existe un derecho fundamental autónomo a la no recepción jurisdiccional de las pruebas de posible origen antijurídico.

El art. 11.1 LOPJ prohíbe que surtan efecto las pruebas obtenidas «indirectamente» violentando los derechos o libertades fundamentales. Sin embargo, este efecto indirecto se producirá cuando no exista otra posibilidad de obtención de la prueba indirecta, en cuyo caso se produciría una desconexión de la antijuridicidad de la intervención ilícita.

Por tanto, tomando en consideración tres factores como son: a) uno de los criterios de desconexión, por ejemplo el «descubrimiento inevitable»; b) el valor «Justicia» consagrado en el art. 1.1 CE, y c) que no existe un derecho autónomo a la no recepción jurisdiccional de las pruebas de posible origen antijurídico; y en atención a los mismos se realiza una reflexión sobre las consecuencias de que en el enjuiciamiento de un delito grave quedase acreditado que, incluso cuando se hubiera descubierto el cuerpo del delito como consecuencia de una información que pudiera entenderse derivada de una intervención ilícita, tal descubrimiento se hubiera producido de forma segura e inevitable por otras circunstancias, y aun así los delincuentes quedaran absueltos, definitivamente el valor «Justicia» quedaría gravemente dañado.

En consecuencia, debe ser aplaudido el esfuerzo que tanto la jurisprudencia del TC como la del TS han llevado a cabo para que, al igual que ocurre en países como Portugal, Italia, Francia, Alemania, Holanda, Estados Unidos de América, Canadá, Reino Unido o Australia —absolutamente respetuosos con los derechos fundamentales—, no se aplique de forma estricta la teoría de los frutos del árbol envenenado, no pudiendo afirmarse que la teoría de la conexión de antijuridicidad sea irrespetuosa con los derechos fundamentales.

Sin perjuicio de todo lo anterior, es conveniente una adecuada regulación que desarrolle el art. 11.1 LOPJ, a fin de determinar los supuestos en los que la prueba

indirectamente obtenida no se encontrará bajo una conexión de antijuridicidad con la prueba ilícita directamente obtenida y, por tanto, deberá surtir todos los efectos en el proceso. Esta reforma debería establecer, asimismo, un sumario procedimiento para la sustanciación del incidente, tanto en fase de instrucción como de enjuiciamiento.

XXIII

El aseguramiento de la prueba desde su obtención en fase de instrucción hasta su definitiva incorporación al juicio oral, proceso al que, jurisprudencialmente, se le ha denominado «cadena de custodia», es un tema de crucial importancia, que, sin embargo, no ha sido abordado por el legislador, a pesar de que su ruptura puede tener influencia en la vulneración de los derechos a un proceso con todas las garantías y a la presunción de inocencia.

Es necesaria su urgente incorporación a la LECrim, mediante una regulación de las principales directrices del procedimiento y fases conformadoras de la cadena de custodia, contribuyendo así a la reducción de los numerosos recursos interpuestos, a conseguir una mayor uniformidad en las resoluciones de los tribunales, y, con ello, a la necesitada agilización y mejora en el funcionamiento de la Administración de Justicia.

Resultaría muy apropiada la reproducción del intento de regulación que se llevó a cabo en el Anteproyecto de 2011, que trató la materia en un capítulo independiente con cuatro artículos. En ellos, tras disponer que todas las fuentes de prueba obtenidas durante la investigación de los hechos delictivos serán debidamente custodiadas, a fin de asegurar su disponibilidad en el acto del juicio oral, así como la obligación de todos cuantos tengan relación con la fuente de prueba, fueren funcionarios públicos o particulares, de constituir, aplicar y mantener la cadena de custodia, garantizando la inalterabilidad de aquella, estableció los parámetros principales de un procedimiento de gestión y custodia que debería ser desarrollado reglamentariamente, estableciendo finalmente que el quebrantamiento de la cadena de custodia fuese valorado por el tribunal a los efectos de determinar la fiabilidad de la fuente de prueba.

XXIV

Se ha planteado cierta controversia en relación con la necesidad de que tanto el interesado como su letrado defensor se encuentren presentes durante el acto de volcado

de datos, habiéndose instado la nulidad de la prueba en algún caso por no haber sido citados para dicho acto.

Resulta notorio que, cuando el registro se practique durante el transcurso de una diligencia de entrada y registro, en la mayoría de los casos se encontrará presente el investigado, pudiendo presenciar el proceso de copiado y pegado de los datos en otro soporte. Sin embargo, no ocurre lo mismo en aquellos casos en los que resultase necesario un volcado completo de los datos una vez concluido el registro domiciliario, por no ser posible, por su complejidad y duración, realizarlo durante la diligencia de entrada y registro, debiéndose intervenir los dispositivos para la práctica del volcado en dependencias policiales o judiciales tras la aprehensión de los mismos.

Aun cuando existen algunas opiniones y resoluciones judiciales que no consideran justificada la citación del interesado y su letrado, en mi opinión, se hace necesaria su citación por si considerarse oportuno comparecer, con base en los siguientes argumentos:

a) Cabe la posibilidad de alteración algún archivo obrante en los dispositivos de almacenamiento, habida cuenta de que el letrado de la Administración de Justicia carece de conocimientos informáticos así como que tampoco interviene la figura de un funcionario de un hipotético cuerpo de informáticos forenses.

b) Resulta incongruente que sí se encuentre prevista la comparecencia del investigado en relación con la detención y apertura de la correspondencia y no tenga el mismo derecho con el volcado de datos, dado que lo único que cambia es el tipo de soporte: papel o documento electrónico.

Por tanto, disponiendo el art. 584 LECrim, que «para la apertura y registro de la correspondencia postal será citado el interesado» y que «este o la persona que designe podrá presenciar la operación», aunque el legislador no haya previsto dicho ofrecimiento al investigado, debe citarse al mismo para que pueda presenciar la operación asistido de su letrado o un perito informático.

XXV

La jurisprudencia del TS ha declarado de forma reiterada que la presencia del letrado de la Administración de Justicia no podría aportar ninguna garantía durante la operación de volcado de los datos obtenidos tras un registro informático, habida cuenta

de que, en principio, el referido funcionario es un profano en cuestiones informáticas avanzadas, por lo que su presencia no es necesaria, siendo lo decisivo que, ya sea mediante su intervención 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.

No obstante lo anterior, el letrado de la Administración de Justicia, deberá dejar constancia, mediante la oportuna diligencia, de los dispositivos informáticos intervenidos tras una entrada y registro domiciliario o los que fueran puestos a disposición del tribunal tras una intervención policial fuera del domicilio, todo ello con una descripción de los mismos, quedando de este modo una adecuada constancia en autos de la naturaleza y cantidad de los equipos o instrumentos informáticos.

Aunque la presencia de este profesional de la Administración de Justicia no sea necesaria, dada la complejidad que puede tener en determinados casos el volcado de datos, resulta necesaria la intervención de un experto informático, siendo lo ideal que se trate de un funcionario de la Administración de Justicia perteneciente a un cuerpo a crear de informáticos forenses, que dotaría estas actuaciones de un mayor grado de seguridad e imparcialidad. Ello no debe dificultar la tarea llevada a cabo por las FCSE, que debe mantenerse a los fines de investigación, pero tratándose del auxilio a los tribunales de justicia en materia probatoria, nos encontramos ante un campo como la informática, en constante avance, que desde hace un tiempo viene reclamando, de forma muy especial para los informes periciales en relación con la prueba digital, esta autonomía y especialización.

XXVI

Al igual que el resto de piezas de convicción, con carácter general, los equipos intervenidos por las FCSE como consecuencia de las diligencias de registros informáticos, se custodian en las propias dependencias judiciales, Actualmente, como regla general, las piezas de convicción, incluidos dispositivos informáticos, se custodian sin las adecuadas garantías de seguridad que, para su conservación, precisan las fuentes de prueba digital contenida en los mismos.

Sin embargo, el legislador, aun cuando reconoce, al referirse en el apartado IV del preámbulo de la LO 13/2015 a los equipos informáticos, que «esos instrumentos de

comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción» (efectivamente es así por el contenido que pueden albergar, de gran incidencia en los derechos fundamentales a la vida privada), no ha establecido mecanismos que los aseguren debidamente.

Aun cuando el art. 459 LOPJ encomienda a los Letrados de la Administración de Justicia el depósito de los efectos del delito, este precepto exceptúa los de aquellos en los que se disponga reglamentariamente la remisión al organismo competente.

Por ello, es necesaria la creación de un organismo que podría denominarse Instituto de Informática Forense, que, sin perjuicio de las tareas llevadas a cabo en materia de investigación por la Policía Científica, debe ejercer todas las tareas de auxilio a los tribunales propias de la informática forense, tales como recogida, depósito y preservación de los equipos electrónicos y la prueba digital. Este organismo debería estar asistido por un cuerpo de informáticos forenses al servicio de la Administración de Justicia, que dotaría estas actuaciones de un mayor grado de seguridad e imparcialidad.

XXVII

La prueba digital podrá ser introducida en el juicio oral por cualquiera de los medios de prueba legalmente previstos. Sin embargo, el medio idóneo para que tenga lugar la incorporación es, sin duda, el de la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo. Aun cuando otros medios de prueba, como por ejemplo la testifical, sirvan en casos excepcionales, lo más correcto es que su uso tenga un carácter suplementario y, en este sentido, la reproducción en el acto de juicio oral, es el medio de prueba genuino para que la prueba digital tenga entrada en el proceso, logrando con el mismo un mayor grado de convencimiento del tribunal sobre la verdad material que con cualquier otra fuente de prueba.

Sin embargo, nuestra LECrim, por razones obvias si se tiene en cuenta el estado de la técnica a finales del siglo XIX, nada establece en cuanto a la posibilidad de la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo en el acto del juicio oral, por lo que es necesario acudir a la LEC como legislación supletoria.

Esta lógica omisión del legislador decimonónico no es óbice para que, ya en el siglo XXI, teniendo en cuenta las modificaciones de las que ha sido objeto la LECrim, y muy especialmente la operada por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la

regulación de las medidas de investigación tecnológica, se hubiera incluido en la Ley procesal una regulación en cuanto a la reproducción de la palabra, el sonido, la imagen e instrumentos de archivo.

Por otro lado, no resulta comprensible que habiéndose abordado este tema en el Anteproyecto de LECrim de 2013 —donde se establecía un procedimiento para que, si era instado por las partes se procediese a la audición o el visionado del contenido de soportes de datos que no se limitasen a almacenar información escrita—, el legislador no lo tuviese finalmente en consideración con la reforma de 2015.

Esta carencia legislativa viene provocando que, en numerosas ocasiones, como consecuencia de la ingente carga de trabajo que sufren nuestros tribunales, y la escasez de medios electrónicos que permitan la simultánea grabación del acto de juicio y la reproducción de imagen, audio y video, se opte por la incorporación al juicio mediante otros medios de prueba, que aun cuando son totalmente válidos, no son tan determinantes para el convencimiento del tribunal como lo es la reproducción en juicio.

Por ello, *de lege ferenda*, debería llevarse a cabo una minuciosa regulación para el proceso penal, del medio de prueba consistente en la reproducción de la imagen, el audio, el video e instrumentos de archivo que, en todo caso, hiciese necesaria la incorporación de la prueba digital por este medio, al menos cuando menos si así lo solicitase alguna de las partes.

XXVIII

La impugnación de la prueba digital se produce con cierta frecuencia en la práctica de los tribunales, dado su carácter volátil y la facilidad de alteración de determinados documentos electrónicos, como por ejemplo un documento de texto u hoja de cálculo. Otros fraudes, como la suplantación de identidad, tomar el control de la cuenta de otro en redes sociales, el acceso a sistemas informáticos ajenos, etc. —aun cuando será necesaria una preparación técnica y no estarán exentos de dificultades por los sistemas de seguridad existentes, tanto a nivel particular en los dispositivos informáticos mediante programas de seguridad como de las propias compañías titulares de redes sociales y de todo tipo de plataformas a las que se accede por los particulares para distintos fines a través de la red internet—, estarán al alcance de organizaciones y grupos criminales.

Se ha planteado la cuestión acerca de la necesidad de razonar la impugnación de la prueba digital cuando esta sea formulada por el encausado, problema que no se encuentra previsto en las leyes procesales. Aunque en otras jurisdicciones como la civil o la laboral, podría entenderse como un trámite natural, a fin de que no se vea comprometido el principio de igualdad de armas, no resulta del todo claro que, con base en el principio de presunción de inocencia, recaiga sobre el encausado la carga procesal de tener que razonar o aportar un principio de prueba en relación con su impugnación, sin que su actuación se limite sencillamente a negar la autenticidad de un determinado documento electrónico, como por ejemplo la negación de la autoría de un correo electrónico.

Se ha señalado doctrinalmente que será necesario un principio de prueba para dar curso a la impugnación. En mi opinión, debe exigirse que se exprese algún razonamiento que apoye la falta de autenticidad invocada, dado que una impugnación no concretada, debería considerarse una actuación con fines estratégicos no ajustada a las exigencias de la buena fe, compartiendo las opiniones que proponen una regulación en la LECrim de un trámite específico para estos casos de impugnación que contemplase esta particularidad.

XXIX

En caso de admitirse la impugnación de la prueba digital, una vez planteada mediante la aportación de algún indicio o argumento que le atribuya cierta credibilidad, resulta doctrinal y jurisprudencialmente aceptado que, con carácter general, podrá producirse un resultado parecido a un desplazamiento de la carga de la prueba. Como consecuencia del mismo, lo normal será que la parte proponente de la prueba deba acreditar mediante algún otro medio de prueba la autenticidad y en su caso integridad del documento.

Lo normal será que esta prueba adicional sea una pericial que acredite la realidad de los aspectos controvertidos, como la autenticidad del documento electrónico, origen de la comunicación, identidad de los interlocutores, si se ha producido un acceso indebido a un determinado equipo informático, etc.

Sin embargo, esta prueba solo será necesaria cuando no sea posible la acreditación de los puntos controvertidos por otros medios de prueba, por lo que el juez o tribunal deberá tomar en consideración los razonamientos de ambas partes en relación

con la prueba digital impugnada así como los demás elementos probatorios incorporados al proceso, para determinar si es necesaria una pericial contradictoria que garantice la autenticidad del documento electrónico o, en su caso, debe valorarse el documento electrónico objeto de prueba de forma conjunta con las demás pruebas, sin que aquella sea necesaria.

XXX

La valoración de la prueba digital se ajustará, como cualquier otra prueba en el ámbito del proceso penal, al principio de libre valoración y por tanto a las reglas de la sana crítica, llevándose a cabo un examen individual, seguido, si procede según el juez o tribunal, de una apreciación conjunta y contrastada con el resto del material probatorio.

La prueba digital tiene, sin embargo, algunas particularidades. Una de ellas se plantea en cuanto que, dadas las especiales características de esta prueba, el juez deberá atender especialmente a la autenticidad del origen y a la integridad del contenido, es decir a la coincidencia del autor y de los datos de los documentos electrónicos con los inicialmente obtenidos.

En este punto, aun cuando rige el principio de libre valoración, tratándose de documento electrónico, tendrán mayor fiabilidad a los efectos de su autenticidad e integridad, y por tanto otorgarán un mayor nivel de credibilidad, los documentos firmados electrónicamente con arreglo a lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, que aquellos que no tengan tal cualidad. Todo ello, sin perjuicio de que un documento con las garantías de la firma electrónica, también podría ser manipulado, en cuyo caso sería imprescindible una pericial para acreditar tal extremo.

En este sentido, en el ámbito de la prueba digital adquiere especial importancia la prueba pericial, principalmente en los supuestos de impugnación de la autenticidad o integridad de los documentos electrónicos, debiéndose proceder a su libre valoración de acuerdo con las reglas de la sana crítica, sin que los informes periciales sean vinculantes para el juez o tribunal, no obstante la importancia de los mismos.

Finalmente, se ha afirmado por algún sector doctrinal que la valoración de la prueba digital se halla sujeta a una «sana crítica especialísima», en atención a la mención del art. 384.3 LEC que, en relación con la valoración de los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso, dispone que la

misma se efectuará conforme a las reglas de la sana crítica aplicables a aquellos «según su naturaleza». Sin embargo, considero que este inciso del art. 384.3 LEC, no aporta nada, especialmente en el proceso penal, dado que, de acuerdo con el principio de libre valoración, el tribunal siempre deberá considerar la naturaleza del concreto medio de prueba.

BIBLIOGRAFÍA

ABEL LLUCH, X., «Prueba electrónica», en Abel LLuch, X., Picó i Junoy, J. (dirs.), *La prueba electrónica*, Barcelona, Bosch Editor, 2011, pp. 15-240.

ABEL LLUCH, X.; PICÓ I JUNOY, J.; SERRANO MOLINA, A., «Preguntas con respuesta: la prueba a consulta», *Diario La Ley - Sección Práctica Forense*, n.º 7564, 2011.

ABEL LLUCH, X., «Los medios de prueba a la luz de las reglas de la sana crítica», *Diario La Ley - Sección Tribuna*, n.º 8658, 2015.

AGUILERA DE PAZ, E.; RIVAS MARTÍ, F., *Derecho Judicial Español*, Madrid, Editorial Reus, 1920.

ALEXY, R., «Los derechos fundamentales y el principio de proporcionalidad», *Revista Española de Derecho Constitucional*, n.º 91, 2011, pp. 11-29.

ALONSO SALGADO, C., «Algunos elementos problemáticos de la intervención del correo electrónico como diligencia de investigación en el sistema penal español: Un camino de claroscuros», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, pp. 125-147.

ÁLVAREZ CONDE, E., «El sistema constitucional español de derechos fundamentales», *Corts: Anuario de derecho parlamentario*, n.º 15, 2004, pp. 115-146.

ÁLVAREZ DE NEYRA KAPPLER, S., «Los descubrimientos casuales en el marco de una investigación penal (Con especial referencia a las diligencias de entrada y registro en domicilio)», *Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, n.º 2, 2011, pp. 1-69.

ÁLVAREZ SUÁREZ, L., «El Ministerio Fiscal y las Diligencias de Investigación Tecnológica», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, pp. 105-113.

ANGUAS BALSERA, J., «El peritaje en informática en el marco de las disciplinas que le son afines. Puntos de contacto y perfil de la actividad», *Diario La Ley - Sección Práctica Forense*, n.º 7329, 2010.

ANGUAS BALSERA, J., «La pericial informática», en Abel LLuch, X. (coord.), *Tratado pericial judicial*, Las Rozas (Madrid), La Ley, 2014, pp. 313-376.

AÑÓN CALVETE, J., «Diligencias de Investigación Tecnológica y Derechos Fundamentales», *Tirant Online*, *Documento TOL5.429.306*, 2015.

ARAGONESES MARTÍNEZ, S., «El Sumario (II)», en De la Oliva Santos, A. y otros, *Derecho Procesal Penal*, Madrid, Editorial Universitaria Ramón Areces, 2007, pp. 329-391.

ARMENTA DEU, T., «Prueba ilícita y reforma del proceso penal», *Revista del Poder Judicial*, n.º especial XIX, 2006.

ARMENTA DEU, T., *Lecciones de Derecho Procesal Penal*, Madrid, Marcial Pons, 2017.

ARRABAL PLATERO, P., *La Prueba Tecnológica: Aportación, Práctica y Valoración*, Valencia, Tirant Lo Blanch, 2019.

ASENCIO GALLEGO, J. M., «Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la Ciberdelincuencia», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, pp. 43-67.

ASENCIO MELLADO, J. M., *Prueba prohibida y prueba preconstituida*, Madrid, Editorial Trivium, 1989.

ASENCIO MELLADO, J. M., *Derecho Procesal Penal*, Valencia, Tirant Lo Blanch, 2010.

ASENCIO MELLADO, J. M., «Prueba ilícita: Declaración y efectos», *Revista General de Derecho Procesal*, n.º 26, 2012, pp. 1-55.

ASENCIO MELLADO, J. M., «Otra vez sobre la exclusión de las pruebas ilícitas en fase de instrucción penal: respuesta al Prof. Gimeno Sendra», *Diario La Ley - Sección Doctrina*, n.º 8026, 2013.

ASENCIO MELLADO, J. M., «La exclusión de la prueba ilícita en la fase de instrucción como expresión de garantía de los derechos fundamentales», *Diario La Ley - Sección Doctrina*, n.º 8009, 2013.

ASENCIO MELLADO, J. M., «La STC 97/2019, de 16 de julio. Descanse en paz la prueba ilícita», *Diario La Ley - Sección Tribuna*, n.º 9499, 2019.

BACHMAIER WINTER, L., «Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015», *Boletín del Ministerio de Justicia*, n.º 2195, 2017.

BARNES, J., «El principio de proporcionalidad. Estudio preliminar», *Cuadernos de Derecho Público*, vol. 5, 1998, pp. 15-49.

BARONA VILAR, S., «La prueba (I y II)», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, pp. 373-410.

BARRIOS GONZÁLEZ, B., «Teoría de la sana crítica», *Opinión Jurídica: Publicación de la Facultad de Derecho de la Universidad de Medellín*, vol. 2, n.º 3, 2003, pp. 99-132, Consultado en https://revistas.udem.edu.co/index.php/opinion/index, el 1 de junio de 2020.

BAYO DELGADO, J., «La protección de datos en la investigación policial y en el proceso penal», *Jueces para la Democracia. Información y Debate*, n.º 63, 2008, pp. 11-25.

BENITEZ IGLESIAS, J. F., «La cadena de custodia: fuente de prueba de dispositivos informáticos y electrónicos», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2014, Consultado en http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 25 de junio de 2020.

BERTRÁN PARDO, A. I., «Los contenidos de whatsapp como medio probatorio en el ámbito de las diligencias urgentes por delitos de violencia contra la mujer. Cuestiones en torno a su impugnación y a la práctica de la prueba pericial a la que se refiere la STS 300/2015, de 19 de mayo», *Noticias jurídicas*, 2015, Consultado en http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10533-las-contenidos-de-whatsapp-como-medio-probatorio-en-el-ambito-de-las-diligencias-urgentes-por-delitos-de-violencia-contra-la-muje/, el 6 de junio de 2018.

BONILLA CORREA, J. A., «Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio», *Diario La Ley - Sección Doctrina*, n.º 8522, 2015.

BUENO DE MATA, F., «Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la LO 13/2015», en Bueno de Mata, F. (coord.), *Fodertics 4.0*, Albolote (Granada), Editorial Comares, 2015, pp. 117-123.

BUENO DE MATA, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», *Diario La Ley - Sección Doctrina*, n.º 8627, 2015.

BUJOSA VADELL, L. M., «La valoración de la prueba electrónica», en Bueno de Mata, F. (coord.), *Fodertics 3.0*, Albolote (Granada), Editorial Comares, 2015, pp. 75-85.

BUJOSA VADELL, L. M., «Tecnologías de la imagen y valoración de la prueba», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, pp. 213-239.

CABEZUDO RODRÍGUEZ, N., «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín del Ministerio de Justicia*, n.º 2186, 2016, pp. 7-60.

CABEZUDO RODRÍGUEZ, N., «Algunas reflexiones acerca de la reglamentación de las nuevas medidas de investigación tecnológica en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la LECrim», en Jimeno Bulnes, M., Perez Gil, J. (coords.), *Nuevos horizontes del derecho procesal*, Barcelona, Bosch Editor, 2016, pp. 541-558.

CALVO CABELLO, J. L., «La valoración de la prueba en el juicio oral», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, pp. 425-451.

CARNELUTTI, F., *La prueba civil*, Buenos Aires, Ediciones Depalma, 1982.

CASTILLEJO MANZANARES, R., «Alguna de las cuestiones que plantean las diligencias de investigación tecnológica», *Revista Aranzadi de Derecho y Proceso Penal - Parte Análisis Doctrinal*, n.º 45, 2017.

CASTILLEJO MANZANARES, R., «Hallazgos casuales y medidas tecnológicas de investigación», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 1, 2018.

CASTILLO RIGABERT, F., «Derechos fundamentales e investigación en las diligencias previas (Estudio de la reciente jurisprudencia de la Sala II del TS)», *Anales de Derecho (Universidad de Murcia)*, n.º 13, 1995, pp. 13-37.

COLOMA CORREA, R.; AGÜERO SAN JUAN, C., «Lógica, ciencia y experiencia en la valoración de la prueba», *Revista Chilena de Derecho*, vol. 41, n.º 2, 2014, pp. 673-703, Consultado en https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-34372014000200011&lng=en&nrm=iso&tlng=es, el 3 de junio de 2020.

COMISARÍA, G. DE P. J., «La investigación de los delitos cometidos a través de las TIC'S por el CNP», 2011, Consultado en http://www5.poderjudicial.es/CVdi/TEMA06-ES.pdf, el 14 de agosto de 2018.

CONDE-PUMPIDO TOURÓN, C., «La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies LECRIM)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Conde-Pumpido Tourón.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47, el 12 de junio de 2020.

CONSEJO DE ESTADO, *Dictamen 97/2015, 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 tecnológica*, 2015, Consultado en http://www.boe.es/buscar/doc.php?id=CE-D-2015-97, el 8 de marzo de 2018.

CONSEJO FISCAL DE LA FISCALÍA GENERAL DEL ESTADO, *Informe 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 tecnológica*, 2015, Consultado en https://www.fiscal.es/documents/20142/fee385a4-e606-4d8c-677a-20605cb1185f, el 11 de junio de 2020.

COUTURE, E. J., *Fundamentos del Derecho Procesal Civil*, Buenos Aires, Ediciones Depalma, 1958.

CUADRADO SALINAS, C., «Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa», *La Ley Penal - Sección Estudios*, n.º 107, 2014.

DE JORGE MESAS, L. F., «La incorporación de las nuevas tecnologías informáticas y de telecomunicaciones al proceso penal (...más sobre las nuevas tecnologías)», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 2, 2007, pp. 355-413.

DE LA ROSA CORTINA, J. M., *Confesiones. Declaraciones de imputados y acusados. Coimputados, testigos imputados y testigos condenados*, Cizur Menor (Navarra), Editorial Aranzadi, 2012.

DE URBANO CASTRILLO, E., «Prueba ilícita en particular», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, pp. 211-292.

DE URBANO CASTRILLO, E., «La investigación tecnológica del delito», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 2, 2007, pp. 19-76.

DE URBANO CASTRILLO, E., *La valoración de la prueba electrónica*, Valencia, Tirant Lo Blanch, 2009.

DE URBANO CASTRILLO, E.; TORRES MORATO, M. A., *La prueba ilícita penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2012.

DEL MORAL GARCÍA, A., «Tratamiento procesal de la prueba ilícita por vulneración de derechos fundamentales», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2001, Consultado en http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 22 de marzo de 2020.

DEL MORAL GARCÍA, A., «¿Cuándo debe declarar la inutilizabilidad de un medio de prueba por vulneración de derechos fundamentales?», *Revista de Jurisprudencia - El Derecho*, n.º 2, Marzo, 2017.

DEL POZO PÉREZ, M., «La cadena de custodia: Tratamiento jurisprudencial», *Revista General de Derecho Procesal*, n.º 30, 2013.

DELGADO MARTÍN, J., «La prueba del whatsapp», *Diario La Ley - Sección Tribuna*, n.º 8605, 2015.

DELGADO MARTÍN, J., «Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015», *Diario La Ley - Sección Doctrina*, n.º 8693, 2016.

DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, Las Rozas (Madrid), Wolters Kluwer, 2016.

DELMAS-MARTY, M., *Procesos penales de Europa*, Zaragoza, Editorial Edijus, 2000.

DÍAZ CABIALE, J. A.; MARTÍN MORALES, R., *La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, Madrid, Civitas, 2001.

DÍEZ-PICAZO GIMÉNEZ, L. M., *Sistema de Derechos Fundamentales*, Cizur Menor (Navarra), Editorial Aranzadi, 2013.

DÍAZ PITA, M. P., *El coimputado*, Valencia, Tirant Lo Blanch, 2000.

EIRANOVA ENCINAS, E., «Cadena de custodia y prueba de cargo», *Diario La Ley - Sección Doctrina*, n.º 6863, 2008.

ESCOBAR JIMÉNEZ, R., «La prueba de peritos», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo II*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, pp. 49-155.

ESPÍN LÓPEZ, I., «La necesidad de una adecuada regulación de las Diligencias Indeterminadas en el Proceso Penal», *Acta Judicial - Revista del Ilustre Colegio Nacional de Letrados de la Administración de Justicia*, n.º 6, 2020, pp. 48-64.

FERNÁNDEZ, C.A., «Prueba Pericial Delitos y tecnología de la Información Características y valoración en el Proceso Penal Argentino», *Derecho Informático y de las Nuevas Tecnologías*, n.º 5, Boletín n.º 5, enero de 2003.

FERNÁNDEZ ENTRALGO, J., «Las reglas del juego. Prohibido hacer trampas: la prueba ilegítimamente obtenida», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 9, 1996, pp. 55-210.

FERNÁNDEZ ENTRALGO, J., «Los conocimientos privados del juez en materia psicológica. Las posibilidades de introducirlos para argumentar su convicción», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 53, 2010.

FERNÁNDEZ-GALLARDO FERNÁNDEZ GALLARDO, J. Á., «Registro de dispositivos de almacenamiento masivo de información», *Dereito - Revista xurídica da Universidade de Santiago de Compostela*, vol. 25, 2016, pp. 25-58.

FIGUEROA NAVARRO, C., «El aseguramiento de las pruebas y la cadena de custodia», *La Ley Penal - Sección Estudios*, n.º 84, 2011.

FIGUEROA NAVARRO, C.; DEL AMO RODRÍGUEZ, A., «La cadena de custodia de las pruebas y los protocolos de actuación de la policía científica», en *Policía científica-100 Años de Ciencia al Servicio de la Justicia*, Madrid, 2011, pp. 315-330, Consultado en http://www.interior.gob.es/documents/642317/1203227/Policía+Científica+-100+años+de+Ciencia+al+servicio+de+la+justicia+%28NIPO+126-11-081-7%29.pdf/b983385f-ec1c-48c0-a6fe-98ede304c2fc, el 13 de julio de 2019.

FISCALÍA GENERAL DEL ESTADO, *Circular 1/1999, de 29 de diciembre, sobre la intervención de las comunicaciones telefónicas en el seno de los procedimientos penales*, 1999, Consultado en https://www.fiscal.es/documents/20142/667c2dd9-e80b-0f7b-c761-a3f24d86c701, el 2 de junio de 2020.

FISCALÍA GENERAL DEL ESTADO, *Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, 2013, Consultado en https://www.fiscal.es/documents/20142/b9b37701-c716-79ab-d1dc-111350113518, el 27 de mayo de 2020.

FISCALÍA GENERAL DEL ESTADO, *Circular 4/2013, de 30 de diciembre, sobre las Diligencias de Investigación*, 2013, Consultado en https://www.fiscal.es/documents/20142/3649479c-27aa-8369-f83e-4c5c18514c0c, el 10 de junio de 2020.

FISCALÍA GENERAL DEL ESTADO, UNIDAD DE CRIMINALIDAD INFORMÁTICA, *Dictamen 1/2016 sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones*

electrónicas, 2016, Consultado en https://www.fiscal.es/documents/20142/f1f4b75c-5a89-511d-cca5-ce94c544adf5, el 12 de junio de 2020.

FISCALÍA GENERAL DEL ESTADO, *Instrucción 2/2017, sobre procesos incoados a raíz de la deducción de testimonios de una causa principal*, 2017, Consultado en https://www.fiscal.es/documents/20142/e823a65b-d869-3c12-4fdc-3329dbfcbd88, el 10 de junio de 2020.

FISCALÍA GENERAL DEL ESTADO, *Circular 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*, 2019, Consultado en https://www.fiscal.es/documents/20142/972fdb98-5e62-2609-f99f-7a6d887b5d03, el 1 de junio de 2020.

FISCALÍA GENERAL DEL ESTADO, *Circular 5/2019, sobre registro de dispositivos y equipos informáticos*, 2019, Consultado en https://www.fiscal.es/documents/20142/282a82d1-da36-8e8d-4dbc-c1bc0f02c6f0, el 4 de junio de 2020.

FRÍGOLS I BRINES, E., «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», en Boix Reig, Javier (dir.) Jareño Leal, A. (coord.), *La protección jurídica de la intimidad*, Madrid, Iustel, 2010, pp. 37-91.

FUENTES SORIANO, O., «Videos, comunicación electrónica y redes sociales: cuestiones probatorias», *Práctica de Tribunales*, n.º 135, 2018.

FUENTES SORIANO, O., «Los procesos por violencia de género. Problemas probatorios tradicionales y derivados del uso de las nuevas tecnologías», *Revista General de Derecho Procesal*, n.º 44, 2018, pp. 1-39.

FUENTES SORIANO, O., «La impugnación de la prueba digital», en Álvarez Alarcón, A., García Molina, P. (dirs.), Conde Fuentes, J., Arrabal Platero, P. (coords.), *Tendencias actuales del Derecho Procesal*, Albolote (Granada), Editorial Comares, 2019, pp. 277-290.

GALÁN MUÑOZ, A., «¿Nuevos riesgos, viejas respuestas? Estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la

información y la comunicación», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2014, pp. 203-279.

GALLEGO SÁNCHEZ, G. Y OTROS, «El "delito grave" en relación a la obligación de conservación de datos, según la Ley 25/2007 y las reformas penales recientes», *Revista de Jurisprudencia - El Derecho*, n.º 1, Noviembre, 2015.

GARCÍA MOLINA, P., «El registro, físico o remoto, de dispositivos de almacenamiento masivo de información y de equipos informáticos de abogados», en Bueno de Mata, F. (coord.), *Fodertics 5.0*, Albolote (Granada), Editorial Comares, 2016, pp. 121-135.

GARCÍA SAN MARTÍN, J., «La prueba penal ilícita y la prueba penal refleja: Hacia una restrictiva aplicación de la doctrina de los frutos del árbol envenenado», *Tirant Online, Documento TOL2.249.759*, 2011.

GARCÍA SAN MARTÍN, J., «Consideraciones en torno 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», *Diario La Ley - Sección Doctrina*, n.º 8648, 2015.

GARCÍA-ATANCE Y GARCÍA DE MORA, M. V., «La Constitución Dogmática (I). Estado de Derecho y naturaleza de los derechos», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 25-54.

GARCIMARTÍN MONTERO, R., *Los medios de investigación tecnológicos en el proceso penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2018.

GASCÓN ABELLÁN, M. Y OTROS, «La motivación fáctica», en Hernández García, J. (dir.), *123 cuestiones básicas sobre la motivación de las resoluciones judiciales*, Madrid, Cuadernos Digitales de Formación del Consejo General del Poder Judicial, 2012, pp. 149-393.

GIMENO SENDRA, J. V., *Derecho Procesal Civil. I. El Proceso de Declaración. Parte General.*, Majadahonda (Madrid), Editorial Colex, 2007.

GIMENO SENDRA, J. V., «Medidas limitadoras de derechos fundamentales en el proceso penal», en Perez-Cruz Martín, A.J., Ferreiro Baamonde, X. (dirs., Neira Pena, A. (coord.), *Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011*, A Coruña, Universidade da Coruña, 2012, pp. 73-90.

GIMENO SENDRA, J. V., «Corrupción y propuestas de reforma», *Diario La Ley*, n.º 7990, 2012.

GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación al artículo del Prof . Asencio)», *Diario La Ley - Sección Tribuna*, n.º 8021, 2013.

GIMENO SENDRA, J. V., «La improcedencia de la exclusión de la prueba ilícita en la instrucción (contestación a la réplica del Prof. Asencio)», *Diario La Ley - Sección Tribuna*, n.º 8027, 2013.

GIMENO SENDRA, J. V., *Manual de Derecho Procesal Penal*, Madrid, Ediciones Jurídicas Castillo de Luna, 2015.

GÓMEZ COLOMER, J. L., «La terminación del proceso penal», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, pp. 427-445.

GÓMEZ COLOMER, J. L., «Prueba admisible y prueba prohibida: Cambios en el garantismo judicial motivados por la lucha contra el crimen organizado en la realidad jurisprudencial española actual», *Doctrina y Jurisprudencia Penal*, n.º 22, 2015, pp. 3-47.

GÓMEZ COLOMER, J. L., «Los actos de investigación no garantizados», en Montero Aroca, J. y otros, *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, pp. 193-214.

GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., *Derecho Procesal Civil, Vol. I*, Madrid, Artes Gráficas y Ediciones, 1979.

GÓMEZ ORBANEJA, E.; HERCE QUEMADA, V., *Derecho Procesal Penal*, Madrid, Artes Gráficas y Ediciones, 1987.

GONZÁLEZ-CUÉLLAR SERRANO, N., «El principio de proporcionalidad en el Derecho procesal español», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 191-215.

GONZÁLEZ-CUÉLLAR SERRANO, N., «Garantías constitucionales de la persecución penal en el entorno digital», en Díaz Maroto y Villarejo, J. y otros), *Derecho y Justicia Penal en el Siglo XXI*, Madrid, Colex, 2006, pp. 887-916.

GONZÁLEZ-MONTES SÁNCHEZ, J. L., «La prueba ilícita», *Persona y Derecho*, n.º 54, 2006, pp. 363-383.

GONZÁLEZ-MONTES SÁNCHEZ, J. L., «Reflexiones sobre el proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas», *Revista Electrónica de Ciencia Penal y Criminología*, vol. 17, n.º 06, 2015, Consultado en http://criminet.ugr.es/recpc/17/recpc17.html el 26 de febrero de 2019.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E., «Incorporación al proceso del material informático intervenido durante la investigación penal», *Boletín del Ministerio de Justicia*, n.º 2163, 2014.

GUTIÉRREZ SANZ, M. R., *La cadena de custodia en el proceso penal español*, Cizur Menor (Navarra), Editorial Aranzadi, 2016.

HERNÁNDEZ GARCÍA, J., «Exigencias éticas y motivación», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 12, 2009.

HOFFMANN-RIEM, W., «Innovaciones en la jurisprudencia del Tribunal Constitucional alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la sociedad de la información», *Revista de Derecho Constitucional Europeo*, vol. 11, n.º 22, 2014, pp. 123-146.

HUETE NOGUERAS, J. J., «La regulación de las medidas de investigación tecnológica. Análisis de los aspectos referentes a la incorporación al proceso de datos electrónicos de tráfico o asociados», *Revista del Ministerio Fiscal*, n.º 2, 2016, pp. 59-81.

IGARTUA SALAVERRÍA, J.; HERNÁNDEZ GARCÍA, J., «Valoración de la prueba», en Hernández Garcia, J. (dir.), *113 cuestiones básicas sobre la prueba en el proceso penal*,

Madrid, Cuadernos Digitales de Formación del Consejo General del Poder Judicial, 2013, pp. 696-792.

INSA MÉRIDA, F.; LÁZARO HERRERO, C., «La admisibilidad de las pruebas electrónicas en los tribunales: Luchando contra los delitos tecnológicos», *Diario La Ley - Sección Doctrina*, n.º 6708, 2007.

JAMARDO LORENZO, A., «La preconstitución de la prueba en el proceso penal», *Diario La Ley - Sección Doctrina*, n.º 8906, 2017.

JIMÉNEZ CONDE, F., *La apreciación de la prueba legal y su impugnación*, Salamanca, Universidad, Departamento de Derecho Procesal, 1978.

JIMÉNEZ CONDE, F., *Introducción al Derecho Procesal Penal*, Murcia, Diego Marín Librero Editor, 2017.

JIMÉNEZ SEGADO, C.; PUCHOL AIGUABELLA, M., «Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos», *Diario La Ley - Sección Doctrina*, n.º 8676, 2016.

KLUTH, W., «Prohibición de exceso y principio de proporcionalidad en Derecho alemán», *Cuadernos de Derecho Público*, n.º 5, 1998, pp. 219-237.

LADRÓN TABUENCA, P., «La regulación de la cadena de custodia en España: previsiones legales y desarrollos jurisprudenciales sobre la cadena de custodia de las fuentes de prueba», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, pp. 19-38.

LANZAROTE MARTÍNEZ, P., «Intervención de las comunicaciones», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo II*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, pp. 233-578.

LANZAROTE MARTÍNEZ, P., «La nueva regulación de las intervenciones telefónicas y telemáticas: Algunas cuestiones claves y otras discutibles», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 58-85.

LEAL MEDINA, J., «Ruptura de la cadena de custodia y desconexión con las fuentes de prueba. Supuestos concretos. Reflexiones que plantea», *Diario La Ley - Sección Doctrina*, n.º 8846, 2016.

LLORENTE VEGA, M. J., «Informática forense», en *Policía científica - 100 Años de Ciencia al Servicio de la Justicia*, 2011, pp. 275-302, Consultado en http://www.interior.gob.es/documents/642317/1203227/Policía+Científica+-100+años+de+Ciencia+al+servicio+de+la+justicia+%28NIPO+126-11-081-7%29.pdf/b983385f-ec1c-48c0-a6fe-98ede304c2fc, el 13 de julio de 2019.

LÓPEZ BARJA DE QUIROGA, J., *Tratado de Derecho Procesal Penal*, Cizur Menor (Navarra), Editorial Aranzadi, 2010.

LÓPEZ CAUSAPÉ, E., «Las medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín Digital Asociación de Jueces y Magistrados Francisco de Vitoria*, n.º 6, 2016.

LÓPEZ LOMA, L., «El registro oculto on line y su conflicto con los derechos fundamentales según la doctrina alemana tras la sentencia del Tribunal Constitucional Federal de 27 de febrero de 2008», *Revista Española de Protección de Datos*, n.º 5, 2008, pp. 223-228.

LÓPEZ ORTEGA, J. J., «La utilización de medios técnicos de observación y vigilancia en el proceso penal», en Boix Reig, J. (dir.), Jareño Leal, Á. (coord.), *La protección jurídica de la intimidad*, Madrid, Iustel, 2010, pp. 261-334.

LÓPEZ ORTEGA, J. J., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (II): Captación y grabación de comunicaciones orales mediante dispositivos electrónicos. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización», *Formación a distancia-Consejo General del Poder Judicial*, n.º 3, 2016.

LÓPEZ-BARAJAS PEREA, I., «Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos», *IDP: Revista de Internet, Derecho y Política*, n.º 24, 2017, pp. 64-76.

LÓPEZ-BARAJAS PEREA, I., «Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la Ley», *Revista de Derecho Político*, n.º 98, 2017, pp. 91-119.

LÓPEZ-BARAJAS PEREA, I., «El derecho a la protección del entorno virtual y sus límites: el registro de los sistemas informáticos», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant Lo Blanch, 2019, pp. 135-168.

LORENZ, D., «El registro oculto de ordenadores como desafío en la dogmática de los derechos fundamentales y la reciente respuesta por la Constitución alemana», *Revista Española de Protección de Datos*, n.º 5, 2008, pp. 9-23.

LUCENA CID, I. V., «El concepto de la intimidad en los nuevos contextos tecnológicos», en Galán Muñoz, A. (coord.), *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2014, pp. 15-53.

MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Valencia, 1984.

MAESO VENTUREIRA, A., «Medidas de investigación tecnológica en el proceso penal tras la reforma efectuada por la Ley Orgánica 13/2015», en Pérez Machío, A.I., Goizueta Vértiz, J. (dirs.), *Tiempo de reformas: perspectiva académica y realidad judicial*, Bilbao, Servicio Editorial de la Universidad del País Vasco, 2017, pp. 15-56.

MAGRO SERVET, V., «La instrucción de los delitos informáticos», *Estudios de Derecho Judicial del Consejo General del Poder Judicial*, n.º 64, 2004.

MAGRO SERVET, V., «¿Como se aporta la prueba digital al proceso civil?», *Revista de Jurisprudencia - El Derecho*, n.º 2, Junio, 2015.

MARCA MATUTE, J., «El imputado y el anticipo probatorio», en Abel Lluch, X., Richard González, M. (dirs.), *Estudios sobre prueba penal - Vol. III*, Las Rozas (Madrid), La Ley, 2013.

MARCHENA GÓMEZ, M., «Dimensión jurídico-penal del correo electrónico», *Diario La Ley - Sección Doctrina*, n.º 6475, 2006.

MARCHENA GÓMEZ, M., «La reforma de las diligencias de investigación limitativas de los derechos reconocidos en el Art. 18 de la CE. Proceso penal y nuevas tecnologías», en Marchena Gómez, M., González-Cuellar Serrano, N.), *La reforma de la*

Ley de Enjuiciamiento Criminal en 2015, Madrid, Ediciones Jurídicas Castillo de Luna, 2015, pp. 171-403.

MARCHENA GÓMEZ, M., «La "Sentencia Falciani": ¿hacia un nuevo concepto de prueba ilícita entre particulares?», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 43-57.

MARTÍN MARTÍN DE LA ESCALERA, A. M., «El registro de dispositivos de almacenamiento masivo de la información», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Martín Martín de la Escalera, Ana Mª.pdf?idFile=bf66c357-e4d4-4701-8a4d-83d6c103ebe5, el 28 de mayo de 2020.

MARTÍN RÍOS, P., «La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información ¿un supuesto de autoincriminación?», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, pp. 149-159.

MARTÍNEZ JIMÉNEZ, J., *Derecho Procesal Penal*, Madrid, Tecnos, 2015.

MARTÍNEZ JIMÉNEZ, J., «El reconocimiento judicial», en Rives Seva, A.P. (coord.), *La prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo - Tomo I*, Cizur Menor (Navarra), Editorial Aranzadi, 2016, pp. 341-385.

MEGÍAS QUIRÓS, J. J., «Privacidad e internet: intimidad, comunicaciones y datos personales», *Anuario de Derechos Humanos - Nueva Época*, n.º 3, 2002, pp. 515-560.

MELÓN MUÑOZ, A.; MARTÍN NIETO, P. Y OTROS, *Memento Procesal Penal*, Madrid, Francis Lefebvre, 2017.

MESTRE DELGADO, E., «La cadena de custodia de los elementos probatorios obtenidos de dispositivos informáticos y electrónicos», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, pp. 39-79.

MINISTERIO DEL INTERIOR, S. DE E. DE S., *Estudio sobre la Cibercriminalidad en España*, 2017, Consultado en http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercrimi

nalidad+en+España.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70, el 8 de marzo de 2019.

MIRANDA ESTRAMPES, M., «La declaración del coimputado como prueba de cargo suficiente: análisis desde la perspectiva de la doctrina del TC. (Radiografía de un giro constitucional involucionista)», *Revista Xurídica Galega*, n.º 58, 2008, pp. 13-24.

MIRANDA ESTRAMPES, M., «La prueba ilícita: la regla de exclusión probatoria y sus excepciones», *Revista Catalana de Seguridad Pública*, n.º 22, 2010, pp. 131-151.

MIRANDA WALLACE, D., «Registro remoto de equipos informáticos. Comentario crítico al artículo 588 septies LECRIM», *Revista General de Derecho Procesal*, n.º 42, 2017, pp. 1-14.

MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.

MONTERO AROCA, J., «Nociones generales sobre la prueba (Entre el mito y la realidad)», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 7, 2000.

MONTERO AROCA, J., «Los conceptos esenciales», en Montero Aroca, J. y otros), *Derecho Jurisdiccional III - Proceso penal*, Valencia, Tirant Lo Blanch, 2015, pp. 27-47.

MONTERO AROCA, J., *Derecho Jurisdiccional I - Parte general*, Valencia, Tirant Lo Blanch, 2017.

MONTES ÁLVARO, M. A., «La regulación de las medidas de investigación tecnológica y la protección de los derechos reconocidos en el art. 18 CE», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 86-116.

MORENO CATENA, V., «Ley de conservación de datos y garantías procesales», en Domínguez Peco, E. (coord.), *La protección de datos en la cooperación policial y judicial*, Cizur Menor (Navarra), Editorial Aranzadi, 2008, pp. 163-171.

MORENO CATENA, V.; CORTÉS DOMÍNGUEZ, V., *Derecho Procesal Penal*, Valencia, Tirant Lo Blanch, 2019.

MUERZA ESPARZA, J. J., «Sobre el valor de la prueba preconstituida en el proceso penal», en Jimeno Bulnes, M., Pérez Gil, J. (coords.), *Nuevos horizontes del derecho procesal*, Barcelona, Bosch Editor, 2016, pp. 769-785.

MUÑOZ CARRASCO, P., «Análisis del estado actual de la prueba ilícitamente obtenida en el proceso penal español», *Revista Aranzadi Doctrinal*, n.º 1, 2019.

NADAL GÓMEZ, I., «El régimen de los hallazgos casuales en la ley 13/2015, de modificación de la ley de enjuiciamiento criminal», *Revista General de Derecho Procesal*, n.º 40, 2016, pp. 1-70.

NIEVA FENOLL, J., «La inexplicable persistencia de la valoración legal de la prueba», *Ars Iuris Salmanticensis*, n.º 5, Junio, 2017, pp. 57-76.

ORTIZ PRADILLO, J. C., «Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas», *La Ley Penal - Sección Jurisprudencia aplicada a la práctica*, n.º 75, 2010.

ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, Madrid, Colex, 2013.

ORTIZ PRADILLO, J. C., «Desafíos legales de las diligencias de investigación tecnológica», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, pp. 303-315.

ORTIZ PRADILLO, J. C., «Comunicaciones, tecnología y proceso penal: Viejos delitos, nuevas necesidades», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, pp. 15-42.

ORTUÑO NAVALÓN, M. C., *La prueba electrónica ante los tribunales*, Valencia, Tirant Lo Blanch, 2014.

PAZ RUBIO, J. M., «La prueba en el proceso penal», *Cuadernos de Derecho Judicial del Consejo General del Poder Judicial*, n.º 1, 1992.

PEDRAZ PENALVA, E., «La utilización en el proceso penal de datos personales recopilados sin indicios de comisión delictiva», en Pedraz Penalva, E. (coord.), *Protección de datos y proceso penal*, Madrid, Wolters Kluwer, 2010, pp. 17-52.

PERALS CALLEJA, J., «La cadena de custodia. Problemas probatorios», *Repertorio Jurídico-Científico del Centro de Estudios Jurídicos*, 2014, Consultado en http://www.cej-mjusticia.es/cej_dode/servlet/CEJServlet?dispatcher=vacio&action=getPresentationForm&advance=0&type=JSPL, el 25 de junio de 2020.

PERELLÓ DOMENECH, I., «El principio de proporcionalidad y la jurisprudencia constitucional», *Jueces para la Democracia. Información y Debate*, n.º 28, 1997, pp. 69-75.

PÉREZ GIL, J.; GONZÁLEZ LÓPEZ, J. J., «Cesión de datos personales para la investigación penal. Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Doctrina*, n.º 7401, 2010.

PÉREZ GIL, J.; GONZÁLEZ LÓPEZ, J. J., «La incorporación de datos personales automatizados al proceso en la propuesta de Código Procesal Penal», *Diario La Ley - Sección Doctrina*, n.º 8217, 2013.

PICÓ I JUNOY, J., «La denuncia de la prueba ilícita en el proceso penal», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, pp. 317-326.

REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*, Madrid, Dykinson, 2000.

REBOLLO DELGADO, L., «Derecho al Honor, Derecho a la Intimidad y a la Propia Imagen. Inviolabilidad del domicilio, Secreto de las Comunicaciones y límites al uso de las nuevas tecnologías», en García-Atance y García de Mora, M. V., Gutiérrez Nogueroles, A., Navas Castillo, A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 177-203.

RICHARD GONZÁLEZ, M., «La cadena de custodia en el proceso penal español», *Diario La Ley - Sección Tribuna*, n.º 8187, 2013.

RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», *Diario La Ley - Sección Tribuna*, n.º 8808, 2016.

RICHARD GONZÁLEZ, M., «La Investigación y prueba de hechos y dispositivos electrónicos», *Revista General de Derecho Procesal*, 2017, pp. 1-55.

RICHARD GONZÁLEZ, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, Las Rozas (Madrid), Wolters Kluwer, 2017.

RÍOS PINTADO, J. F., «La Reforma Procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (Arts. 588 ter J y 588 octies de la Ley de Enjuiciamiento Criminal)», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Rios Pintado.pdf?idFile=9bb2604a-0ca5-432c-8124-f51611957c7b, el 10 de junio de 2020.

RIVES SEVA, A. P., «Reflexiones sobre el efecto reflejo de la prueba ilícita», *Noticias jurídicas*, 2010, Consultado en http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4605-reflexiones-sobre-el-efecto-reflejo-de-la-prueba-ilicita/, el 7 de febrero de 2020.

RIVES SEVA, A. P., «La prueba ilícita penal y su efecto reflejo», *Revista del Ministerio Fiscal*, n.º 3, 2017, pp. 8-42.

RODRÍGUEZ ÁLVAREZ, A., «Intervención de las comunicaciones telefónicas y telemáticas y smartphones», en Asencio Mellado, J.M. (dir.), Fernández López, M. (coord.), *Justicia Penal y nuevas formas de delincuencia*, Valencia, Tirant Lo Blanch, 2017, pp. 149-182.

RODRÍGUEZ FERNÁNDEZ, R., «Prueba preconstituida y prueba anticipada. Análisis jurisprudencial», *Diario La Ley - Sección Doctrina*, n.º 8487, 2015.

RODRÍGUEZ JIMÉNEZ, E. Y OTROS, «La cadena de custodia en los laboratorios oficiales de criminalística y ciencias forenses de España», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, pp. 138-163.

RODRÍGUEZ LAINZ, J. L., «En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución», *Diario La Ley*, n.º 8143, 2013, pp. 1-14.

RODRÍGUEZ LAINZ, J. L., «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley - Sección Doctrina*, n.º 8122, 2013.

RODRÍGUEZ LAINZ, J. L., «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», *Diario La Ley - Sección Doctrina*, n.º 8308, 2014.

RODRÍGUEZ LAINZ, J. L., «Sobre la Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales: La regulación de las medidas de investigación tecnológica», *Ponencias de formación continuada - Ministerio Fiscal*, 2015, Consultado en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia Sr Rodriguez Lainz.pdf?idFile=b9f4cc67-da93-4aa5-8eee-1507857092b8, el 18 de abril de 2019.

RODRÍGUEZ LAINZ, J. L., «Intervención judicial de comunicaciones vs. registro remoto sobre equipos informáticos: los puntos de fricción», *Diario La Ley*, n.º 8896, 2017, pp. 1-14.

RODRÍGUEZ LAINZ, J. L., «Sobre el concepto de alcance de la medida de injerencia tecnológica en la Ley Orgánica 13/2015», en Díaz Martínez, M., López-Barajas Perea, I. (dirs.), *La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas*, Valencia, Tirant Lo Blanch, 2019, pp. 17-48.

ROSENBERG, L., *Tratado de Derecho Procesal Civil. Tomo II*, Buenos Aires, Ediciones Jurídicas Europa-América, 1955.

RUBIO ALAMILLO, J., «La informática en la reforma de la Ley de Enjuiciamiento Criminal», *Diario La Ley - Sección Tribuna*, n.º 8662, 2015.

RUBIO ALAMILLO, J., «Conservación de la cadena de custodia de una evidencia informática», *Diario La Ley - Sección Doctrina*, n.º 8859, 2016.

RUBIO ALAMILLO, J., «Cadena de custodia y análisis forense de smartphones y otros dispositivos móviles en procesos judiciales», *Diario La Ley - Sección Ciberderecho*, n.º 22, 2018.

RUIZ RUIZ, R.; DE LA TORRE MARTÍNEZ, L., «Algunas aplicaciones e implicaciones del principio de proporcionalidad», *Revista Telemática de Filosofía del Derecho*, n.º 14, 2011, pp. 27-44.

RUZ GUTIÉRREZ, P. R., «La confección del dictamen pericial informático y su incorporación al proceso como medio de prueba objeto de valoración judicial», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009.

SALOM CLOTET, J., «Incidencias de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos», en Emaldi Cirion, A. y otros, *La protección de datos en la cooperación policial y judicial*, Cizur Menor (Navarra), Editorial Aranzadi, 2008, pp. 133-152.

SÁNCHEZ MELGAR, J., «La nueva regulación de las medidas de investigación tecnológica», *Práctica Penal - Cuaderno Jurídico*, n.º 82, 2016, Madrid, Editorial Jurídica Sepín.

SÁNCHEZ RUBIO, A., «Los registros remotos sobre equipos informáticos: La investigación del "hacker legal"», en Bueno de Mata, F. (dir. y coord.), *Fodertics 6.0 - Los nuevos retos del derecho ante la era digital*, Albolote (Granada), Editorial Comares, 2017, pp. 205-216.

SÁNCHEZ YLLERA, I., «Dudas razonables: la declaración de los coimputados», *Revista Xurídica Galega*, n.º 50, 2006, pp. 13-33.

SÁNCHEZ YLLERA, I., «La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas», *Formación a distancia-Consejo General del Poder Judicial*, n.º 3, 2016.

SANTOS MARTÍNEZ, A. M., «Examen de las disposiciones comunes de las medidas de investigación tecnológica», *Tirant Online, Documento TOL6.677.116*, 2018.

SANZ-GADEA GÓMEZ, J. B., «Los informes periciales informáticos en el ámbito de las nuevas tecnologías y prueba ilícita», *Tirant Online, Documento TOL5.638.931*, 2015.

SERRA DOMÍNGUEZ, M., «La instrucción de los procesos penal y civil: El sumario», en *Estudios procesales*, Barcelona, Editorial Ariel, 1969, pp. 716-738.

STEIN, F., *El conocimiento privado del juez* (traducido por DE LA OLIVA SANTOS, A.), Madrid, Editorial Ramón Areces, 1990.

SUBIJANA ZUNZUNEGUI, I. J., «Policía judicial y derecho a la intimidad en el seno de la investigación criminal», *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n.º 10, 1997, pp. 121-160.

TARUFFO, M., *La prueba de los hechos*, Madrid, Editorial Trotta, 2005.

TIEDEMANN, K. «El Derecho Procesal Penal», en Roxín, C. y otros, *Introducción al Derecho Penal y al Derecho Procesal Penal*, Barcelona, Ariel, 1989.

TOMÉ GARCÍA, J. A., «Fase decisoria (II). La prueba», en De la Oliva Santos, A. y otros, *Derecho Procesal Penal*, Madrid, Editorial Universitaria Ramón Areces, 2007, pp. 475-513.

TORRES DULCE LIFANTE, E., «Prólogo», en Figueroa Navarro, C. (dir.), *La cadena de custodia en el proceso penal*, Madrid, Edisofer, 2015, pp. 7-9.

URIARTE VALIENTE, L. M., «Nuevas técnicas de investigación restrictivas de derechos fundamentales», *Ponencias de formación continuada - Ministerio Fiscal*, 2015, Consultado en https://www.fiscal.es/fiscal/publico/ciudadano/documentos/ponencias_formacion_continuada, el 2 de marzo de 2019.

URIARTE VALIENTE, L. M., «25 cuestiones prácticas acerca de las medidas de investigación tecnológica en la LECrim», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Uriarte Valiente Luis Mª 02-11.pdf?idFile=2489f09c-09de-40d0-920d-d3cb65048a8f, e 11 de junio de 2020.

VALIÑO CES, A., «El agente encubierto informático y la ciberdelincuencia: el intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil», en Bueno de Mata, F. (coord.), *Fodertics 5.0*, Albolote (Granada), Editorial Comares, 2016, pp. 275-285.

VALIÑO CES, A., «La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015», en Fuentes Soriano, O. (coord.), *El Proceso Penal - Cuestiones fundamentales*, Valencia, Tirant Lo Blanch, 2017, pp. 377-388.

VEGAS TORRES, J., «La presunción de inocencia y el escenario de la prueba penal: STC 31/1981, de 28 de julio», *Persona y Derecho*, n.º 55, 2006, pp. 741-770.

VEGAS TORRES, J., «Las medidas de investigación tecnológica», en Cedeño Hernán, M. (coord.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2017, pp. 21-47.

VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales (1ª Parte)», *Revista de Jurisprudencia - El Derecho*, n.º 4, Febrero, 2009.

VELASCO NÚÑEZ, E., «Pericias informáticas: aspectos procesales penales (2ª Parte)», *Revista de Jurisprudencia - El Derecho*, n.º 4, Abril, 2009.

VELASCO NÚÑEZ, E., «Correo electrónico, SMS y virus troyanos: aspectos procesales penales», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 22, 2009.

VELASCO NÚÑEZ, E., *Delitos cometidos a través de internet. Cuestiones procesales*, Las Rozas (Madrid), La Ley, 2010.

VELASCO NÚÑEZ, E., «Investigación Tecnológica de Delitos: Disposiciones Comunes e Interceptaciones Telefónicas y Telemáticas», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Velasco Nuñez, Eloy.pdf?idFile=7b2fdf75-4a93-41bd-9adc-fe3042c95cc0, el 9 de junio de 2020.

VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Las Rozas (Madrid), Editorial Jurídica Sepín, 2016.

VELASCO NÚÑEZ, E., «Registros de dispositivos de almacenamiento masivo y registros remotos», *Cuadernos Digitales de Formación del Consejo General del Poder Judicial*, n.º 1, 2018.

VIDAL PRADO, C., «Derechos educativos. Derecho a la tutela judicial efectiva», en García-Atance y García de Mora, M. V., Gutierrez Nogueroles, A., Navas Castillo,

A., Rebollo Delgado, L., Vidal Prado, C., *Derecho constitucional (III). Derechos y libertades*, Madrid, Colex, 2003, pp. 205-225.

VIVES ANTÓN, T. S., «Doctrina constitucional y reforma del proceso penal», *Revista del Poder Judicial*, n.º especial II: Justicia Penal, 1988.

ZARAGOZA TEJADA, J. I., «La modificación operada por la Ley 13/2015. El agente encubierto informático», *Ponencias de formación continuada - Ministerio Fiscal*, 2016, Consultado en https://old.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia Zaragoza Tejada, Javier Ignacio.pdf?idFile=d16b7d76-2654-4b4e-abdf-b00f2540d57b, el 9 de junio de 2020.

ZARAGOZA TEJADA, J. I.; GUTIERREZ AZANZA, D. A., «La prueba ilícita. Una reflexión tras la STS del 23 de febrero del 2017», *Revista Aranzadi de Derecho y Proceso Penal - Parte Jurisprudencia*, n.º 47, 2017.

ZARAGOZA TEJADA, J. I.; GUTIÉRREZ AZANZA, D. A., «La exclusión de la prueba ilícita tras la sentencia del Tribunal Constitucional de 16 de julio de 2019 sobre la "Lista Falciani"», *Revista Aranzadi de Derecho y Proceso Penal - Parte Jurisprudencia*, n.º 56, 2019.

ZUBIRI DE SALINAS, F., «¿Qué es la sana crítica? La valoración judicial del dictamen experto», *Jueces para la Democracia. Información y Debate*, n.º 50, 2004, pp. 52-62.

JURISPRUDENCIA CITADA

NOTA ACLARATORIA

Las sentencias del Tribunal Europeo de Derechos Humanos, se han consultado en el buscador HUDOC puesto a disposición por el Tribunal europeo en la página web https://hudoc.echr.coe.int/spa#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}.

La jurisprudencia del Tribunal Constitucional, en el buscador de jurisprudencia constitucional creado por el propio Tribunal, en página web http://hj.tribunalconstitucional.es/, insertando el número de sentencia y la fecha.

La del Tribunal Supremo, en el Centro de Documentación Judicial (CENDOJ), en la página web http://www.poderjudicial.es/search/indexAN.jsp. Siendo todas las sentencias citadas de la Sala de lo Penal, una vez seleccionada esta, debe consignarse el número de la resolución y fecha de la misma, excepto en las resoluciones de 1995 y anteriores, en las que no figurando el número de resolución se ha facilitado el código del Repertorio Oficial de Jurisprudencia (ROJ), que identifica las resoluciones publicadas en el CENDOJ, con carácter único.

Las resoluciones de las Audiencias Provinciales, igualmente en el CENDOJ, consignando el número de resolución, sección y fecha.

La Sentencia citada del Tribunal Constitucional de Alemania, de 13 de septiembre de 1985, ha sido consultada en «Revista Española de Protección de Datos», n.º 5, 2008, pp. 317-395.

Las Sentencias del Tribunal Supremo de Estados Unidos de América, se han consultado en lengua inglesa en la base de datos de la web https://supreme.justia.com/.

I. Derechos fundamentales limitados por las diligencias de investigación

Tribunal de Justicia de la Unión Europea

Sentencia de 8 de abril de 2014 (Gran Sala) - Asuntos acumulados C-293/12 y C-594/12.

Sentencia de 2 octubre de 2018 (Gran Sala) – Asunto C-207/2016.

Tribunal Europeo de Derechos Humanos

STEDH de 26 de marzo de 1987, caso Leander c. Suecia.

STEDH de 7 de julio de 1989, caso Gaskin c. Reino Unido.

STEDH de 25 de febrero de 1997, caso Z c. Finlandia.

STEDH de 25 de septiembre de 2001, caso P.G. y J.H. c. Reino Unido.

STEDH de 28 de enero de 2003, caso Peck c. Reino Unido.

STEDH de 27 de septiembre de 2005, caso Petri Sallinen y otros c. Finlandia.

STEDH de 3 de abril de 2007, caso Copland c. Reino Unido.

STEDH de 14 de marzo de 2013, caso Bernh Larsen Holding AS y otros c. Noruega.

STEDH de 30 de mayo de 2017, caso Trabajo Rueda c. España.

Tribunal Constitucional

STC 25/1981, de 14 de julio.

STC 114/1984, de 29 de noviembre.

STC 254/1993, de 20 de julio.

STC 57/1994, de 28 de febrero.

STC 143/1994, de 9 de mayo.

STC 34/1996, de 11 de marzo.

STC 11/1998, de 13 de enero.

STC 134/1999, de 15 de julio.

STC 115/2000, de 5 de mayo.

STC 186/2000, de 10 de julio.

STC 292/2000, de 30 de noviembre.

STC 299/2000, de 11 de diciembre.

STC 70/2002, de 3 de abril.

STC 123/2002, de 20 de mayo.

ATC 15/2004, de 20 de enero.

STC 196/2004, de 15 de noviembre.

STC 104/2006, de 3 de abril.

STC 281/2006, de 9 de octubre.

STC 230/2007, de 5 de noviembre.

STC 159/2009, de 29 de junio.

STC 173/2011, de 7 de noviembre.

STC 96/2012, de 7 de mayo.

STC 142/2012, de 2 de julio.

STC 115/2013, de 9 de mayo.

STC 170/2013, de 7 de octubre.

STC 145/2014, de 22 de septiembre.

Tribunal Supremo – Sala de lo Penal

STS 246/1995, de 20 de febrero.

STS 276/1996, de 2 de abril.

STS 132/1997, de 8 de febrero.

STS 137/1999, de 8 de febrero.

STS 1295/1999, de 21 de septiembre.

STS 367/2001, de 22 de marzo.

STS 550/2001, de 3 de abril.

STS 156/2008, de 8 de abril.

STS 236/2008, de 9 de mayo.

STS 766/2008, de 27 de noviembre.

STS 940/2012, de 27 de noviembre.

STS 234/2016, de 17 de marzo.

STS 610/2016, de 7 de julio.

STS 714/2016, de 26 de septiembre.

ATS 353/2017, de 2 de febrero.

STS 720/2017, de 6 de noviembre.

Audiencias Provinciales

AAP 418/2011, Sección 6.ª de Madrid, de 8 de julio.

AAP 508/2011, Sección 4.ª Pontevedra, de 30 de noviembre.

AAP 909/2012, Sección 3.ª de Barcelona, de 28 de septiembre.

AAP 572/2013, Sección 30.ª Madrid, de 11 de julio.

SAP 13/2014, Sección 2.ª de Cáceres, de 16 de enero.

SAP 8/2016, Sección 1.ª de Guadalajara, de 4 de abril.

Tribunal Constitucional de Alemania

Sentencia de 15 de diciembre de 1983.

Tribunal Supremo de Estados Unidos de América

Sentencia de 13 de mayo de 1878, caso Jackson v. United States.

Sentencia de 18 de diciembre de 1967, caso Katz v. United States.

II. Sobre el entorno virtual

Tribunal Constitucional

STC 173/2011, de 7 de noviembre.

Tribunal Supremo – Sala de lo Penal

STS 342/2013, de 17 de abril.

STS 97/2015, de 24 de febrero.

STS 786/2015, de 4 de diciembre.

STS 204/2016, de 10 de marzo.

STS 426/2016, de 19 de mayo.

III. Presupuestos para la validez de las diligencias de investigación tecnológica

Tribunal Europeo de Derechos Humanos

STEDH de 7 de diciembre de 1976, caso Handyside c. Reino Unido.

STEDH de 22 de octubre de 1981, caso Dudgeon c. Reino Unido.

STEDH de 2 de agosto de 1984, caso Malone c. Reino Unido.

STEDH de 18 de febrero de 2003, caso Prado Bugallo c. España.

STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España.

STEDH de 24 de abril de 1990, caso Kruslin c. Francia.

STEDH de 24 de abril de 1990, caso Huvig c. Francia.

Decisión TEDH de 25 de septiembre de 2006, caso Abdulkadir Coban c. España.

Tribunal Constitucional

STC 22/1981, de 2 de julio.

STC 36/1986, de 12 de marzo.

STC 37/1989, de 15 de febrero.

STC 207/1996, de 16 de diciembre.

STC 49/1999, de 5 de abril.

STC 166/99, de 27 de septiembre.

STC 171/1999, de 27 de septiembre.

STC 14/2001, de 29 de enero.

STC 138/2001, de 18 de junio.

STC 202/2001, de 15 de octubre.

STC 82/2002, de 22 de abril.

STC 167/2002, de 18 de septiembre.

STC 25/2005, de 14 de febrero.

STC 261/2005, de 24 de octubre.

STC 220/2006, de 3 de julio.

STC 253/2006, de 11 de septiembre.

STC 26/2010, de 27 de abril.

STC 115/2013, de 9 de mayo.

Tribunal Supremo – Sala de lo Penal

STS de 16 de enero de 1992 - ROJ: STS 158/1992.

ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992.

STS de 1 de diciembre de 1995 - ROJ: 6105/1995.

STS 1335/2001, de 19 de julio.

STS 297/2006, de 6 de marzo.

STS 487/2007, de 29 de mayo.

STS 610/2007, de 28 de mayo.

STS 861/2007, de 24 de octubre.

STS 363/2008, de 23 de junio.

STS 712/2008, de 4 de noviembre.

STS 778/2008, de 18 de noviembre.

STS 9/2010, de 22 de enero.

STS 85/2013, de 4 de febrero.

STS 250/2014, de 14 de marzo.

STS 513/2014, de 24 de junio.

STS 746/2014, de 13 de noviembre.

STS 775/2014, de 20 de noviembre.

STS 168/2015, de 25 de marzo.

STS 454/2015, de 10 de julio.

STS 811/2015, de 9 de diciembre.

STS 387/2016, de 6 de mayo.

STS 991/2016, de 12 de enero de 2017.

IV. Datos de tráfico o asociados: Conservación y cesión

Tribunal Supremo – Sala de lo Penal

STS 249/2008, de 20 de mayo.

STS 739/2008, de 12 de noviembre.

STS 247/2010, de 18 de marzo.

STS 680/2010, de 14 de julio.

STS 7/2014, de 22 de enero.

STS 16/2014, de 30 de enero.

V. Autorización y control judicial de las medidas de investigación

Tribunal Europeo de Derechos Humanos

STEDH de 6 de septiembre de 1978, caso Klass c. Alemania.

STEDH de 20 de noviembre de 1989, Caso Kostovski v. Paises Bajos.

STEDH de 17 de diciembre de 1996, caso Saunders c. Reino Unido.

STEDH de 5 de noviembre de 2002, caso Alian c. Reino Unido.

Tribunal Constitucional

STC 26/1981, de 17 de julio.

STC 62/1982, de 15 de octubre.

STC 49/1996, de 26 de marzo.

STC 116/1998, de 2 de junio.

STC 166/1999, de 27 de septiembre.

STC 239/1999, de 20 de diciembre.

STC 136/2000, de 29 de mayo.

STC 167/2002, de 18 de septiembre.

STC 196/2002, de 28 de octubre.

STC 261/2005, de 24 de octubre.

STC 150/2006, de 22 de mayo.

STC 12/2007, de 15 de enero.

STC 219/2009, de 21 de diciembre.

STC 72/2010, de 18 de octubre.

STC 184/2003, de 23 de octubre.

STC 145/2014, de 22 de septiembre.

Tribunal Supremo – Sala de lo Penal

ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992.

STS 622/1998, de 11 de mayo.

STS 1240/1998, de 27 de noviembre.

STS 1018/1999, de 30 de septiembre.

STS 832/2001, de 14 de mayo.

STS 1060/2003, de 21 de julio.

STS 416/2005, de 31 de marzo.

STS 558/2005, de 27 de abril.

STS 864/2005, de 22 de junio.

STS 1487/2005, de 13 de diciembre.

STS 239/2008, de 30 de abril.

STS 598/2008, de 3 de octubre.

STS 704/2009, de 29 de septiembre.

STS 309/2010, 31 de marzo.

STS 1094/2010, de 10 diciembre.

STS 64/2011, de 8 de febrero.

STS 493/2011, 26 de mayo.

STS 248/2012, de 12 de abril.

STS 492/2012, de 14 de junio.

STS 636/2012, de 13 de julio.

STS 712/2012, de 26 de septiembre.

STS 722/2012, de 2 de octubre.

STS 435/2013, de 28 de mayo.

STS 661/2013, de 15 de julio.

STS 938/2013, de 10 de diciembre.

STS 32/2014, de 30 de enero.

STS 181/2014, de 11 de marzo.

STS 490/2014, de 17 de junio.

STS 454/2015, de 10 de julio.

STS 497/2016, de 9 de junio.

STS 993/2016, de 12 de enero de 2017.

STS 145/2017, de 8 de marzo.

STS 272/2017, de 18 de abril.

STS 1047/2007, de 17 de diciembre.

STS 180/2018, de 13 de abril.

STS 714/2018, de 16 de enero de 2019.

Audiencias Provinciales

SAP 311/2000, Sección 2.ª de Madrid, de 26 de abril.

VI. Duración de las medidas de investigación

Tribunal Europeo de Derechos Humanos

STEDH de 24 de abril de 1990, caso Kruslin c. Francia.

STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España.

Tribunal Constitucional

STS 774/2004, de 16 de junio.

STC 205/2005, de 18 de julio.

STC 148/2009, de 15 de junio.

STC 25/2011, de 14 de marzo.

Tribunal Supremo – Sala de lo Penal

STS de 9 de mayo de 1994 – ROJ: STS 3386/1994.

STS 960/2008, de 26 de diciembre.

STS 453/2013, de 29 de mayo.

VII. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales

Tribunal Constitucional

STC 49/1996, de 26 de marzo.

STC 41/1998, de 24 de febrero.

Tribunal Supremo – Sala de lo Penal

STS 835/1996, de 31 de octubre.

STS 545/1998, de 13 de enero de 1999.

STS 462/1999, de 22 de marzo.

STS 1673/2001, de 24 de septiembre.

STS 498/2003, de 24 de abril.

STS 981/2003, de 3 de julio.

STS 503/2008, de 17 de julio.

STS 187/2009, de 3 de marzo.

STS 326/2009, de 24 de marzo.

STS 777/2009, de 24 de junio.

STS 1313/2009, de 16 de diciembre.

STS 393/2012, de 29 de mayo.

STS 777/2012, 17 de octubre.

STS 279/2014, de 20 de febrero.

STS 428/2014, de 28 de mayo.

STS 469/2016, de 31 de mayo.

VIII. Destrucción de los datos obtenidos tras las diligencias de investigación una vez concluido el procedimiento.

Tribunal Europeo de Derechos Humanos

STEDH de 30 de julio de 1998, caso Valenzuela Contreras c. España.

STEDH de 24 de abril de 1990, caso Kruslin c. Francia.

Tribunal Constitucional

STC 49/1999, de 5 de abril.

Tribunal Supremo – Sala de lo Penal

STS 1200/2009, de 25 de noviembre.

STS 293/2011, de 14 de abril.

STS 565/2011, de 6 de junio.

STS 207/2012, de 12 de marzo.

STS 794/2012, de 11 de octubre.

STS 143/2013, de 28 de febrero.

IX. Extensión y alcance de la medida de registros informáticos

Tribunal Europeo de Derechos Humanos

STEDH de 3 de julio de 2012, caso Robathin c. Austria.

Tribunal Supremo – Sala de lo Penal

STS 926/2007, de 13 de noviembre.

STS 974/2012, de 5 diciembre.

STS 342/2013, de 17 de abril.

STS 83/2013, de 13 febrero.

STS 877/2014, de 22 diciembre.

STS 77/2019, de 12 de febrero.

X. Afectación de terceras personas

Tribunal Constitucional

STC 49/1999, de 5 de abril.

STC 299/2000, de 11 de diciembre.

STC 17/2001, de 19 de enero.

STC 136/2006, de 8 de mayo.

Tribunal Supremo – Sala de lo Penal

STS de 3 de junio de 1995 – ROJ: STS 6832/1995.

STS 1181/2000, de 3 de julio.

STS 934/2004, de 15 de julio.

STS 463/2005, de 13 de abril.

STS 918/2005, de 12 de julio.

STS 1154/2005, de 17 de octubre.

STS 474/2012, de 6 de junio.

STS 48/2013, de 23 de enero.

XI. Registro de dispositivos de almacenamiento masivo de información

Tribunal Europeo de Derechos Humanos

STEDH 22 de mayo de 2008, caso Iliya Stefanov c. Bulgaria.

Tribunal Constitucional

STC 173/2011, de 7 de noviembre.

Tribunal Supremo – Sala de lo Penal

STS 1086/2003, de 25 de julio.

STS 1231/2003, de 25 de septiembre.

STS 256/2008, de 14 de mayo.

STS 691/2009, de 5 de junio.

STS 342/2013, de 17 de abril.

STS 97/2015, de 24 de febrero.

STS 864/2015, de 10 de diciembre.

STS 287/2017, de 19 de abril.

Tribunal Supremo de Estados Unidos de América

Sentencia de 24 de junio de 2014, caso Riley v. California.

XII. Agente encubierto

Tribunal Supremo – Sala de lo Penal

STS 1140/2010, de 29 de diciembre.

STS 140/2019, de 13 de marzo.

XIII. Concepto y alcance constitucional de la prueba

Tribunal Constitucional

STC 30/1986, de 20 de febrero.

STC 86/2008, de 21 de julio.

STC 80/2011, de 6 de junio.

Tribunal Supremo – Sala de lo Penal

STS 371/2017, de 23 de mayo.

XIV. El documento electrónico

Tribunal Supremo – Sala de lo Penal

STS 28/2007, de 11 de enero.

STS 974/2012, de 5 de diciembre.

STS 672/2019, de 15 de enero de 2020.

XV. Preconstitución de la prueba

Tribunal Constitucional

STC 31/1981, de 28 de julio.

STC 145/1985, de 28 de octubre.

STC 80/1986, de 17 de junio.

STC 137/1988, de 7 de julio.

STC 217/1989, de 21 de diciembre.

STC 303/1993, de 25 de octubre.

STC 36/1995, de 6 de febrero.

STC 200/1996, de 3 de diciembre.

STC 40/1997, de 27 de febrero.

STC 153/1997, de 29 de septiembre.

STC 49/1998, de 2 de marzo.

STC 115/1998, de 1 de junio.

STC 97/1999, de 31 de mayo.

STC 141/2001, de 18 de junio.

Tribunal Supremo – Sala de lo Penal

STS de 10 de noviembre de 1972 - ROJ: STS 3584/1972.

STS de 20 de octubre de 1986 - ROJ: STS 9603/1986.

STS 1212/2003, de 9 de octubre.

STS 96/2009, de 10 de marzo.

STS 850/2009, de 28 de julio.

STS 374/2019, de 23 de julio.

XVI. Prueba ilícita

Tribunal Europeo de Derechos Humanos

STEDH de 12 de julio de 1988, caso caso Schenk v. Switzerland.

STEDH de 11 de julio de 2006, caso Jalloh c. Alemania.

STEDH de 17 de octubre de 2006, caso Göcmen c. Turquía.

STEDH de 28 de junio de 2007, caso Harutyunyan c. Armenia.

Tribunal Constitucional

ATC 289/1984, de 16 de mayo.

STC 114/1984, de 29 de noviembre.

STC 85/1994, de 14 de marzo.

STC 86/1995, de 6 de junio.

STC 49/1996, de 26 de marzo.

STC 54/1996, de 26 de marzo.

STC 81/1998, de 2 de abril.

STC 49/1999, de 5 de abril.

STC 94/1999, de 31 de mayo.

STC 161/1999, de 27 de septiembre.

STC 171/1999, de 27 de septiembre.

STC 238/1999, de 20 de diciembre.

STC 239/1999, de 20 de diciembre.

STC 8/2000, de 17 de enero.

STC 136/2000, de 29 de mayo.

STC 87/2001, de 2 de abril.

STC 138/2001, de 18 de junio.

STC 149/2001, de 27 de junio.

STC 28/2002, de 11 de febrero.

STC 167/2002, de 18 de septiembre.

STC 22/2003, de 10 de febrero.

STC 184/2003, de 23 de octubre.

STC 261/2005, de 24 de octubre.

STC 136/2006, de 8 de mayo.

STC 49/2007, de 12 de marzo.

STC 66/2009, de 9 de marzo.

STC 39/2017, de 24 de abril.

STC 97/2019, de 16 de julio.

Tribunal Supremo – Sala de lo Penal

ATS de 18 de junio de 1992 - ROJ: ATS 3773/1992.

STS de 23 de enero de 1995 – ROJ: STS 198/1995.

STS de 23 de enero de 1995 – ROJ: STS 6977/1995.

STS de 23 de enero de 1995 – ROJ: STS 11600/1995.

STS 448/1997, de 4 de marzo.

STS 472/1997, de 14 de abril.

STS 538/1997, de 23 de abril.

STS 974/1997, de 4 de julio.

STS 431/2001, de 19 de marzo.

STS 550/2001, de 3 de abril.

STS 1203/2002, de 18 de julio.

STS 498/2003, de 24 de abril.

STS 999/2004, de 19 de septiembre.

STS 1/2006, de 9 de enero.

STS 320/2011, de 22 de abril.

STS 811/2012, de 30 de octubre.

STS 69/2013, de 31 de enero.

STS 912/2013, de 4 de diciembre.

STS 963/2013, de 18 de diciembre.

STS 113/2014, de 17 de febrero.

STS 1273/2014, de 12 de marzo.

STS 115/2015, de 5 de marzo.

STS 511/2015, de 17 de julio.

STS 515/2015 de 21 de julio.

STS 116/2017, de 23 de febrero.

STS 2/2018, de 9 de enero.

STS 86/2018, de 19 de febrero.

STS 259/2018, de 30 de mayo.

STS 651/2018, de 14 de diciembre.

STS 423/2019, de 19 de septiembre.

Tribunal Supremo de Estados Unidos de América

Caso Boyd v. United States, de 1 de febrero de 1886.

Caso Weeks v. United States, de 24 de febrero de 1914.

Caso Nardone v. United States, de 11 de diciembre de 1939.

Caso Bynum v. United States, de 7 de enero de 1960.

Caso Wong Sun v. United States, de 14 de enero de 1963.

Caso Michigan v. DeFillippo, de 25 de junio de 1979.

Caso Nix v. Williams, de 11 de junio de 1984.

Caso Herring v. United States, de 14 de enero de 2009.

XVII. Cadena de custodia

Tribunal Constitucional

STC 170/2003, de 29 de septiembre.

Tribunal Supremo – Sala de lo Penal

STS 1599/1999, de 15 de noviembre.

STS 256/2008, de 14 de mayo.

STS 187/2009, de 3 de marzo.

STS 480/2009, de 22 de mayo.

STS 6/2010, de 27 de enero.

STS 629/2011, de 23 de junio.

STS 545/2012, de 22 de junio.

STS 1072/2012, de 11 de diciembre.

STS 339/2013, de 20 de marzo.

STS 342/2013, de 17 de abril.

STS 208/2014, de 10 de marzo.

STS 303/2014, de 4 de abril.

STS 587/2014, de 18 de julio.

STS 129/2015, de 4 de marzo.

STS 147/2015, de 17 de marzo.

STS 775/2015, de 3 de diciembre.

STS 157/2016, de 26 de febrero.

STS 277/2016, de 6 de abril.

STS 383/2016, de 5 de mayo.

ATS 425/2016, de 4 de febrero.

STS 676/2016, de 22 de julio.

STS 714/2016, de 26 de septiembre.

STS 990/2016, de 12 de enero de 2017.

STS 250/2017, de 5 de abril.

STS 726/2017, de 8 de noviembre.

STS 787/2017, de 5 de diciembre.

STS 513/2018, de 30 de octubre.

STS 541/2018, de 8 de noviembre.

STS 469/2019, de 14 de octubre.

STS 649/2019, de 20 de diciembre.

STS 167/2020, de 19 de mayo.

STS 298/2020, de 11 de junio.

Audiencias Provinciales

SAP 319/2008, Sección 3.ª de Almería, de 1 de octubre.

SAP 52/2009, Sección Bis de Las Palmas de Gran Canaria, de 29 de julio.

SAP 132/2009, Sección 2.ª de Barcelona, de 25 de febrero.

SAP 430/2009, Sección 3.ª de Almería, de 21 de diciembre.

SAP 82/2010, Sección 3.ª de Barcelona, de 25 de enero.

SAP 11/2011, Sección 29.ª de Madrid, de 27 de enero.

SAP 541/2012, Sección 8.ª de Barcelona, de 3 de septiembre.

SAP 1074/2012, Sección 17.ª de Madrid, de 27 de julio.

SAP 550/2014, Sección 6.ª de Madrid, de 28 de julio.

SAP 34/2015, Sección 9.ª de Málaga, de 29 de enero.

SAP 4/2017, Sección 2.ª de Toledo, de 1 de febrero.

SAP 90/2018, Sección 2.ª de Barcelona, de 8 de febrero.

XVIII. Medios de prueba

Tribunal Constitucional

STC 137/1988, de 7 de julio.

STC 24/1991, de 11 de febrero.

STC 51/1995, de 23 febrero.

STC 280/2005, de 7 noviembre.

STC 34/2006, de 13 de febrero.

STC 196/2006, de 20 de junio.

STC 230/2007, de 5 de noviembre.

STC 102/2008, de 28 de julio.

STC 56/2009, de 9 de marzo.

Tribunal Supremo – Sala de lo Penal

STS de 21 de junio de 1985 - ROJ: STS 1180/1985.

STS de 5 de mayo de 1995 - ROJ: STS 9679/1995.

STS 806/1999, de 10 de junio.

STS 328/2001, de 6 de marzo.

STS 807/2001, de 11 de mayo.

STS 1244/2001, de 25 de junio.

STS 1778/2001, de 3 de octubre.

STS 112/2002, de 17 de junio.

STS 1070/2003, de 22 de julio.

STS 1212/2003, de 9 de octubre.

STS 1302/2005, de 8 de noviembre.

STS 363/2008, de 23 de junio.

STS 480/2009, de 22 de mayo.

STS 276/2013, de 18 de febrero.

STS 492/2016, de 8 de junio.

STS 881/2016, de 23 de noviembre.

XIX. Impugnación de la prueba

Tribunal Supremo – Sala de lo Penal

STS de 29 de noviembre de 1975 - ROJ: STS 1650/1975.

STS 1336/1999, de 20 de septiembre.

STS 276/2013, de 18 de febrero.

STS 409/2014, de 21 de mayo.

STS 300/2015, de 19 de mayo.

STS 754/2015, de 27 de noviembre.

STS 358/2016, de 26 abril.

STS 375/2018, de 19 de julio.

STS 169/2019, de 28 de marzo.

STS 332/2019, de 27 de junio.

STS 499/2019, de 23 de octubre.

Audiencias Provinciales

SAP 291/2019, Sección 3.ª de Murcia, de 13 de septiembre.

SAP 99/2020, Sección 22.º de Barcelona, de 26 de febrero.

SAP 154/2020, Sección 5.ª de Valencia, de 24 de abril.

SAP 283/2020 Sección 2.ª de Cáceres, de 23 de marzo.

XX. Valoración de la prueba

Tribunal Constitucional

STC 31/1981, de 28 de julio.

STC 76/90, de 26 de abril.

STC 140/1985, de 21 de octubre.

STC 150/1987, de 1 de octubre.

STC 94/1990, de 23 de mayo.

STC 120/1994, de 25 de abril.

STC 70/2002, de 3 de abril.

STC 172/2005, de 20 de junio.

STC 136/2006, de 8 de mayo.

STC 125/2017, de 13 de noviembre.

Tribunal Supremo – Sala de lo Penal

STS de 12 de junio de 1991 - ROJ: STS 3181/1991.

STS de 9 de septiembre de 1992 - ROJ: STS 6715/1992.

STS 133/1998, de 9 de febrero.

STS 951/1999, de 14 de junio.

STS 1582/2002, de 30 de septiembre.

STS 120/2003, de 28 de febrero.

STS 23/2007, de 23 de enero.

STS 1103/2007, de 21 de diciembre.

STS 374/2009, de 28 de enero.

STS 1125/2011, de 2 de noviembre.

STS 364/2015, de 23 de junio.

STS 162/2019, de 26 de marzo.

STS 216/2019, de 24 de abril.

STS 555/2019, de 13 de noviembre.

STS 19/2020, de 28 de enero.

STS 149/2020, de 18 de mayo.

STS 466/2019, de 14 de octubre.

Audiencias Provinciales

SAP 695/1999, Sección 3.ª de Granada, de 10 de septiembre.

SAP 410/2016, Sección 1.ª de Pontevedra, de 8 de septiembre.