TESIS DOCTORAL

Aspectos procesales

de los delitos informáticos y tecnológicos

Autor:

Don Álvaro Gómez Rodríguez

Directora:

Doña María Belén Sánchez Domingo

Programa de Doctorado en Ciencias Jurídicas

Escuela Internacional de Doctorado

2021

ÍNDICE

ABREVIATURAS

LECrim.	Ley de Enjuiciamiento Criminal.
CP	Código Penal
LEC	Ley de Enjuiciamiento Civil.
L.O.	Ley Orgánica.
LOPJ	Ley Orgánica del Poder Judicial.
SAN	Sentencia de la Audiencia Nacional.
STS	Sentencia del Tribunal Supremo.
SAP	Sentencia de la Audiencia Provincial.
STC	Sentencia del Tribunal Constitucional.
TEDDHH	Tribunal Europeo de Derechos Humanos.
TC	Tribunal Constitucional.
TS	Tribunal Supremo.
TSJ	Tribunal Superior de Justicia.
AAP	Auto de la Audiencia Provincial.
ATC	Auto del Tribunal Constitucional.
ATS	Auto del Tribunal Supremo.
CE	Constitución Española.
CGPJ	Consejo General del Poder Judicial.
EOMF	Estatuto Orgánico del Ministerio Fiscal.

FGE	Fiscal General del Estado.
LORPM	Ley Orgánica reguladora de la Responsabilidad Penal del Menor.
R	Reglamento.
D	Directiva.
D. M.	Decisión Marco.

Introducción

La elección del tema de investigación, que se presenta como tesis doctrinal, se justifica, tanto desde el punto de vista penal como procesal. De esta manera, desde el enfoque penal, son diversas las cuestiones que se han planteado en la regulación de los delitos informáticos y tecnológicos, cuestiones que quedarán reflejadas en su desarrollo.

Por su parte, uno de los aspectos más problemáticos en nuestro ordenamiento jurídico penal son los ilícitos perpetrados a través de la red, pues no son reconducibles a una categoría única y homogénea, sino que están dispersos por todo el código penal, razón por la cual, la expresión "*delito informático y tecnológico*" no se utiliza en ninguno de los tipos previstos en la norma sustantiva penal.

De igual modo, el legislador penal español ha realizado numerosas modificaciones en el contenido de los tipos penales relacionados con la tecnología e informática, con el fin de luchar contra el fenómeno de la ciberdelincuencia. Sin embargo, surge principalmente como respuesta de los mandatos de la Unión Europea que obligan a transponer a nuestro ordenamiento jurídico penal los distintos instrumentos normativos, pretendiendo con ello, la aproximación de las legislaciones criminales entre los Estados miembros. Desde el punto de vista procesal penal, son numerosos los problemas que plantean los delitos informáticos o tecnológicos, como la transaccionalidad o las dificultades de detención, persecución o enjuiciamiento, de tal forma que, todas estas cuestiones se afrontan en el trabajo de investigación.

Asimismo, se ha abordado las diligencias de investigación que pueden ser acordadas durante la fase del proceso penal de instrucción. Así, resulta preceptivo añadir al desarrollo del presente trabajo la prueba pericial informática, en especial, la preservación, análisis y exhibición de las evidencias electrónicas en el proceso, todo ello, con la perspectiva a su utilización en el juicio oral. Por estas razones, nuestro objetivo ha sido, analizar las distintas soluciones aportadas por la doctrina y la jurisprudencia.

En definitiva, para llegar a todas estas conclusiones, no solo se han examinado las disposiciones legales nacionales, comunitarias e internacionales, sino que también, se han utilizado numerosas fuentes bibliográficas y jurisprudenciales que, nos harán

comprender los problemas existentes en el manejo de las tecnologías de la información y de la comunicación.

De este modo, el presente trabajo tiene la siguiente estructura, en el cual, primeramente se ha desarrollado un capítulo preliminar dedicado a los antecedentes históricos, que aborda, por un lado, la regulación de los delitos informáticos y tecnológicos en los distintos códigos penales, y por el otro, la regulación de las distintas normas procesales, de tal forma que, se realizará un análisis detallado de las modificaciones que se han introducido, todo ello, para comprender el contexto histórico que nos rodea sobre la ciberdelincuencia. De la misma manera, se ha realizado, especial mención al derecho convencional y el derecho comunitario, toda vez que, se trata del gérmen de las reformas que se han ido produciendo en los últimos años.

Seguidamente, se ha examinado un capítulo introductorio dedicado a la parte sustantiva, esto es, la clasificación de los distintos delitos informáticos y tecnológicos regulados en nuestra norma punitiva, con arreglo a las reformas del Código Penal, implementadas mediante la Ley Orgánica 1/2015 y la L.O. 2/2015, ambas de 30 de marzo y la Ley Orgánica 1/2019, de 20 de febrero.

Posteriormente, se ha realizado un capítulo que aborda los aspectos procesales, en especial, todo lo relacionado con las medidas de investigación restrictivas del derecho fundamental del art. 18 CE, reguladas en la Ley de Enjuiciamiento Criminal tras la reforma implementada con arreglo a la *Ley Orgánica 13/2015, de 5 de octubre*, en concreto, la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter LECrim.), la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (art. 588 quater LECrim.), la captación de imágenes en espacios y lugares públicos (art. 588.1 quinquies a. LECrim.), la intervención de las comunicaciones en el ámbito penitenciario o en calabozos de las dependencias policiales: mención especial a las interceptaciones entre el abogado o procurador y su cliente (art. 118.4 y 520.7 LECrim.), la utilización de dispositivos o medios técnicos de geolocalización (art. 588 quinquies b. LECrim.), la entrada o registro domiciliario (art. 545 LECrim. y sig.), el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.), los registros remotos sobre equipos informáticos (art. 588 septies LECrim.), el agente encubierto (art. 282 bis LECrim.), así como, la

problemática de la utilización de otras medidas restrictivas de derechos fundamentales no contempladas en la ley, especialmente el tratamiento de los drones.

Además, dada la complejidad de los problemas que plantean los delitos informáticos y tecnológicos en relación con la prueba, ha sido preciso abordar la prueba pericial "informática".

Finalmente, se cierra el capítulo exponiendo los problemas sobre la jurisdicción y competencia de los juzgados en la persecución y enjuiciamiento de los delitos perpetrados a través de las nuevas tecnologías y la informática.

Por último, el trabajo ha finalizado con las conclusiones, que irán en correspondencia con el desarrollo mencionado anteriormente, de tal forma que, la presente obra pretende ofrecer a la comunidad jurídica una visión pormenorizada de los aspectos sustantivos y procesales de los delitos con un contenido informático y tecnológico.

Capítulo preliminar: Antecedentes históricos

A) Contexto histórico de los delitos informáticos y tecnológicos

Con carácter previo, hemos decidido realizar, un contexto histórico que comprende, por un lado, la evolución de los distintos delitos con incidencia en el ámbito tecnológico e informático, y por el otro, el estudio de las normas que han regulado el proceso penal moderno en España, en especial, abordaremos las distintas reformas implementadas por el legislador. Debido a lo cual, siguiendo la estructura del presente trabajo, comenzaremos analizando la parte sustantiva, esto es, los delitos relacionados con el presente trabajo, para terminar con el examen del proceso penal histórico español.

I. Códigos penales del Franquismo

1) El código penal de 1944

El 17 y 18 de julio de 1936 se produjo el Alzamiento del Movimiento Nacional, lo cual, supuso el comienzo de la guerra civil española hasta el 1 de abril de 1939, implantándose el régimen autoritario del franquismo, prolongándose hasta el 20 de noviembre de 1975.

Durante los primeros años se aplicó el código penal republicano de 1932, pero reformado con normas penales especiales políticamente afines al régimen, hasta que finalmente, mediante Decreto de 23 de diciembre de 1944 se aprobaría el código penal[1], que entraría en vigor el 3 de febrero de 1945, inspirado en las ideas políticas del franquismo.

Sin embargo, el nuevo texto punitivo se trataba en puridad de una reforma parcial del código penal de 1848, pues la estructura era la tradicional del sistema jurídico penal español, al distribuirse en un Título Primero referente a las "*Disposiciones Generales sobre los Delitos y Faltas, las Personas Responsables y las Penas*", el Segundo sobre los "*Delitos y sus Penas*", y el último, "*De las Faltas y sus Penas*", si bien, estaba compuesto por un mayor número de artículos llegando hasta 604.

[1] Hemos estudiado las disposiciones del Código Penal de 1944 mediante la obra de SANCHEZ-TEJERINA, I. *Código penal anotado*. Instituto Editorial Reus. Madrid. 1948.

Debido a las ideas autoritarias franquistas, el código penal de 1944, contenía delitos tendentes a restringir el derecho a la libertad de expresión u opinión, a modo de ejemplo podemos mencionar, la agravante cuando el hecho delictivo fuera cometido con publicidad, como la radio o la imprenta (art. 10 CP 1944)[2]. Además, en los delitos cometidos mediante imprenta siempre se consideraba a alguien responsable de la publicación[3], puesto que, en primer lugar, era responsable el autor del texto o escrito publicado, si bien, cuando no fuera conocido, se presumía como autor los directores de la publicación, en su defecto los editores, y por último los impresores (art. 13 y 15 CP 1944)[4].

[2] Art. 10 CP 1944: *Agravantes: 4º Realizar el delito por medio de la imprenta, radiodifusión u otro medio que facilite la publicidad.*

[3] El texto penal contenía innumerables figuras delictivas que estaban inspiradas en las ideas franquistas. De esta manera, la libertad de expresión y opinión, estaba restringido su ejercicio por normas administrativas (mediante la Ley de prensa de 22 de abril de 1938 y posteriormente la Ley 14/1966, de 18 de marzo, de prensa e imprenta, que suprimió la censura previa) y penales. De hecho, se castigaba incluso a los autores, directores, editores o impresores que realizaran impresos clandestinos, entendiéndose como los que produjeran publicaciones que no estuvieran sometidos a los controles previos establecidos en la ley. De igual modo, se sancionaba, fundar un periódico que no cumpliera con los requisitos legales afines al régimen (art. 165 CP). Además, se podía decomisar la imprenta cuando se cometiera alguno de los hechos delictivos mencionados anteriormente (art. 213 CP). También, se castigaba la propaganda ilegal, cuando su objeto fuera divulgar cualquier idea contraria al franquismo (art. 251 CP sigs.).

[4] Art. 13 CP 1944: *Se exceptúan de lo dispuesto en el artículo anterior los delitos y faltas que se cometan por medio de la imprenta, el grabado u otra forma mecánica de reproducción, radiodifusión u otro procedimiento que facilite la publicidad. De dichas infracciones responderán criminalmente sólo los autores;* Art. 15 CP 1944: *Sin embargo, de lo dispuesto en el artículo anterior, solamente se reputarán autores de las infracciones mencionadas en el art. 13 los que realmente lo hayan sido del texto, escrito o estampa publicados. Si aquellos no fueren conocidos o no estuvieron domiciliados en España, o estuvieron exentos de responsabilidad criminal, con arreglo al art. 8. º de este Código, se reputarán autores los directores de la publicación que tampoco se hallen en ninguno de los tres casos mencionados. En defecto de éstos, se reputarán autores los editores, también conocidos y domiciliados en España y no exentos de responsabilidad criminal, según el artículo anteriormente Cit, y, en defecto de éstos, los impresores. Se entiende por impresores, para el efecto de este artículo, los directores o jefes del establecimiento en que se haya impreso, grabado o publicado por cualquier otro medio el escrito o estampa criminal.*

De la misma manera, la libertad de prensa era prácticamente inexistente, puesto que no se permitía fundar un periódico o cualquier otra publicación sin pasar por el control de la autoridad competente (art. 165 CP 1944), castigándose pues, a los autores, directores, editores o impresores no sometidos a la censura. Además, se castigaba cualquier tipo de propaganda, publicidad o publicación que fuera contraria al régimen franquista (art. 251 CP 1944), incluso, como pena accesoria, se podía decomisar la imprenta (art. 213 CP 1944), así como los efectos provenientes del mismo.

De la misma forma, se castigaba como falta las publicaciones que ofendieran *a la moral, a las buenas costumbres o a la decencia pública* (art. 466.4º CP 1944), así como, las divulgaciones de hechos relativos a la vida privada que ocasionaran perjuicios en la familia (art. 466.2º CP 1944)[5].

Por su parte, en los delitos contra el honor, su regulación era similar a la de los textos punitivos precedentes (art. 453 sigs. CP 1944). Asimismo, se mantenía la agravante de calumnia o injuria cometida por escrito o mediante algún medio de publicidad, como los papeles impresos, litografiados o grabados, por carteles o pasquines fijados en sitios públicos o por papeles manuscritos (Art. 463 CP 1944).

En lo relativo a la protección de la intimidad, el código penal contenía el delito de descubrimiento y revelación de secretos, el cual, tenía una redacción prácticamente idéntica a sus predecesores (art. 497 CP sigs. CP 1944), puesto que, se sancionaba el apoderamiento de papeles o cartas, pero, además, se diferenciaba a los efectos punitivos, del secreto divulgado, de aquel otro que fuera para uso privado. De la misma forma, como delito especial impropio, se sancionaba las violaciones de secretos cometidos por funcionarios públicos a consecuencia del ejercicio de su cargo u oficio (art. 367 CP 1944).

[5] Art. 566 CP 1944: *Incurrirán en la pena de multa superior a 50 pesetas e inferior a 1.000:… 2.º Los que por medio de la imprenta, litografía u otro medio de publicación, divulgaran maliciosamente hechos relativos a la vida privada que, sin ser injuriosos, puedan producir perjuicios, o graves disgustos, en la familia a que la noticia se refiera… 4.º Los que en igual forma provocaran a la desobediencia de las leyes y de las autoridades constituidas, hicieren la apología de acciones calificadas por la ley de delito, u ofendieron a la moral, a las buenas costumbres o a la decencia pública.*

Por otro lado, dentro de los delitos patrimoniales, se encontraba la estafa o defraudaciones, el cual, tenía una redacción más depurada técnicamente respecto a sus versiones anteriores, así como se agravaron las penas en comparación con el código penal republicano de 1932 (art. 528 CP 1944). De esta manera, se restringió el casuismo de la estafa, puesto que se redujeron los supuestos considerados hechos delictivos (art. 529 CP 1944), si bien, el último precepto castigaba cualquier engaño no contemplado en los supuestos aludidos con anterioridad (art. 534 CP 1944). Se trataba de una excepción a la norma, sin embargo, debido a su generalidad, se aplicaba con mayor frecuencia. Cabe advertir que, el código penal de 1944, no contenía un capítulo dedicado a la protección de la propiedad intelectual, sin embargo, se sancionaba las transgresiones a dicha propiedad como una clase de defraudación (art. 533 CP 1944).

Por último, se continuaba sancionado como delito de daños los cometidos en propiedad ajena, que no fueran considerados como incendio (art. 557 CP 1944), destacando a los efectos del presente trabajo, los menoscabos producidos en un archivo o registro cuando su valor excediera de 250 pesetas (arts. 558.5º y 559 CP 1944).

2) Código Penal, Texto revisado de 1963

La Ley 79/1961, de 23 de diciembre[6] establecía las bases para la reforma del código penal franquista, de tal forma que, fue desarrollada mediante dos Decretos, de 24 de enero y de 28 de marzo de 1963[7]. Posteriormente, de acuerdo con la Ley 3/1967 de 8 de abril[8], motivada a raíz de la Ley de Prensa e Imprenta de 18 de marzo 1966[9], fue nuevamente reformado el código penal, en el sentido de otorgar una cierta liberación al

[6] «BOE» Núm. 309, de 27 de diciembre de 1961.

[7] Sobre las modificaciones implementadas al código penal franquista de 1944, véase, CUELLO CALÓN, E. *Código Penal. Texto revisado 1963 y leyes penales especiales*. Editorial Bosch. Barcelona. 1963.

[8] «BOE» Núm. 86, de 11 de abril de 1967.

[9] «BOE» Núm. 67, de 19 de marzo de 1966.

suprimir la censura previa[10], lo cual, supuso una modificación parcial de los delitos de prensa (arts. 165 sigs. CP 1963).

Una de las novedades más importantes, fue crear dentro de los delitos patrimoniales, una sección autónoma dedicada a las infracciones del derecho de autor y de la propiedad industrial (art. 534 CP 1963), de modo que, a partir de la reforma no se castigaban estas infracciones como una variante de las defraudaciones o estafas, sino como una figura delictiva independiente. Además, el tipo penal, tenía la consideración de "ley penal en blanco", pues precisaba de ser completada con los preceptos contenidos en la Ley de Propiedad Intelectual de 10 de enero de 1879[11], y por la Ley de Propiedad Industrial de 16 de mayo de 1902[12] (con modificaciones posteriores).

En cuanto a los delitos relacionados con el presente trabajo, como la estafa (arts. 528 y sig. CP 1963), contra la intimidad (art. 497 sigs. CP 1963) y el honor (art. 453 sigs. CP 1963), no sufrieron modificaciones en su redacción, si bien, se adecuaron las cuantías de las multas. En lo concerniente a los daños tampoco tuvo cambios significativos, sin embargo, debido a sucesos acaecidos en la época, se incorporaron a los menoscabos ya existentes, los producidos en un archivo o registro, otros lugares o cosas (art. 558.5º CP 1963).

3) Código Penal, Texto refundido de 1973 y sus reformas democráticas

Por la necesidad de acomodar la legislación penal a la realidad social de la época, se aprobó la Ley 44/1971, de 15 de noviembre, *sobre la reforma del Código Penal*[13], en la

[10] DAVARA TORREGO, F. J. "Los periódicos españoles en el tardo franquismo consecuencias de la nueva ley de prensa*".* Comunicación y Hombre: Revista Interdisciplinar de Ciencias de la Comunicación y Humanidades. Núm. 1. 2005. Págs. 131-148, así entiende que, el ministro de Información y Turismo, Manuel Fraga Iribarne, y cito textualmente: "propone realizar una reforma en el sector de la prensa, como muestra de la relativa liberalización del nuevo Gobierno, trayendo consigo unos nuevos aires al Ministerio de Información al abordar con decisión la necesidad de enterrar definitivamente la caduca y anacrónica Ley de Prensa de 1938 y de sustituirla por otra de cariz más liberal".

[11] «Gaceta de Madrid» Núm. 12, de 12 de enero de 1879. Págs. 107 a 108.

[12] «Gaceta de Madrid» Núm. 138, de 18 de mayo de 1902. Págs. 787 a 788.

[13] «BOE» Núm. 274, de 16 de noviembre de 1971. Págs. 18415 a 18419.

cual, en su disposición final, obligaba al Gobierno a publicar un texto refundido del código penal, siendo éste, con arreglo al Decreto 3096/1973, de 14 de septiembre[14].

Sin embargo, con el fallecimiento de Francisco Franco el 20 de noviembre de 1975, y con la aprobación de la Ley 1/1977, de 4 de enero, *para la Reforma Política*[15], sometida a referéndum el 15 de diciembre de 1976, resultaba imprescindible adaptar la norma penal al nuevo proceso democrático que se venía produciendo en nuestro país.

Por este motivo, el legislador fue encadenando una serie de reformas tendentes a adecuar la norma punitiva a los principios democráticos, de tal forma que, la primera reforma destacable en lo relativo a la libertad de expresión fue mediante el Real Decreto-ley 24/1977, de 1 de abril[16], el cual, vino a derogar el delito de prensa (art. 165 bis b) CP 1973)[17], así como se introdujeron requisitos de procedibilidad y otras peculiaridades en los delitos de calumnia e injuria cometidos con publicidad (arts. 453 sigs. CP 1973). Posteriormente, en el mismo sentido se modificaron los delitos relativos a la libertad de expresión, reunión y asociación (art. 165 sigs. CP 1973), mediante la Ley Orgánica 4/1980, de 21 de mayo[18], así como se suprimieron las faltas de imprenta

[14] «BOE» Núm. 297, de 12 de diciembre de 1973, en relación con RODRIGUEZ DEVESA, J. M. *Derecho Penal español.* Artes Gráficas Carasa. Madrid. 1980.

[15] «BOE» Núm. 4, de 5 de enero de 1977.

[16] «BOE» Núm. 87, de 12 de abril de 1977.

[17] Artículo 165 bis b) CP 1973 (redacción dada en virtud de Ley 3/1967, de 8 de abril): *Serán castigados con las penas de arresto mayor y multa de cinco mil a cincuenta mil pesetas los que infringieren por medio de impresos las limitaciones impuestas por las leyes a la libertad de expresión y al derecho de difusión de información mediante la publicación de noticias falsas o informaciones peligrosas para la moral o las buenas costumbres; contrarias a las exigencias de la defensa nacional, de la seguridad del Estado y del mantenimiento del orden público interior y de la paz exterior, o que ataquen a los Principios del Movimiento Nacional o a las Leyes Fundamentales, falten al respeto debido a las instituciones y a las personas en la crítica de la acción política o administrativa, o atenten contra la independencia de los Tribunales.*

[18] «BOE» Núm. 142, de 13 de junio de 1980.

(art. 566 CP 1973), por medio de la Ley Orgánica 2/1984, de 26 de marzo[19] y la Ley Orgánica 5/1988, de 9 de junio[20].

La reforma más importante del código penal de 1973 se realizó mediante la Ley Orgánica 8/1983, de 25 de junio, de *Reforma Urgente y Parcial del Código Penal*[21], en la cual, la propia exposición de motivos aludía que, el objeto de la ley era adaptar el código penal a las exigencias del Estado de Derecho, pero sin realizar un nuevo código punitivo, puesto que ello requeriría un período de reflexión más profundo, si bien, supuso un parche a la espera de elaborar una nueva norma punitiva.

Además, la L.O. 8/1983 modificó notablemente el delito de estafa (art. 528 CP 1973), eliminado el casuismo imperante hasta entonces y procediendo a mejorar técnicamente su redacción, al incluir la regulación de los elementos del tipo de la estafa, en concreto el ánimo de lucro, engaño bastante y error producido a consecuencia de dicha conducta engañosa[22], así como, se introdujo el delito cualificado, estableciendo una lista de supuestos de hecho que agravaban las penas (art. 529 CP 1973).

Posteriormente, en relación con el derecho a la intimidad, mediante la Ley Orgánica 7/1984, de 15 de octubre, *sobre tipificación penal de la colocación ilegal de escuchas telefónicas*[23] (modificada por la Ley Orgánica 18/1994, de 23 de diciembre[24]), se introdujo el delito de interceptación ilícita de las comunicaciones telefónicas, realizada por particular (art. 497 bis CP 1973), así como por funcionario público (art. 192 bis CP 1973).

---

[19] «BOE» Núm. 74, de 27 de marzo de 1984.

[20] «BOE» Núm. 140, de 11 de junio de 1988.

[21] «BOE» Núm. 152, de 27 de junio de 1983.

[22] Art. 528 CP 1973 (redacción dada LO 8/1983): *los que con ánimo de lucro utilizan engaño bastante para producir error en otro, induciéndole a realizar un acto de disposición en perjuicio de sí mismo o de tercero*.

[23] «BOE» Núm. 255, de 24 de octubre de 1984.

[24] «BOE» Núm. 307, de 24 de diciembre de 1994.

Por otra parte, con arreglo a la Ley Orgánica 6/1987, de 11 de noviembre[25], como corolario de la Ley 22/1987 de Propiedad Intelectual[26] de la misma fecha, se modificaron profusamente los delitos contra los derechos de autor y la propiedad industrial (arts. 534 y sigs. CP 1973), de tal forma que, se incorporaron los elementos descriptivos del tipo[27], debido a que, con anterioridad a la reforma[28], el delito contenía la pena, pero no incluía los elementos del supuesto de hecho, pues había que acudir a las normas especiales de derecho privado (Ley de 10 de enero de 1879 *de propiedad intelectual*; Ley de 24 de junio de 1941 *por la que se instituye la Sociedad General de Autores de España*; Real decreto-ley de 26 de Julio de 1929 *sobre Propiedad Industrial),* para conformar el delito.

No obstante, se advertiría pronto que, las reformas realizadas no colmaban las expectativas, por lo que se aprobaron varias leyes que tenían por objeto, modificar el código penal, si bien, se trataban de meros parches que emborronaban la norma punitiva, pues dejaban sin contenido determinados preceptos y se añadieron otros mediante la fórmula del *bis, ter, quater, quinquies, sexies,* etc. De este modo, las reformas más importantes fueron las introducidas por la Ley Orgánica 3/1989, de 21 de junio[29], que modificaría las faltas y las actualizaciones de las cuantías económicas, la

[25] «BOE» Núm. 275, de 17 de noviembre de 1987.

[26] «BOE» Núm. 275, de 17 de noviembre de 1987.

[27] Art. 534 bis, a). CP 1973 (regulación posterior a la reforma): *Será castigado con la pena de multa de 30.000 a 600.000 pesetas quien intencionadamente reprodujere, plagiare, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística o científica o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. La misma pena se impondrá a quien intencionadamente importare, exportare o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.*

[28] Art. 534 CP 1973 (regulación anterior a la reforma): *El que infringiere intencionadamente los derechos de autor será castigado con las penas de arresto mayor y multa de 10.000 a 100.000 pesetas, independientemente de las sanciones determinadas en las leyes especiales. La misma pena se aplicará a los que de igual manera infringieren los derechos de propiedad industrial.*

[29] «BOE» Núm. 148, de 22 de junio de 1989.

Ley Orgánica 9/1991, de 22 de marzo[30], que vino a mejorar técnicamente el delito de revelación de secretos cometido por funcionario público en el ejercicio de su cargo u oficio (arts. 367 y 368 CP 1973), así como, la Ley Orgánica 4/1995, de 11 de mayo[31], que en cumplimiento de las obligaciones internacionales vino a crear los delitos de apología al genocidio, si bien, fue aprobada unos meses antes de que saliera a la luz el código penal vigente de 1995[32].

II. Código Penal de 1995 (Ley Orgánica 10/1995, de 23 de noviembre)

La tradición histórica jurídico penal española demuestra que toda norma fundamental del Estado trae consigo la aprobación de un código penal que recoge las ideas conservadoras o progresistas de cada periodo. Aunque fuera de forma tardía, la Constitución de 1978[33] ha traído un nuevo texto punitivo inspirado con las ideas de la democracia.

Tras la elaboración de varios anteproyectos frustrados, el Pleno del Congreso de los Diputados aprobaría el 8 de noviembre de 1995 un nuevo texto penal, que supuso la publicación de la Ley Orgánica 10/1995, de 23 de noviembre[34], que finalmente entró en vigor, después de seis meses de *vacatio legis* (disposición final séptima), el 24 de mayo de 1996. De esta manera, la propia Exposición de Motivos del código penal de 1995 afirma que, el nuevo texto punitivo está inspirado en el régimen democrático, pues resulta imprescindible adaptar la legislación penal a los valores constitucionales. La novedad más importante es que los delitos aparecen clasificados en función del bien

[30] «BOE» Núm. 74, de 27 de marzo de 1991.

[31] «BOE» Núm. 113, de 12 de mayo de 1995.

[32] Acerca de las reformas implementadas desde el código penal de 1973, hasta el código penal de 1995, véase, SERRANO BUTRAGUEÑO, I. "La transición del antiguo al nuevo Código Penal (una visión absolutamente práctica)*".* La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 2. 1996. Págs. 1466-1472.

[33] «BOE» Núm. 311, de 29 de diciembre de 1978.

[34] «BOE» Núm. 281, de 24 de noviembre de 1995.

jurídico protegido[35], es decir, el derecho penal tutela los intereses más importantes valorados socialmente por su vinculación con la persona y su desarrollo (por ejemplo, la vida, salud pública, integridad física o moral, libertad, indemnidad, patrimonio, etc.).

Por su parte, el texto original del nuevo código penal estaba compuesto por 639 artículos, tres disposiciones adicionales, doce disposiciones transitorias, una disposición derogatoria y siete disposiciones finales, distribuidos en un título preliminar denominado *"De las garantías penales y de la aplicación de la ley penal"*, un libro primero con el título de las "*Disposiciones generales sobre los delitos y las faltas, las personas responsables, las penas, medidas de seguridad y demás consecuencias de la infracción penal*", otro bajo la rúbrica de los "*Delitos y sus penas*" y finalmente, bajo el rótulo de las "*Faltas y sus penas*", sin embargo, éste último ha sido derogado por la Ley Orgánica 1/2015, de 30 de marzo[36].

Desde la aprobación del código penal de 1995, se han realizado numerosas modificaciones[37], muchas encaminadas a endurecer las penas, más marcadas por un tinte político, que por tener alguna justificación para la ciencia jurídico penal[38], y otras, por obligaciones internacionales asumidas por España. Seguidamente se examinarán las

[35] Señala, DE LA CUESTA ARZAMENDI, J. L. "Introducción al nuevo Código penal español líneas directrices y contenido fundamental*".* Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. Extra 10. 1997. Pág. 30, en relación al nuevo código penal que "se encuentran confrontadas las exigencias procedentes de la tutela penal de los bienes jurídicos dignos, necesitados y susceptibles de protección penal y el respeto del principio de necesidad, con sus corolarios de subsidiaridad e intervención mínima". De igual modo, ASUA BATARRITA, A. *Jornadas sobre el nuevo Código penal de 1995, celebradas del 19 al 21 de noviembre de 1996.* Servicio de Publicaciones de la Universidad del País Vasco. 1998, viene a exponer la clasificación del Código Penal de 1995 en bienes jurídicos protegidos.

[36] «BOE» Núm. 77, de 31 de marzo de 2015. Págs. 27061 a 27176.

[37] BARQUÍN SANZ, J. "El Código Penal de 1995, cinco años después*"*. Revista Electrónica de Ciencia Penal y Criminología. Núm. 2. 2000; GONZÁLEZ RUS, J. J. *El Código Penal de 1995, cinco años después. Jornadas de Derecho Penal.* Editorial Servicio de Publicaciones de la Universidad de Córdoba. 2002.

[38] Acerca del endurecimiento de las penas, nos remitimos a CORCOY BIDASOLO, M. Y OTROS. *Nuevas tendencias en política criminal: una auditoría al Código Penal español de 1995*. Editorial Reus. Madrid. 2006, el cual, mantiene que, tienen un marcado tinte político.

reformas más relevantes del código penal de 1995, relacionadas con los delitos objeto de nuestro estudio.

Debido a una recomendación dada por el Defensor del Pueblo al Ministerio de Justicia en fecha 28 de noviembre de 1997, y como consecuencia de las directrices provenientes de la Unión Europea (Resolución 1099 (1996) de 25 de septiembre, relativa a la explotación sexual de los niños), se aprobó la Ley Orgánica 11/1999, de 30 de abril, en la cual, se reformaron los delitos contra la libertad e indemnidad sexual, en especial, se mejoró técnicamente el delito de utilización de menores para la elaboración de pornografía infantil, se creó los cimientos del delito de producción, transmisión, y exhibición de material pornográfico de menores, así como de la posesión de dicho material para la realización de dichas conductas (art. 189 CP 1995)[39].

Posteriormente, el código penal de 1995 sufrió una reforma importante con arreglo a la Ley Orgánica 15/2003, de 25 de noviembre[40], especialmente en los delitos de pornografía infantil. Se endurecieron las penas[41], incrementaron los supuestos agravados (art. 189.3 CP 1995), se introdujo el delito de pornografía infantil virtual o simulada, es decir, supuestos que no aparecen menores reales, sino imágenes ficticias o incluso mayores de edad que simulan ser menores de edad (art. 189.7 CP 1995)[42]. Además, se creó el tipo de mera tenencia de material pornográfico de menores o incapaces, independientemente del uso que posteriormente se pueda hacer del mismo

[39] POLAINO-ORTS, M. "Los delitos sexuales a la luz del Código penal de 1995 (especial referencia a la Ley Orgánica 11/1999, de 30 de abril)". Cuadernos de Política Criminal. Núm. 67. 1999. Págs. 143-216.

[40] «BOE» Núm. 283 de 26 de noviembre de 2003.

[41] Aborda, DÍEZ RIPOLLÉS, J. L. "La evolución del sistema de penas en España: 1975-2003". Revista Electrónica de Ciencia Penal y Criminología. Núm. 8. 2006. Págs. 13 a 21, la evolución de las penas en el sistema punitivo español, de tal forma que, se puede apreciar la tendencia a endurecer las penas.

[42] "Circular 1/2005, sobre aplicación de la reforma del Código Penal operada por Ley Orgánica 15/2003, de 25 de noviembre (segunda parte)". Revista de Derecho Penal. Núm. 15. 2005. Págs. 279-310; "Circular núm. 1/2005 aplicación de la reforma del Código Penal operada por Ley Orgánica 15/2003, de 25 de noviembre (segunda parte)". Boletín del Ministerio de Justicia. Año 60. Núm. Extra 2008. 2006. Págs. 17-47; "Circular 2/2004, sobre aplicación de la reforma del Código Penal operada por Ley Orgánica 15/2003, de 25 de noviembre (primera parte)". Revista de Derecho Penal. Núm. 14. 2005. Págs. 311-335.

(art. 189.2 CP 1995), pues con la legislación anterior únicamente se castigaba la tenencia, cuando el material que se poseía para la producción, venta, distribución, exhibición, etc. del mismo. También se reformó el delito de estafa informática, de tal forma que, se amplió los supuestos de hecho del delito al añadir la posesión, fabricación, introducción o facilitar programas de ordenador destinados a la comisión de esta clase de estafa (art. 248.3 CP 1995). De la misma manera, los delitos relativos a la propiedad intelectual e industrial se mejoraron técnicamente, se agravaron las penas, así como se incluyeron, como nuevo supuesto de hecho la supresión o neutralización de dispositivo técnico utilizado para la protección de programas de ordenador u otras obras (art. 270.3 CP 1995). Por último, se introdujo un nuevo tratamiento a las defraudaciones en los servicios de radiodifusión sonora o televisiva (art. 286 CP 1995)[43].

Otra de las reformas operadas en el código penal de 1995, en relación el tema objeto de estudio, y que supuso un avance considerable, fue con arreglo a la Ley Orgánica 5/2010, de 22 de junio[44], sin embargo, en su mayor parte se trataba de transponer al derecho interno distintas Decisiones Marco de la Unión Europea. De este modo, en cumplimiento de la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003[45], *relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil*[46], se vino a castigar lo que en el ámbito de la psicológía se conoce como *«child grooming»*[47], es decir, la conducta encaminada a contactar con un menor de trece años a

[43] CRUZ DE PABLO, J. A. *Derecho penal y nuevas tecnologías, aspectos sustantivos: adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 de noviembre, especial referencia al nuevo artículo 286 CP*. Editorial Marcial Pons (Difusión Jurídica y Temas de actualidad). Madrid. 2006.

[44] «BOE» Núm. 152, de 23 de junio de 2010.

[45] «DOUE» Núm. 13 de 20 de enero 2004.

[46] Sobre los delitos cometidos a través de internet, introducidos a raíz de la reforma implementada con la L.O. 5/2010, en especial, con la transposición de la Decisión Marco 2004/68/JAI, véase a BARRIO ANDRÉS, M. "Los delitos cometidos en internet, marco comparado, internacional y derecho español tras la reforma penal de 2010". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 86. 2011. Pág. 4.

[47] RAMOS VÁZQUEZ, J. A. "El nuevo delito de ciberacoso de menores a la luz del derecho comparado". Diario La Ley. Núm. 7746. 2011; MAGRO SERVET V. "El «grooming» o ciberacoso

través de medios de comunicación, con la finalidad de obtener favores de índole sexual[48] (art. 183 bis CP 1995), así como, se modificó nuevamente el delito de pornografía infantil, al agravarse las penas e incluir como nueva conducta típica la captación de menores para la participación de espectáculo pornográfico, así como, el lucro obtenido por el mismo (art. 189.1.a CP 1995). Además, como consecuencia de la transposición de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005[49], *relativa a los ataques contra los sistemas de información*, se introdujeron figuras delictivas relacionadas con los daños y los delitos contra la intimidad. De esta manera, para el primero, se vino a crear el delito de daños informáticos consistente en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos, así como, obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264 CP 1995), mientras que para el segundo, dentro del delito del descubrimiento y revelación de secretos, se vino a añadir los accesos no autorizado a datos o programas contenidos en un sistema informático (art. 197.3 CP 1995)[50]. De la misma forma, se modificó el delito de estafa, pues se vino a incorporar al tipo básico, las acciones consistentes en realizar operaciones fraudulentas llevadas a cabo mediante la utilización de tarjetas de crédito o débito, así como cheques de viaje (art. 248.2.c CP 1995). Por su parte, el legislador pensando en conductas consistentes en la venta a pequeña escala de copias fraudulentas de obras amparadas por los derechos autor, conocida vulgarmente como "top manta", creó el delito atenuado relativo a la propiedad intelectual (art. 270.1 *in fine* CP 1995) para los supuestos de reducida cuantía del beneficio obtenido y en atención a

infantil, el nuevo artículo 183 bis del Código Penal*".* Diario La Ley. Núm. 7492. 2010; GARCÍA GONZÁLEZ, J., *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet.* Editorial Tirant lo blanch. Valencia. 2010.

[48] DOLZ LAGO M. J. "Child grooming y sexting: anglaicismos, sexo y menores en el Código Penal tras la reforma del 2015*".* Diario La Ley. Núm. 8758. 2016.

[49] «DOUE» Núm. 69, 16 de marzo de 2005.

[50] Sobre los accesos no autorizado a datos o programas contenidos en un sistema informático, véase, SÁNCHEZ DOMINGO, M. B. "Delincuencia informática y el delito de intrusismo informático aspectos de su regulación en instrumentos normativos europeos y su transposición al código penal español acorde a la lo 5/2010 de reforma de código penal español*".* Revista General de Derecho Penal. Núm. 18. 2012.

las características del autor, así como, la falta cuando el beneficio fuera inferior a 400 euros[51].

Seguidamente, otra reforma importante del código penal de 1995 ha sido realizada mediante la Ley Orgánica 1/2015, de 30 de marzo[52], por la cual, como en las modificaciones precedentes, vino mayoritariamente a transponer al derecho interno español normas de la Unión Europea. En cuanto al objeto del presente trabajo, la transposición de la Directiva 2011/93/UE[53], *relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil*, en relación con el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, hecho en Lanzarote el 25 de octubre de 2007[54], supuso la modificación del tipo penal de *«child grooming»* o *ciberacoso* (art. 183 ter CP 1995), el aumento de la edad del sujeto pasivo de trece a dieciséis años, la restricción de la finalidad del sujeto activo de prácticamente cualquier delito contra la libertad sexual a únicamente delitos de abusos o agresiones sexuales a menores de dieciséis años (art.

[51] Abordan la reforma implementada mediante la L.O. 5/2010, ÁLVAREZ GARCÍA, F. "La reforma de 2010 del Código penal*"*. Revista en Cultura de la Legalidad. Núm. 1. 2011. Págs. 75-84; SOLAZ SOLAZ E. "La prescripción, delitos contra la libertad sexual, estafas y propiedad intelectual e industrial, en la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 77. 2010. Pág. 4, si bien, lo que interesa aquí exponer es, la creación del delito atenuado y falta de propiedad intelectual, que encaja en las conductas relativas al "top manta".

[52] «BOE» Núm. 77, de 31 de marzo de 2015, en relación con dicha reforma, véase, JAÉN VALLEJO, M. y PERRINO PÉREZ, Á. L. *La reforma penal de 2015: análisis de las principales reformas introducidas en el Código Penal por las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*. Editorial Dykinson. Madrid. 2015; QUINTERO OLIVARES, G. *Comentario a la reforma penal de 2015*. Editorial Thomson Reuters-Aranzadi. Pamplona. 2015; MUÑOZ CUESTA. J. *Cuestiones prácticas sobre la reforma penal de 2015* Editorial Thomson-Aranzadi. Pamplona. 2015; MANZANARES SAMANIEGO, J. L. "La reforma del código penal de 2015: conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*"*. Editorial La Ley. Madrid. 2015; MATALLÍN EVANGELIO, Á. *Comentarios a la reforma del código penal de 2015*. Editorial Tirant lo Blanch. Valencia. 2015.

[53] «DOUE» Núm. 335, 17 de diciembre de 2011.

[54] «BOE» Núm. 274, de 12 de noviembre de 2010.

183 CP 1995), o de pornografía infantil (art. 189 CP 1995)[55], la creación del delito de embaucamiento con el objeto de facilitar material pornográfico o mostrar imágenes pornográficas de menores (art. 183.2 ter CP 1995), la inclusión del concepto legal de pornografía infantil (art. 189.1 CP 1995), el cual, prescinde de la mera desnudez, para decantarse por reproducciones visuales de menores teniendo sexo explícito, o bien, imágenes de órganos sexuales con tales fines, la incorporación como supuesto de hecho, la adquisición para uso propio y acceso a material pornográfico de menores (art. 189.5 CP 1995), la mejora técnicamente y la inclusión de nuevos supuestos de hecho de los tipos cualificados (aparatados 2º y 3º del art. 189 CP 1995), así como, la previsión de la adopción de medidas cautelares y definitivas para que los tribunales puedan retirar o bloquear el acceso de páginas web o aplicaciones de internet que contengan o difundan material de ésta índole en el territorio nacional (art. 189.8 CP 1995). Además, en cumplimiento de la Directiva 2013/40/UE, *relativa a los ataques contra sistemas de información y por la que sustituye la Decisión marco 2005/222/JAI*[56], se han modificado los daños informáticos (art. 264 sig. CP 1995), de tal forma que, se ha mejorado técnicamente esta clase de delitos, se han clasificado sistemáticamente los mismos, se han agravado las penas respecto del tipo ordinario (art. 264.1 CP 1995) así como, se han incluido nuevos supuestos de hecho para el delito cualificado (art. 264.2 CP 1995), y se ha añadido una nueva conducta punible consistente en la utilización, producción o adquisición de programas informáticos o contraseñas de ordenador para la comisión de algún delito de daños informáticos (art. 264 ter CP 1995). Asimismo, se han reformado los delitos de descubrimiento y revelación de secretos (arts. 197 y sig. CP 1995), de modo que, se han alterado la sistemática de los tipos penales, así como, se han creado nuevos delitos relacionados con la violación de la intimidad, destacando entre éstos la conducta de *sexting*, que consiste en la difusión, revelación o cesión de imágenes o grabaciones privadas, sin la autorización de la persona afectada, pese haberse obtenido con el consentimiento de su titular, siempre que menoscabe gravemente la intimidad personal del sujeto pasivo (art. 197.7 CP 1995). De hecho, se trata de la consecuencia jurídico penal de la repercusión pública en verano del 2012 que

[55] DE LEMUS VARA, F. J. "El delito de child groomimg tras la modificación operada en el artículo 183 ter del Código Penal, por la Ley Orgánica 1/2015*".* Diario La Ley. Núm. 8604. 2015.

[56] «DOUE» Núm. 218, de 14 de agosto de 2013. Págs. 8 –14.

tuviera la difusión de un video íntimo por la red ("*Caso Hormigos*"[57]). Además, se ha modificado el delito de intrusismo informático (art. 197 bis CP 1995), de manera que, se trata ahora como un precepto autónomo, así como, se ha mejorado técnicamente su redacción y se ha incluido como nuevo supuesto de hecho la utilización de artificios o instrumentos técnicos, con la finalidad de interceptar transmisiones de datos informáticos, al igual que, se ha añadido una nueva conducta punible consistente en la producción, adquisición, importación o facilitar la comisión de alguno de éstos delitos (apartados 1 y 2 del art. 197 o del art. 197 bis CP 1995) de programas informáticos o contraseñas de ordenador (art. 197 ter CP 1995). Del mismo modo, se han reformado los delitos contra la propiedad intelectual (art. 270 CP 1995)[58], de tal forma que, se han agravado las penas, se ha transformado el elemento subjetivo del injusto de *ánimo de lucro* por el *ánimo de obtener un beneficio económico directo o indirecto* (art. 270.1 CP 1995), lo cual, supone la ampliación de nuevos supuestos de hecho, se ha restringido la aplicación del tipo atenuado únicamente para supuestos de distribución o comercialización ambulante o meramente ocasional (art. 270.4 CP 1995), se ha creado el tipo penal de facilitar el acceso o la localización en internet de obras o prestaciones (art. 270.2 CP 1995), se ha mejorado técnicamente la redacción de las conductas tendentes a la distribución, venta o comercio no autorizada de obras (art. 270.5 CP 1995), o bien, la supresión o neutralización de dispositivos técnicos para la protección de dichas obras (art. 270.6 CP 1995). También, se ha dotado a los tribunales de la posibilidad de adoptar medidas, incluso de forma cautelar, para proteger los derechos de propiedad intelectual, de modo que, pueden ordenar la retirada de las obras, la

[57] Acerca de la reforma penal de 2015, DE LA ROCHA RUBÍ, M. "La reforma del Código Penal, populismo e ideología*"*. Temas para el Debate. Núm. 247. 2015. Págs. 35-39, viene a abordar, la conveniencia respecto a la política criminal, o bien, si se han realizado las modificaciones por razones populistas, decantándose más, por esta última opción.

[58] MORILLAS CUEVA, L. *Sistema de derecho penal: parte especial, revisada y puesta al día conforme a las leyes Orgánicas 1/2015 y 2/2015.* Editorial Dykinson. Madrid. 2015. Págs. 623-737.

interrupción de la prestación del servicio o del portal de internet, así como, el bloqueo del acceso al servicio (art. 270.3 1995)[59].

Por otro lado, en materia de ciberterrorismo, se ha modificado el código penal, mediante la L.O. 2/2015, de 30 de marzo[60], inspirada en la Decisión Marco 2008/919/JAI[61], así como, posteriormente con arreglo a la Ley Orgánica 1/2019, de 20 de febrero[62], que transpone la Directiva 2017/541/UE del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, *relativa a la lucha contra el terrorismo*[63], se han introducido ligeros ajustes respecto la legislación anterior.

B) Antecedente histórico del proceso penal español

Seguidamente vamos a desarrollar brevemente las diferentes normas adjetivas que han regulado el proceso penal en España, en concreto, la Ley de Enjuiciamiento Criminal de 1872 y 1882, especialmente, las reformas más importantes realizadas sobre ésta última, así como, la Compilación General de las disposiciones vigentes sobre el Enjuiciamiento Criminal aprobada mediante Real Decreto de 16 de octubre de 1879.

---

[59] *Principales novedades de la ley orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.* Revista Aranzadi Doctrinal. Núm. 5. 2015. Págs. 265-286.

[60] «BOE» Núm. 77, de 31 de marzo de 2015. En relación a la reforma mencionada sobre terrorismo, véase, CANO PAÑOS, M. A. *La reforma de los delitos de terrorismo.* Editorial Dykinson. Madrid. 2015. Págs. 905-951; SIMÓN DE LAS HERAS, B. "La reforma del Código Penal de 2015 conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*".* Revista de Derecho, Empresa y Sociedad. Núm. 6. 2015. Págs. 241-242; CANO PAÑOS, M. A. "La reforma penal de los delitos de terrorismo en el año 2015 cinco cuestiones fundamentales*".* Revista General de Derecho Penal. Núm. 23. 2015.

[61] «DOUE» Núm. 330, de 9 de diciembre de 2008.

[62] «BOE» Núm. 45, de 21 de febrero de 2019.

[63] «DOUE» Núm. 88, de 31 de marzo de 2017.

I. Ley de Enjuiciamiento Criminal de 1872

La Constitución de Cádiz aprobada el 19 de marzo de 1812, instaba a la creación de una norma que regulara el proceso penal en España (art. 286 C.E. 1812)[64], si bien, debido a su corta vigencia, fue derogada el 4 de mayo de 1814, no se aprobó ningún proyecto de ley. Posteriormente, la Ley Orgánica del Poder Judicial de 1870 contenía una Disposión Transitoria Primera[65] que, obligaba al gobierno a reformar los procedimientos penales, el cual, se llevaría a cabo, mediante el Real Decreto de 22 de diciembre de 1872, promulgado por el Rey Amadeo I, por el que, se aprobaría la Ley Provisional de Enjuiciamiento Criminal del ministro de Gracia y Justicia Eugenio Montero Ríos, entrando en vigor el 15 de enero del año siguiente[66], sin embargo, debido a la inadecuada estructura judicial entonces existente, no pudo surtir efecto alguno. Además, mediante Decreto de 3 de enero de 1875 promovido por el Ministro de Gracia y Justicia Francisco Cárdenas, dejaría en suspenso la parte más importante de la norma, el juicio oral y público, así como el jurado. Finalmente, con arreglo al Real Decreto de 16 de octubre de 1879, se aprobaría la Compilación General de las disposiciones vigentes sobre el Enjuiciamiento Criminal, en la cual, venía a realizar un texto refundido de los distintos decretos adoptados hasta la fecha sobre el proceso penal. En consecuencia, supuso la supresión definitiva del juicio oral y público, del jurado, así como, del principio de Juez no prevenido, al no concretar una clara distinción entre las fases de instrucción y plenario.

De este modo, la Ley de Enjuiciamiento de 1872 estaba estructurada en 962 artículos y una disposición final derogatoria, distribuidos en un Título Preliminar sobre *Disposiciones Generales*, un Libro Primero que regulaba el *Sumario*, un Segundo que

[64] Art. 286 de la Constitución Española de 1812, de 19 de marzo, promulgada en Cádiz: *Las leyes arreglarán la administración de justicia en lo criminal, de manera que el proceso sea formado con brevedad, y sin vicios, a fin de que los delitos sean prontamente castigados.*

[65] Disposición Transitoria Primera de la Ley Orgánica del Poder Judicial, de 15 de septiembre de 1870: *Procederá el Gobierno: 3. ° A reformar los procedimientos criminales.*

[66] Hemos estudiado las disposiciones de la LECrim. de 1872 a través de MONTERO RÍOS, E. *Ley Provisional de Enjuiciamiento Criminal*. Edición Oficial. Imprenta del Ministerio de Gracia y Justicia. Madrid. 1872.

versaba sobre el *Juicio Oral*, un Tercero relativo al *Procedimiento para el Juicio de Faltas*, y finalmente, un Título Adicional que contenía el *Procedimiento de Extradición*[67].

Seguidamente, se examinarán las disposiciones más importantes de la LECrim. de 1872 que tengan relación con la materia del presente trabajo, en concreto, las diligencias de investigación de entrada y registro domiciliario, la intervención en las comunicaciones, el informe pericial, así como, el enjuiciamiento de los delitos, pues con ello, será posible comprender el contexto histórico del proceso penal.

De este modo, dentro del Libro Primero sobre el *Sumario* de la ley procesal de 1872, se regulaba la entrada y registro en lugar cerrado, de libros y papeles y la detención y apertura de la correspondencia escrita y telegráfica (arts. 428 a 468 LECrim. 1872), pues se origina como resultado de la Constitución entonces vigente de 1869, que instauraba el derecho a la inviolabilidad del domicilio y el secreto epistolar, salvo resolución motivada acordada por el Juez competente, o bien, consentimiento de su titular (arts. 5 y 8 Constitución 1869)[68]. De manera que, el Juez instructor que conocía

---

[67] RODRÍGUEZ MARTÍN, C. *"*Consideraciones sobre el capítulo 1º, título preliminar de la ley provisional de enjuiciamiento criminal de 22 de diciembre de 1872. (I)*".* Revista General de Legislación y Jurisprudencia. Vol. 22. Núm. 44. 1874. Págs. 293-320; MISMO AUTOR. "Consideraciones sobre el capítulo 1º, título preliminar de la ley provisional de enjuiciamiento criminal de 22 de diciembre de 1872. (II)*".* Revista General de Legislación y Jurisprudencia. Vol. 22. Núm. 45. 1874. págs. 88-113; MISMO AUTOR. "Consideraciones sobre el Capítulo II, Título preliminar de la ley provisional de Enjuiciamiento Criminal de 22 de diciembre de 1872. (III)*".* Revista General de Legislación y Jurisprudencia. Vol. 23. Núm. 46. 1875. Págs. 111-111; MISMO AUTOR. "Consideraciones sobre el Capítulo II, Título preliminar de la ley provisional de enjuiciamiento criminal de 22 de diciembre de 1872. (IV)*".* Revista General de Legislación y Jurisprudencia. Vol. 23. Núm. 47. 1875. Págs. 47-84.

[68] Art. 5º Constitución 1869: *Nadie podrá entrar en el domicilio de un español, o extranjero residente en España, sin su consentimiento, excepto en los casos urgentes de incendio, inundación u otro peligro análogo, o de agresión ilegítima procedente de dentro, o para auxiliar a persona que desde allí pida socorro. Fuera de estos casos, la entrada en el domicilio de un español, o extranjero residente en España, y el registro de sus papeles o efectos, sólo podrán decretarse por el Juez competente y ejecutarse de día. El registro de papeles y efectos tendrá siempre lugar a presencia del interesado o de un individuo de su familia, y, en su defecto, de dos testigos vecinos del mismo pueblo. Sin embargo, cuando un delincuente, hallado in fraganti y perseguido por la Autoridad o sus agentes, se refugiare en su domicilio, podrán éstos penetrar en él, sólo para el acto de la aprehensión. Si se refugiare en domicilio*

de la causa, podía acordar la entrada y registro en cualquier edificio público (art. 428 LECrim. 1872)[69], o bien, lugar cerrado o domicilio (art. 432 LECrim. 1872)[70]. De esta manera, venía a considerar este último, como aquel edificio o lugar cerrado destinado principalmente a la habitación de cualquier español o extranjero residente en España y de su familia (art. 434.2º LECrim. 1872)[71], cuando hubiere indicios de encontrarse el procesado o efectos del delito que pudieran servir para su descubrimiento o comprobación. Además, la resolución que acordara el registro domiciliario debía ser fundada, salvo consentimiento del particular (art. 438 LECrim. 1872)[72]. También, se podían adoptar las medidas de vigilancia precisas para evitar la fuga del procesado o la sustracción de los instrumentos del delito (art. 448 LECrim. 1872)[73], cuando fuere

---

ajeno, procederá requerimiento al dueño de éste; Art. 8º Constitución 1869: *Todo auto de prisión, de registro de morada, o de detención de la correspondencia escrita o telegráfica, será motivado. Cuando el auto carezca de este requisito, o cuando los motivos en que se haya fundado se declaren en juicio ilegítimo o notoriamente insuficientes, la persona que hubiere sido presa, o cuya prisión no se hubiere ratificado dentro del plazo señalado en el art. 4º., o cuyo domicilio hubiere sido allanado, o cuya correspondencia hubiere sido detenida, tendrá derecho a reclamar del Juez que haya dictado el auto una indemnización proporcionada al daño causado, pero nunca inferior a 500 pesetas…*

[69] Art. 428 LECrim. 1872. *El Juez instructor o el Tribunal que conocieren de la causa podrán decretar la entrada y registro de día o de noche en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento o comprobación.*

[70] Art. 432 LECrim. 1872: *Podrá asimismo el Juez instructor ordenar en los casos indicados en el art. 428 la entrada y registro de día en cualquier edificio o lugar cerrado, o parte, de él que constituya domicilio de cualquier español o extranjero residente en España. Podrá también ordenar que se haga de noche en los casos previstos en los párrafos primero y cuarto del artículo 5. ° de la Constitución del Estado, o cuando prestare su consentimiento el interesado o su representante.*

[71] Art. 434 LECrim. 1872: *Se reputan domicilio para los efectos de los artículos anteriores: 2º El edificio o lugar cerrado, o la parte de él destinada principalmente a la habitación de cualquier español o extranjero residente en España y de su familia.*

[72] Art. 438 LECrim. 1872: *La resolución en que el Juez ordenare la entrada y registro en el domicilio de un particular será fundada, a no ser que éste o su representante los consintieren…*

[73] Art. 448 LECrim. 1872: *Desde el momento en que el Juez instructor acordare la entrada y registro en cualquier edificio o lugar cerrado, adoptará las medidas de vigilancia convenientes para evitar la fuga*

necesario, la autoridad competente o la Policía Judicial en su ejecución (art. 444 LECrim. 1872)[74], podía emplear el uso de la fuerza (art. 449 LECrim. 1872)[75], así como, el registro debía efectuarse principalmente en presencia del interesado (art. 450 LECrim. 1872)[76].

En otro orden de ideas, la Ley procesal de 1872 regulaba también la diligencia de investigación de interceptación de las comunicaciones, de modo que, el Juez instructor de forma motivada (art. 463 LECrim. 1872)[77] podía acordar la detención, la apertura y el examen de la correspondencia privada, postal y telegráfica del procesado para el descubrimiento o la comprobación de hechos delictivos (art. 459 LECrim. 1872)[78]. De manera que, la ejecución de la medida se podía encomendar a la autoridad competente, a los agentes de Policía Judicial (art. 444 LECrim. 1872), así como, al Administrador de Correos o Telégrafos del lugar donde se hallare la comunicación (art. 460 LECrim.

---

del procesado o la sustracción de los instrumentos, efectos del delito, libros, papeles o cualesquiera otras cosas que hubieren de ser objeto del registro.

[74] Art. 444 LECrim. 1872: *Si el edificio o lugar cerrado estuviere en el territorio propio del Juez de instrucción y éste fuere el que instruyere el sumario, podrá encomendar la entrada y registro… a cualquiera autoridad o agente de Policía Judicial.*

[75] Art. 449 LECrim. 1872: *Practicadas las diligencias que se establecen en los artículos anteriores, se procederá a la entrada y registro, empleando para ello, si fuere necesario, el auxilio de la fuerza.*

[76] Art. 450 LECrim. 1872: *El registro se hará a presencia del interesado o de la persona a quien encomendare sus veces...*

[77] Art. 463 LECrim. 1872: *La resolución acordando la detención y registro de la correspondencia o la entrega de copias de telegramas trasmitidos, será fundada y determinará la correspondencia que haya de ser entregadas por medio de la designación de las personas a cuyo nombre se hubieren expedido, o por otras circunstancias igualmente concretas.*

[78] Art. 459 LECrim. 1872: *Podrá el Juez instructor acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere, y su apertura y examen si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante en la causa.*

1872)[79], de tal forma que, el empleado de correos o telégrafos debía retener la epístola (art. 461 LECrim. 1872)[80], o en su caso, realizar una copia del telegrama (art. 462 LECrim. 1872)[81], para su entrega al Juez. En cuanto a la forma de practicar la apertura de cartas, se realizaba de forma similar a lo dispuesto en la Ley de Enjuiciamiento Criminal vigente de 1882, pues se efectuaba en presencia del interesado (art. 464 LECrim. 1872)[82], salvo que estuviera en rebeldía (art. 465 LECrim. 1872)[83]. De esta manera, el Juez leía para sí el contenido, apartaba para su conservación lo relevante a la causa (art. 466 LECrim. 1872)[84], mientras que la correspondencia que no tuviera interés la devolvía al procesado (art. 467 LECrim. 1872)[85].

Por otra parte, dentro del sumario, contenía unas disposiciones que regulaban el informe pericial (arts. 352 a 381 LECrim. 1872), de modo que, podía ser ordenado por el Juez de instrucción para prestar en la causa conocimientos científicos o artísticos (art. 352

[79] Art. 460 LECrim. 1872: *Es aplicable a la detención de la correspondencia lo dispuesto en los artículos 444 y 445. Podrá también encomendarse la práctica de esta operación al Administrador de Correos o Telégrafos, jefe de la oficina en que la correspondencia debiere hallarse.*

[80] Art. 461 LECrim. 1872: *El empleado que hiciere la detención remitirá inmediatamente la correspondencia detenida al Juez instructor.*

[81] Art. 462 LECrim. 1872: *Podrá asimismo el Juez instructor ordenar que por cualquiera Administración de telégrafos se le faciliten copias de los telegramas por ella trasmitidos si pudieran contribuir al esclarecimiento de los hechos de la causa.*

[82] Art. 464 LECrim. 1872: *Para la apertura y registro de la correspondencia postal habrá de ser Cit el interesado…*

[83] Art. 465 LECrim. 1872: *Si el procesado estuviere en rebeldía o si Cit para la apertura no quisiere presenciarla ni nombrar otra persona para que lo haga en su nombre, al Juez instructor procederá, sin embargo, a la apertura de dicha correspondencia.*

[84] Art. 466 LECrim. 1872: *La operación se practicará abriendo el Juez instructor por sí mismo la correspondencia y después de leerla para sí apartará la que hiciere referencia a los hechos de la causa y cuya conservación considere necesaria…*

[85] Art. 467 LECrim. 1872: *La correspondencia que no se relacionare con la causa, será entregada en el acto al procesado o a su representante…*

LECrim. 1872)[86]. Además, los peritos podían ser titulares cuando tuvieran un título oficial reglamentado por la Administración, o bien, no titulares cuando careciendo de título, tuvieren conocimientos o práctica especiales en alguna ciencia o arte (art. 353 LECrim. 1872)[87].

Por otro lado, como hemos aludido *supra*, la redacción originaria de la Ley de Enjuiciamiento Criminal de 1872, se caracterizaba por la aplicación del principio de Juez no prevenido, es decir, los jueces de instrucción formaban el sumario (art. 213 LECrim. 1872)[88] con la práctica de las diligencias que fueran necesarias, para una vez terminado, las actuaciones y las piezas de convicción, eran remitidas al Tribunal competente para su enjuiciamiento (art. 537 LECrim. 1872)[89]. Además, dependiendo del delito cometido, podía corresponder a un juicio oral ante el Tribunal de derecho, es decir, Audiencias formadas únicamente por jueces profesionales (arts. 596 a 657 LECrim. 1872), o bien, un Tribunal de jurado, compuesto por doce españoles particulares y tres magistrados (arts. 658 a 785 LECrim. 1872), todo ello, sin perjuicio del tratamiento específico que presentaban los procedimientos de juicio de faltas (arts. 935 a 955 LECrim. 1872), o especiales en el sumario como los delitos de injuria o calumnia contra particulares (arts. 498 a 501 LECrim. 1872), los cometidos por medio de imprenta, grabado u otro medio mecánico (art. 502 a 508 LECrim. 1872) o las infracciones cometidas por senadores o diputados (art. 491 a 497 LECrim. 1872).

---

[86] Art. 352 LECrim. 1872: *El Juez de instrucción ordenará proceder al informe pericial cuando para conocer o apreciar algún hecho o circunstancia importante en el sumario fueren necesarios o convenientes conocimientos científicos o artísticos.*

[87] Art. 353 LECrim. 1872: *Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración. Son peritos no titulares los que careciendo de título oficial tienen, sin embargo, conocimientos o práctica especiales en alguna ciencia o arte.*

[88] Art. 213 LECrim. 1872: *Los jueces de instrucción competentes formarán los sumarios de los delitos públicos, con la inspección del Fiscal del Tribunal del partido.*

[89] Art. 537 LECrim. 1872: *Practicadas todas las diligencias decretadas de oficio o a instancia de parte por el Juez de instrucción, si éste considerare terminado el sumario, lo declarará así, mandando remitir los autos y todas las piezas de convicción al Tribunal que tenga por competente para conocer del delito.*

Por último, la forma de la celebración del juicio oral para los tribunales profesionales (Tribunal de derecho) era similar al de la actualidad, pues comenzaba la vista con la confesión de los procesados (arts. 596 a 610 LECrim. 1872), en caso contrario, continuaba con la práctica de la prueba (arts. 611 a 644 LECrim. 1872), concluía con el informe de conclusiones de las partes, siendo el último en intervenir la defensa (arts. 645 a 652 LECrim. 1872), y finalmente, el tribunal dictaba sentencia absolutoria o condenatoria (art. 655 LECrim. 1872), para lo cual, regía el principio de libre valoración de las pruebas de los juzgadores (art. 653 LECrim. 1872)[90].

II. Compilación General de las disposiciones vigentes sobre el Enjuiciamiento Criminal de 1879

Restaurada la monarquía borbónica en 1874, con Alfonso XII, se aprobaron distintas normas procesales, de las cuales, la de mayor calado fue el Decreto de 3 de enero de 1875, que dejó en suspenso el juicio oral y público, así como, el jurado.

Sin embargo, se abre una época de confusión acerca de la vigencia de las distintas normas procesales anteriores. De este modo, el 30 de diciembre de 1878 se adoptó una ley que facultaba al gobierno para elaborar una norma que refundiera de forma ordenada y metódica las disposiciones que regían y que estuvieran relacionadas con el procedimiento criminal. De esta manera, se aprobó el Real Decreto de 16 de octubre de 1879, de la Compilación General de las disposiciones vigentes sobre el Enjuiciamiento Criminal[91]. Cuyos principales materiales, como expresamente aludía la Exposición de

[90] Art. 653 LECrim. 1872: *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 ésta se resolverán todas las cuestiones que hubiesen sido objeto del juicio, condenando o absolviendo a los procesados no solo por el delito principal y sus conexos, sino también por las faltas incidentales de que se hubiese conocido en causa...*

[91] BESSÓN, E. "Novísima compilación general de las disposiciones vigentes sobre el Enjuiciamiento criminal. Burgos, 1879. (Recensión)*".* Revista General de Legislación y Jurisprudencia. Vol. 28. Núm. 56. 1880. Págs. 111-111; *Manual de Enjuiciamiento criminal. Madrid, 1879. (Recensión).* Revista General de Legislación y Jurisprudencia. Vol. 27. Núm. 55. 1879. Págs. 494-494.

Motivos del ministro de Gracia y Justicia Pedro Nolasco Aurioles provenían de la Ley Orgánica de 1870 y de la Ley de Enjuiciamiento Criminal de 1872[92].

La Compilación General de las disposiciones vigentes sobre el Enjuiciamiento Criminal de 1879 estaba compuesta por 1.026 artículos y una Disposición Final, distribuidos en un Título Primero denominado *De la justicia en lo criminal*, un Título Segundo sobre las *Disposiciones generales relativas al Enjuiciamiento criminal*, un Título Tercero que regulaba el *Sumario*, un Titulo Cuarto que contenía las disposiciones sobre *el Plenario*, un Título Quinto acerca de *Los recursos de casación y de revisión*, un Título Sexto relacionado con *La ejecución de las sentencias*, un Título Séptimo respeto al *Procedimiento para el juicio sobre faltas*, y finalmente, un Título Adicional sobre *El procedimiento para la extradición de los procesados o condenados por sentencia firme que se hallen refugiados en país extranjero.*

Seguidamente, vamos a abordar, las disposiciones más importantes de la Compilación General de 1879, relacionadas con la parte procesal del presente trabajo, esto es, las diligencias de investigación de entrada y registro domiciliario, la intervención en las comunicaciones, así como, el informe pericial.

De esta manera, dentro del Título Tercero acerca del sumario, se regulaba en el Capítulo Noveno la entrada y registro en lugar cerrado, los libros y papeles y la detención y apertura de la correspondencia escrita y telegráfica (arts. 686 a 732 CG 1879). No obstante, la Compilación General de 1879, se trataba, en suma, de un texto refundido de las normas procesales existentes, de tal forma que, las disposiciones que regulaban éstas medidas, fueron extraídas prácticamente en su integridad de la Ley de Enjuiciamiento de 1872 (arts. 428 a 468 LECrim. 1872). Por este motivo, nos remitimos a lo expuesto anteriormente sobre la LECrim. de 1872, sin embargo, dejar apuntado que, nadie podía entrar en un domicilio sin el consentimiento de su titular (art. 6 CE 1876, en relación

[92] Hemos estudiado las disposiciones de la Compilación General de 1879 a través de RUIZ Y RODRIGUEZ, H. M. *Compilación general de las disposiciones vigentes sobre el Enjuiciamiento Criminal, concordada, anotada y seguida de observaciones*. Imprenta de la Revista de Legislación. Madrid. 1880.

con el art. 689 CG 1879)[93], salvo que el Juez lo acordara de forma motivada, cuando hubiere indicios de encontrarse el procesado, efectos o instrumentos del delito que hubieran podido servir para su descubrimiento o comprobación (art. 8 CE 1876 en relación con los arts. 690, 694 y 701 CG 1879)[94]. De igual modo, el Juez podía acordar, de forma motivada también, la detención de la correspondencia privada, postal y telegráfica del procesado, cuando hubiera indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa, para lo cual, el empleado de correos debía detener la correspondencia, o bien, la Administración de telégrafos debía facilitar las copias del telegrama al Juez (arts. 7 y 8 CE 1876 en relación con los arts. 723, 725, 726 y 727 CG 1879)[95].

---

[93] Arts. 6 CE 1876 y 689 CG 1879: *Nadie podrá entrar en el domicilio de un español, o extranjero residente en España, sin su consentimiento, excepto en los casos y en la forma expresamente prevista en las leyes*.

[94] Art. 8 CE 1876: *Todo auto de prisión, de registro de morada o de detención de la correspondencia, será motivado*; Art. 690 CG 1879: *El Juez ó el Tribunal que conocieren de la causa podrán decretar la entrada y registro de día ó de noche en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando, hubiere indicios de encontrarse allí el procesado, ó efecto ó instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento o comprobación;* Art. 694 CG 1879: *Podrá asimismo el Juez ordenar en los casos indicados en el art. 690 la entrada y registro de día en cualquier edificio o lugar cerrado, o parte de él que constituya domicilio de cualquier español o extranjero residente en España;* Art. 701 CG 1879: *La resolución en que el Juez ordenare la entrada y registro en el domicilio de un particular, será siempre fundada.*

[95] Art. 7 CE 1876: *No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo.* Art. 8 CE 1876: *Todo auto de prisión, de registro de morada o de detención de la correspondencia, será motivado;* Art. 723 CG 1879: *Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica, que el procesado remitiere ó recibiere, y su apertura y examen, si hubiere indicios de obtener por estos medíos el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa;* Art. 725 CG 1879: *El empleado que hiciere la detención remitirá inmediatamente la correspondencia detenida al Juez de la causa;* Art. 726 CG 1879: *Podrá asimismo el Juez ordenar que por cualquiera Administración de telégrafos se le faciliten copias de los telegramas por ella trasmitidos, si pudieran contribuir al esclarecimiento de los hechos de la causa;* Art. 727 CG 1879: *La resolución acordando la detención y registro de la correspondencia ó la entrega de copias de telegramas trasmitidos, será motivada y determinará, la correspondencia que haya de ser detenida o registrada, ó los telegramas cuyas copias hayan de ser entregadas, por medio de la*

Asimismo, las disposiciones que regulaban el informe pericial (arts. 611 a 640 CG 1879), no sufrieron modificaciones respecto a su predecesora, esto es, la Ley de Enjuiciamiento Criminal de 1872 (arts. 352 a 381 LECrim. 1872), pues, en definitiva, tenían por objeto, ilustrar al Juez, cuando fuera necesario, sobre conocimientos científicos o artísticos (art. 611 CG 1879)[96].

Por otro lado, la Compilación General eliminaba, además del jurado, el juicio oral, así como, la distinción entre la fase de instrucción y plenario, como si se tratara de un proceso civil. De esta manera, el proceso penal consistía en que los jueces de primera instancia formaban los sumarios (art. 455 CG 1879)[97], bajo la supervisión del Presidente de la Audiencia (arts. 458 y 459 CG 1879)[98]. Una vez practicadas las diligencias necesarias, se remitían las actuaciones al Ministerio fiscal y al acusador privado para que calificaran el delito (art. 801 CG 1879)[99]. Seguidamente, se daba traslado al abogado y procurador de la defensa para que manifestaran si se daban por enterados de la calificación y si precisaban de la ratificación de testigos (art. 834 CG 1879)[100], si

---

designación de las personas á cuyo nombre se hubieren expendido, ó por otras circunstancias igualmente concretas.

[96] Art. 611 CG 1879: *El Juez ordenará proceder al informe pericial cuando para conocer o apreciar algún hecho o circunstancia importante en el sumario fueren necesarios o convenientes conocimientos científicos o artísticos.*

[97] Art. 455 CG 1879: *Los Jueces de primera instancia instruirán los sumarios por los delitos públicos que se cometan dentro de su partido ó demarcación, con intervención del Ministerio fiscal.*

[98] Art. 458 CG 1879: *Los Jueces de primera instancia darán también parte de la formación de los sumarios al presidente de la Audiencia en los dos días siguientes al en que hubieren principiado a conocer de los mismos.* Art. 459 CG 1879: *En el parte expresarán las circunstancias principales del hecho, la persona contra quien se dirija el procedimiento, y si está o no detenida o presa.*

[99] Art. 801 CG 1879: *Luego que se hayan practicado todas las diligencias del sumario acordadas por el Juez, se mandará entregar la causa al Ministerio fiscal y al acusador privado, si lo hubiere, para une dentro del término que se les señalará, según el volumen y complicación del proceso, manifiesten por escrito, pero sin razonar ni fundar su juicio…*

[100] Art. 834 CG 1879: *Al devolver la causa, los procesados y los responsables civilmente presentarán un escrito firmado por su Abogado y Procurador en que manifiesten: 1° Que se han enterado de la calificación hecha por el Ministerio fiscal, y acusador privado si lo hubiere. 2° Si se conforman con las*

bien, el Juez podía denegarlo (art. 836 CG 1879)[101]. A continuación, el acusador privado y el ministerio fiscal formalizaban por escrito la acusación (art. 846 CG 1879)[102], que se remitía a los procesados para que presentaran el escrito de defensa (art. 847 CG 1879)[103]. Finalmente, el Juez dictaba sentencia (art. 852 CG 1879)[104], que podía ser apelada ante la Audiencia (arts. 854 a 857 CG 1879) que, como hemos aludido, había tenido conocimiento desde el principio de la formación del sumario.

III. Ley de Enjuiciamiento Criminal de 1882

La Ley de Bases sancionada el 11 de febrero de 1881 y promulgada el 22 de junio de 1882, autorizaba al Gobierno para redactar y publicar una Ley de Enjuiciamiento Criminal, tomando como base la Compilación general de 16 de octubre de 1879. De este modo, el Gobierno del que era Ministro de Gracia y Justicia Manuel Alonso Martinez, publicaba el 14 de septiembre de 1882 la Ley de Enjuiciamiento Criminal[105], en la cual, como novedad más destacable, se incorporaba nuevamente el juicio oral y se restituía el principio del Juez no prevenido[106], de tal forma que, se separaba con

---

declaraciones de los testigos del sumario, a efecto de omitir su ratificación, y renuncian la prueba; o si, por el contrario, piden la ratificación de todos ó algunos de dichos testigos y el recibimiento de la causa a prueba…

[101] Art. 836 CG 1879: *De la providencia en que se desestime toda o parte de la prueba propuesta o se niegue la ampliación del término probatorio concedido, podrá pedirse reposición dentro del término de segundo día. Si el Juez declarare no haber Jugar á ella, se admitirá la protesta que hiciere el interesado para los efectos del art. 855 de esta Compilación.*

[102] Art. 846 CG 1879: *Tanto en el caso de que se haya renunciado la prueba, como en el de haber trascurrido el término probatorio, el Juez dictará providencia maridando entregar el proceso al acusador privado si lo hubiere y al Ministerio fiscal, para que formalicen la acusación…*

[103] Art. 847 CG 1879: *De las acusaciones se conferirá traslado á los procesados y personas responsables civilmente, para que presenten sus defensas…*

[104] Art. 852 CG 1879: *Las sentencias se redactarán consignando en párrafos separados y numerados…*

[105] «La Gaceta de Madrid» Núm. 260, de 17 de septiembre de 1882.

[106] Señala, DE LA OLIVA SANTOS, A. (y OTROS), *Derecho Procesal Penal*. Editorial Universitaria Ramón Areces. Madrid. 2007. Págs. 90-94, que, el principio de juez no prevenido contenido en la Ley de

claridad, la fase sumarial del plenario, como expresamente refiere su Exposición de Motivos[107].

La edición originaria de la Ley de Enjuiciamiento Criminal de 1882 constaba de 998 artículos y una disposición final, distribuidos en un Libro Primero sobre *Disposiciones Generales*, un Libro Segundo que regulaba el *Sumario*, un Libro Tercero relativo al *Juicio Oral*, un Libro cuarto acerca *De los Procedimientos Especiales*, un Libro Quinto referente a *Los Recursos de Casación y Revisión*, un Libro Sexto que comprendía el *Procedimiento para el Juicio sobre Faltas*, y por último, un Libro Séptimo sobre *La Ejecución de las Sentencias*.

Por otro lado, las disposiciones de la la Ley de Enjuiciamiento Criminal de 1882 que regulaban las medidas de investigación, al igual que en la Compilación General de

---

Enjuiciamiento Criminal de 1882, que, el juez que investiga en fase de instrucción debe ser distinto al juez que juzga en fase de plenario.

[107] Exposición de motivos LECrim. 1882: …*que el Juez que instruye éste es el mismo que pronuncia la sentencia con todas las preocupaciones y prejuicios que ha hecho nacer en su ánimo la instrucción, que, confundido lo civil con lo criminal y abrumados los Jueces de primera instancia por el cúmulo de sus múltiples y variadas atenciones, delegan frecuentemente la práctica de muchas diligencias en el Escribano, quien, a solas con el procesado y los testigos, no siempre interpreta bien el pensamiento, ni retrata con perfecta fidelidad las impresiones de cada uno por grande que sea su celo y recta su voluntad; y que, por la naturaleza misma de las cosas y la lógica del sistema, nuestros Jueces y Magistrados han adquirido el hábito de dar escasa importancia a las pruebas del plenario, formando su juicio por el resultado de las diligencias sumariales y no parando mientes en la ratificación de los testigos, convertida en vana formalidad; que, en ausencia del inculpado y su defensor, los funcionarios que intervienen en la instrucción del sumario, animados de un espíritu receloso y hostil que se engendra en su mismo patriótico celo por la causa de la sociedad que representan, recogen con preferencia los datos adversos al procesado, descuidando a las veces consignar los que pueden favorecerle; y que, en fin, de este conjunto de errores, anejos a nuestro sistema de enjuiciar, y no imputable, por tanto, a los funcionarios del orden judicial y fiscal, resultan dos cosas a cual más funestas al ciudadano: una, que al compás que adelanta el sumario se va fabricando inadvertidamente una verdad de artificio que más tarde se convierte en verdad legal, pero que es contraria a la realidad de los hechos y subleva la conciencia del procesado; y otra, que cuando éste, llegado al plenario, quiere defenderse, no hace más que forcejear inútilmente, porque entra en el palenque ya vencido o por lo menos desarmado. Hay, pues, que restablecer la igualdad de condiciones en esta contienda jurídica, hasta donde lo consientan los fines esenciales de la sociedad humana.*

1879, estaban inspiradas en las libertades básicas recogidas en la Constitución de 1876[108], pues se establecía la inviolabilidad del domicilio (art. 6 CE 1876)[109] y el secreto de la correspondencia (art. 7 CE 1876)[110]. Además, cualquier injerencia en los derechos fundamentales mencionados, podía realizarse únicamente mediante auto judicial motivado (art. 8 CE 1876)[111]. Por esta razón, las normas reguladoras de la entrada y registro expresaban que nadie podía entrar en el domicilio sin el consentimiento de su titular (art. 545 LECrim. 1882)[112], salvo que el Juez lo acordara de forma fundada cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, que pudieran servir para su descubrimiento y comprobación (arts. 546 y 550 LECrim. 1882)[113]. De igual modo, la detención de la correspondencia privada, postal y telegráfica podía ser acordada por el Juez de forma motivada (art. 583

[108] SEGURA ORTEGA, M. *Los derechos en el constitucionalismo histórico español.* Editorial Servicio de Publicaciones de la Universidad de Santiago de Compostela. 2002. Págs. 135-176; VARELA SUANZES-CARPEGNA, J. *La Constitución de 1876.* Editorial Iustel. Madrid. 2009.

[109] Art. 6º Constitución 1876: *Nadie podrá entrar en el domicilio de un español, o extranjero residente en España, sin su consentimiento, excepto en los casos y en la forma expresamente prevista en las leyes…*

[110] Art. 7º Constitución 1876: *No podrá detenerse ni abrirse por la autoridad gubernativa la correspondencia confiada al correo.*

[111] Art. 8º Constitución 1876: *Todo auto de prisión, de registro de morada o de detención de la correspondencia, será motivado.*

[112] Art. 545 LECrim. 1882: *Nadie podrá entrar en el domicilio de un español o extranjero residente en España sin su consentimiento, excepto en los casos y en la forma expresamente prevista en las leyes.*

[113] Art. 546 LECrim. 1882: *El Juez o Tribunal que conociere de la causa podrá decretar la entrada y registro, de día o de noche, en todos los edificios y lugares públicos, sea cualquiera el territorio en que radiquen, cuando hubiere indicios de encontrarse allí el procesado o efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación;* Art. *550* LECrim. 1882: *Podrá asimismo el Juez instructor ordenar en los casos indicados en el artículo 546 la entrada y registro, de día o de noche, si la urgencia lo hiciere necesario, en cualquier edificio o lugar cerrado o parte de él, que constituya domicilio de cualquier español o extranjero residente en España, pero precediendo siempre el consentimiento del interesado conforme se previene en el artículo 6.º de la Constitución, o a falta de consentimiento, en virtud de auto motivado, que se notificará a la persona interesada inmediatamente, o lo más tarde dentro de las veinticuatro horas de haberse dictado.*

LECrim. 1882)[114], cuando hubiere indicios de obtener por estos medios el descubrimiento o comprobación de algún hecho o circunstancia importante a la causa (art. 579 LECrim. 1882)[115].

Por su parte, dentro de la parte de la Ley de Enjuiciamiento Criminal de 1882 que regula el sumario, dedica un capítulo al informe pericial (arts. 456 a 485 LECrim. 1882). No obstante, las disposiciones que regulan esta cuestión, son prácticamente idénticas a la de sus normas procesales predecesoras (arts. 352 a 381 LECrim. 1872 y 611 a 640 CG 1879). Basta mencionar que, el Juez puede acordar un informe pericial cuando precise de conocimientos científicos o artísticos sobre algún hecho o circunstancia importante en el sumario (art. 456 LECrim. 1882)[116], para lo cual, podrá solicitar el auxilio de peritos titulares cuando tengan un título oficial reglamentado por la Administración, o bien, peritos no titulares cuando carezcan de título, pero tengan conocimientos o prácticas especiales (art. 457 LECrim. 1882)[117], si bien, habrá de valerse con preferencia de peritos titulares (art. 458 LECrim. 1882)[118].

---

[114] Art. 583 LECrim. 1882: *El auto motivado acordando la detención y registro de la correspondencia o la entrega de copias de telegramas transmitidos determinará la correspondencia que haya de ser detenida o registrada, o los telegramas cuyas copias hayan de ser entregadas, por medio de la designación de las personas a cuyo nombre se hubieran expedido, o por otras circunstancias igualmente concretas.*

[115] Art. 579 LECrim. 1882: *Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura a examen, si hubiere indicios de obtener por estos medios el descubrimiento o comprobación de algún hecho o circunstancia importante de la causa*.

[116] Art. 456 LECrim. 1882: *El Juez acordará el informe pericial cuando, para conocer o apreciar algún hecho o circunstancia importante en el sumario, fuesen necesarios o convenientes conocimientos científicos o artísticos.*

[117] Art. 457 LECrim. 1882: *Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración. Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte*.

[118] Art. 458 LECrim. 1882: *El Juez se valdrá de peritos titulares con preferencia a los que no tuviesen título.*

Seguidamente, vamos a exponer las reformas más destacables relacionadas con las cuestiones planteadas en la parte procesal del presente trabajo. De este modo, la medida de investigación de entrada y registro domiciliario, no ha sufrido prácticamente modificaciones, pues se mantiene su redacción originaria, si bien, se ha mejorado su organización, con arreglo a la Ley Orgánica 13/2015, de 5 de octubre[119]. De esta manera, se ha separado, mediante dos capítulos diferenciados, la entrada y registro en lugar cerrado (arts. 545 a 572 LECrim. 1882) y el registro de libros y papeles (arts. 573 a 578 LECrim. 1882). Tampoco ha sufrido prácticamente variaciones las disposiciones reguladoras del informe pericial (arts. 456 a 485 LECrim. 1882), salvo las transferencias de atribuciones del Juez al Secretario Judicial efectuada mediante la Ley 13/2009, de 3 de noviembre[120]. Sin embargo, la medida de investigación de intervención de las comunicaciones, en su redacción originaria únicamente se circunscribía a la detención de la correspondencia privada, postal y telegráfica (art. 579 LECrim. 1882)[121]. De hecho, no fue hasta la reforma implementada con la Ley Orgánica 4/1988, de 25 de mayo[122], la cual, vino a incluir también, las comunicaciones telefónicas. El Juez podía acordar mediante resolución motivada, por un plazo inicial de tres meses, prorrogables por iguales períodos sin límite alguno, la injerencia en las comunicaciones telefónicas para el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa (art. 579 LECrim. 1882 con la redacción dada por la LO 4/1988)[123]. No obstante, las nuevas formas de comunicación, propiciada por los avances tecnológicos,

[119] BOE» Núm. 239, de 6 de octubre de 2015.

[120] «BOE» Núm. 266, de 4 de noviembre de 2009.

[121] Art. 579 LECrim. 1882 con la redacción originaria… O.P. Cit.

[122] «BOE» Núm. 126. de 26 de mayo de 1988.

[123] Art. 579.2 LECrim. 1882 con la redacción dada por la LO 4/1988: *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...*

demostrarían que, esta reforma fue claramente insuficiente. De hecho, como examinaremos en el presente trabajo, los tribunales acordaban diligencias no previstas expresamente en la ley, de tal forma que, encajaban estas nuevas formas de investigación por la vía de la analogía, aplicando otros supuestos semejantes contenidos en la norma procesal, colmando la falta de cobertura legal por la jurisprudencia[124]. Esta situación se mantuvo, hasta que el Tribunal Constitucional acordara la nulidad de las grabaciones obtenidas en los calabozos en dependencias policiales, por *ausencia total y completa de ley,* puesto que la Ley de Enjuiciamiento Criminal (art. 579.2 LECrim. con la redacción dada por la LO 4/1988) regulaba únicamente las *intervenciones telefónicas, no a escuchas de otra naturaleza* (STC 145/2014)[125]. Por este motivo, el Estado al temer que el Tribunal Constitucional pudiera declarar la nulidad de otras medidas de investigación no reguladas en la ley, vino a modificar la ley de Enjuiciamiento Criminal, con arreglo a la Ley Orgánica 13/2015, de 5 de octubre[126]. De esta manera, la reforma tenía por objeto, actualizar las medidas de investigación existentes, así como,

[124] ATS, de 18 junio 1992. Recurso 610/1990 (F. D. 2º): *llevar a cabo una especie de construcción por vía jurisprudencial de la forma correcta de realización de tal medida, utilizando la vía analógica de la Ley de Enjuiciamiento Criminal respecto a la detención de la correspondencia privada y otros supuestos semejantes...*; STS 1078/2009, de 5 de noviembre (F. D. 8º); STC 26/2006, de 30 de enero (FJ 5); STEDDHH, de 18 febrero 2003 *asunto Prado Bugallo contra España*, en el apartado 32 refiere a las lagunas en la regulación de las intervenciones telefónicas, si bien, estas insuficiencias han sido suplidas por la jurisprudencia, principalmente del Tribunal Supremo; STEDDHH de 30 julio 1998., *asunto Valenzuela Contreras contra España,* así como la Decisión inadmisoria del STEDDHH, de 25 de septiembre de 2006, *asunto Abdulkadir Coban vs. España*.

[125] STC 145/2014, de 22 de septiembre de 2014 (F. J 7º). Acerca de la sentencia mencionada, véase a GONZÁLEZ MONJE, A. "Sentencia del Tribunal Constitucional (Sala Segunda), 145/2014, de 22 de septiembre (BOE núm. 261, de 28-10-2014). Intervención de comunicaciones en dependencias policiales*"*. Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología. Vol. 3. Núm. 1. 2015. Págs. 355-357; NISTAL BURÓN, J. "La intervención de las comunicaciones verbales de los detenidos en dependencias policiales (A propósito de la Sentencia 145/2014, de 22 septiembre, de la Sala segunda del Tribunal Constitucional, dictada en el recurso de amparo número 6157-2010)*"*. Revista Aranzadi Doctrinal. Núm. 1 (enero 2015). 2015. Págs. 139-153; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones Jurídicas. Castillo de Luna. Madrid. 2015. Págs. 173-198.

[126] «BOE» Núm. 239, de 6 de octubre de 2015.

dar cobertura legal a otras diligencias de investigación restrictivas de derechos fundamentales relacionadas con las nuevas tecnologías[127]. De este modo, se vino a crear un Título Octavo bajo la rúbrica *De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*, que a su vez, se distribuía en diez capítulos con la regulación de las distintas diligencias de investigación[128], en concreto, *la entrada y registro en lugar cerrado* (arts. 545 a 572 LECrim.), *el registro de libros y papeles* (arts. 573 a 578 LECrim.), *la detención y apertura de la correspondencia escrita y telegráfica* (arts. 579 a 588 LECrim.), las *Disposiciones Comunes* a las medidas tecnológicas (arts. 588 bis LECrim.), *la interceptación de las comunicaciones telefónicas y telemáticas* (arts. 588 ter LECrim.), la *captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos* (arts. 588 quater LECrim.), la *utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización* (arts. 588 quinquies LECrim.), el *registro de dispositivos de almacenamiento masivo de información* (arts. 588 sexies LECrim.), el *registros remotos sobre equipos informáticos* (arts. 588 septies LECrim.), las *medidas de aseguramiento* (arts. 588 octies LECrim.). A esto, hay que añadir, pues se tratan de diligencias de investigación, aunque se encuentren dispersos en otras partes de la ley, la captación o intervención de las comunicaciones entre el abogado y el encausado (art. 118.4 LECrim.) y el agente encubierto informático (apartados 6 y 7 del art. 282 bis. LECrim.). No obstante, nos remitimos a la parte

[127] Sobre las medidas tecnológicas, véase, JIMÉNEZ SEGADO, C. y 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. Núm. 8676. 2016; RODRÍGUEZ LAINZ, J. L. "La detención y observación de la correspondencia escrita y telegráfica en la Ley Orgánica 13/2015*".* Diario La Ley. Núm. 8792. 2016; GUTIÉRREZ ROMERO, F. M. "Algunas claves de la reforma de la Ley de Enjuiciamiento Criminal*".* Revista Aranzadi Doctrinal. Núm. 2. 2016. Págs. 69-90; RUBIO ALAMILLO, J. "La informática en la reforma de la Ley de Enjuiciamiento Criminal*".* Diario La Ley. Núm. 8663. 2015; VELASCO SÁNCHEZ, J. C. y FUSTER-FABRA TOAPANTA, J. I. "Novedades de la reforma de la Ley de Enjuiciamiento criminal*".* Economist & Jurist. Vol. 23. Núm. 195. 2015. Págs. 10-24. Sin embargo, unicamente se deja aquí apuntado, pues será objeto posteriormente de análisis en el presente trabajo.

[128] BUENO DE MATA, F. *FODERTICS 4.0 (estudios sobre nuevas tecnologías y justicia): "IV Fórum de expertos y jóvenes investigadores en derecho y nuevas tecnologías, celebrado en la Facultad de Derecho de Salamanca, en 2015"*. Editorial Comares. Granada. 2015. Págs. 95-172.

procesal del presente trabajo sobre las diligencias de investigación, donde se desarrolla cada una.

CAPÍTULO INTRODUCTORIO: La Parte Sustantiva; Los Delitos Tecnológicos e informáticos

A) Breve contexto histórico del derecho penal informático y tecnológico

En torno a los años sesenta, los Estados comenzaron a conservar datos personales de sus ciudadanos en grandes archivos, para lo cual, las Administraciones Públicas pronto se preocuparían por el tratamiento y uso de los datos de carácter personal. Con la aparición de los primeros ordenadores en este periodo, la información de los ciudadanos conservada en las bases de datos, se fue informatizando gradualmente. Por este motivo, resultaba imprescindible la regulación de las bases de datos informatizadas, pues afectaba a la privacidad de los administrados, lo cual, supuso el inicio del derecho informático[129].

Posteriormente, a finales de los años setenta y principios de los ochenta, se fue generalizando la utilización de los ordenadores en el mundo empresarial. Sin embargo, los ordenadores en este período eran primitivos, además, debido a sus deficientes medidas de seguridad, puesto que era relativamente sencillo su manipulación. A su vez, las carencias legislativas de la época, que permitían a los delincuentes actuar con impunidad, motivo por el cual, surgieron problemas relacionados con la informática en el ámbito mercantil. En concreto, se produjeron ataques a empresas como apropiación de información, espionaje empresarial, sabotajes o daños informáticos.

Seguidamente, en la década de los ochenta, se generalizó el uso de ordenadores entre los particulares (PC, *personal computer*), de modo que, la informática fue accesible a un mayor número de personas, y con ello, trajo consigo un aumento de la delincuencia derivada de los medios tecnológicos, como, por ejemplo, la práctica consistente en reproducir, plagiar o distribuir programas o *software* sujetos a derechos de autor[130], lo

[129] DAVARA RODRÍGUEZ, M. A. *Manual de derecho informático.* Editorial Thomson-Aranzadi. Navarra. 2008.

[130] Afirma, HERNÁNDEZ DÍAZ, L. *Aproximación a un concepto de derecho penal informático.* Editorial Thomson-Reuters. Navarra. 2010. Págs. 34 – 35, que, en los años ochenta, se generalizó el uso de ordenadores, originando con ello, la piratería de su software, por lo que surgieron las primeras infracciones contra la propiedad intelectual.

que vulgarmente se conoce como "*piratería informática*". Por este motivo, los Estados comenzaron a legislar con el fin de otorgar protección a estas nuevas formas de delincuencia, lo cual, supuso el inicio del derecho penal informático.

Por su parte, en los años noventa, se extendería el uso de Internet[131] entre los usuarios particulares, de modo que, el nuevo canal de comunicación favorecía la comisión de delitos desde la privacidad de los domicilios, como por ejemplo la pornografía infantil. En consecuencia, los Estados comenzaron a adaptar sus legislaciones penales a éstas nuevas formas de delincuencia realizadas a través de la red.

A partir del año 2000 y hasta la actualidad, se han generalizado notablemente la utilización de los medios informáticos y tecnológicos entre casi la totalidad de la sociedad. Este hecho, es lo que se conoce como la era digital, la cual, conlleva que prácticamente cualquier hecho delictivo, pueda ser cometido directa o indirectamente mediante la utilización de las nuevas tecnologías de la información y la comunicación (TIC). Por esta razón, los Estados tienen la obligación de adaptar continuamente sus legislaciones penales a los nuevos avances tecnológicos, si bien, el Derecho por su propia naturaleza, siempre va un paso por detrás de la realidad social.

B) Delitos informáticos y tecnológicos: definición

Dentro del derecho informático, entendido éste, como un *"conjunto de normas jurídicas que regula el medio informático"*[132], tenemos los delitos informáticos. Sin embargo, se viene discutiendo por la doctrina sobre la existencia de un delito informático específico, es decir, si se trata de una rama del derecho penal independiente, con autonomía y sustantividad propia[133], o por el contrario, si esta clase de delitos son una categoría

[131] Véase sobre los delitos cometidos en la red, FERNÁNDEZ TERUELO, J. G. *Cibercrimen. Los delitos cometidos a través de Internet.* Editorial Constitutio Criminalis Carolina. Oviedo. 2007.

[132] La definición es nuestra.

[133] En opinión de BLAS ZULETA, L. "Delitos informáticos*".* Revista General de Derecho. Núm. 495. 1985. Págs. 3705-3707, TORTRAS, C. "El delito informático*".* Icade: Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales. Núm. 17. 1989 Págs. 45-50 y ESTRADA POSADA, R. y SOMELLERA R. "Delitos informáticos*".* Informática y Derecho: Revista Iberoamericana de Derecho

criminológica derivada[134]. De este modo, la doctrina actual se decanta por ésta última tesis, al afirmar que, existe una pluralidad de ilícitos penales que inciden en los medios informáticos, pero, además, tampoco existe una regulación específica en el código penal que se refiera expresamente a esta clase de delitos. Asimismo, en el código penal se regulan numerosas conductas que inciden en las nuevas tecnologías de la información y la comunicación (TIC), de tal forma que, pueden afectar directa o indirectamente a los medios informáticos y tecnológicos. De esta manera, Davara Rodríguez[135] define los delitos informáticos como *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un*

Informático. Núm. 27-29. 1998. Págs. 423-442, el delito informático se trata de una rama autónoma del derecho.

[134] En opinión de VELASCO NÚÑEZ, E. *Los delitos informáticos.* Práctica Penal: Cuaderno Jurídico. Núm. 81. 2015. Págs. 14-28, HERNÁNDEZ DÍAZ, L. "El Delito Informático*".* Revista Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. 23. 2009. Págs. 227-243, GONZÁLEZ RUS, J. J. *Delito e Informática: algunos aspectos*. Universidad de Deusto. Bilbao. 2007, ZORRAQUINO RICO, A. "Delitos informáticos*".* Cuadernos de Derecho Judicial. Núm. 5. 2006. Págs. 147-168, GIMÉNEZ GARCÍA, J. "Delito e informática algunos aspectos de Derecho penal material*".* Revista Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. 20. 2006. Págs. 197-215, SALOM CLOTET, J. "Delito informático y su investigación*".* Cuadernos de Derecho Judicial. Núm. 3. 2006 Págs. 91-130 y RODRÍGUEZ DAMIÁN, A. *Delitos informáticos.* Anuario de la Facultad de Derecho de Ourense. Núm. 1. 2004. Págs. 409-426, los delitos informáticos son una categoría derivada de los tipos delictivos ordinarios.

[135] Acerca de la definición de delitos informáticos, véase, DAVARA RODRÍGUEZ, M. A. "Los delitos informáticos*".* Consultor de los Ayuntamientos y de los Juzgados: Revista Técnica Especializada en Administración Local y Justicia Municipal. Núm. 15-16. 2016. Págs. 1825-1830; MISMO AUTOR. *Código de Internet*. Editorial Aranzadi. 2004. Cizur Menor (Navarra); MISMO AUTOR. *XVII Encuentros sobre Informática y Derecho, 2002-2003*. Editorial de la Universidad Pontificia Comillas. Madrid. 2003; MISMO AUTOR. *X años de encuentros sobre informática y derecho, 1996-1997*. Editorial Aranzadi. 1997. Cizur Menor (Navarra); MISMO AUTOR. "II Encuentro sobre la informática en las Facultades de Derecho*".* Revista Universitaria de Derecho Procesal. Núm. 2. 1989. Págs. 485-487; MISMO AUTOR. "Iuscibernética e Informática jurídica*".* Revista Universitaria de Derecho Procesal. Núm. 3. 1989. Págs. 757-768; MISMO AUTOR. "Informática y Derecho*".* Revista Universitaria de Derecho Procesal. Núm. 0. 1988. Págs. 333-348; MISMO AUTOR, "*Manual de Derecho Informático"*... O.P. Cit. Pág. 358-359.

elemento informático, ya sea hardware o software". También, en el mismo sentido añade que, esta clase de delitos corresponde a *"toda conducta sancionada por el Código Penal que tengan vinculación con la informática bien en su medio comisivo, bien en el objeto sobre el que recae la conducta, bien en ambos u otros ilícitos que en su momento puedan entrar a formar parte de él.* [136]*"*. Por este motivo, el sistema informático es intrínseco a esta clase de delitos. Por su parte, traemos a colación la definición dada por el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, en el cual, establece que *sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa* (art. 1.a del Convenio)[137].

De este modo, los delitos informáticos pueden examinarse desde un enfoque restrictivo del término, es decir, los cometidos únicamente contra o a través de sistemas informáticos, como por ejemplo, los daños informáticos (art. 264 CP) o la estafa informática (art. 248.2.a CP). Aunque, se pueden analizar también, desde una perspectiva amplia, pues se pueden incluir aquellos otros que inciden en las nuevas tecnologías, esto es, los que se realizan contra o a través de dispositivos electrónicos, como un *smartphone* o la red. Entre estos delitos se encuentran, la estafa nigeriana (art. 248.1 CP) o la pornografía infantil (art. 189 CP)[138]. Por este motivo, nos referiremos en el presente trabajo a esta clase de delitos, como delitos informáticos y tenológicos, pues

[136] Afirma, DE LA CUESTA ARZAMENDI, J. L. "Sociedad de la información y derecho penal a la luz del XIX Congreso Internacional de derecho penal*".* Revista Brasileira de Ciências Criminais. Núm. 112. 2015. Págs. 79-106; MISMO AUTOR. *Aspectos criminológicos y victológicos. (Derecho Penal informático).* Editorial Civitas. Madrid. 2010. Pág. 52, que, los delitos informáticos son toda conducta sancionada en el código penal que tenga vinculación con la informática.

[137] Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, publicado en el «BOE» Núm. 226, de 17 de septiembre de 2010. Págs. 78847 a 78896.

[138] Con respecto al concepto de delito tecnológico, VELASCO NUÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y de la Ley de Enjuiciamiento Criminal de 2015*. Editorial Sepin. Madrid. 2016. Pág. 175, lo define como, aquellos cometidos contra o a través de las nuevas tecnologías.

venimos a distinguir los que inciden solo en los sistemas informáticos, de aquellos otros que, afectan a las nuevas tecnologías. No obstante, la clasificación de estos delitos será examinada en el epígrafe siguiente.

En otro orden de ideas, existe cierta polémica sobre si la aparición de la informática y las nuevas tecnologías han creado nuevos bienes jurídicos dignos de tutelar, o por el contrario, siguen siendo los mismos bienes tradicionales[139]. Se debe advertir que, los bienes jurídicos son valores que trascienden de las meras conductas, o dicho de otro modo, los intereses más importantes valorados socialmente por su vinculación con la persona y su desarrollo (por ejemplo la vida, salud pública, integridad física o moral, libertad, indemnidad, patrimonio, etc.), y por ello, son tutelados por el derecho penal, o como diría el profesor Roxin[140], son aquellas "*circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema"*[141]. De este modo, el derecho penal únicamente tutela intereses de relevancia para la sociedad. Sin embargo, los delitos informáticos y tecnológicos son heterogéneos, es decir, esta clase infracciones son de muy diversa naturaleza (por ejemplo, la estafa informática, daños informáticos, pornografía infantil, etc.), por lo que, los bienes jurídicos tutelados (patrimonio, indemnidad sexual, etc.) son también muy diversos. De esta manera, las conductas relacionadas con elementos informáticos o tecnológicos no han creado nuevos bienes jurídicos, sino que siguen

[139] Señala FLORES PRADA, I., *Criminalidad Informática. Aspectos sustantivos y procesales.* Tirant lo Blanch. Valencia. 2012. Pág. 45, que, "aceptar que los sistemas informáticos no han creado nuevos bienes jurídicos, no significa que su utilización sea penalmente irrelevante*"*.

[140] Afirma ROXIN, C. *El concepto de bien jurídico como instrumento de crítica legislativa sometido a examen.* Revista Electrónica de Ciencia Penal y Criminología. Núm. 15. 2013. Pág. 5, que, "la misión del Derecho penal está en asegurar a sus ciudadanos una convivencia libre y pacífica, garantizando todos los derechos establecidos jurídico-constitucionalmente. Si esta misión es denominada, a modo de síntesis, protección de bienes jurídicos, por bienes jurídicos han de entenderse todas las circunstancias y finalidades que son necesarias para el libre desarrollo del individuo, la realización de sus derechos fundamentales y el funcionamiento de un sistema estatal edificado sobre esa finalidad".

[141] La definición de bien jurídico protegido se ha extraído de ROXIN C., *Derecho Penal Parte General. Tomo I. Fundamentos. La estructura de la Teoría del Delito.* Thomson Civitas. Madrid. 2006. Pág. 56.

siendo los tradicionales tutelados por el derecho penal[142], si bien, estas conductas delictivas han originado la existencia de nuevos intereses que deben ser protegidos por el derecho penal.

C) Clasificación de los delitos informáticos y tecnológicos

Seguidamente vamos a observar los diferentes delitos contenidos en el código penal relacionados con la informática y las nuevas tecnologías, para lo cual, hemos realizado una clasificación extraída de los autores que citamos a continuación: de la Mata Barranco, Hernandez Díaz[143], Flores Prada[144], Fernández Teruelo[145] y Velasco Nuñez[146].

De este modo, hemos propuesto una clasificación tripartita de los delitos informáticos y tecnológicos, si bien, como nos hemos referido anteriormente, abordaremos los que el

[142] Sírvase de ejemplo el bien jurídico del delito de estafa informática que, como advierte, SÁNCHEZ BERNAL, J. *El bien jurídico protegido en el delito de estafa informática.* Cuadernos del Tomás. Núm. 1. 2009. Págs. 105-121, se trata de bienes tradicionales tutelados por el derecho penal.

[143] Acerca de la clasificación de los delitos informáticos, DE LA MATA BARRANCO, N. J. y HERNANDEZ DÍAZ, L. *Los delitos vinculados a la informática en el derecho penal español. (Derecho Penal informático).* 2010… O.P. Cit. Págs. 159-197, viene a proponer la siguiente: los cometidos contra sistemas informáticos, a través de sistemas informáticos y contra la gestión de derechos digitales.

[144] Sobre la clasificación de los delitos informáticos, FLORES PRADA, I, *Criminalidad Informática. Aspectos sustantivos y procesales…* O.P. Cit. Págs. 43-298, propone: los cometidos contra sistemas informáticos y otros delitos cometidos a través de internet.

[145] En relación a la clasificación de los delitos informáticos, FERNÁNDEZ TERUELO, J.G, *Cibercrimen. Los delitos cometidos a través de Internet.* 2007… O.P. Cit. Págs. 10-175, plantea: los delitos cometidos a través de internet, en estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la red.

[146] Con respecto a la clasificación de los delitos informáticos, VELASCO NUÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y de la Ley de Enjuiciamiento Criminal de 2015*. Editorial Sepin. Madrid. 2016. Págs. 175-176, siguiendo a Ulrich Sieber, plantea: 1º Ciberdelincuencia económica. 2º Ciberdelincuencia intrusiva. 3º Ciberespionaje y ciberterrorismo.

elemento nuclear de lo mismos son estrictamente sistemas informáticos, pero también aquellos que se realizan contra o a través de la red o las nuevas tecnologías.

En consecuencia, el primer grupo contiene las infracciones delictivas cometidas contra los sistemas informáticos, de tal forma que, el más representativo es el delito de daños informáticos, aunque también aquellos otros que, las nuevas tecnologías son objeto del hecho delictivo, como por ejemplo, las defraudaciones, las falsificaciones, los delitos contra la intimidad y el ciberterrorismo.

Así, dada su relevancia y su incidencia con el objeto del presente trabajo, vamos examinar a título de ejemplo, el delito de daños informáticos.

De este modo, los daños informáticos consisten en realizar como conducta ilícita, destruir o menoscabar sistemas informáticos, equipos, datos, programas o documentos electrónicos (art. 264 CP). Por su parte, el delito de daños informáticos fue creado de acuerdo con la Ley Orgánica 5/2010, de 22 de junio[147], que transponía la Decisión Marco 2005/222/JAI, de 24 de febrero[148], si bien, posteriormente fue modificado por la Ley Orgánica 1/2015, de 30 de marzo[149], como consecuencia de la transposición a nuestro derecho interno la Directiva 2013/40/UE[150]. De la misma manera, como ya hemos advertido *supra*, el Convenio sobre Cibercriminalidad, define sistema informático como aquel *dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa* (art. 1.b C.).

Previamente, dentro de los daños informáticos, cabe distinguir los daños materiales o físicos, de los daños internos o lógicos. De esta suerte, los elementos físicos o

[147] «BOE» Núm. 152, de 23 de junio de 2010. En relación con la reforma penal implementada con arreglo a la L.O. 5/2010, véase, JUANES PECES, A. y ALBA FIGUERO, C. *Reforma del Código Penal perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio: situación jurídico-penal del empresario.* Editorial El Derecho. Madrid. 2010. Págs. 149-178.

[148] «DOUE» Núm. 69, de 16 de marzo de 2005.

[149] «BOE» Núm. 77, de 31 de marzo de 2015.

[150] «DOUE» Núm. 218, de 14 de agosto de 2013.

materiales corresponden al denominado *hardware*, de esta forma, valiéndose de la definición del diccionario de la RAE, consiste en un *conjunto de los componentes que conforman la parte material (física) de una computadora*[151], o bien, según el diccionario de María Moliner fija el concepto de *hardware* como un *conjunto de elementos físicos de un ordenador*[152]. Por este motivo, el término *hardware* es utilizado para referirse a los componentes eléctricos, electrónicos, electromecánicos y mecánicos de un sistema informático, que a su vez se pueden distinguir entre, los componentes internos (disco duro, placa base, microprocesador, circuitos, cables, etc.) de los periféricos (escáner, impresora, ratón, etc.). Sin embargo, cabe precisar que, cualquier menoscabo producido en los componentes periféricos, nunca sería subsumible la conducta en el tipo de daños informáticos (art. 264 CP), sino que se aplicaría el tipo básico (art. 263 CP), toda vez que se tratan de partes externas e independientes del ordenador, por lo que cualquier menoscabo producido se realizaría de forma física o tangible. Por su parte, el soporte lógico o interno, también conocido como *software*, comprende todo conjunto de componentes necesarios que hacen posible la realización de ciertas tareas específicas en un sistema informático, de tal manera que, de acuerdo con el diccionario de la RAE, el termino *software* se refiere al *conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora*[153], mientras que, el diccionario de María Moliner lo define como el *conjunto de programas y otros elementos no físicos con que funciona un ordenador*[154], de modo que, el concepto de *software* abarca todas las aplicaciones o programas informáticos utilizados en un ordenador. En conclusión, el delito de daños informáticos consiste en realizar menoscabos en los elementos físicos o *hardware*, a excepción de los elementos periféricos, pues son daños producidos como si se tratara de cualquier otro bien, sin

[151] Definición extraída: https://dle.rae.es/?id=K1Wwkf7.

[152] Definición examinada, MOLINER, M. *Diccionario de uso del español*. Editorial Gredos. Madrid. 2007. Pág. 1524.

[153] Definición observada: https://dle.rae.es/?id=YErlG2H.

[154] Definición sacada, MOLINER, M. *Diccionario de uso del español*. Editorial Gredos. Madrid. 2007. Pág. 2747.

relevancia alguna a los efectos informáticos, pero además, los producidos en los lógicos o *software*.

La acción penalmente reprochable de daños informáticos se perfecciona con la acción de producir menoscabos "*por cualquier medio*" en datos informáticos, programas informáticos o documentos electrónicos ajenos, de modo que, siguiendo la literalidad del precepto, hipotéticamente permite también la comisión de forma física, mediante por ejemplo un acto violento, si bien, lo importante aquí es la realización de modo material, es decir, con el acceso a un sistema informático de forma ilegítima, por tanto, no consentida o autorizada por el propietario o poseedor del sistema objeto del ataque[155] (arts. 264 y 264 bis. CP).

Como se ha mencionado, el delito de daños informáticos (art. 264 CP), supone la destrucción o menoscabo de los elementos físicos y lógicos de los sistemas[156], si bien, éste último será el que con más frecuencia se de en la práctica. Por este motivo, hemos focalizado el análisis en los elementos lógicos, es decir, el *software* y sus componentes, de manera que, el objeto del ataque puede ser la información introducida, tratada o almacenada por el titular, los programas o aplicaciones, esto es, los recursos que permiten desarrollar diferentes tareas en un ordenador, así como los documentos electrónicos, siendo estos un tipo de información archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

---

[155] Sobre el elemento objetivo del tipo de daños informáticos, véase, PÉREZ ÁLVAREZ, F y DÍAZ CORTÉS, L. M. *Moderno discurso penal y nuevas tecnologías memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013.* Ediciones Universidad de Salamanca. 2014. Págs. 201-217; DE LA MATA BARRANCO, N. J. y HERNÁNDEZ DÍAZ, L. "El delito de daños informáticos una tipificación defectuosa*".* Estudios Penales y Criminológicos. Núm. 29. 2009. Págs. 311-362.

[156] SAP de Madrid (Sección 23ª) 23/2017, 10 de enero (F.D. 1º) dispone que el tipo penal de daños informáticos refiere, por un lado, a datos, programas informáticos o documentos electrónicos ajenos dañados mediante alguna de las acciones descritas en el precepto, y por el otro, se refiere a la obstaculización o interrupción del funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos.

Además, los efectos producidos deben ser considerados como graves. Al tratarse de un concepto jurídico indeterminado, habrá de recaer en los tribunales el determinar la trascendencia de la infracción. Sin embargo, cuando se trata del tipo penal de daños ordinarios, se realiza una cuantificación económica del menoscabo producido, a los efectos de calificar la conducta de leve o grave (art. 263.1 *in fine* CP), estableciéndose el límite entre uno y otro en 400 euros, mientras que, para los daños imprudentes, se fija el límite de la reprochabilidad penal en 80.000 euros (art. 267 CP). De igual modo, en la cuantificación de los daños, cabe diferenciar los reparables[157], que para su valoración habrá que valerse de la reparación realizada, de aquellos otros irreparables, que se calculan atendiendo al valor de mercado del bien destruido. Con respecto a los daños informáticos, debemos realizar las siguientes consideraciones, de tal manera que, como sucede en el tipo básico, un perito habrá de valorar o tasar económicamente los menoscabos producidos, pues se exige para su tipicidad la gravedad de lo hechos, si bien, no se fija límite económico alguno, pero además, existe una dificultad añadida que deriva de la intangibilidad de los hechos que supone valorar económicamente las acciones cometidas a través de medios tecnológicos. De igual modo, para su tasación habra de atender si el menoscabo es reparable o irreparable, con las consideraciones realizadas anteriormente. Por este motivo, la situación descrita puede resolverse con la cuantificación económica del perjuicio ocasionado de acuerdo con la utilidad prestada en el medio informático, de tal manera que, habrá de observar el "*valor funcional*", es decir, aquel fijado con arreglo al provecho que se pueda obtener o la utilidad que presten en el medio informático[158]. Piénsese en el sabotaje a un *software* que con una simple copia de seguridad, un formateo del sistema o una instalación nueva del programa objeto de ataque bastaría para solucionar el problema, sin embargo, dicha conducta ha podido ocasionar un grave perjuicio, como por ejemplo con el funcionamiento de una página web que esté inoperativa durante un periodo de tiempo, derivando con ello grandes pérdidas económicas.

[157] Acerca de la valoración/tasación en el delito de daños, véase, RODRÍGUEZ MESA, M. J. *Conducta típica. (Los delitos de daños)*. Editorial Tirant lo Blanch. Valencia. 2017. Págs. 73 – 77.

[158] Sobre el valor funcional en el delito de daños, véase, GARCÍA GARCÍA-CERVIGÓN, J. "Daños informáticos. Consideraciones penales y criminológicas*"*. Actualidad Jurídica Aranzadi. Núm. 588. 2003. Págs. 10-12; ROMEO CASABONA, C. M. "Los delitos de daños en el ámbito informático*"*. Cuadernos de Política Criminal. Núm. 43. 1991. Págs. 91-118.

Por último, el legislador español, transcribiendo literalmente la Directiva 2013/40/UE[159] (art. 5), ha venido a considerar una serie de acciones típicas que pueden ser realizadas contra los sistemas informáticos, que además, tienen la categoría de *numerus clausus*. De este modo, a continuación se describen las acciones contenidas en nuestro código penal (art. 264.1 CP)[160]; *borrar* que consiste en hacer desaparecer, quitar o eliminar por cualquier medio datos, documentos electrónicos, programas, archivos o ficheros almacenados en un soporte informático; *dañar* o *deteriorar*, que alude a causar detrimento, perjuicio menoscabo o inutilización de un soporte informático tanto físico como lógico; *alterar* que se trata de modificar los sistemas informáticos, cambiar configuraciones de datos, programas o sistemas, o bien, sustituir elementos físicos o lógicos; *suprimir* que se refiere a borrar o eliminar, por ejemplo sistemas de protección o determinadas funciones; y finalmente, *hacer inaccesible*, es decir, impedir el acceso, la disponibilidad o el uso de todo o en parte de cualquier elemento de un sistema informático.

En otro orden de ideas, el legislador español, transponiendo la Directiva europea (art. 4 de la Directiva 2013/40/UE[161]) ha creado mediante la L.O. 1/2015 el delito de interrupción en el funcionamiento de un sistema informático, en concreto castiga las conductas graves y sin autorización de obstaculizar o interrumpir el funcionamiento de los sistemas informáticos, mediante la introducción o transmisión de datos, así como la destrucción, inutilización, eliminación, sustitución y daños de los mismos (art. 264 bis CP). De este modo, el tipo penal se refiere a los ataques producidos mediante *software* maliciosos o *malware*, conocidos vulgarmente como "*virus informáticos*"[162], de tal

[159] «DOUE» Núm. 218, de 14 de agosto de 2013.

[160] Acerca de las acciones típicas en el delito de daños informáticos, véase, MAZUELOS COELLO, J. "Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos*".* Derecho Penal y Criminología: Revista del Instituto de Ciencias Penales y Criminológicas. Vol. 28, Núm. 85. 2007. Págs. 29-36.

[161] «DOUE» Núm. 218, de 14 de agosto de 2013.

[162] SAP de Valencia (Sección 4º) Núm. 447/2011, de 10 de junio (F.J. 2º), en el cual, se aborda los "virus informáticos", es decir, programas cuya única finalidad es producir un deterioro o destrucción del "software".

manera que, esta clase de *software* tiene por finalidad infiltrarse en un sistema informático, reproducirse en la memoria del ordenador, contagiar a otros sistemas y producir un daño en el mismo. Sin embargo, existen una gran variedad de clases de *malware*[163], que atacan a los sistemas informáticos, produciendo perjuicios de muy diversa naturaleza[164], debido a lo cual, seguidamente se examinarán brevemente los más representativos[165]:

- *Crash programs* o programas destructores: son rutinas encargadas de destruir una gran cantidad de datos en un corto espacio de tiempo.

- Virus: son códigos de programación maliciosos, creados para alterar un sistema informático, y además tienen capacidad para reproducirse y transmitirse infectando a otros sistemas. Los virus necesitan un programa anfitrión, es decir, se adhirieren a un programa del sistema para poder ejecutarse.

- Gusanos (*worms*)[166]: son códigos de programación maliciosos, independientes, es decir, con capacidad para reproducirse y transmitirse por sí solos, sin necesidad de que exista un programa anfitrión alguno. Como sucede en los virus, los gusanos producen una alteración en los sistemas informáticos. Traemos a colación a título

[163] Sobre el malware, véase, MARTÍN DEL REY, A. M. *Actas de las primeras Jornadas Nacionales de Investigación en Ciberseguridad.* Servicio de Publicaciones de la Universidad de León. 2015. Págs. 1-7.

[164] En relación a los perjuicios que pudieran ser ocasionados a consecuencia de la infectación de un *malware*, véase, FERNÁNDEZ PALMA, R. y MORALES GARCÍA, O. "El delito de daños informáticos y el caso Hispahack*".* La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 1. 2000. Págs. 1522-1529.

[165] Acerca de las distintas clases de *malware* más representativos, véase, MELÓN PÉREZ, J. *Responsabilidad jurídica derivada de la creación, difusión y utilización de virus informáticos.* XVII Encuentros sobre Informática y Derecho coord. por Miguel Ángel Davara Rodríguez. Madrid. 2003. Págs. 435-446.

[166] Sírvase de ejemplo, CABALLERO, D. "Un hacker gallego colapsó internet*".* Cambio 16. Núm. 1658 (SEP 15). 2003. Págs. 26-27, en ésta publicación periodística se informa sobre un gusano propagado en la red.

ilustrativo, el gusano *Stuxnet*[167] que se trataba de un *malware* descubierto en el año 2.010, que atacaba a los sistemas *Windows* encargados de controlar los procesos productivos o industriales, modificando los códigos, para permitir a los atacantes tomar el control sin que los operadores legítimos tuvieran conocimiento de dicha actividad.

- Conejos o bacterias: son programas que se dedican a reproducirse hasta que colapsan los recursos del sistema, produciendo un bloqueo del equipo.

- Troyanos: son programas maliciosos que ocultos en un programa benigno o con la apariencia de utilidad, se introducen en un sistema informático produciendo innumerables daños en el mismo. Los troyanos pueden clasificarse de la forma que se propone a continuación:

  ○ Los que provocan la eliminación, alteración o bloqueo de datos o programas[168]:

  - *Ransomware*[169]: es un software malicioso que provoca restricciones de accesibilidad a determinadas partes o archivos de un sistema infectado, a cambio de solicitar un rescate económico para el restablecimiento del sistema. De este modo, el *malware* ocasiona el bloqueo del sistema informático, encriptando los archivos e impidiendo con ello el control de la información. Para desbloquearlo lanza una ventana emergente en la que se solicita el pago de cierto importe, so pena de destruir o dañar el sistema o archivos afectados.
  - *FakeAV* simulan la actividad de un programa antivirus, solicitando de los usuarios el pago en concepto de detección y eliminación de las amenazas inexistentes del sistema.

---

[167] Aborda, SÁNCHEZ MEDERO, G. "¿El ataque a Irán es el inicio de la ciberguerra?" El Viejo Topo. Núm. 275. 2010. Págs. 8-17, el gusano *Stuxnet.*

[168] Examina, DE LA CUADRA DE COLMENARES F. "Virus informáticos*"*. Informática y Derecho: Revista Iberoamericana de Derecho Informático. Núm. 34. 2002. Págs. 67-88, los virus informáticos.

[169] Aborda el *ransomware* en la publicación periodística: *"*El secuestro de equipos cómo evitar el ransomware, una nueva forma de malware*"*. Revista Personal Computer & Internet. Núm. 130. 2013. Págs. 30-33.

- Los *downloader* o descargas de archivos maliciosos: tienen por finalidad descargar y/o ejecutar archivos produciendo alteraciones diversas en el ordenador.

○ Los que se apropian de contraseñas:

- Los *password stealer* son aplicaciones que tienen por finalidad apropiarse de información introducida en los formularios de las páginas web. Los datos obtenidos son remitidos mediante correos electrónicos o almacenados en un servidor para su posterior adquisición por el atacante.
- Los *keyloggers* o capturador de teclas son programas que sin conocimiento del usuario sustraen las contraseñas introducidas en el sistema, como en los inicios de sesión o las contraseñas de los servidores de correo electrónico.
- Los troyanos bancarios o *banker* tienen por finalidad apropiarse de datos privados o contraseñas de las cuentas bancarias de los usuarios, para lo cual, utilizan diferentes técnicas como sustituir el sitio web de la entidad con falsa apariencia legítima, enviar capturas de pantalla de las páginas de las entidades financieras o la grabación en video de las acciones del usuario mientras accede al sitio web.

○ La apertura de puertas traseras o *backdoor*, que se tratan de programas que proporcionan el control remoto del sistema infectado:

- *Spyware*: espían un sistema informático cuando el mismo es utilizado, mediante la realización de capturas de pantalla o de la *webcam*, subiendo, descargando archivos, enviando información a un tercero o alterando el funcionamiento del sistema.
- *Rootkits*: provoca la ocultación de ciertas actividades de los programas, permitiendo al intruso acceder remotamente a los sistemas, para comandar acciones o extrayendo información del mismo.
- Redes zombies o *botnets*: Por el término zombi se entiende todo sistema informático infectado por algún tipo de *malware* que permita a un ordenador remoto acceder a su sistema. De esta manera, los ordenadores infectados pueden ser dirigidos a una red (*botnet*), o bien, una cantidad importante de ordenadores controlados entre sí, con la finalidad de ser utilizados para actividades ilícitas.

○ Los que provocan la saturación del sistema informático:

- El ataque de denegación de servicios o *DDoS* (Distributed Denial of Service): son conductas tendentes al bloqueo de un sistema informático mediante la saturación de los recursos del mismo por el consumo del ancho de la banda de la red. El ataque puede producirse enviando masivamente mensajes a un destinatario o al propio servidor, provocando la sobrecarga en su funcionamiento, impidiendo con ello el acceso total o parcial del servicio a los usuarios legítimos.

○ Los que están relacionados con la conexión a Internet:

- El *proxy* o servidores de acceso a internet: es una aplicación que permite al atacante utilizar el ordenador infectado como un servidor proxy, es decir, como un servidor que posibilita el acceso a otros ordenadores conectados a Internet a través del mismo, con la finalidad de ocultar su identidad.
- Los *dialers* o conexiones telefónicas: se producen conexiones de alto coste a sitios de pago en Internet, sin que la víctima tenga conocimiento, ocasionando con ello un perjuicio económico al usuario.

• El *Blended threats* o ataque mixto: es un ataque sofisticado a través Internet que combina las características de los virus, gusanos y troyanos, obteniendo con ello una rápida propagación por la red.

• Las bombas lógicas: son aplicaciones que están vinculados a otros códigos, y que tienen por finalidad atacar la parte lógica o *software* del ordenador. Sin embargo, se caracterizan por su capacidad de permanecer suspendidas o inactivas, hasta que se alcance un momento determinado por su desarrollador (una fecha o cumplir un plazo de tiempo fijado), a partir del cual, se ejecuta la acción maliciosa y ocasiona los perjuicios programados.

• *Hijackers* o secuestro*:* son programas que tienen por finalidad "secuestrar" o adueñarse de un sistema determinados datos o información, así como de conexiones a la red, páginas web, sesiones, servicios, del navegador de Internet, etcétera.

- Los *Adware*: producidos por el bombardeo de publicidad o *banners* en ventanas emergente conocidos como *pop-ups*, provocando con ello perturbaciones en el usuario del sistema.

- El correo basura o los *spamming*: se refiere a los mensajes no solicitados, ni deseados o de remitentes desconocidos, normalmente enviados en masa, que provocan molestias en los usuarios. Sin embargo, aparentemente pueden tener un carácter inofensivo, si bien, pueden esconderse detrás otras modalidades delictivas como el *scamming*, que será posteriormente objeto de estudio.

Posteriormente, en el segundo grupo, lo conforman los delitos cometidos a través de los sistemas informáticos, tecnológicos o internet. Dicho de otro modo, aquellas conductas delictivas que, los sistemas informáticos o las nuevas tecnologias constituyen un medio adecuado para la comisión de los tipos penales, en concreto, nos estamos refiriendo a la estafa, delitos contra la libertad e indemnidad sexual, usurpación de identidad (en relación con el delito de usurpación del estado civil), infracciones contra la libertad (amenazas, coacciones, *stalking*) y contra el honor (injuria, calumnia y extorsión).

Dentro de ésta clasificación, como hemos expuesto, se encuentra el delito de estafa. Es por ello que, dada su importancia, vamos a abordar a título de ejemplo el mencionado hecho delictivo.

Primeramente, advertir que, el delito de estafa (art. 248 CP) fue modificado mediante las reformas implementadas por la L.O. 15/2003[170], así como la LO 5/2010[171], mientras que la L.O. 1/2015, vino a crear el delito leve estafa (art. 249 in fine CP) para defraudaciones inferiores a cuatrocientos euros, si bien, ha sido objeto de tratamiento en la parte intruductoria del presente trabajo dedicada a dichas reformas, por lo que, únicamente queda aquí apuntado.

[170] BOE Núm. 283 de 26 de noviembre de 2003.

[171] «BOE» Núm. 152, de 23 de junio de 2010.

Entrando en materia objeto de estudio, de acuerdo con la definición legal de la estafa[172] ordinaria (art. 248.1 CP), podemos decir brevemente que, los elementos objetivos del tipo[173] son, el engaño bastante[174], el error producido por dicho engaño, el acto de disposición patrimonial, así como, el perjuicio propio o ajeno[175] (art. 248.1 CP), de tal forma que, existe una relación de causalidad entre el engaño y el perjuicio económico, esto es, el engaño es el motivo del perjuicio ocasionado[176]. En cuanto al tipo subjetivo, se requiere, además, del dolo, el ánimo de lucro, es decir, enriquecerse patrimonialmente en perjuicio del sujeto pasivo del delito[177].

---

[172] Sobre el delito básico de estafa, con caracter general, véase, ESQUIVIAS JARAMILLO, J. I. "Elementos del delito de estafa". CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 89. 2008. Pág. 194; CERVELLÓ DONDERIS, V. "Algunas cuestiones sobre la delimitación de la estafa". Revista General de Derecho, Núm. 560. 1991. Págs. 3759-3769; CONDE-PUMPIDO FERREIRO, C. *Estafas*. Editorial Tirant lo Blanch. Valencia. 1997; COBO DEL ROSAL, M. *El delito de estafa. Comentarios al Código Penal*. Editorial EDERSA. Madrid. 1999. Págs. 301-311.

[173] Sírvase de ejemplo, algunas resoluciones judiciales donde recogen los elementos del tipo objetivo de estafa, STS 810/2016, 28 de octubre (F.D. 2º), STS 1242/2006, 20 de diciembre (F.D. 3º), STS 880/2005, de 4 de julio (F.D. 4º) y STS 1491/2004, 22 de diciembre (F.D. 1º).

[174] Acerca del engaño bastante, véase, ESQUIVIAS JARAMILLO, J. I. "El engaño bastante en los delitos de estafa". CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 158. 2014. Págs. 185-188; SOTO NIETO, F. "Engaño "bastante" en el delito de estafa. Factor subjetivo". Diario La Ley. Núm. 7087. 2009; BALMACEDA HOYOS, G. "Engaño en la estafa ¿una puesta en escena?" Cuadernos de Política Criminal. Núm. 98. 2009. Págs. 5-30; BONMATÍ ORTEGA, P. "Informe de jurispridencia. El engaño "bastante" como requisito del delito de estafa". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 33. 2006. Págs. 79-94.

[175] Sobre el perjuicio patrimonial en el delito de estafa, véase, SCHLACK MUÑOZ, A. *Aplicación de criterios objetivo-individuales en la constatación del perjuicio patrimonial en el delito de estafa.* Ius Publicum. Núm. 19. 2007. Págs. 133-146; MARTOS NÚÑEZ, J. A. *El perjuicio patrimonial en el delito de estafa.* Editorial Civitas. Madrid. 1990.

[176] Afirma, MUÑOZ CONDE F., *Derecho Penal. Parte Especial…* O.P. Cit. 2015. Pág. 369-372, sobre la relación de causalidad entre el engaño y el perjuicio patrimonial en el delito de estafa.

[177] STS 1476/2004, de 21 de diciembre (F.D. 1º) dispone que "el delito de estafa tanto es sujeto pasivo del delito el sujeto que obra por un error al que ha sido inducido mediante engaño y realizó la disposición

Dicho lo anterior, la estafa tradicional se caracteriza por desenvolverse en un contexto de relaciones personales, es decir, el sujeto activo y el pasivo son individuos concretos que se relacionan entre sí, de modo que, la propia naturaleza de la estafa ordinaria hace que el engaño y el error únicamente se puedan realizar entre individuos. De esta manera, como veremos después, dicha regulación penal podrá ser aplicable también a otras conductas consistentes en engañar a víctimas mediante la utilización de medios tecnológicos, toda vez que, en definitiva, se trata de personas concretas relacionadas entre sí, a través de dispositivos electrónicos.

De este modo, cuando se realizan conductas defraudatorias contra sistemas informáticos, es decir, no va dirigida la acción frente a personas individuales y concretas, no puede ser subsumible la conducta en el tipo penal de estafa ordinaria, debido a que, en puridad, no se puede "engañar a un ordenador". Piénsese en una persona que se introduce en un sistema de una entidad financiera y ordena una transferencia a su favor o modifica el programa con el fin de que le transfieran pequeñas cantidades de dinero de numerosas cuentas diferentes, por ejemplo transfiriendo los decimales de las cuentas o mediante el método del redondeo para que sea imperceptible por los usuarios ("*técnica del salami"*); o bien, cuando se realiza una actuación dirigida a manipular una máquina expendedora de productos de consumo o *vendig* para producir con ello un acto de disposición ilícito. Por este motivo, numerosas conductas defraudatorios dirigidas contra elementos informáticos quedaban impunes, para lo cual, el legislador del código penal de 1995 (LO/1995)[178], al observar esta deficiencia, decidió añadir un apartado segundo que incluyera las manipulaciones informáticas o artificios semejantes (art. 248.2.b CP)[179]. De esta manera, la nueva regulación del delito

---

patrimonial, como el que sufre el daño patrimonial, que puede ser un sujeto distinto del que realizó la disposición patrimonial".

[178] «BOE» Núm. 281, de 24 de noviembre de 1995.

[179] Con carácter general en relación al delito de estafa informática cometida mediante manipulación o artificio semejante, véase, SÁNCHEZ BERNAL, J. "El bien jurídico protegido en el delito de estafa informática*"*. Cuadernos del Tomás. Núm. 1. 2009. Págs. 105-121; FERNÁNDEZ TERUELO, J. G. "Respuesta penal frente a fraudes cometidos en Internet estafa, estafa informática y los nudos de la red*"*. Revista de Derecho Penal y Criminología. Núm. 19. 2007. Págs. 217-243; CALLE RODRÍGUEZ, M. V. "El delito de estafa informática*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario.

de estafa en su modalidad informática, para poder abarcar todas las posibilidades existentes, se sustituyeron los elementos del tipo de "*engaño bastante para producir error en otro"*, por la "*manipulación informática o artificio semejante*", si bien, se mantenía su naturaleza tradicional defraudatoria, al exigir la relación de causalidad con el perjuicio económico con una transferencia no consentida de un activo patrimonial[180].

De todo lo mencionado hasta el momento, a los efectos del presente trabajo, podemos sacar la siguiente conclusión, la conducta consistente en defraudar a una persona individual a través de las nuevas tecnologías, como por ejemplo con las "*cartas nigerianas*" que posteriormente será examinada, será subsumible en la estafa ordinaria del art. 248.1 CP, pues la acción ilícita es cometida a través de las nuevas tecnologías, generando un engaño bastante y consecuente error, induciendo al sujeto pasivo a realizar un acto de disposición, por lo que, en definitiva, se trata de una estafa tradicional, pero realizada a través de medios tecnológicos[181]. En cambio, la conducta consistente en defraudar a un sistema informático mediante la realización de alguna clase de "*manipulación o artificio semejante*"[182], no va dirigida la acción frente a una persona individual, como en nuestro ejemplo en la "*técnica del salami"*, por lo que, será subsumible la acción en el tipo penal de estafa informática del art. 248.2.a. CP. Esto es, las alteraciones o manipulaciones que pudieran ser realizadas, van dirigidas a efectuar modificaciones de datos en un sistema o las configuraciones de un programa, con el fin

---

Núm. 37. 2007. Págs. 40-56; SÚAREZ SÁNCHEZ, A. *La estafa informática*. Derecho Penal y Criminología. Vol. 27. Núm. 81. 2006. Págs. 195-223.

[180] Sobre la manipulación informática o artificio semejante, como elemento objetivo de la estafa informática, véase a título de ejemplo, STS 860/2008, 17 de diciembre (F.D. 2º); STS 369/2007, 9 de mayo (F.D. 7º); STS 692/2006, 26 de junio: (F.D. 5º); SAP de Madrid (Sección 1ª) 128/2015, 17 de marzo (F.D. 2º); SAP de Madrid (Sección 6ª) 185/2013, 21 de marzo (F.D. 1º).

[181] En relación con la estafa ordinaria cometida a través de medios tecnológicos, traemos a colación los siguientes ejemplos extraídos de la jurisprudencia: STS 161/2009, 25 de febrero; SAN 43/2010, 12 de julio.

[182] Aborda, FARALDO-CABANA, P. "Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática*"*. Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. 21. 2007. Págs. 33-57, la manipulación informática y el artificio semejante realizado en la estafa informática del art. 248.2.b CP.

de transferir un activo patrimonial en prejuicio de tercero[183]. De esta manera, nos encontramos ante dos conductas defraudatorias, que a nuestro entender encajarían en la categoría de delitos informáticos, pues se habrían utilizado medios electrónicos o redes de internet para cometer el delito, si bien, dependerá de contra quien o que vaya dirida la defraudación, para que pueda ser aplicable una tipificación u otra.

Por su parte, el uso generalizado de internet por los usuarios, ha traído consigo la aparición de numerosas conductas que pueden ser subsumibles en el delito de estafa ordinaria cometida a través de medios tecnológicos (art. 248.1 CP), o bien, estafa informática (art. 248.2.b CP). Por este motivo, seguidamente se examinarán las conductas defraudatorias más importante cometidas a través de la red[184], en concreto, el *pharming* y *phising*[185], *spyware* o programa espía, las páginas web fraudulentas o envíos de correos electrónicos (*scamming)*, fraudes en operaciones de comercio electrónico, *dialers* o pago por servicio y la denominada "técnica del salami".

Pharming y Phising

El *pharming*[186] (proviene de "granja" en inglés) consiste en atacar los sistemas de nombres de dominio (DNS: *Domain Name System*)[187] de las direcciones IP asignadas (número de identificación de red), con la finalidad de redirigir el DNS a otro terminal distinto. De este modo, cuando un usuario introduce una dirección en su navegador, ésta

[183] Sobre la técnica del salami, véase, STS 364/2011, 11 de mayo (F.D. 3º), STS 692/2006, de 26 de junio (F.D. 5º); STS 172/2013, 8 de febrero (F.D. 2º); STS 860/2008, de 17 de diciembre (F.D. 2º); SAP de Barcelona (Sección 5ª) 903/2015, 26 de octubre (F.D. 2º); SAP de Baleares (Sección 1ª) 65/2015, 10 de marzo (F.D. 1º); SAP de Albacete (Sección 2ª) 167/2015, 8 de mayo (F.D. 5º).

[184] Advierte, FERNÁNDEZ TERUELO J.G., *Cibercrimen. Los delitos cometidos a través de Internet…* O.P. Cit. Págs. 27-53, sobre las técnicas defraudatorias más importantes cometidas a través de la red.

[185] En relación al *"pharming"*, SAP de Zaragoza (Sección 6ª) 358/2010, 2 de noviembre (F.D. 2º).

[186] Describe, DE CUADRA, F. "Pharming, nueva técnica de fraude*".* Sólo Programadores. Núm. 124. 2005. Págs. 10-11, la técnica del *Pharming*.

[187] DNS es un sistema que asocia nombres en lenguaje comprensible (nombre de dominio) con direcciones numéricas IP, con la finalidad de facilitar la navegación a través de la red por los usuarios.

se convierte en una dirección IP numérica, denominándose este proceso de resolución de nombres, encargándose los servidores DNS. De tal forma que, el usuario accede a un sitio web, confiado que se encuentra en un lugar seguro, realiza distintas operaciones, como introducir claves y/o datos personales, en especial números de cuentas y tarjetas bancarias, sin embargo, realmente se halla en un sitio simulado, que pretende sustraerle la información para su uso ilício. De esta manera, los ataques mediante *pharming* pueden realizarse de dos formas, directamente contra los servidores DNS, entonces todos los ordenadores conectados se verían afectados, o bien, atacando a ordenadores concretos mediante la modificación de archivos *hosts*, esto es, el método que utilizan los sistemas operativos Windows y Linux para resolver la correspondencia entre los DNS y las direcciones IP.

Por su parte, *phising*[188] ("pescando" en inglés) consiste en la técnica de suplantar la identidad de correos electrónicos o páginas web fiables, para obtener información confidencial de los usuarios[189]. Cabe precisar que, la técnica de obtener información privada mediante la suplantación de usuarios legítimos se conoce como ingeniería social, si bien, el *phishing* no es la única técnica de ingeniería social, sino que, existen otros métodos que tienen por objeto también la sustracción de datos confidenciales, como el *smishing,* cuando la vía del engaño se realiza por medio de mensajes de texto (SMS) o el *vishing* que consiste en contactar con la víctima a través del teléfono[190].

---

[188] Describen, FÁTIMA FLORES MENDOZA. "Respuesta penal al denominado robo de identidad en las conductas de phishing bancario". Estudios Penales y Criminológicos. Núm. 34. 2014. Págs. 301-339; POLO RODRÍGUEZ, J. J. "Modalidad de estafa informática el phishing*"*. Estudios Jurídicos. Núm. 2012, la técnica del *phishing.*

[189] STS 834/2012, *25 de octubre (F.D. 2º)* dispone *"*que el autor pesca los datos protegidos -de ahí la denominación *phishing*-, que permiten el libre acceso a las cuentas de los particulares y, a partir de ahí, el desapoderamiento*"*. En el mismo sentido, la SAP de Las Palmas (Sección 2ª) 22/2013, de 11 de febrero (F.D. 2º), SAP de La Rioja (Sección 1ª) 15/2015, de 23 de enero (F.D. 2º) y SAP de Valencia (Sección 3ª) 579/2012, de 31 de julio (F.D. 2º).

[190] Describe, VELASCO NÚÑEZ, E. "Estafa informática y banda organizada. Phishing, pharming, smishing y «muleros»*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario, Núm. 49. 2008, la técnica de ingienería social de *vishing.*

En cualquier caso, con frecuencia, se combinarán ambas técnicas[191], por un lado, el *pharming,* esto es, atacando los servidores DNS con el fin de redirigir una página web de confianza a otra simulada de apariencia idéntica a la original, y por otro, el *phishing,* suplantando la identidad de las páginas web supuestamente seguras para obtener datos privados de los usuarios. De esta manera, cuando el sujeto activo (*phisher)* haya obtenido los datos de la víctima, en especial, los números de las cuentas bancarias y sus claves de acceso, procederá a realizar transferencias a cuentas extranjeras, o bien, nacionales, pero con una identidad falsa, para dificultar su persecución. También, con frecuencia, los delincuentes se sirven de terceras personas o intermediarios, conocidos como "muleros", el cual, proviene el término de los narcotraficantes que trasladan oculto sustancias estupefacientes. Así, lo habitual será que los "muleros" reciban por correo electrónico o de una página web simulada, una oferta laboral supuestamente fiable, en la cual, para poder acceder al puesto de trabajo, deberán superar un aparente riguroso proceso de selección, que tiene por finalidad hacer creer a sus víctimas de la veracidad de la empresa. Tras superar el proceso de selección, se les remite un contrato laboral falso con aspecto de legalidad, si bien, el único requisito que se les exige es poner a disposición de la organización su cuenta bancaria personal. De tal forma que, siguiendo las instrucciones dadas por el defraudador (*phisher),* los intermediarios realizarán la actividad consistente en recibir una transferencia económica en su cuenta bancaria personal, para inmediatamente después, retirar el dinero y remitirlo al destinatario indicado. Normalmente para no dejar rastro, la entrega se realiza mediante empresas de envío de dinero como *Western Union*, *Money Gramm o Paypal*, una vez realizada la entrega, los "muleros" reciben una contraprestación económica, que en ocasiones incluso es de elevado importe. De esta manera, los intermediarios o "muleros" son la última fase del *iter criminis* del delito, toda vez que, son los encargados de materializar el engaño, pero además, son la cabeza visible del hecho delictivo, puesto que el *phisher* permanece en el anonimato. Sin embargo, los "muleros", con frecuencia, no son conscientes de haber cometido infracción alguna, dado que habrían actuado bajo mentiras de la organización.

[191] Sobre el *phishing y el pharming,* véase, REY HUIDOBRO, L. F. "La estafa informática relevancia penal del phising y el pharming*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 101. 2013. pág. 2.

La situación descrita plantea problemas sobre las implicaciones penales de las conductas cometidas por los *phisher* y de los "muleros", en especial, éstos últimos, ya que la doctrina viene siendo contradictoria. Seguidamente vamos a analizar de forma pormenorizada las conductas de los mencionados intervinientes en el *iter criminis* del hecho delictivo expuesto.

De esta manera, la calificación jurídico penal del *phisher* no entraña grandes dificultades, toda vez que, el hecho delictivo puede ser subsumible en el delito de estafa informática (art. 248.2.a. CP)[192], de modo que, existe un ánimo de lucro, hay una manipulación informática o artificio semejante en el sentido de que se produce una modificación material en los elementos de las páginas web o correos electrónicos con datos falsos de las mismas, el cual, ocasiona que los usuarios introduzcan sus números de cuentas bancarias y claves, secuestrando dicha información, para a continuación, realizar transferencias no consentida en su activo patrimonial y en su perjuicio. Cabe añadir que, la consumación del delito se produce en el momento de la ejecución de la trasferencia de dinero, esto es, cuando se origina el perjuicio económico en el sujeto pasivo. De esta manera, habrá que inferir que, la mera obtención subrepticia de las claves de acceso de la cuenta bancaria, pero sin realizar disposición patrimonial alguna, conlleva la no concurrencia de los elementos del tipo de la estafa informática. Claro está, sin perjuicio de las responsabilidades penales que pudieran haber incurrido por los actos ejecutados, como por ejemplo por los delitos de falsedad documental (art. 390 y sig. CP) o descubrimiento y revelación de secretos (art. 197 CP).

Sin embargo, la conducta de los "muleros", el cual, recuérdese que consistía en la actuación del intermediario que ponía su cuenta bancaria personal a disposición del *phisher*, a cambio de una gratificación económica, se vienen dando diversas interpretaciones doctrinales[193]. Sin embargo, al existir un ánimo de lucro de éstos, los

[192] STS 834/2012, 25 de octubre (F.D. 2º) y STS 860/2008, 17 de diciembre (F.D. 3º).

[193] Acerca de la conducta de los muleros en el *phishing*, véase, CORRECHER MIRA, J. y OXMAN, N. "La imputación del «mulero» en los delitos de estafa por manipulación informática la jurisprudencia a examen*".* Revista General de Derecho Penal. Núm. 21. 2014; MIRÓ LLINARES, F. "La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing*".* Revista Electrónica de Ciencia Penal y Criminología. Núm. 15. 2013; FLORES MENDOZA, F. "La responsabilidad penal

tribunales de manera unánime vienen entendiendo que incurren en responsabilidad penal. Sin embargo, la problemática estriba en cuál debe ser la correcta calificación jurídica de los hechos, planteándose si la conducta debe subsumirse en el delito de estafa informática (art. 248.2.a. CP), o bien, como receptación o blanqueo de capitales (art. 298 CP).

De este modo, algunos órganos jurisdiccionales entienden que la calificación de la conducta del "mulero" debe ser por delito de estafa informática (art. 248.2.a. CP), si bien, como cooperador necesario del mismo (art. 28 b. CP)[194]. Se viene poniendo de manifiesto que, la actuación del intermediario consistente en, poner a disposición del *phisher* su cuenta bancaria personal y realizar un acto voluntario de remisión del dinero transferido, al lugar donde se le haya indicado, hace que contribuya directamente en la ejecución de la estafa informática, puesto que, sin dicha acción, nunca se habría consumado el hecho delictivo. Además, el "mulero" disfruta de una gratificación económica por los servicios realizados, por lo que, los tribunales normalmente aprecian la participación en la ilicitud del hecho.

Por otro lado, Velasco Nuñez[195] mantiene que, al ayudar el "mulero" a los responsables de un delito patrimonial y al beneficiarse de los efectos del mismo, encajaría la conducta en el delito de receptación (art. 298.1 CP). De esta manera, el tipo penal mencionado exige para su ejecución, haber actuado mediante ánimo de lucro, así como tener conocimiento de la comisión de un delito contra el patrimonio o el orden

---

del denominado mulero o "phisher-mule" en los fraudes de banca electrónica*".* Cuadernos de Política Criminal. Núm. 110. 2013. Págs. 155-188.

[194] Seguidamente mencionamos algunas sentencias a título de ejemplo de condenas a la conducta del "mulero" por cooperador necesario de estafa informática: STS 556/2009, 16 de marzo (F.D. 7º) y STS 533/2007, 12 de junio (F.D. 2º).

[195] En relación con la conducta del "mulero" incardinable en el delito de receptación, véase, VELASCO NUÑEZ E., *Delitos cometidos a través de Internet. Cuestiones Procesales...* OP. Cit. Págs. 491. MISMO AUTOR, E. "Estafa informática y banda organizada. Phishing, pharming, smishing y «muleros»...*"* O.P. Cit; MISMO AUTOR, E. *Fraudes informáticos en red del phishing al pharming…* O.P. Cit. Págs. 57-66, así, SAP de Soria (Sección 1ª) 29/2014, 14 de abril de 2014 (F.D. 3º), SAP de Ávila (Sección 1ª) 35/2013, 18 de febrero de 2013 (F.D. 4º), SAP de Soria (Sección 1ª) 16/2012, 27 de febrero de 2012 (F.D. 2º) y SAP de León (Sección 3ª) 186/2011, 29 de julio de 2011 (F.D. 2º).

socioeconómico, en el que no se haya intervenido ni como autor ni como cómplice. Por este motivo, se trata de un hecho delictivo conexo o de referencia a un delito patrimonial, concretamente de estafa informática (art. 248.2.a. CP). Además, el "mulero" no intervendría en la ejecución del mismo, ni como autor ni como cómplice, dado que participaría cuando ya se habría consumado el delito precedente de estafa informática, pero también, existiría un ánimo de lucro al recibir una gratificación económica por su actuación. No obstante, como se ha mencionado, el intermediario debe tener conocimiento del origen ilícito de los efectos del delito, esto es, actuar mediante dolo, aunque sea eventual. Sin embargo, nuestros tribunales vienen entendiendo que, no es necesario que el "mulero" conozca con exactitud la ilicitud del hecho, sino que se podrá llegar a dicha conclusión si concurren una serie de indicios, tales como *la irregularidad de las circunstancias de la compra o modo de adquisición, la clandestinidad de la misma, la inverosimilitud de las explicaciones aportadas para justificar la tenencia de los bienes sustraídos, la personalidad del adquirente acusado o de los vendedores o transmitentes de los bienes o la mediación de un precio vil o ínfimo, desproporcionado con el valor real de los objetos adquiridos (SSTS. 8/2000 de 21 de enero y 1128/2001 de 8 de junio),* que hagan presumir que, conocen con un alto grado de probabilidad el origen ilícito de los bienes[196], todo ello, sin perjuicio de la aplicación del error como causa de justificación, que será objeto de estudio *infra*.

En otro orden de ideas, algunos tribunales mantienen que, la conducta cometida por los "muleros" será subsumible en delito de blanqueo de capitales (art. 301.1 CP)[197]. De esta manera, su actuación consiste en ocultar o encubrir bienes de procedencia delictiva, ya sea cometido por el propio "mulero", o bien, por tercera persona. Además, prestarían la ayuda necesaria a las personas que hayan participado en las infracciones, mediante la realización de distintas operaciones con el fin de dar la apariencia de legitimidad a dichos bienes. De esta manera, la diferencia principal con el delito de receptación es la posibilidad de haber intervenido en el delito precedente o de referencia, que en este

[196] STS 476/2012, 12 de junio (F.D. 3º) dispone que "el origen ilícito de los bienes receptados aparezca con un alto grado de probabilidad, dadas las circunstancias concurrentes."

[197] Aborda, GÓMEZ INIESTA, D. J. "Estafa y blanqueo de dinero a través de Internet*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 105. 2013. Pág. 4, la subsunción de la conducta de los "muleros" en el delito de blanqueo de capitales.

caso, es la estafa informática (art. 248.2.a. CP). De la misma manera, lo importante aquí, será determinar si la conducta del "mulero" ha sido cometida mediante dolo, esto es, como refiere el propio precepto, *sabiendo que éstos tienen su origen en una actividad delictiva* (art. 301.1 CP). Cabe advertir que, el delito doloso de blanqueo de capitales se castiga con una pena de seis meses a seis años de prisión, mientras que el delito de estafa informática (art. 248.2.a. CP) se sanciona con una pena privativa de libertad de seis meses a tres años, de tal forma que, la norma viene a establecer que, en ningún caso podrá imponerse una pena de prisión que exceda de la señalada al delito encubierto (art. 298.3 CP). Por este motivo, los tribunales que se decantan por esta posición jurídica, vienen calificando los hechos como delito imprudente de blanqueo de capitales (art. 303.3 CP)[198], de tal forma que, la pena a imponer no excede en ningún caso de los límites legalmente establecidos. Así, la conducta de los "muleros" también podría ser considerada negligente, en tanto en cuanto, su actuación sería cometida por no haber prestado los cuidados mínimos necesarios que son exigidos a cualquier persona precavida[199].

Una vez que se han expuesto las distintas interpretaciones realizadas por la doctrina y la jurisprudencia en relación con la conducta cometida por los "muleros", cabe mencionar que, nuestra posición es que, no se debería calificar el hecho como cooperador necesario del delito de estafa informática (art. 248.2.a. CP), pues éste, se perfecciona con la transferencia del activo patrimonial por la víctima captada mediante correo electrónico o la página web manipulada, lo cual, supone que, la intervención del "mulero" se realiza con el delito de estafa informática ya consumada. De esta manera, cualquier actuación posterior que se realice, habrá de efectuarse con una nueva subsunción en un tipo penal, que además, al no intervenir el "mulero" en el delito precedente, únicamente podría encajar la conducta en el delito de receptación (art. 298.1 CP), o bien, por los motivos expuestos *supra*, como delito imprudente de blanqueo de capitales (art. 303.3 CP).

Sin perjuicio de lo mencionado anteriormente, en ocasiones, para determinadas personas con un nivel cultural bajo, y por ende, legos en el campo de la informática y en el sector

[198] STS 834/2012, 25 de octubre (F.D. 2º) dispone que "considera como una acción imprudente de blanqueo de capitales con encaje en el art. 301.1 y 3 del CP".

[199] SAN 40/2010, de 31 de mayo (F.J. 2º) sobre la imprudencia.

financiero o bancario. Incluso, habrían sido objeto de engaño, al creer que el trabajo ofertado era totalmente lícito, nuestros tribunales han apreciado error de prohibición invencible como causa de justificación, excluyendo la responsabilidad criminal[200] de los "muleros" (art. 14.1 CP). Sin embargo, cabe precisar que, la regla general asumida por nuestros tribunales es no haber actuado bajo error, toda vez que, lo habitual será que éstas personas tengan una formación mínima que impida razonablemente apreciar la exclusión de la antijuridicidad del hecho[201].

Spyware o programa espía

De forma similar que en el *pharming* y *phising*, los ciberdelincuentes se pueden apoderar de los datos de los usuarios de internet mediante la introducción en los sistemas informáticos de un archivo *malware*, denominado programa espía o *spyware.* De este modo, el archivo maligno se autoinstala en el sistema sin que el usuario sea consciente de ello (por ejemplo cuando el usuario accede a determinados sitios web, cuando se descarga archivos de internet, etc.), provocando que se ejecute cada vez que se inicia el ordenador, para después transmitir la información de forma subrepticia al ciberdelincuente. Dicho de otro modo, los archivos *spyware* están programados para permitir el acceso de forma remota a los sistemas informáticos de sus víctimas, de tal forma que, mediante el uso de estos archivos permitir que ambos dispositivos localizados en puntos geográficos diferentes, mientras uno desconoce que está siendo vigilado, servirse el otro de la información. De esta manera, los datos apoderados pueden ser muy variados, tales como, obtener la información de las páginas web visitadas, para conocer sus preferencias, y utilizarlos con fines publicitarios o comerciales, apropiarse de las claves de acceso de páginas web, o bien, lo que interesa al objeto del presente trabajo, obtener los números y claves de las cuentas bancarias[202] o

[200] SAP de Madrid (Sección 15ª) 400/2008, 10 de septiembre (F.D. 2º) viene a considerar que el "mulero" es más bien víctima de la estafa.

[201] STS 533/2007, 12 de junio (F.D. 2º).

[202] Examina, FLORES MENDOZA, F. "*Respuesta penal al denominado robo de identidad en las conductas de phishing bancario".* Estudios Penales y Criminológicos. Núm. 34. 2014. Págs. 301-339, los programas espías con fines delictuales.

tarjetas de crédito o débito cuando los usuarios acceden a sitios webs de entidades financieras, o cuando realizan alguna transacción a través del comercio electrónico.

Por su parte, la utilización de los archivos de *spyware,* inciden directamente en la privacidad[203] de los usuarios, si bien, lo relevante aquí es que los datos secuestrados, en especial las claves de las cuentas bancarias o tarjetas de crédito o débito, pueden ser utilizadas de forma fraudulenta[204], de la misma manera que lo referido *supra* para el *pharming* y *phising.*

En otro orden de ideas, los principales programas que se emplean para la propagación de los *spyware* entre los sistemas informáticos son los troyanos, esto es, un *software* malicioso oculto que tiene apariencia de utilidad. Seguidamente, vamos a examinar brevemente a modo de ejemplo los *spyware*[205] más importantes:

- *CoolWebSearch* o *CoolWWWSearch,* se trata de un software que secuestra la información contenida en los buscadores de internet como *Internet Explorer*, *Mozilla, Firefox,* o *Google Chrome.*
- *Transponder* o *vx2,* de forma similar que, en el caso anterior, se trata de un programa que recoge la información sobre las páginas web visitadas, como los nombres de usuario y los datos de formularios.
- Los *keyloggers* o capturador de teclas como el *Perfect Keylogger*, consiste en un *software* que tiene por objeto recopilar la información que se escribe a través de los teclados, como contraseñas, número de cuentas bancarias, etc, incluso permitiendo registrarla mediante capturas de pantalla.

---

[203] Pone de manifiesto, ALVAREZ MARAÑÓN, G. "Derecho a la privacidad e Internet el spyware y otras amenazas a la intimidad*".* Estudios Jurídicos. Ministerio Fiscal, Núm. 2. 2003. Págs. 13-46, que los programas espías afectan a la privacidad de los usuarios.

[204] STC 173/2011, 7 de noviembre (F.J. 4º), STS 795/2016, 25 de octubre (F.D. 12º); STS 426/2016, 19 de mayo (F.D. 7º); STS 97/2015, 24 de febrero (F.D. 4º); SAP de Madrid (Sección 27ª) 168/2014, 17 de marzo (F.D. 6º).

[205] Sobre los programas espías más importantes, véase, WALKER, A. *Seguridad, spam, spyware y virus.* Editorial Anaya Multimedia. Madrid. 2006.

Páginas web fraudulentas o envíos de correos electrónicos (Scamming)

El *scamming*[206] es una práctica fraudulenta consistente en remitir masivamente al azar correos electrónicos o contactar con los usuarios mediante páginas web, ofreciendo propuestas sugestivas, de modo que, ilusionan a la víctima, consiguiendo de ésta, haga un desembolso económico por un ofrecimiento que nunca se llega a materializar.

De esta manera, existen varias versiones de *scamming*, como "*las cartas nigerianas*", la estafa de la lotería, de la herencia, *scammers* rusas, si bien, todas ellas mantienen la misma forma de actuar[207]. Seguidamente vamos examinar brevemente en que consiste cada una. De este modo, el *scamming* más difundido es el fraude de "*las cartas nigerianas*"[208], de modo que, consiste en que una supuesta autoridad administrativa de un Estado africano (normalmente Nigeria) contacta con su víctima mediante correo electrónico, solicitando que haga entrega de los datos de su cuenta bancaria, para transferir una importante suma de dinero, poniendo como excusa que debe ser retirado de dicho país por algún motivo (una revuelta política, fallecimiento de su titular, etc.), a cambio de la operación, recibirían una sustanciosa comisión. Además, para ganarse la confianza de la víctima, intercambian varios correos electrónicos, y finalmente, solicitar por adelantado cierta cantidad económica a fin de solventar unas hipotéticas complicaciones inesperadas (impuestos, tasas, sobornos a determinadas autoridades del país, honorarios de abogado, etc.). Sin embargo, una vez realizado el ingreso solicitado, desaparece toda comunicación con la supuesta autoridad administrativa.

---

[206] Se ha extraído el concepto de *scamming* de AREITIO BERTOLÍN, J. *Identificación de riesgos en el correo electrónico. Spam y pishing/scam*. Eurofach Electronica: Actualidad y Tecnología de la Industria Electrónica. Núm. 394. 2010. Págs. 42-47; ALVAREZ MARAÑÓN, G. *Scam, Spam, Spim, Phishing y más*. PC World. Núm. 212. 2004. Págs. 212-215.

[207] Seguidamente exponemos a modo de ejemplo, algunas resoluciones judiciales donde se recoge los delitos de estafas con la técnica de scamming, en especial, las "cartas nigerianas": STS 788/2009, de 12 de julio, SAP de Valencia (Sección 4ª) 154/2016, 8 de marzo, SAP de Valencia (Sección 5ª) 701/2015, 29 de octubre; SAP de Valencia (Sección 3ª) Núm. 664/2013, 30 de septiembre.

[208] Aborda, RUILOBA, J. C. "La actuación policial frente a los déficits de seguridad de Internet". IDP: Revista de Internet, Derecho y Política. Núm. 2. 2006, el fraude de las cartas nigerianas.

Por otro lado, existen otras variantes que, tienen todas las características del *scamming*, la cual, una de las más importantes es el fraude de la lotería[209], de tal forma que, consiste en contactar con la víctima mediante correo electrónico, en el cual, informan de haber ganado un premio de lotería, normalmente de un país extranjero. Además, en la mayoría de las ocasiones las víctimas no han participado en sorteo alguno. Sin embargo, para poder recibir el premio, solicitan por adelantado el desembolso de cierta cantidad, para satisfacer unos supuestos gastos de gestión, si bien, una vez realizado el ingreso, desaparece toda comunicación.

Otra variante de *scamming* es la estafa de la herencia[210] que, como en los casos anteriores, consiste en contactar con la víctima mediante correo electrónico, informando del fallecimiento de un familiar lejano, y que además, son beneficiarios de su herencia, o bien, poner en conocimiento del fallecimiento de una persona, o a punto de fallecer por una supuesta enfermedad terminal, con una gran herencia, si bien, carece de legítimos herederos. No obstante, para recibir su parte correspondiente de la herencia, resulta necesario desembolsar por adelantado cierta cantidad económica para satisfacer los gastos de gestión, como de abogado o notario.

Otra modalidad de fraude es el conocido como "*scammers* rusas"[211], de tal forma que, consiste en contactar con un varón mediante correo electrónico, asegurando que es una chica joven de un país extranjero, normalmente de Europa del Este (Rusia o Ucrania) y que desea iniciar una amistad. Para dar mayor credibilidad al engaño, se intercambian varios mensajes y le remite supuestas fotografías suyas, para a continuación, manifestar

[209] Sírvase de ejemplo de resoluciones judiciales donde se condena por estafa, en las cuales, se habría utilizado la técnica de la lotería: SAP de Madrid (Sección 3ª) 401/2016, 29 de junio; SAP de Málaga (Sección 8ª) s195/2016, 20 de abril.

[210] Sobre la estafa de la herencia, STS 413/2015, 30 de junio y SAP de Baleares (Sección 1ª) 151/2015, 16 de diciembre.

[211] Sírvase de ejemplo de la estafa de "*scammers* rusas", SAP de Alicante (Sección 2ª) 214/2015, 4 de mayo (F.D.1º), SAP de Valladolid (Sección 4ª) 496/2014, 27 de noviembre (F.D. 3º), SAP de Valencia (Sección 2ª) 791/2014, 10 de septiembre (F.D. 3º); SAP de Álava (Sección 2ª) 115/2014, 14 de marzo (F.D. 2º), SAP de Álava (Sección 2ª) 226/2013, 4 de julio (F.D. 5º); SAP de Ávila (Sección 1ª) 35/2013, 18 de febrero (F.D. 3º); SAP de Soria (Sección 1ª) 29/2014, 14 de abril (F.D. 3º).

la "*scammer*" que está enamorada y que desea concertar una cita pero, para poder viajar a España necesita que le envíe dinero para pagar el billete de avión o el visado. Sin embargo, una vez realizado el ingreso, se extingue definitivamente toda comunicación.

De esta manera, todas las modalidades de *scamming* descritas, tienen prácticamente las mismas características, de tal forma que, existe un primer contacto por correo electrónico narrando una historia más o menos verosímil, normalmente ocurrida fuera de España o de la Unión Europea, una vez que se ha ganado la confianza de la víctima, se solicita anticipadamente cierta cantidad por unos supuestos gastos ocasionados, y finalmente, cuando se desembolsa dicho importe, se extingue toda comunicación.

Fraudes en operaciones de comercio electrónico

El fraude en operaciones de comercio electrónico consiste en realizar transacciones comerciales[212] ilícitas a través de internet[213], pudiendo ser objeto del ataque tanto los consumidores como las empresas. Seguidamente vamos a examinar los más relevantes.

De este modo, el primer fraude en operaciones de comercio electrónico que será examinado es el de las ventas *on line*, el cual, consiste en la práctica de anunciar un determinado producto en páginas web de venta de segunda mano o de aplicaciones análogas por un precio inferior al de mercado. Cuando la víctima contacta con el vendedor, normalmente extranjero o se encuentra fuera de España, le indica que el abono del producto deberá efectuarse por adelantado y mediante un sistema de pago en línea, como *Paypal* o *Paysafecard*, los cuales, no permite conocer los datos personales y bancarios entre los usuarios, una vez realizada la transferencia, el vendedor desaparece sin hacer entrega de producto alguno. De la misma manera, una variante de esta clase de fraude es la falsa venta de mascotas por internet[214], la cual, se trata de publicar anuncios

[212] Aborda, LAFUENTE LÓPEZ, J. J. *El fraude en el comercio electrónico*. Auditoría Interna: Publicación Periódica del Instituto de Auditores Internos de España. Año 19. Núm. 65. 2003. Págs. 13-17, los fraudes en operaciones de comercio electrónico.

[213] Como ejemplo de fraude cometido a través de comercio electrónico, SAP de La Coruña (Sección 1ª) 238/2015, de 12 de mayo, en concreto, se realiza una venta a través de la página web *Ebay.es.*

[214] En relación a la estafa de ventas de mascotas a través de las nuevas tecnologías, SAP de Madrid (Sección 3ª) 18/2016, 14 de enero: SAP de Albacete (Sección 1ª) 76/2015, 6 de marzo, SAP de Lugo

de venta de crías de gatos o perros en páginas web, una vez que la víctima contacta con el vendedor, éste solicita el pago por adelantado que, tras realizar el ingreso solicitado, desaparecen sin enviar al animal. Por otro lado, puede darse el caso que el objeto del ataque sean las propias empresas ofertantes de productos, de modo que, consiste en adquirir un producto por medio de comercio electrónico, pero dicha operación se realiza sin desembolsar importe alguno, de tal forma que, se suplanta la verdadera identidad o se hace soportar el pago a una tercera persona ajena a la transacción.

De igual modo, otra clase de fraude en operaciones de comercio electrónico son las falsas subastas *e-Bay*[215], u otras aplicaciones electrónicas análogas. De esta manera, la plataforma *e-Bay* permite subastar productos, de tal forma que, unos usuarios ofertan y otros pujan, el que haga la oferta más alta, adquiere el producto. De esta suerte, el fraude consiste en subastar productos que, una vez pagados, nunca se llegan a entregar, o bien, los productos que finalmente se envían no se ajustan a la realidad de lo publicado en la plataforma. En relación a esto último, un ejemplo sería subastar o vender un producto en la plataforma a un precio muy inferior al de mercado, cuando se realiza el pago acordado, la víctima recibe una fotografía en lugar del original. Por otro lado, existe una práctica extendida entre los usuarios de *e-Bay* que consiste en subastar un producto, mientras que otro usuario confabulado, o bien, él mismo con otra cuenta de usuario, puja por el producto, con el fin de encarecerlo. Primeramente, advertir que, será difícil acreditar que se trata de una persona en conivencia con el vendedor, o bien, el mismo usuario con otra cuenta. Además, a nuestro entender, resulta cuestionable que dicha práctica merezca reproche penal alguno.

(Sección 2ª) 70/2015, 15 de abril; SAP de Pontevedra (Sección 5ª) 391/2015, 20 de julio; SAP de Zaragoza (Sección 6ª) 208/2014, 17 de julio; SAP de Cantabria (Sección 3ª) 355/2013, 17 de septiembre; SAP de Valladolid (Sección 4ª) 301/2013, 4 de septiembre; SAP de Cádiz (Sección 8ª) 117/2013, 12 de abril.

[215] Sobre las falsas subastas de e-Bay, SAP de Madrid (Sección 16ª) 179/2015, 11 de marzo: SAP de Zaragoza (Sección 6ª) 176/2011, 16 de mayo: SAP de Granada (Sección 2ª) 35/2009, 30 de enero; SAP de Madrid (Sección 6ª) 129/2008, 13 de marzo.

Dialers o pago por servicio

Los *dialers* son programas que tienen por objeto marcar números de teléfono con una tarifa especial, cuyo coste es superior al de una llamada nacional común. Así, el fraude consiste en ejecutar los programas *dialers* de forma subrepticia, de tal forma que, se instala en el sistema de manera oculta, facturando por unos servicios no deseados y sin informar al usuario de sus costes[216]. Sin embargo, como los *dialers* únicamente afectan a los establecimientos de llamadas telefónicas (como por ejemplo las líneas de 906 o 907), o bien, a los usuarios que accedan a internet mediante la Red Telefónica Básica (RTB) o Red Digital de Servicios Integrados (RDSI), la técnica ha caído en desuso, debido a que está más extendido el uso del modem o la línea de banda ancha de pago unificado (ADSL: *Asymmetric Digital Subscriber Line*).

Técnica del Salami

La "*técnica del salami*"[217] consiste en mediante la utilización de un programa informático, acceder a cuentas bancarias de numerosos usuarios con la finalidad de realizar transferencias de pequeñas cantidades de dinero, con el propósito de que el titular legítimo no perciba el fraude. Además, lo habitual será realizar la técnica del redondeo, esto es, sustraer escasos céntimos de los movimientos observados en la cuenta, de tal forma que, la cifra que se obtiene, no repare dudas en el titular, si bien, al ser objeto de ataque numerosas cuentas bancarias, el importe que finalmente se defrauda puede ser bastante elevado.

La conducta de la "*técnica de salami*" debe ser calificada como delito de estafa informática (art. 248.2.a. CP), toda vez que, nos encontramos ante una manipulación informática o artificio semejante ejecutado para conseguir una transferencia no consentida, y además, todo ello con ánimo de lucro y en perjuicio de su titular.

[216] SAP de Málaga (Sección 2ª) 131/2008, 11 de marzo (F.D. 1º), SAP de Barcelona (Sección 7ª) 1001/2005, 11 de noviembre (F.D. 2º).

[217] La "*técnica del salami*" tiene su origen en la práctica de cortar pequeñas rodajas de salami, pero imperceptible con respecto a la totalidad del mismo.

En el último grupo, lo componen ciertas conductas que, pese a tener aspectos comunes con los mencionados anteriormente, se han hecho constar de forma independiente. De esta manera, nos estamos refiriendo a los delitos contra la gestión de los derechos digitales, esto es, aquellos que tutelan la propiedad intelectual. No obstante, hemos decidido prescindir de un examen exhaustivo de cada uno de estos delitos, toda vez que, excedería del objeto del presente trabajo de investigación.

Una vez realizada la anterior introducción sobre los delitos informáticos y las nuevas tecnologías, pasaremos a explicar los aspectos procesales, pues el presente trabajo centra su estudio de investigación en analizar éstas cuestiones. De hecho, procede estudiar las previsiones legales y jurisprudenciales sobre la investigación y enjuiciamiento de los hechos delictivos relacionados con el fenómeno tecnológico, toda vez que, no servíria de nada una exaustiva legislación punitiva, sin que que pueda ser llevada a los juzgados y tribunales para su conocimiento.

CAPÍTULO PRIMERO: ASPECTOS PROCESALES

En este capítulo la investigación se va a centrar exclusivamente en explicar la parte procesal que, como se sabe, comprende las distintas diligencias de investigación que pueden ser acordadas para la averiguación de los hechos delictivos, en especial, los delitos objeto del presente trabajo, la prueba pericial informática y la jurisdicción y competencia de los tribunales para conocer de los ilícitos penales cometidos contra o a través de sistemas informáticos o tecnológicos.

Sin embargo, las diligencias para la comprobación del delito y la averiguación del delincuente es la parte más importante de la parte adjetiva del presente trabajo, pues se trata de medios de investigación que inciden en los derechos fundamentales, así como, tienen por finalidad inferir sobre la existencia de indicios racionales de criminalidad respecto del presunto responsable, y en consecuencia, decidir sobre la apertura de la fase decisoria o de plenario. De esta manera, para llegar a la conclusión sobre la pertinencia de la apertura del juicio oral respecto de una persona, resulta necesario que se basen en datos fácticos que conlleven en altas probabilidades de la comisión de un delito, y se llega, únicamente a dicha conclusión, cuando se han practicado las diligencias de investigación necesarias. Por este motivo, la parte más extensa del presente capítulo será la dedicada a las distintas medidas de investigación y averiguación delictiva, por estas razones, el presente estudio comenzará con la exposición de las diligencias de investigación.

A) LAS DILIGENCIAS DE INVESTIGACIÓN

La investigación penal relacionada con los delitos cometidos a través o contra los sistemas informáticos o tecnológicos pueden afectar a los derechos fundamentales garantizados en la Constitución española[218], en concreto, la averiguación de los

[218] Sobre las diligencias de investigación tecnológicas y su incidencia en los derechos fundamentales consagrados en la Constitución española, LÓPEZ-BARAJAS PEREA, I. "Garantías constitucionales en la investigación tecnológica del delito. Previsión legal y calidad de la Ley*"*. Revista de Derecho Político. Núm. 98. 2017. Págs. 91-119, señala que, "los sofisticados instrumentos que aporta la revolución tecnológica también ha exigido una reinterpretación o interpretación funcional del artículo 18 de la Constitución Española". (Pág. 95).

responsables autores de la comisión del hecho delictivo, o también, las diligencias encaminadas a recabar pruebas incriminatorias, normalmente, inciden en la privacidad o intimidad regulada en el artículo 18 de la *lex superior*. De esta forma, la investigación de los delitos tecnológicos, normalmente puede incidir en la intimidad personal y familiar y a la propia imagen (art. 18.1 CE), en la inviolabilidad del domicilio (art. 18.2 CE), en el secreto de las comunicaciones (art. 18.3 CE) o en el derecho a la protección de datos personales (art. 18.4 CE)[219]. Por este motivo, la consecuencia directa de la afectación a los derechos fundamentales es que, con carácter general, se requiere mandamiento judicial para su injerencia, pues en caso contrario se incurriría en nulidad de pleno derecho por prueba obtenida ilícitamente (art. 11 LOPJ), sin perjuicio que, además, pudiera conllevar en responsabilidad penal. De esta manera, el Juez es el encargado de la investigación, debiendo ponderar bajo su discrecionalidad, los diferentes intereses en conflicto, esto es, por un lado, el derecho particular del investigado a la privacidad o intimidad, mientras que por el otro, el interés público de perseguir la actividad criminal. De igual modo, el resto de los poderes públicos a la hora de prevenir o investigar delitos, también deben sopesar los intereses en conflicto, de tal forma que, nos encontramos ante dos intereses generales contrapuestos, por un lado, la seguridad, y por el otro, la privacidad o la libertad de los ciudadanos (seguridad *versus* privacidad/libertad)[220], por lo que, los poderes públicos dentro de sus funciones encomendadas, deberán decidir qué intereses tienen preferencia respecto del otro.

---

[219] 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. Núm. 8676. 2016; FERNÁNDEZ ESTEBAN, M. L. *El impacto de las nuevas tecnologías e Internet en los derechos del artículo 18 de la Constitución.* Anuario de la Facultad de Derecho. Núm. 17. 1999. Págs. 523-544; PARDO FALCÓN, J. "Los Derechos del Artículo 18 de la Constitución española en la Jurisprudencia del Tribunal Constitucional*"*. Revista Española de Derecho Constitucional. Año Núm. 12. Núm. 34. 1992. Págs. 141-180.

[220] Señala, AGUSTINA SANLLEHÍ, J. R. "Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia sobre la garantía del derecho a la intimidad en el registro del ordenador (a propósito de la STC 173/2011)*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 98-99. 2012. Pág. 10, que, existen unos intereses contrapuestos entre libertad y privacidad o seguridad de los ciudadanos que, se deben valorar, en el momento de acordar una medida de investigación restrictiva de derechos fundamentales, de modo que, viene afirmando que, "nos hallamos ante una colisión de derechos fundamentales y otros intereses constitucionalmente protegidos (intimidad versus intereses en la

Una vez realizada la anterior introducción, se van a examinar a continuación, las diligencias de investigación contenidas en la Ley de Enjuiciamiento Criminal[221] con arreglo a la reforma implementada con la Ley Orgánica 13/2015, *de 5 de octubre*[222], para lo cual, comenzaremos con las disposiciones comunes (art. 588 bis LECrim.), esto es, las normas genéricas aplicables a todas las medidas, seguiremos analizando específicamente cada una de ellas, y en concreto, la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 bis LECrim.), la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (art. 588 quater LECrim.), la captación de imágenes en espacios y lugares públicos (art. 588 quinquies a. LECrim.), la intervención de las comunicaciones en el ámbito penitenciario o en calabozos de las dependencias policiales: mención especial a las interceptaciones entre el abogado o procurador y su cliente (art. 118.4 y 520.7 LECrim.), la utilización de dispositivos o medios técnicos de geolocalización (art. 588 quinquies b. LECrim.), la entrada o registro domiciliario (arts. 545 y siguientes LECrim.), el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.), los registros remotos sobre equipos informáticos (art. 588 septies LECrim.), el agente encubierto (art. 282 bis LECrim.), para terminar, con la problemática de la utilización de otras diligencias restrictivas de derechos fundamentales no comprendidas en la Ley de Enjuiciamiento Criminal como por ejemplo los *drones*.

---

investigación criminal), en los que sería aplicable la doctrina general de la proporcionalidad (vid., entre otras, STC nº 70/2002, de 3 de abril, FJ 10; STC 207/1996, de 16 de diciembre, FJ 4; STC nº 89/2006, de 27 de marzo (21773/2006), FJ 3). Sin embargo, conviene descender al caso concreto y examinar si dicho examen de proporcionalidad debió estar mediatizado necesariamente por una previa autorización judicial. Para ello se debe atender a las facultades de la Policía en los primeros estadios de la investigación criminal y a las particularidades del caso concreto".

[221] La Gaceta Núm. 260, de 17 de septiembre de 1882.

[222] «BOE» Núm. 239, de 6 de octubre de 2015.

I. DISPOSICIONES COMUNES APLICABLES A LAS MEDIDAS TECNOLÓGICAS RESTRICTIVAS DE LOS DERECHOS FUNDAMENTALES DEL ART. 18 CE

Centrando nuestro estudio en las disposiciones comunes, cabe mencionar que, constituye la piedra angular o base donde pivotan las medidas restrictivas de derechos fundamentales contenidas en la LECrim. De esta forma, seguidamente pasamos a exponer las normas genéricas aplicables a todas las medidas, en concreto, los principios rectores (art. 588 bis a. LECrim.), la autorización judicial (art. 588 bis b y c LECrim.), el secreto (art. 588 bis d. LECrim.), el cese de la medida (art. 588 bis j. LECrim.) y la destrucción de los archivos (art. 588 bis k. LECrim.), la cuestión procesal de utilización de la información obtenida en un procedimiento distinto (art. 588 bis i. en relación con el art. 579 bis. LECrim.) y las medidas de aseguramiento y custodia de la prueba tecnológica (art. 588 octies LECrim.).

1) Los principios rectores

La norma procesal penal contiene unos principios que deben ser tenidos en cuenta a la hora de adoptar medidas restrictivas de los derechos fundamentales, y en especial, las diligencias de investigación tecnológicas. Cabe precisar que, aunque su regulación fue a raíz de la L.O. 13/2015, lo cierto es que, ya venían siendo aplicados por la jurisprudencia[223]. De este modo, seguidamente vamos a exponer los principios que sirven de base a las diligencias de investigación, tales como, legalidad, autorización judicial, especialidad, idoneidad, excepcionalidad y necesidad, así como, de proporcionalidad.

a) Principio de legalidad

Aunque el principio de legalidad no esté expresamente previsto en la norma procesal, lo cierto es que, se puede inferir el mismo, cuando el art. 588.1 bis a. LECrim. dice que "*durante la instrucción de las causas se podrá acordar alguna de las medidas de*

[223] Traemos a colación algunas resoluciones judiciales, en las cuales, mencionan los principios rectores con anterioridad a la reforma procesal implementada en el año 2015: STS 128/2007, de 22 febrero (F.D. 1º); STC 253/2006, de 11 de septiembre de 2006 (F.J. 2º).

investigación reguladas en el presente capítulo". De la misma manera, autores como Velasco Núñez[224] afirman que, el Juez de instrucción únicamente puede acordar medidas de investigación restrictiva de derechos fundamentales que estén expresamente regulados en la ley. De igual modo, nuestro Tribunal Constitucional[225] mantiene que *toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, de una habilitación legal.* En consecuencia, cualquier diligencia de investigación limitativa de derechos fundamentales que se adopte sin amparo legal, puede correr la suerte de ser anulada por inconstitucional, como ya sucedería con la Sentencia del TC Núm. 145/2014, que será objeto de análisis en un momento posterior.

b) Autorización judicial

La autorización judicial es una garantía para las injerencias en los derechos fundamentales, por tanto, se trata del núcleo principal donde deben pivotar las diligencias de investigación. Por este motivo, el art. 588.1 bis a. LECrim, de conformidad con el mandato constitucional (art. 18 CE), se limita a establecer como principio rector la exigencia de autorización judicial, para después, desarrollarlo en distintos preceptos de la norma procesal, si bien, este extremo será objeto de análisis posteriormente. De esta manera, queda aquí señalado que, las medidas restrictivas de derechos fundamentales únicamente pueden ser acordadas durante la fase de instrucción del proceso penal mediante autorización judicial (art. 588.1 bis a) LECrim.), pero

[224] En relación al principio de legalidad, advierte, VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015.* Editorial SEPIN. Madrid. 2016. Pág. 68, que, "la ley no lo dice, pero es obvio que la autorización judicial habilitante del uso -y validez- de la medida, por restrictiva de derechos fundamentales, no puede prestarse de forma arbitraria, a capricho del Juez Instructor, sino cuando concurran varios principios que le sirven para dircernir si se puede o no limitar temporalmente al investigado derechos que las tecnologías le pueden restringir, el primero de los cuales, aun cuando la LECrim. lo obvia y silencie, es el principio de legalidad*"*.

[225] STC 145/2014, de 22 de septiembre (F.J. 7º), hace mención a la necesaria habilitación legal para acordar una medida restrictiva de derechos fundamentales.

además, debe respetar los principios rectores que estamos exponiendo y estar motivada, lo cual, supone que debe revestir la forma de auto[226].

c) Principio de especialidad

El principio de especialidad conduce a que la autorización judicial habilitante de la medida restrictiva de derechos fundamentales debe estar siempre vinculada con la investigación de un delito concreto (art. 588.2 bis a. LECrim.), y en consecuencia, se debe evitar las intervenciones prospectivas, o dicho de otro modo, no están autorizadas las injerencias, por el mero hecho de "ver que se obtiene"[227]. Por este motivo, se debe concretar el delito previamente a la adopción de la medida, lo cual, supone que, la autorización judicial debe contener la base objetiva suficiente en relación con la actividad delictiva del investigado, de manera que, debe prescindirse de meras sospechas para acordarse la misma. Sin embargo, al encontrarnos en un momento incipiente del proceso penal, sin haber realizado las pesquisas necesarias para la averiguación del delito, la precisión del mismo puede resultar compleja. Ciertamente, la concreción delictiva se determina de forma progresiva mientras transcurre la investigación, o lo que nuestro Tribunal Supremo ha venido a llamar "*cristalización progresiva*"[228], es por ello que, el principio de especialidad exige que se mantenga inalterado el bien jurídico, aunque se pudieran modificar elementos accesorios.

d) Principio de idoneidad

La medida acordada mediante resolución judicial debe ser el resultado de un juicio de idoneidad, de manera que, se pondere el objeto de la diligencia concreta, los sujetos

[226] Al respecto, VILLANUEVA TURNES, A. *Las comunicaciones electrónicas, su encuadre constitucional y la autorización judicial como requisito para su intervención. (FODERTICS 5.0: estudios sobre nuevas tecnologías y justicia).* Editorial Comares. Granada. 2016. Págs. 287-296; CONTRERAS CEREZO, P. V. "Internet y la privacidad*".* Diario La Ley. Núm. 7.819. 2012; ROBLES ACERA, A. *La autorización judicial y el secretario en las entradas y registros domiciliarios.* Actualidad Jurídica Aranzadi. Núm. 43. 1992. Pág. 2; GUTIÉRREZ GONZÁLEZ, C. "Prueba ilícita. Entrada y registro sin previa autorización judicial*".* Revista General de Derecho. Núm. 552. 1990. Págs. 6.375-6.391.

[227] STS 1592/2003, de 25 noviembre (F.D. 2º).

[228] STS 385/2011, 5 de mayo y STS 412/2011, 11 de mayo.

afectados y la duración de la misma, de acuerdo con, su utilidad con los fines del proceso (art. 588.3 bis a. LECrim.)[229].

e) Principios de excepcionalidad y necesidad

El principio de excepcionalidad y necesidad suponen que la medida restrictiva de derechos fundamentales únicamente podrá ser acordada cuando no existan otras menos gravosas, pero de igual utilidad para el buen fin de la investigación, o bien, cuando sin el recurso de la medida sea gravemente dificultoso comprobar la actividad delictiva o sus autores (art. 588.4 bis a. LECrim.). Además, la necesidad implica que únicamente cabe acudir a una medida cuando la misma sea imprescindible respecto a su utilidad en la investigación[230].

Estrechamente relacionado con lo mencionado anteriormente, nuestro Tribunal Supremo ha venido a denominar el principio de subsidiariedad, esto es, no resulta procedente acordar una medida de investigación concreta cuando existan otros medios de investigación alternativos menos lesivos en los derechos fundamentales[231].

f) Principio de proporcionalidad

La decisión judicial deberá ponderar en una hipotética balanza los intereses en conflicto, por un lado, el beneficio para la sociedad o interés público de perseguir hechos delictivos, y por el otro, el sacrificio en los derechos fundamentales particulares del investigado. De esta manera, supone una prohibición en cuanto al exceso[232], es decir, se deberán evitar medidas de investigación a costa de injerencias en los derechos fundamentales intolerables[233]. Por este motivo, el Juez deberá ponderar los criterios de

[229] STS 727/2003, de 16 mayo (F.D. 1º).

[230] STS 1225/1995, de 1 diciembre.

[231] STS 393/2012, 29 de mayo (F.D. 2º).

[232] Sobre el principio de proporcionalidad, MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones Jurídicas. Castillo de Luna. Madrid. 2015. Págs. 215-216, señalan que, supone una prohibición en cuanto al exceso.

[233] STC 96/2012, de 7 de mayo (F.J. 10º).

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, en el momento de decidir sobre la pertinencia de la medida (art. 588.5 bis a. LECrim.)[234].

Sin embargo, como advierten nuestros tribunales[235], la gravedad de los hechos no puede estar determinada únicamente por la calificación de la pena legalmente prevista, pues de acuerdo con la ley sustantiva penal, fija como grave, entre otras, los delitos que superen los cinco años de prisión (art. 13.1 y 33.2 CP), sino que también deben de tenerse en cuenta otros factores, como el bien jurídico protegido o la relevancia social del hecho.

2) La autorización judicial

Aunque anteriormente hemos analizado la autorización judicial como principio rector, seguidamente vamos a desarrollarla, de tal forma que, para una mejor compresión, debemos distinguir, por un lado, la solicitud u oficio (art. 588 bis b. LECrim), esto es, la petición del Ministerio o la Policía Judicial al Juez de instrucción para que acuerde una diligencia de investigación, y por el otro, estudiaremos la resolución judicial (art. 588 bis c. LECrim), es especial, el contenido mínimo que debe comprender la misma.

a) Solicitud u oficio

De este modo, la adopción de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución puede ser de oficio, esto es, a propia iniciativa del Juez de instrucción, o bien, lo más frecuente, a instancia del Ministerio

[234] En relación al principio de proporcionalidad, ÁLVAREZ SÁNCHEZ DE MOVELLÁN, P. *Las nuevas medidas de investigación tecnológica y la enésima invocación al principio de proporcionalidad.* Justicia: Revista de Derecho Procesal. Núm. 1. 2018. Págs. 85-136, al advertir que, "la adopción de les medidas de investigación restrictivas de derechos exigen una proporcionalidad; y que esa proporción debe darse entre el sacrificio de los derechos que se limitan y el beneficio que se derive para el interés público o de terceros" (Pág. 105).

[235] STC Núm. 167/2002… O.P. Cit. (F. J. 4º) y Auto TS, de 18 junio 1992 (F.D. 4º).

Fiscal o la Policía Judicial (art. 588.1 bis b. LECrim)[236], pues, en definitiva, se tratan de los que tienen el primer contacto con la actividad delictiva. Sin embargo, la decisión del Juez de instrucción es potestativa, de tal forma que, por ejemplo, cuando la Policía Judicial solicita la adopción de una diligencia de investigación, pero el Ministerio Público informa negativamente sobre la conveniencia de la misma, el Juez tendrá plena libertad de acordarla o no, pues el criterio de la Fiscalía no es vinculante para el Juez. De la misma manera, las medidas restrictivas de derechos fundamentales tienen carácter público, pero además, para un mejor control y garantías sobre las mismas, se deben sustanciar en pieza separada y secreta (art. 588 bis d. LECrim.). De lo mencionado hasta el momento, se desprende que, las partes particulares del proceso (acusación popular o particular *strictu sensu*) no pueden solicitar medidas, si bien, cualquiera de las partes particulares podrá informar al Juez sobre la pertinencia de la adopción de alguna diligencia, aunque, si finalmente fuera acordada, la medida tendrá el tratamiento jurídico de oficio[237], lo cual, conllevará que, al sustanciarse en pieza separada y secreta, la parte particular no tendrá control, ni recibirá comunicación alguna sobre su resultado hasta el cese de la misma, pues únicamente éste derecho recae en la Fiscalía o la Policía Judicial. En consecuencia, la legitimación para la solicitud de las diligencias de investigación únicamente recaen en la Fiscalía y la Policía Judicial, lo cual, esta última

[236] Art. 29 a 36 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad («BOE» Núm. 63, de 14 de marzo de 1986), en la cual, se regula la organización de las Unidades de Policía Judicial.

[237] Así, VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015…* O.P. Cit. Pág. 70-71, en relación con la Circular 1/2019, de 6 de marzo, de la F.G.E, *sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal* («BOE» Núm. 70, de 22 de marzo de 2019), en la conclusión 6. ª, dice expresamente: "Únicamente el Ministerio Fiscal y la Policía Judicial estarán legitimados para instar del Juez de Instrucción medidas de investigación tecnológica. Lo anterior no impide que la acusación particular o popular, a pesar de que la ley no les otorga legitimación, propongan al Juez alguna de estas medidas. En estos supuestos únicamente cabría la adopción de oficio por el Juez, si llega a asumir la propuesta, si bien, en tal caso, la resolución que se dicte será notificada a la parte acusadora en el momento en que se alce el secreto de la pieza separada que habrá de incoarse (art. 588 bis d LECrim) con la finalidad de no frustrar la eficacia de la medida*"*.

engloba tanto las Fuerzas y Cuerpos de Seguridad del Estado (art. 283 LECrim.)[238], cuando posean en sus estructuras unidades orgánicas de Policía Judicial[239], como los Agentes de Vigilancia Aduanera[240] en sus funciones[241] de investigación, persecución y represión de los delitos de contrabando[242], blanqueo de capitales conexo al contrabando, fiscales y otros relacionados con investigaciones patrimoniales.

[238] Acerca de la Policía judicial, ORTIZ PRADILLO, J. C. *El ministerio fiscal y la policía judicial. (Nociones preliminares de derecho procesal penal para criminólogos).* Editorial Atelier. Madrid. 2017. Págs. 33-42; VALLÉS CAUSADA, L. *La policía judicial, un referente en la defensa de los derechos fundamentales en la era de las TIC. (Nuevas tendencias en la interpretación de los derechos fundamentales)*. Universitas Editorial. Madrid. 2015. Págs. 697-716, mantienen que, se deberá concretar las funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente.

[239] La Ley Orgánica 2/1986, de 13 de marzo *de Fuerzas y Cuerpos de Seguridad* otorga como competencia exclusiva de la Policía Judicial a los cuerpos estatales de Cuerpo Nacional de Policía y Guardia Civil, sin embargo, otros cuerpos autonómicos desempeñan también funciones de Policía Judicial. En este sentido, los arts. 13 a 15 de la Ley 10/1994, de 11 de julio, *de la Policía de la Generalidad*, crean unidades de policía judicial dentro de la policía autonómica de Cataluña denominada "*Mossos d'Esquadra";* los arts. 112 a 115 de la Ley 4/1992, de 17 de julio, *de Policía del País Vasco*, crean unidades de policía judicial dentro de la policía autonómica del País Vasco bajo el nombre de "*Ertzaintza"*; el art. 13 de la Ley Foral 8/2007, de 23 de marzo, *de las Policías de Navarra* establece que, la Policía Foral de Navarra o "*Foruzaingoa*" ejercerá las funciones generales de Policía Judicial; el art. 19 de la Ley 2/2008, de 28 de mayo, *del Cuerpo General de la Policía Canaria*, establece que ejercerán funciones de policía judicial en colaboración con las Fuerzas y Cuerpos de Seguridad del Estado.

[240] El Acuerdo del Pleno no Jurisdiccional de la Sala Segunda, adoptado el día 14 de noviembre de 2003, en la aplicación del mismo en la STS 297/2006, de 6 de marzo, así como, la Consulta de la Fiscalía General del Estado Num. 2/1999, 1 de febrero de 1999, consideran a los Agentes de Vigilancia Aduanera como Policía Judicial.

[241] Señalan, MORALES GARCÍA, O. y FERRERES COMELLA, V. "El Servicio de Vigilancia Aduanera como policía judicial la dimensión constitucional del problema". Diario La Ley. Núm. 8666. 2015; FERNÁNDEZ VÁZQUEZ, A. "El Servicio de Vigilancia Aduanero. Problemática sobre su consideración como policía judicial". Boletín del Ministerio de Justicia. Año 63. Núm. 2088. 2009. Págs. 1838-1853, que, los Agentes de Vigilancia Aduanera tienen la consideración de Policía Judicial.

[242] Ley Orgánica 12/1995, de 12 de diciembre, *de represión del contrabando*. («BOE» Núm. 297, de 13 de diciembre de 1995).

En otro orden de ideas, para facilitar la labor a los funcionarios, la norma procesal regula el contenido mínimo que debe comprender la petición al órgano judicial, como si de un formulario se tratara. De esta manera, el contenido de la solicitud comprende, los aspectos formales, como la identidad de los investigados, la duración, los medios de comunicación empleados, pero también, otros de mayor trascendencia, como la descripción del hecho objeto de investigación, la exposición detallada de las razones que justifiquen la medida o los indicios racionales de criminalidad, todo ello encaminado para que el Juez, ponderando los principios rectores examinados *supra*, así como presupuestos establecidos en la ley, valore la justificación de la adopción de la medida.

Seguidamente, vamos a examinar los aspectos que deben contener la petición de autorización judicial para acordar una medida restrictiva de derechos fundamentales (art. 588.2 bis b. LECrim). De este modo, en cumplimiento del principio de especialidad que, como hemos estudiado anteriormente, prohíbe realizar intervenciones prospectivas[243], la petición deberá *concretar el hecho objeto de la investigación* (art. 588.2.1º bis b. LECrim), si bien, no se exige una calificación jurídico penal del hecho, aunque nada impide que se haga una subsunción de los hechos en el tipo penal que corresponda. Además, la solicitud necesariamente deberá contener detalladamente los *motivos que justifiquen acordar la medida* (art. 588.2.2º bis b. LECrim), con el fin de que el Juez pueda ponderar los principios rectores, en especial el de proporcionalidad (art. 588.2 bis b. LECrim). Sin embargo, en ocasiones, la jurisprudencia ha dado validez a la denominada *"autorización o motivación por remisión"*[244], esto es, el Juez en su resolución se limita a integrar en el auto el contenido de la solicitud policial, siendo ésta

[243] STS 870/2012, de 30 de octubre (F.D. 1º).

[244] Sobre la autorización o motivación por remisión en las diligencias de investigación restrictiva de derechos fundamentales, ANDRÉS IBÁÑEZ, P. *Motivación "por delegación" de las decisiones judiciales que limitan derechos fundamentales. (Derecho y justicia penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuéllar García).* Editorial Constitución y Leyes, COLEX. La Coruña. 2006. Págs. 743-761, mantiene que, será conforme a Derecho, cuando el oficio o solicitud, en el cual, se remite el auto habilitante, cumple con todos los presupuestos establecidos en las normas procesales y respeta las garantías constitucionales.

ajustada a Derecho cuando se incorporen todos los requisitos exigidos en la ley[245]. De la misma manera, se exige hacer constar los *indicios de criminalidad*, si bien, equivalen a sospechas fundadas en datos objetivos constatables, pero al encontrarnos en un momento incipiente del proceso penal, no pueden ser comparados con los indicios racionales de criminalidad o de determinación de los hechos punibles a que se refiere el auto de procesamiento (art. 384 LECrim.) o de transformación a procedimiento abreviado (art. 779.1.4º LECrim). También, se precisa hacer constar la *investigación previa a la solicitud*, esto se debe a que, las medidas restrictivas de derechos fundamentales pueden ser el comienzo o el motivo para la incoación de un procedimiento penal, o bien, pueden acordarse dentro de un procedimiento penal en curso, de manera que, la *investigación previa* aludida, comprende las pesquisas llevadas a cabo por la policía o en Fiscalía antes de su remisión al órgano jurisdiccional encargado de la instrucción (por ejemplo seguimientos, denuncias a la policía o fiscalía, etc.), o bien, las distintas investigaciones realizadas en sede judicial. Además, se precisa que figure, la identidad del investigado, así como, siempre que sea posible, cualquier otro sujeto afectado por la medida, esto es, habrá que indicar los sujetos que van a sufrir injerencias en sus derechos fundamentes independientemente de su condición de parte o de tercero (art. 588.2.1º bis b. LECrim). De igual modo, la petición deberá incluir los medios de comunicación empleados (art. 588.2.3º bis b. LECrim), de hecho, resulta irrelevante la titularidad de los terminales o sistemas, dado que únicamente importa la persona que utiliza habitualmente u ocasionalmente los mismos. Asimismo, el Ministerio Público y la Policía Judicial deberá contener *la extensión de la medida con especificación de su contenido* (art. 588.2.4º bis b. LECrim.). Esta exigencia legal tiene por objeto evitar la práctica generalizada de los tribunales con anterioridad a la reforma procesal de 2015 (L.O. 13/2015), pues, con frecuencia, el Juez instructor acordaba "órdenes generales" de injerencia en los derechos fundamentales, es decir, dictaba una autorización judicial sin especificar el alcance concreto de la misma. Por ejemplo, se acordaba un auto de entrada y registro domiciliario, lo cual, aunque no se especificara, se permitía registrar todo lo que se encontraba en la vivienda, incluyendo también, los equipos informáticos o tecnológicos que pudieran ser hallados, o bien, en la diligencia de interceptación no se concretaba que clase de comunicación podría abarcar la injerencia (telefónica o telemática), o bien, si comprendía también, los datos

[245] STS 343/2007, 20 de abril (F.D. 4º) y STS 119/2007, 16 de febrero: (F.D. 3º).

asociados a la misma. También se obliga a los legitimados a fijar en la solicitud u oficio la *duración de la medida* (art. 588.2.7º bis b. LECrim.), con arreglo a los plazos máximos fijados en las normas reguladoras de cada una de ellas (art. 588 bis e. LECrim.), de manera que, esta limitación temporal se produce como consecuencia a que la legislación anterior a la reforma procesal de 2015 en materia de diligencias de investigación fuera insuficiente.

De hecho, una de las deficiencias más notables era en relación con la duración de la medida de interceptación de las comunicaciones telefónicas (art. 579 LECrim. con la redacción dada en virtud de la L.O. 4/1988, de 25 de mayo)[246], pues se establecía un plazo máximo de tres meses, prorrogable por iguales periodos, sin limitación alguna, lo cual, suponía que, en ocasiones estuviera vigente *ad infinitum.* Del mismo modo, a los efectos de control judicial, los agentes actuantes deberán indicar la unidad investigadora de la Policía Judicial que se hará cargo de la intervención (art. 588.2. 5º bis b. LECrim.), así como, proporcionar al órgano jurisdiccional una explicación comprensible de la forma de ejecución de la medida (art. 588.2. 6º bis b. LECrim.), toda vez que, con frecuencia, el Juez es ajeno a las cuestiones técnicas, en especial, las relativas a los medios tecnológicos. Por último, se exige expresar en la petición el *sujeto obligado* (art. 588.2.8º bis b. LECrim), el cual, debe entenderse como los prestadores de servicios de telecomunicaciones, que ostentan el deber de colaboración con la Administración de Justicia, o dicho de otro modo, aquellas empresas que están obligadas a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las comunicaciones, incluso, en caso contrario, pudiendo incurrir en un delito de desobediencia a la autoridad (art. 588 ter e LECrim).

[246] Advierten sobre las deficiencias en la regulación de las medidas restrictivas de derechos fundamentales con arreglo al art. 579 LECrim, conforme a la redacción dada, anterior a la reforma del 2015, RODRÍGUEZ LAINZ, J. L. "Peculiaridades de la intervención judicial de comunicaciones electrónicas*"*. Diario La Ley. Núm. 7125. 2009; MUÑOZ DE MORALES ROMERO, M. "Hacia la cobertura legal de las intervenciones telefónicas en el Ordenamiento Jurídico Español, la reforma del artículo 579 LECrim." BFD: Boletín de la Facultad de Derecho de la UNED. Núm. 27. 2005. Págs. 47-92.

b) Resolución judicial

Una vez obtenida la solicitud de medidas de investigación tecnológica, el Juez de instrucción competente decidirá mediante auto la adopción de la misma en el plazo de veinticuatro horas (art. 588.1 bis c. LECrim), si bien, como nos hemos referido *supra*, no existe impedimento alguno para que el propio Juez, de oficio, si lo entendiere necesario para el buen fin de la investigación, pueda acordar alguna diligencia, de manera que, en este caso, como es obvio, no se cumpliría el trámite de solicitud referido. Sin embargo, cuando el Juez creyera que el contenido de la solicitud es insuficiente, en especial, en lo referente a los motivos relacionados con los principios rectores, podrá requerir aclaración o ampliación al Fiscal o a la Policía Judicial, si bien, en este caso, se interrumpirá el plazo hasta que obtenga respuesta. De la misma forma, la norma procesal exige la intervención preceptiva del Fiscal, el cual, deberá informar, con carácter previo a la resolución judicial, sobre la conveniencia de su adopción (art. 588.1 bis b. LECrim.), si bien, no será vinculante para el Juez instructor. Dicho lo anterior, se trae a colación la polémica jurisprudencial[247] suscitada con anterioridad a la reforma procesal implementada con la ley del 2015, acerca de si resulta necesario comunicar formalmente al fiscal la adopción de las medidas restrictivas de derechos fundamentales, no obstante, su intervención resulta ahora incuestionable con la nueva regulación. De esta manera, se pretende someter a control las injerencias en los derechos fundamentales, por parte del órgano encargado de velar por los intereses públicos (art. 3 EOMF)[248], pero además, se trata de evitar la incoación de procedimientos penales, con medidas restrictivas de derechos fundamentales acordadas en el mismo, o con la intervenciones prospectivas ajenas a cualquier control, por ejemplo iniciando una investigación sin especificar el delito concreto mediante la incoación de un procedimiento penal con la fórmula de "*diligencias indeterminadas*".

[247] STC 197/2009, de 28 de septiembre (F.J. 7º); STS 309/2010, 31 de marzo (F.D. 2º).

[248] Señala, ÁLVAREZ SUÁREZ, L. *El ministerio fiscal y las diligencias de investigación tecnológica (FODERTICS 6.0: los nuevos retos del derecho ante la era digital).* Editorial Comares. Granada. 2017. Págs. 117-125, que, el Ministerio Fiscal debe velar por los intereses públicos cuando se acuerde una diligencia de investigación restrictiva de derechos fundamentales.

En cualquier caso, la autorización y la denegación de la medida de investigación debe ser motivada (arts. 588.1 bis c, 579.2[249] y 558 LECrim.). En efecto, la exigencia legal de motivación supone que el Juez debe exteriorizar los criterios que justifican su decisión, para dar a conocer los razonamientos fácticos y jurídicos de la medida a las partes[250], permitiendo con ello ejercer el derecho de defensa y facilitar la interposición de eventuales recursos. Además, como mantiene nuestro Tribunal Constitucional, la falta de motivación suficiente[251] puede derivar en la nulidad de la diligencia de investigación[252], toda vez que, se atenta contra el derecho a la tutela judicial efectiva (art. 24.1 CE), así como con el deber de motivación de las resoluciones limitativas de los derechos fundamentales. Sin embargo, aunque la autorización judicial deba ser exhaustiva e individualizada, lo cierto es que, como ya se ha comentado, la doctrina mayoritaria permite la motivación por remisión al oficio de los agentes de policía o solicitud del Ministerio Fiscal[253], esto, seguramente se debe a que normalmente el Juez desconoce más hechos que los proporcionados por la Policía Judicial o la Fiscalía, lo cual, la decisión judicial se limitará a resolver sobre la pertinencia o necesariedad de la medida. No obstante, para la validez por remisión del oficio policial o solicitud de fiscalía, deberá contener los *elementos necesarios*, en especial, los principios rectores, *a efectos de considerar satisfechas las exigencias de ponderación de la restricción de*

[249] La redacción del art. 579 de la LECrim. tras la reforma implementada con arreglo al art. segundo de la Ley Orgánica 4/1988, de 25 de mayo, *de reforma de la Ley de Enjuiciamiento Criminal*, se trata de la primera regulación en el ordenamiento jurídico español de la medida de interceptación en las comunicaciones telefónicas, de tal forma que, se establecía expresamente que, para su adopción, la resolución judicial debía ser motivada.

[250] Auto TS, de 18 junio 1992 (F.J. 4º); STC 150/2006, de 22 mayo (F.J. 3º).

[251] En efecto, LEAL MEDINA, J. "La motivación de las resoluciones penales, parámetros de validez formal y material*"*. Diario La Ley. Núm. 8.576. 2015, mantiene que, la falta de motivación provocaría la nulidad de la decisión, con arreglo al art. 11 LOPJ.

[252] STC 54/1996, de 26 marzo (F.J. 7º); STC 85/1994, de 14 marzo (F.J. 3º); STC 123/1997, de 1 julio (F.J. 3º).

[253] La motivación por remisión, ha sido aludido anteriormente en las resoluciones que se reseñan a continuación: STS Núm. 343/2007, 20 de abril; STS Núm. 119/2007, 16 de febrero de 2007; STS Núm. 1229/1998, 15 de octubre… O. P. Cit.

derechos fundamentales[254], si bien, aunque contenga una transcripción literal del oficio o solicitud, el Juez deberá hacer una valoración ponderada e individualizada de los hechos, lo cual, supone que se excluyan todas las solicitudes basadas en formularios estereotipados o de referencias genéricas[255].

Por otro lado, para facilitar la labor del Juez de instrucción en el momento de acordar una medida tecnológica, y no incurrir en graves defectos, que pudieran conllevar, incluso a la nulidad, el legislador ha previsto, como si de un formulario se tratara, una enumeración de extremos que al menos deberá incluir la resolución judicial (art. 588.3 bis c. LECrim).

Seguidamente, se expondrá los distintos extremos que debe contener como mínimo la resolución judicial, siendo esta enumeración *numerus apertus*, lo cual, implica que pueden ser incluidos otros a criterio judicial. Así, se procederá a exponer los siguientes aspectos de la autorización judicial.

a´. El hecho punible objeto de investigación y su calificación jurídica.

La autorización judicial deberá concretar el hecho punible, sin embargo, de ordinario, la diligencia de investigación se adopta en un momento *in limine* del proceso penal, es decir, en una etapa inicial del mismo, lo cual, el conocimiento de los hechos delictivos no se produce en toda su magnitud. De esta manera, la delimitación de los hechos punibles se produce de forma paulatina[256], mientras se avanza la investigación o se llevan a cabo determinadas diligencias, esto es, lo que nuestro Tribunal Supremo ha venido a denominar "*cristalización progresiva"*[257]. Sin embargo, según el principio rector de especialidad, la concreción del *factum* o hecho punible determinado en la resolución habilitante de la medida no puede sufrir alteraciones sustanciales, pues en

[254] STC 166/1999, de 27 de septiembre (F.J. 7º); STC 299/2000, de 11 de diciembre (F.J. 4º).

[255] STS 1316/1995, de 30 diciembre, alude a la irregularidad en motivar las resoluciones judiciales con formularios estereotipados o referencias genéricas.

[256] STS 248/2012, de 12 de abril (F.D. 8º); STS 433/2012, de 1 de junio (F.D. 3º).

[257] STS 385/2011, 5 de mayo (F.D. 6º) y STS 412/2011, 11 de mayo (F.D. 6º).

caso contrario, la diligencia podría incurrir en nulidad (art. 11.1 LOPJ). De este modo, no existe infracción al principio de especialidad de la resolución cuando se respeta el bien jurídico protegido, aunque se modifiquen elementos accesorios, como por ejemplo, se acuerda una medida para pretender descubrir un delito de pornografía infantil, cuando finalmente se aprehende material de personas con discapacidad necesitada de especial protección, de manera que, en ambos supuestos el bien jurídico protegido "libertad e indemnidad sexual" queda inalterado, y la resolución judicial es ajustada a Derecho, pese a sufrir una variación no sustancial respecto a los hechos.

Estrechamente relacionado con lo anterior, traemos a colación, el problema que surge cuando al ejecutar una medida de investigación restrictiva de derechos fundamentales para un determinado hecho delictivo, los investigadores detectan casualmente la comisión de otro delito distinto no previsto en la resolución[258]. De esta manera, aunque esta cuestión será examinada profusamente cuando se analicen las medidas específicas, queda aquí únicamente apuntado que, cuando se produce un hallazgo casual de un delito distinto que el previsto en la autorización judicial, la jurisprudencia venía entendiendo que en las medidas de interceptación de las comunicaciones telefónicas y telemáticas se exige una nueva motivación ampliatoria que comprenda la justificación de la investigación en el propio procedimiento o en otro distinto del nuevo delito. De este modo, para continuar con la investigación de un delito nuevo y sorpresivo, habrá que ampliar el contenido de las escuchas mediante una nueva resolución judicial que legitime la intervención telefónica o telemática[259]. Esta cuestión, la denominada *doctrina del hallazgo casual* ha sido incorporada por el legislador en nuestro ordenamiento jurídico, al expresar en la LECrim que, *la continuación de la medida para*

[258] 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. Núm. 40. 2016; GARCÍA SAN MARTÍN, J. "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 109. 2014. Pág. 10; PÁRAMO Y DE SANTIAGO, C. "Entrada y registro: hallazgo casual". CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 132. 2012. Págs. 143-148; RIVERO ORTIZ, R. "Hallazgos casuales en los delitos y faltas, nuevos pronunciamientos jurisprudenciales". Diario La Ley. Núm. 7846. 2012; ECHARRI CASI, F. J. "Prueba ilícita, conexión de antijuridicidad y hallazgos casuales". Revista del Poder Judicial. Núm. 69. 2003. Págs. 261-301.

[259] STS 777/2012, de 17 de octubre y STS 616/2012, de 10 de julio.

la investigación del delito casualmente descubierto requiere autorización del Juez competente, para la cual, éste 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 (arts. 579.3 bis y art. 588 bis i de la LECrim). Cosa distinta es, el tratamiento procesal de los hallazgos casuales en la diligencia de investigación de entrada y registro en un domicilio (art. 545 LECrim. y sig.), de modo que, al acceder a un domicilio en un registro autorizado judicialmente para la investigación de un delito concreto, se advierte la comisión de otro delito distinto, por ejemplo, se realiza un registro domiciliario por narcotráfico, y se halla sorpresivamente un fallecido a causa de un disparo. Para este supuesto, la jurisprudencia ha ido perfilando el tratamiento del hallazgo casual, pues, inicialmente se entendía que al descubrir delitos no amparados por la autorización judicial, el registro debía suspenderse y dar inmediato traslado al Juez competente, para que decidiera sobre la conveniencia de extender el mandamiento a los nuevos hechos delictivos encontrados[260]. Sin embargo, la tesis rigorista ha sido superada, al dar validez a resoluciones judiciales que no contienen los delitos hallados sorpresivamente, pues la jurisprudencia mayoritaria mantiene que, la policía actuante al entrar en un domicilio no puede vendarse los ojos para no percibir el posible cuerpo o efecto de otro delito que allí se le pusiera de manifiesto. Sin duda, la Constitución española permite que, en caso de flagrancia delictiva (art. 18.2 CE), es decir, en el momento de cometer un delito, recién cometido o sorprendido inmediatamente después de haberlo cometido, pueda accederse al domicilio para su investigación, sin necesidad de autorización judicial. Por este motivo, el argumento expuesto concluye que, la protección constitucional del domicilio no se extiende a los delitos flagrantes, en consecuencia, se permite investigar el nuevo hecho delictivo, sin necesidad de acordar una nueva resolución judicial que contenga las novedades punitivas encontradas, en aplicación de la dispensa constitucional mencionada[261]. Además, en este mismo sentido, no faltan sentencias que afirman que,

[260] STS 2306/1992, de 28 octubre, dispone que, cuando en la práctica de una diligencia de entrada y registro se descubren otros delitos, para poder proceder a su investigación, se precisa de habilitación judicial.

[261] STS 578/1995, de 28 abril, se viene a aplicar el criterio de flagrancia, con el objeto de dispensar de la necesidad de ampliar la resolución judicial ante el nuevo delito descubierto en una entrada y registro domiciliario.

cuando la autorización respeta las exigencias y previsiones legales y constitucionales, en especial el principio de proporcionalidad, la práctica del registro tiene plena validez. De igual modo, nuestros tribunales sostienen que, el principio de proporcional se respeta cuando se trata de un delito grave, toda vez que, la concesión de una autorización habilitante de invasión domiciliaria de las personas sospechosas se justifica autónomamente sin necesidad de ampliar la resolución inicial[262]. Por otro lado, los funcionarios de policía tienen siempre el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuvieren conocimiento, practicando incluso las diligencias de prevención que fueran necesarias por razón de urgencia, por lo que, cuando los agentes encuentren hechos delictivos no previstos inicialmente no pueden dejar de proceder a su investigación[263]. En definitiva, lo que realmente otorga validez a la práctica del registro es la correcta habilitación judicial, una vez cumplido tal requisito esencial, la actuación policial discurre en un ámbito perfectamente legítimo, de modo que, cualquier hallazgo que se produzca no puede ser tachado de ilícito, dada la legalidad en que discurre la diligencia, siempre que concurra una proporción entre la injerencia en el derecho fundamental y la gravedad del ilícito inesperadamente descubierto. De tal forma que, el hecho de hallar, en un registro domiciliario, válido y autorizado en su origen, efectos u objetos distintos de los correspondientes al ilícito inicialmente investigado, no convierte en ilegítima la práctica de la diligencia realizada. Por este motivo, lo realmente importante es que la autorización de registro domiciliario sea ajustada a Derecho, respetando los requisitos exigidos en la ley, de tal forma que, una vez cumplida dicha exigencia, los hallazgos encontrados desplegarán en el propio o distinto proceso pleno valor probatorio, sin necesidad de ampliar la resolución judicial habilitante[264].

Asimismo, la resolución judicial, además de contener el hecho punible objeto de investigación, deberá realizar una calificación jurídica de los mismos. No obstante, como ha sido mencionado anteriormente, esta exigencia de subsunción de los hechos en un tipo penal concreto, no era predicable en la solicitud del Ministerio Público u oficio

[262] STS 91/1999, de 1 febrero (F.D. 1º).

[263] STC 41/1998, de 24 febrero.

[264] STS 981/2003, de 3 julio (F.D. 2º).

de la Policía Judicial, pues, seguramente se debe, a que el Juez, como jurista encargado de dirigir la investigación, debe ponderar la gravedad de los hechos, para lo cual, deberá tomar como primera cuestión a tener en cuenta, la pena en abstracto asociada. De igual modo, la calificación jurídica de los hechos permite observar si los delitos cometidos corresponden a los presupuestos dados en la ley, pues, por ejemplo, la medida de interceptación de las comunicaciones telefónicas y telemáticas (art. 579.1 por remisión del art. 588 ter a. LECrim), como después se estudiará, únicamente puede ser acordada para determinados delitos[265].

Por último, la resolución judicial deberá expresar los indicios racionales en los que se funde la medida, sin embargo, al tratarse de una medida normalmente adoptada en los inicios de un proceso penal, siendo está además, acordada para descubrir la actividad delictiva (se adoptan medidas para investigar hechos que no se conocen plenamente, toda vez que, si se conocen plenamente los hechos la medida resulta innecesaria), no debe exigirse gran precisión o exhaustividad de los indicios, sino únicamente será necesaria hacer constar en la autorización judicial sospechas fundadas en datos objetivos constatables.

b´. La identidad de los investigados y de cualquier otro afectado por la medida

De igual modo, la resolución judicial autorizante de las medidas, como ámbito subjetivo, precisa hacer constar la identificación del investigado, así como, delimitar a todos los que eventualmente pudieran verse afectados. De esta manera, pueden acordarse medidas tecnológicas que incidan en terceras personas en los casos y con las condiciones reguladas en las disposiciones específicas de cada una de ellas (art. 588 bis h LECrim). Por su parte, cuando la medida esté relacionada con elementos informáticos o de telecomunicaciones, como sucede con la interceptación de las comunicaciones (art. 588 ter LECrim.), la intervención puede recaer en uno o más terminales de titularidad del sujeto pasivo, o también, aquellos otros que únicamente lo utilice como usuario, esto

[265] Art. 579.1 por remisión del art. 588 ter a. LECrim contiene los presupuestos de una medida de interceptación de las comunicaciones, y en concreto, viene a establecer que, se podrá acordar únicamente para delitos dolosos con pena con límite máximo de tres años de prisión, cometidos en un grupo u organización criminal, terrorismo, delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

es, los dispositivos utilizados de forma ocasional y no ostente la titularidad de los mismos. Esto se debe, a que, con frecuencia, los autores de los delitos, para intentar eludir la acción de la justicia, utilizan dispositivos que están a nombre de otras personas. En cualquier caso, la resolución judicial deberá motivar la decisión de haber adoptado una medida restrictiva de derechos fundamentales sobre un terminal ajeno al investigado. Además, puede suceder que, el investigado se sirva de un tercero sin conocimiento de aquel de dicha situación, o bien, el propio tercero colabore con la actividad delictiva, lo cual, en este último supuesto, podría derivar en responsabilidad penal, al menos como cómplice (art. 29 CP).

No obstante, no faltan ejemplos en la jurisprudencia que, han dado validez a medidas adoptadas sin hacer constar en la resolución autorizante, los datos de identidad de los afectados, pues dada la tecnología actual (por ejemplo, con tarjetas prepago o manipulación de los dispositivos), averiguar la identidad de los titulares o usuarios de los terminales puede ser de gran complejidad para los investigadores. Por este motivo, esta exigencia legal, puede resultar desproporcionada y gravemente perturbadora para la investigación, especialmente para delitos graves, pues, en ocasiones, la propia medida será acordada con el fin de identificar a los titulares o usuarios de los dispositivos, o incluso, otros delincuentes relacionados con la actividad delictiva. En cambio, nuestros tribunales, vienen rechazando la nulidad de la medida por indeterminación subjetiva[266], pues se trata de una irregularidad procesal, que no afecta a los derechos fundamentales.

De igual modo, la legitimidad de la medida no sufre alteración alguna, cuando las personas que inicialmente fueron investigadas y sufrieron la injerencia en sus derechos fundamentales, después quede acreditada la falta de implicación en los hechos, y en consecuencia, se acuerde el sobreseimiento y archivo de las actuaciones, pues la investigación se va delimitando de forma paulatina, en función del resultado de las diligencias de investigación practicadas (como nos hemos referido anteriormente, la denominada por el Tribunal Supremo "*cristalización progresiva"*), toda vez que, tienen por finalidad averiguar y hacer constatar la perpetración de los delitos, dejando para la

[266] STS 712/2012, de 26 septiembre (F.D. 2º).

fase intermedia el momento procesal para decidir que personas deben ser objeto de acusación[267].

c´. La extensión y alcance de la medida de injerencia

Con anterioridad a la reforma procesal implementada con la L.O. 13/2015[268], no existía precepto alguno, que regulara el contenido de la resolución judicial de la medida, sino que se dejaba íntegramente a la discrecionalidad judicial la motivación de la decisión. Por este motivo, con frecuencia, los jueces de instrucción no detallaban suficientemente la extensión de la medida de injerencia, pues en algunas resoluciones no se especificaba el alcance de la restricción en los derechos fundamentales. De esta manera, la fundamentación de la medida no puede consistir en una motivación implícita, esto es, la injerencia no puede abarcar todo tipo de restricciones, sino que se debe determinar con carácter previo a su adopción, el alcance de la misma. Como nos hemos referido anteriormente, existía una práctica generalizada por los juzgados en adoptar resoluciones autorizantes de entradas y registros domiciliarios, en las cuales, aunque no se hiciera constar expresamente, permitía inspeccionar todos los objetos que se encontraran en la misma, incluso los dispositivos electrónicos o informáticos, o bien, la resolución que acordaba una intervención en las comunicaciones telefónicas, se extendía además, a las comunicaciones telemáticas, pese a no precisar dichos extremos en el auto. Por este motivo, la reforma del 2015 ha despejado todas las dudas, al establecer la obligación de los jueces a detallar la extensión y el alcance de la injerencia,

[267] Sobre la "*cristalización progresiva*" en las diligencias de investigación restrictiva de derechos fundamentales, véase, STS 385/2011, de 5 de mayo y STS 412/2011, 11 de mayo. O.P. Cit.

[268] Advierten, GUTIÉRREZ ROMERO, F. M. "Algunas claves de la reforma de la Ley de Enjuiciamiento Criminal*"*. Revista Aranzadi Doctrinal. Núm. 2. 2016. Págs. 69-90; BUENO DE MATA, F. "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 [BOE n.º 239, 6-X-2015]*"*. Ars Iuris Salmanticensis: AIS: Revista Europea e Iberoamericana de Pensamiento y Análisis de Derecho, Ciencia Política y Criminología. Vol. 4. Núm. 1. 2016. págs. 326-328; MISMO AUTOR. "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*"*. Diario La Ley. Núm. 8627. 2015, sobre la deficiente regulación de las medidas de investigación con la legislación anterior a la reforma implementada en el 2015.

en la cual, se deberá precisar con exactitud el grado de afectación en los derechos fundamentales. En consecuencia, aunque se estudiará con más detalle en la parte del presente trabajo dedicada a las medidas específicas, para los registros domiciliarios, habrá que hacer constar expresamente si alcanza la autorización a los dispositivos de almacenamiento masivo de información (art. 588 sexies a. LECrim.), esto es, los equipos informáticos o terminales de telecomunicaciones que se encuentren en la vivienda, o bien, en la interceptación en las comunicaciones telefónicas habrá que indicar si la autorización comprende también, las telemáticas y los datos asociados o metadatos de las mismas, por entender que se debe garantizar el derecho al entorno virtual.

d´. La unidad investigadora de Policía Judicial que se hará cargo de la intervención.

El Juez de instrucción que autoriza una medida restrictiva de derechos fundamentes debe conocer previamente la unidad encargada de la ejecución, para ello, como nos hemos referido anteriormente, la solicitud u oficio del Ministerio Público o la Policía Judicial, deberá precisar la identificación de la unidad investigadora de la Policía Judicial (art. 588.2.5º bis b LECrim.). En consecuencia, la resolución autorizante de la medida deberá hacer constar también expresamente dicho extremo, con el fin de que pueda ser verificado en todo momento de la ejecución, toda vez que, el control judicial abarca también quienes llevan a cabo la misma. Sin embargo, como mantiene Marchena Gómez[269], las imprecisiones en la identificación de los agentes de Policía Judicial en la decisión judicial, puede no constituir una infracción constitucional que origine la nulidad de acuerdo con el art. 11 LOPJ, si bien, inevitablemente, supondrá que se vea mermado el control judicial de la medida.

e´. La duración y prórroga de la medida.

La duración máxima de una medida restrictiva de derechos fundamentales es una novedad implementada con la L.O. 13/2015, pues, como ya nos hemos referido, con la

[269] Señala MARCHENA GÓMEZ, M. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*... O.P. Cit. Pág. 263, que, la falta de precisión en la identificación de los agentes de Policía Judicial encargados de ejecutar la medida, no supone una infracción constitucional, si bien, acarreará una merma en el control judicial.

legislación anterior, no se establecía límite alguno, sino que, el Juez podía acordar la interceptación de las comunicaciones postales, telegráficas o telefónicas por un plazo de hasta tres meses, prorrogable por iguales períodos (antiguo art. 579.3 LECrim.)[270], lo cual, suponía que mediante sucesivas prórrogas, podía intervenirse las comunicaciones durante un largo periodo de tiempo sin restricción alguna. De igual modo, el ordenamiento jurídico carecía de una regulación específica sobre la interceptación de las comunicaciones telemáticas, así como de otras medidas restrictivas de derechos fundamentales, lo cual, hacía que se aplicara las disposiciones reguladoras de la intervención en las comunicaciones telefónicas (antiguo art. 579 LECrim.) para todos los supuestos, ocasionando un vacío legal que, era completado por la jurisprudencia emanada de nuestro Tribunal Supremo y el Tribunal garante de la Constitución. Sin embargo, la duración de la medida *sine die* no parecía muy respetuosa con las garantías constitucionales, por lo que resultaba imprescindible fijar un plazo máximo. Por este motivo, el panorama jurídico descrito sufrió un cambio radical con la legislación implementada con arreglo a la reforma procesal de 2015[271], al establecer que, la duración de la medida será la que se especifique para cada una de ellas (arts. 588.3.e. bis c. en relación con el 588.1 bis e. ambos de la LECrim.).

De la misma manera, la duración de la medida no podrá exceder del tiempo imprescindible para el esclarecimiento de los hechos, por lo que, si antes de llegar a término, se observara que se han descubierto los delitos investigados, o bien, se ha descartado la actividad delictiva, no resultara justificado agotar los plazos. Sin embargo, en el supuesto de que sea necesario acordar una prórroga, será adoptada, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la

[270] En relación a la imprecisa regulación de la interceptación de las comunicaciones, con arreglo a la redacción antigua del art. 579 LECrim, GIMENO SENDRA, J. V. "La intervención de las comunicaciones..." O.P. Cit; RODRÍGUEZ LAINZ, J. L. "Peculiaridades de la intervención judicial de comunicaciones electrónicas..." O.P. Cit. ponen de manifiesto que, la medida podía ser acordada sin límite temporal alguno, lo cual, venía a ocasionar, una infracción en los derechos fundamentales.

[271] Acerca de la duración de las medidas tecnológicas, FUENTES SORIANO, O. *El proceso penal cuestiones fundamentales*. Editorial Tirant lo Blanch. Valencia. 2016. Pág. 277-337; GIMENO BEVIÁ, J. "Análisis crítico de la reforma de LECrim 2015*"*. Revista de Derecho y Proceso Penal. Núm. 40. 2015. Págs. 185-216, indican que, la restricción temporal de la mismas, supone el respeto de las garantías constitucionales.

motivaron. En el caso de que la prórroga no sea acordada de oficio, la petición será efectuada por el Ministerio Fiscal o la Policía Judicial[272] con suficiente antelación, haciéndose constar el resultado de la medida, así como la justificación de los motivos de la continuación de la misma, para ello, se entregará al Juez un informe documentado que incluya las transcripciones del contenido con el resultado de la investigación, para que el Juez, pueda valorar la conveniencia de la continuación de la diligencia, debiendo resolver éste, en el plazo de dos días desde la presentación de la solicitud u oficio (art. 588 bis f. LECrim.). En cambio, cuando transcurra el plazo, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos, lo cual, conlleva que, toda actuación que exceda la habilitación será nula de pleno derecho (art. 588 bis e. LECrim.).

En otro orden de ideas, con carácter formal, la adopción de las distintas prórrogas, deberán ser mediante auto motivado (art. 588.2 bis e LECrim.), pues, el legislador ha hecho suya la reiterada jurisprudencia constitucional sobre esta cuestión[273].

f´. Control judicial de la medida

El Juez velará por el cumplimiento de la medida, de manera que, tiene por objetivo controlar que sean respetadas las garantías constitucionales, para ello, habrá de fijar en la resolución los términos en que la unidad de Policía Judicial encargada de su ejecución informe de su desarrollo. En consecuencia, la resolución judicial deberá contener la forma y la periodicidad en que los agentes actuantes deban dar traslado al Juez de la información sobre el desarrollo y el resultado de la medida, y, en todo caso, cuando por cualquier causa se ponga fin a la misma (arts. 588.3.f) bis c. y el 588 bis g. LECrim.).

[272] Respecto a la solicitud de la prórroga en las diligencias de investigación efectuada por la Policía Judicial, LLORENTE DE PEDRO, P. A. "Las diligencias policiales en la reforma de 2015 de La Ley de Enjuiciamiento Criminal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 118. 2016, señala que, "la autorización de la intervención inicial no será mayor a tres meses, plazo que se antoja para delitos e investigaciones complejas quizá insuficiente, al igual que con las prórrogas no se puedan superar los 18 meses*"*.

[273] STC 181/1995, de 11 diciembre (F.J. 4º); STC 25/2011, de 14 marzo (F.J. 2º) y STC 202/2001, de 15 de octubre (F.J. 5º).

De esta manera, el Juez tiene como cometido supervisar la medida desde la adopción hasta su cese.

Sin ánimo de ser exhaustivo, toda vez que, será objeto de estudio en la parte del presente trabajo dedicada a las medidas de aseguramiento y prueba pericial informática, cuando se trate de una diligencia de interceptación de las comunicaciones telefónicas y telemáticas, la Policía Judicial deberá poner a disposición del Juez, bajo custodia del Letrado de la Administración de Justicia, dos soportes digitales, uno con la transcripción de los pasajes que considere de interés y otro con las grabaciones íntegras realizadas, a los efectos de que en cualquier momento puedan ser cotejadas. Además, para garantizar que la interceptación de las comunicaciones no ha sufrido alteración alguna, se deberá hacer constar el origen y destino de cada una. De esta manera, se deberá respetar la cadena de custodia de las grabaciones realizadas, o también, denominado procedimiento controlado de los vestigios relacionados con el delito, esto es, las comunicaciones intervenidas contenidas en los soportes digitales, desde que se obtiene la información, hasta que llegan a la fase de plenario para su valoración judicial, deben ser exactamente lo mismo, es decir, sin haber sufrido adulteración o contaminación alguna[274]. De igual modo, se habrá de realizar un encriptado electrónico

[274] Acerca de la cadena de custodia, con carácter general, véase, LEAL MEDINA, J. "Ruptura de la cadena de custodia y desconexión con las fuentes de prueba supuestos concretos, reflexiones que plantea". Diario La Ley. Núm. 8.846. 2016; RUBIO ALAMILLO, J. "Conservación de la cadena de custodia de una evidencia informática". Diario La Ley. Núm. 8.859. 2016; GARCÍA MATEOS, J. A. *Cadena de custodia vs mismidad*. *(La prueba electrónica, validez y eficacia procesal). La Prueba Electrónica*. Editorial Juristas con Futuro. Desafíos Legales. Madrid. 2016. Pág. 130; FIGUEROA NAVARRO, M. C. "La cadena de custodia en el proceso penal". EDISOFER. Madrid. 2015; RICHARD GONZÁLEZ, M. "La cadena de custodia en el proceso penal español". Diario La Ley. Núm. 8.187. 2013; DEL POZO PÉREZ, M. "La cadena de custodia. Tratamiento jurisprudencial". Revista General de Derecho Procesal. Núm. 30. 2013; LACUEVA BERTOLACCI, R. "La importancia de la cadena de custodia en el proceso penal". La Ley. Núm. 8.071. 2013; FIGUEROA NAVARRO, M. C. "El aseguramiento de las pruebas y la cadena de custodia". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 84. 2011. Pág. 1; MAGRO SERVET, V. "Cadena de Custodia y Prueba de Cargo". Diario La Ley. Núm. 6.863. 2008.

con algoritmo *hash*[275] que garantice la autenticidad e integridad de la información volcada del ordenador central o sistema informático denominado con el acrónimo SITEL[276] a los soportes digitales en que las comunicaciones hubieran sido grabadas (art. 588 ter f. LECrim)[277].

[275] PEREIRA I PUIGVERT, S. *Sistema de "hash" y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas "inaudita parte". (FODERTICS II: hacia una justicia 2.0)*. Editorial Ratio Legis. Salamanca. 2014. Págs. 75-83.

[276] Sistema Integrado de Interceptación de Telecomunicaciones (SITEL) ha sido respaldado por la STS 250/2009, de 13 marzo. Asimismo, con carácter general, véase, RUIZ DORADO, M., VIDAL MARÍN, T. "Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de Reforma de la Ley de Enjuiciamiento Criminal*"*. Revista Aranzadi Doctrinal. Núm. 9. 2016. Págs. 135-162; RODRÍGUEZ LAINZ, J. L. "SITEL nuevas tendencias, nuevos retos*"*. Diario La Ley. Núm. 8.082. 2013; MISMO AUTOR. "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas*"*. Diario La Ley. Núm. 7.689. 2011; MISMO AUTOR. "Consideraciones jurídicas en torno a la licitud constitucional de SITEL*"*. Diario La Ley. Núm. 7.344. 2010; MISMO AUTOR. L. *De vueltas con SITEL*. Diario La Ley. Núm. 7.515. 2010; CASTILLEJO MANZANARES, R. "Medios de investigación en la lucha contra la criminalidad organizada*"*. Revista General de Derecho Procesal. Núm. 27. 2012; FERNÁNDEZ RODRÍGUEZ, J. J. *La intervención de las comunicaciones digitales a propósito del sistema SITEL. (Cuestiones de inteligencia en la sociedad contemporánea)*. Editorial del Ministerio de Defensa. Madrid. 2011. Págs. 61-76; "Nuevo respaldo al Sistema Integral de Interceptación de Comunicaciones Electrónicas*"*. Diario La Ley. Núm. 7.350. 2010; JORGE MARTÍNEZ FERRÍZ, J. L. "La operatividad de SITEL su discutida legalidad dentro de un Estado de derecho que actúa bajo el imperio de la ley*"*. Diario La Ley. Núm. 7.434. 2010; BELÉN DEL POZO, A. *Escuchas telefónicas dudas y certezas respecto a la interceptación de comunicaciones por SITEL*. Iuris: Actualidad y Práctica del Derecho. Núm. 146. 2010. Págs. 6-9; PULIDO QUECEDO, M. "El programa SITEL y las escuchas de las comunicaciones. Apuntes de la STS (2ª), de 5 de noviembre de 2009*"*. Revista Aranzadi Doctrinal. Núm. 9. 2010. Págs. 89-95; MISMO AUTOR. "Jurisprudencia. Tribunal Supremo. Interceptación de las comunicaciones (SITEL). Derecho de los Negocios. Año Núm. 21. Núm. 232. 2010". Págs. 64-66; ZOCO ZABALA, C. "Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE*"*. Revista para el Análisis del Derecho. Núm. 4. 2010. 17 Págs; DOLZ LAGO, M. J. "¿Hacia una jurisprudencia electrónica? breves reflexiones sobre SITEL". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 74. 2010. Pág. 5; MISMO AUTOR. *Problemática de SITEL*. Estudios Jurídicos. 2010.

[277] STS 1215/2009, de 30 diciembre: Voto Particular de Manuel Marchena Gómez, al que se adhiere José Manuel Maza Martin, en el cual, expone la forma de realizar el volcado con garantías.

Por su parte, respecto al control judicial en el seguimiento de la medida, la jurisprudencia de nuestro Tribunal Constitucional, en contrariedad con la ley vigente, venía manteniendo que, no era necesario que la Policía Judicial remitiera las transcripciones íntegras y las cintas originales, así como que, el Juez procediera a la audición de las mismas, sino que resultaba suficiente el conocimiento de los resultados obtenidos a través de las transcripciones más relevantes y de los informes policiales. Además, el Tribunal garante de la Constitución[278] diferenciaba las irregularidades cometidas en los derechos fundamentales de privacidad e intimidad (art. 18 CE), de aquellas otras que, afectaban al valor probatorio de los resultados obtenidos sin el debido control judicial. No obstante, con la nueva regulación, no cabe duda que, el control judicial debe estar sometido a las garantías establecidas en la ley, si bien, no es posible dar el mismo tratamiento a las violaciones en los derechos fundamentales, que las deficiencias cometidas en el control judicial, que únicamente afectan al valor probatorio de la medida.

De la misma manera, lo mencionado anteriormente sobre el control y la autenticidad de la medida, también resulta predicable para otras diligencias de investigación, como en el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.), si bien, únicamente queda aquí indicado, puesto que, será objeto de estudio en su lugar correspondiente.

g´ La finalidad perseguida con la medida.

La resolución judicial que autorice la medida deberá contener una breve explicación sobre lo que se pretende obtener con la misma. Sin embargo, al encontrarnos en un momento inicial de la investigación no se debe exigir que la información sobre la finalidad perseguida sea extremadamente precisa, si bien, tampoco debe suponer que, la explicación se circunscriba a fórmulas estereotipadas.

h´. El sujeto obligado que llevará a cabo la medida.

Las empresas prestadoras de servicios de telecomunicaciones o de redes públicas de comunicación poseen numerosos datos de sus usuarios (metadatos), que les sirven, entre

[278] STC 82/2002, de 22 de abril (F.J. 6º).

otras cuestiones, para la facturación del servicio. De esta manera, la información de que disponen estas operadoras resulta de gran utilidad al Estado para la averiguación e investigación de los delitos. Por este motivo, las empresas prestadoras de servicios de la información vienen obligadas a prestar al Juez, al Ministerio Fiscal o a los agentes de la Policía Judicial la colaboración precisa para facilitar el cumplimiento de las medidas tecnológicas, incluso en caso contrario podrían incurrir en delito de desobediencia a la autoridad judicial (art. 556 CP). En consecuencia, siempre que sea necesaria la colaboración de esta clase de operadoras para llevar a cabo la diligencia de investigación, se hará constar expresamente en la resolución judicial el nombre de la misma.

3) El secreto

La efectividad de las medidas tecnológicas restrictivas de derechos fundamentales viene subordinada a la declaración de secreto de las actuaciones, toda vez que, cuando los sujetos pasivos desconocen que están siendo investigados, se conseguirá el resultado pretendido con la misma[279]. Sin embargo, se venía discutiendo que, si las resoluciones judiciales que acordaran una medida tecnológica conllevaban implícitamente o de forma

[279] Advierte MAGRO SERVET, V. "Consecuencias jurídicas de la declaración de secreto del sumario". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 58. 2009. Pág. 4, que, "como señala el Tribunal Supremo, Sala Segunda, en sentencia de 19 Ene. 2004, rec. 1121/2002, donde apunta que «no es implícita la declaración de secreto cuando se acuerda una intervención telefónica, so pena de entender esta declaración inútil y absurda, pues la Ley procesal está para cumplirse y el adecuado juego de los arts. 118 y 302 de la LECr no deja otra opción que la obligatoriedad de su cumplimiento: no cabe excluir la comunicación de la existencia del procedimiento penal a los imputados, ordenada por el art. 118, si no se adopta al mismo tiempo la medida de secreto permitida por el 302. Esta es la postura mantenida por esta Sala (sentencia de 25-6-93 y la 610/1997 de 5-5)»". Por su parte, señala, RODRÍGUEZ LAINZ, J. L. "Aspectos polémicos de la intervención de comunicaciones como medida de vigilancia secreta". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 125. 2017, que, "el legislador toma partido por considerar que por el solo hecho de presentarse una solicitud de práctica de alguna de las medidas de investigación tecnológica que seguidamente se desarrollan, o cuando la decisión se adopte de oficio, debe iniciarse una pieza secreta en la que se sustanciarán ésta y todas las actuaciones posteriores hasta que se ponga fin a la intervención; y ello sin necesidad de acordar expresamente el secreto de las actuaciones. El carácter ínsito del secreto ha encontrado con ello un indiscutible apoyo. Pero, eso sí, no se niega la posibilidad de que tal carácter connatural se vea reforzado por una declaración de secreto de las actuaciones".

automática la declaración de secreto, o por el contrario, era necesario acordar de forma expresa la declaración de secreto de las actuaciones en el momento de adoptarse la misma[280]. No obstante, el legislador del 2015 (LO 13/2015) ha despejado toda duda, al señalar expresamente que *la solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa* (art. 588 bis d LECrim.). En cualquier caso, fuera de esta polémica, la tesis mayoritaria afirmaba que, la omisión en la declaración de secreto no tenía relevancia constitucional, sino que se consideraba una mera irregularidad procesal (art. 302 LECrim), y en consecuencia, no permitía declarar la nulidad de la medida[281].

En otro orden de ideas, la tramitación de la pieza separada y secreta se produce desde la petición de autorización de la Fiscalía o de la Policía Judicial (art. 588 bis b. LECrim.), y no desde la decisión judicial de adopción de la medida (art. 588 bis c. LECrim.), esto se debe, a que se pretende que los sujetos pasivos desconozcan que están siendo investigados desde el origen de la diligencia, toda vez que, perdería eficacia si la petición fuera accesible a las partes.

4) Cese de la medida y destrucción de los archivos

De esta manera, cuando desaparezcan las circunstancias que justificaron la adopción o resulte evidente que no se están obteniendo los resultados pretendidos, o en su caso, cuando haya transcurrido el plazo para el que hubiera sido autorizada, procederá el cese de la medida (art. 588 bis j. LECrim).

De igual modo, los archivos resultantes de una investigación delictiva, deben ser tratados con todas las garantías, sometiéndose incluso al control judicial, pues incide en la intimidad personal[282]. Por este motivo, no se deben conservar los registros con material sensible por tiempo ilimitado, en detrimento de los derechos del justiciable. En

[280] STS 9/2004, 19 de enero (F.D. 2º).

[281] STS 358/2004, 16 de marzo (F.D. 5º) y STS 9/2004, 19 de enero (F.D. 2º).

[282] STS 1948/1994 de 4 noviembre (F.D. 5º).

este sentido, se han pronunciado el Tribunal Europeo de Derechos Humanos[283], así como el Tribunal Supremo[284], al mantener que, tras la finalización del procedimiento penal, el Juzgado o Tribunal correspondiente, deberá pronunciarse sobre la destrucción de las grabaciones realizadas en las interceptaciones de las comunicaciones, sobre todo en las resoluciones absolutorias o que acuerden el sobreseimiento y archivo de las actuaciones. En consecuencia, la reforma procesal implementada en 2015, ha venido a regular la destrucción de los archivos, de tal forma 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 (discos clonados, Sistema SITEL, etc,) utilizados en la ejecución de la medida[285], si

[283] STEDDHH, Asunto Valenzuela Contreras contra España, 842/1997, de 30 julio 1998 (párrafo 34).

[284] STS 293/2011, de 14 de abril (F.D. 12º).

[285] Indica RODRÍGUEZ LAINZ, J. L. "Sobre el destino de las grabaciones de conversaciones objeto de una intervención legal de comunicaciones, una vez finalizado el proceso en que se acordaron*"*. Diario La Ley. Núm. 7.982. 2012, que, "la STS 293/2011, de 14 de abril, para encontrarnos con una resolución de nuestro Tribunal Supremo que con valentía propone una solución al destino de las grabaciones una vez agotada su utilidad procesal. Efectivamente, aunque fuera realmente obiter dicta, la sentencia establecía que los tribunales deberían de oficio acordar en sus sentencias la destrucción de las grabaciones originales relacionadas con el proceso que existieran en el centro de recepción, y de todas las copias, conservando solamente de forma segura las copias entregadas a la autoridad judicial; y verificando en ejecución de la sentencia, una vez firme, que la destrucción se ha producido. Esta opción ha sido más recientemente seguida por la STS 380/2012, de 16 de mayo; donde se justifica la exigencia del borrado de datos conservados en la sede de SITEL aduciendo la naturaleza plural de los intervinientes, y el hecho de que la medida «... afecta a más personas que aquéllas a las que alcanza la sospecha delictiva»; o por la STS 794/2012, de 11 de octubre, donde se justifica tal imposición porque «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»". Sin embargo, otros autores como, RUIZ DORADO, M., VIDAL MARÍN, T. "Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de Reforma de la Ley de Enjuiciamiento Criminal*"*. Revista Aranzadi Doctrinal. Núm. 9. 2016. Págs. 135-162, señalan que, "si bien es cierto que se han realizado avances en las medidas de aseguramiento mencionadas, resulta inquietante que se permita la conservación de una copia de los datos intervenidos, sin más cautelas que la puesta de dichos datos bajo custodia del Secretario Judicial, por el tiempo de duración previsto en la norma. Nada se dice, pues, acerca de las precauciones que se han de adoptar para evitar la ruptura de la cadena de custodia y las filtraciones de información, ni se establecen

bien, se conservará una copia bajo custodia del Letrado de Administración de Justicia[286] (art. 588.1 bis k. LECrim). De igual modo, la mencionada copia del archivo se conservará durante cinco años desde que la pena se haya ejecutado, cuando el delito o la pena haya prescrito, se decrete el sobreseimiento libre, o bien, recaiga sentencia absolutoria firme, salvo que a juicio del Tribunal sea necesaria la conservación de la misma por un período superior (art. 588.2 bis k LECrim). En definitiva, la destrucción de los archivos originales se producirá en el momento de la firmeza de la resolución que ponga término al proceso penal, mientras que la copia del material permanece en el tribunal durante un mayor periodo de tiempo. De esta manera, se dispone en la ley, el criterio jurisprudencial de nuestro Tribunal Supremo[287], el cual, venía sosteniendo que, el borrado y la eliminación de los archivos es una exigencia de todos los poderes públicos, para evitar, la tentación de su utilización para otros fines que no sean los propios del proceso penal, así como, para salvaguardar el menoscabo sufrido por el titular en los derechos fundamentales. Sin embargo, como se ha podido observar, la conservación de la copia durante cinco años con posibilidad de prórroga a criterio judicial, se produce cuando se acuerde la sentencia condenatoria, pero también, cuando haya recaído una sentencia absolutoria, o bien, sobreseimiento libre, esto es, se conservan durante un largo período de tiempo un material que no sirvió como prueba incriminatoria suficiente, lo cual, a mi modo de ver, se trata de una norma que excede

---

parámetros para su conservación más allá del período establecido (quedando esta decisión al arbitrio judicial)".

[286] En efecto, TOMASELLI ROJAS, A. L. "Actuación del Secretario Judicial: conservación, transcripción y cotejo de las grabaciones*"*. Diario La Ley. Núm. 8.615. 2015, advierte que, "la conservación de los datos contenidos en el soporte electrónico queda vacía de regulación con el nuevo proyecto, no habiendo ninguna regulación específica de qué pasa con los CD unidos a los autos en donde constan las grabaciones con datos íntimos de la persona el nuevo proyecto solo habla de la incorporación de los datos electrónicos de tráfico, quedando en mano la conservación de los datos por los prestadores de servicios*."*

[287] STS 565/2011, 6 de junio y la STS 659/2013, 9 de julio, ambas O.P. Cit. *supra*, así como, en el mismo sentido la STS 207/2012, 12 de marzo; STS 794/2012, 11 de octubre; STS 109//2012, 14 de febrero, así, los tribunales han adoptado medidas encaminadas a la destrucción de las grabaciones una vez que ya no sean necesarias para la operatividad probatoria en la causa.

de los límites de la proporcionalidad, pero además, puede suponer una vulneración en los derechos fundamentales de la persona afectada.

Por último, la ejecución de la destrucción de los archivos recae en la Policía Judicial, que se llevará a cabo a instancias del Juez competente (art. 588.3 bis k LECrim). En este sentido, resulta cuanto menos insólito que, sean las Fuerzas y Cuerpos de Seguridad del Estado las encargadas del borrado y eliminación del material, sin estar sometidos a ninguna fiscalización, pues el Juez ordena la destrucción, pero no se precisa que reciba información alguna sobre el resultado de su ejecución.

5) Cuestión procesal: La utilización de la información obtenida en un procedimiento distinto

Otro de los puntos a desarrollar por ser de interés a lo expuesto en las líneas anteriores es, si las grabaciones realizadas o informaciones obtenidas en una diligencia de investigación, pueden ser utilizadas en un proceso penal distinto[288], pues podría cuestionarse la validez del material obtenido, toda vez que la habilitación judicial únicamente recaía para la investigación en otro procedimiento. De acuerdo con ello, el Tribunal Supremo ha adoptado el Acuerdo no jurisdiccional de la Sala Segunda (26 de mayo de 2009)[289], en el cual, se concedía validez a las escuchas telefónicas procedentes de diligencias distintas a las del propio procedimiento, sin embargo, se permitía al interesado impugnar en la instancia, la legitimidad del medio de prueba, debiendo la parte que lo propuso justificar de forma contradictoria la legitimidad cuestionada,

[288] Sobre la utilización de información en un proceso penal distinto, RODRÍGUEZ LAINZ, J. L. "Tratamiento procesal de la prueba obtenida en una previa investigación criminal con restricción de derechos fundamentales*"*. Diario La Ley. Núm. 7.283. 2009, venía manteniendo que, "debería normalizarse la cesión de información deducida de previos procedimientos en los que la fuente de conocimiento tuviera por origen una restricción de derechos fundamentales, con exigencia de las resoluciones habilitantes y elementos de convicción que dieran lugar a su decisión, además de los elementos de convicción en sí mismos. Es trascendental para tal valoración, no sólo por las partes, sino también por los órganos jurisdiccionales destinatarios de tal fuente de conocimiento, contar con la información mínima suficiente para poder tomar una postura sobre la licitud de aquélla. Salvada tal adición de información, correspondería a la iniciativa de las partes interesar una mayor extensión en los particulares remitidos".

[289] Acuerdo no jurisdiccional de la Sala Segunda del TS de 26 de mayo de 2009.

aunque si el interesado no promoviera dicho debate, no se podría suscitar en ulteriores instancias[290]. Sin embargo, el acuerdo mencionado no resuelve con claridad cuál es el momento procesal idóneo para la impugnación de las intervenciones traídas de otro procedimiento, aunque en aplicación de la jurisprudencia mayoritaria[291], se deberá entender que el momento para iniciar el debate contradictorio sobre la validez de la prueba será hasta el trámite del turno de intervenciones que se concede a las partes como cuestión previa al comienzo de la vista en los procedimientos abreviados (art. 786.2 LECrim.), o bien, como cuestiones de previo pronunciamiento en el juicio ordinario (arts. 666 a 678 LECrim.), de hecho, toda manifestación al respecto con posterioridad, como por ejemplo en el trámite de conclusiones definitivas, se debería considerar extemporánea. No obstante, esta cuestión será criticada por del Moral García, al entender que, esperar para formular impugnación como cuestión previa en la propia vista, provocando incluso la suspensión de la vista por acaecer hechos sorpresivos, cuando bien se podría haberse hecho con anterioridad en la fase de instrucción o intermedia con la interposición de los escritos de calificación, es una *estrategia defensiva que carece de nobleza y lealtad*[292].

Con este panorama jurisprudencial, la Ley de Enjuiciamiento Criminal sería reformada en 2015[293], de modo que, se incorporaría a nuestro ordenamiento jurídico procesal el tratamiento sobre la utilización de la información obtenida en un procedimiento distinto. De esta manera, se establece con carácter general para todas las medidas tecnológicas que, las informaciones obtenidas, podrán ser utilizadas como medio de investigación o prueba en otro proceso penal (arts. 579.1 bis y 588 bis i. LECrim), si bien, para acreditar

[290] Seguidamente se mencionan algunas resoluciones judiciales que asumieron en sus pronunciamientos el Acuerdo no jurisdiccional de la Sala Segunda del TS de 26 de mayo de 2009: STS 737/2009, de 6 de julio y la STS 725/2009, 24 de junio, si bien, posteriormente, también fue acogido entre otras por la STS 1138/2010, de 16 diciembre; STS 223/2011, de 31 marzo.

[291] STS 477/2013, 3 de mayo (F.D. 3º).

[292] Voto Concurrente de Excmo. Sr. Don Antonio del Moral García, realizado en la STS 477/2013, 3 de mayo.

[293] Art. único 12 y 13 de la Ley Orgánica 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal.* («BOE» Núm. 239, de 6 de octubre de 2015).

la legitimidad de la injerencia se deberá deducir testimonio de los particulares necesarios, haciéndose constar como mínimo entre los antecedentes indispensables, 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 (arts. 579.2 bis y 588 bis i. LECrim).

No obstante, la nueva regulación no aclara cuando es el momento procesal idóneo para impugnar la legitimidad del material traído al procedimiento desde otro distinto, por lo que, cobra importancia el criterio jurisprudencial y el Acuerdo no jurisdiccional mencionado *supra*. Laguna que podría haber sido solucionada por el legislador al establecer claramente que el momento procesal para la impugnación sea hasta las cuestiones previas.

6) Medidas de aseguramiento y custodia de la prueba tecnológica

En la práctica de una diligencia de investigación que sea necesario obtener el efecto o cuerpo del delito tecnológico (art. 334 LECrim.), como por ejemplo en el delito de pornografía infantil, para que éste, no sufra alteraciones se deberán tomar ciertas cautelas para su aseguramiento. Seguidamente, se darán unas líneas generales sobre asegurar y custodiar los efectos intervenidos del delito informático y tecnológico, que son comunes a todas las diligencias de investigación tecnológicas restrictivas de derechos fundamentales, sin perjuicio, de lo que se dirá cuando se examinen específicamente cada diligencia de investigación.

En determinados supuestos, como en delitos de poca entidad que hace innecesaria otra forma de corporeizar la evidencia, bastará con la impresión en soporte papel del "pantallazo"[294] donde se evidencie el delito cometido, que además, cuando el Letrado de la Administración de Justicia se encuentre presente, podrá corroborar fehacientemente la veracidad del mismo. De esta manera, por ejemplo, en el delito de amenazas leves (art. 171.7 CP) cometidas a través de *WhatsApp*[295], será suficiente la impresión en papel

[294] STS 300/2015, 19 de mayo (F. D. 4º).

[295] Acerca de la sentencia del TS 300/2015 sobre la validez de los "pantallazos" como prueba en el proceso judicial, véase GONZÁLEZ LAGE, J. *La prueba pericial en la práctica judicial penal las redes sociales en el proceso penal. (Peritaje y prueba pericial).* Editorial Bosch. Barcelona. 2017. Págs. 563-

de la amenaza proferidas, pudiendo el Letrado de la Administración de Justicia en el acto de juicio oral sobre delitos leves, corroborar la coincidencia de la impresión con los mensajes remitidos por la aludida mensajería instantánea en el terminal móvil del denunciado, o bien, en el transcurso de una entrada y registro, en la investigación de un delito de tenencia de pornografía infantil (art. 189.5 CP), se podrán realizar impresiones en papel del material encontrado, en presencia del L.A.J. como fedatario público, así como del investigado.

Sin embargo, en otros casos más complejos, como por ejemplo en un delito de elaboración de pornografía infantil (art. 189.1 CP), será necesario tomar mayores medidas de aseguramiento de la evidencia; para ello, habrá de fijar las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación (art. 588.1 *in fine* sexies c. LECrim.). De este modo, el aseguramiento de la evidencia se consigue mediante el clonado o volcado de los datos contenidos en el dispositivo (art. 479 LECrim.), es decir, se realiza un proceso de copiado exacto del contenido a través de un dispositivo tecnológico o "clonador". Además, para garantizar la veracidad de la totalidad del trasvase de información se realizará en presencia del Letrado de la Administración de Justicia, que como garante de la legalidad, tiene por cometido velar por la fe pública, conservando el original precintado y sellado bajo su custodia en sede judicial, por si precisara de ulteriores clonados, o bien, realizar alguna prueba de contraste, mientras que el "clon" o copia exacta podrá ser objeto de análisis para la elaboración de prueba pericial. En consecuencia, se asegura la inalterabilidad de la

569; BUENO DE MATA, F. "La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica*"*. Diario La Ley. Núm. 8.728. 2016; MISMO AUTOR. *La validez de los "screenhots" o "pantallazos" como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo. (Los desafíos de la justicia en la era post crisis).* Atelier. Barcelona. 2016. Págs. 141-152; RODRÍGUEZ LAINZ, J. L. "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea a propósito de la STS, Sala 2.ª, 300/2015, de 19 de mayo*"*. Diario La Ley. Núm. 8.569. 2015, si bien, éste último, afirma que, "por una parte que la corroboración de tal fuente probatoria puede obtenerse por vías diversas a una prueba pericial; por otra, que el ofrecimiento del acceso a la fuente original rompe esa pantalla de prevención suscitada por el Alto Tribunal a las impresiones de mensajes o datos, a la vez que impone a quien pretende la impugnación, y más ante la corroboración de su realidad y origen, cierto deber de diligencia a la hora de hacer valer su mera impugnación formal".

fuente de prueba, se garantiza la integridad de los datos y de su contenido, permitiendo también, su análisis, sin problema de que sea dañado o modificado[296].

Por otro lado, para garantizar la autenticidad, al final del clonado se deberá encriptar los contenidos mediante la técnica *hash*[297], es decir, mediante una serie de algoritmos se permite reconocer la identidad, pues cualquier cambio en la numeración, supone la inexactitud entre los contenidos, y con ello, hace posible contrastar la certeza del trasvase de los datos a la copia.

Asimismo, para garantizar los derechos del investigado, el clonado deberá realizarse en su presencia o de sus abogados (art. 333 LECrim.), especialmente cuando se encuentre detenido. De esta manera, el proceso de clonado se puede realizar, en el momento de la aprehensión de los dispositivos, por ejemplo, en la práctica de una entrada y registro domiciliario o registro de dispositivos masivos de información, pues estará presente el Letrado de la Administración de Justicia y el investigado, o bien, cuando se prevea que el clonado va a ser largo, complejo o no esté presente el investigado, se podrá dejar para un momento posterior en sede judicial o donde técnicamente pueda llevarse a cabo, por

[296] Con carácter general sobre la prueba electrónica obtenida a través de diligencias de investigación restrictivas de derechos fundamentales, nos remitimos, a: LÓPEZ-BARAJAS PEREA, I. "Nuevas tecnologías aplicadas a la investigación penal, el registro de equipos informáticos*"*. IDP: Revista de Internet, Derecho y Política. Núm. 24. 2017; AIGE MUT, Mª B. *La nueva diligencia de registro de dispositivos de almacenamiento masivo. (El proceso penal cuestiones fundamentales)*. Editorial Tirant lo Blanch. Valencia. 2016. Págs. 389-397; RODRÍGUEZ ÁLVAREZ, A. *Diligencia de registro de dispositivos y "smartphones". (FODERTICS 5.0: estudios sobre nuevas tecnologías y justicia)* Editorial Comares. Granada. 2016. Págs. 255-263; DELGADO MARTÍN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015*"*. Diario La Ley. Núm. 8.693. 2016, sin embargo, este último afirma que, "el principal reto consiste en la realización del clonado garantizando que «original» y «copia» son exactamente iguales, para lo cual es necesario utilizar dos tipos de garantías: técnicas, esto es, la utilización de instrumentos tecnológicos y procedimientos adecuados, resultando positiva su estandarización/homologación; y jurídicas, es decir, presencia de testigos y/o fedatario público (Notario o Secretario Judicial) siendo preferible la segunda opción por los propios efectos de la fe pública".

[297] PEREIRA I PUIGVERT, S. *Sistema de "hash" y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas "inaudita parte". (FODERTICS II: hacia una justicia 2.0)*... O.P. Cit. Págs. 75-83.

ejemplo, en dependencias policiales en las unidades especializadas de delitos tecnológicos o telemáticos. De esta forma, cuando se decida realizar el proceso de clonación para un momento ulterior, el Letrado de la Administración de Justicia deberá precintar y sellar el dispositivo técnico ocupado (art. 570 LECrim.), debiendo permanecer los efectos bajo su custodia, o bien, ordenando que se custodie en un lugar que garantice la inalterabilidad de su estado (en un lugar seguro en dependencias policiales), de modo que, cuando llegue el momento, se abra y se desprecinte en su presencia, dando fe pública de su realización, pero además, se podrá citar al afectado o su abogado para que presencie el acto procesal.

De esta manera, de lo mencionado hasta el momento se desprende que, se debe respetar la cadena de custodia[298], de tal forma que, se garantice la identidad, la integridad y la autenticidad (art. 338 y 326 LECrim.) de los efectos intervenidos, para lo cual, desde que se ocupan los efectos o se clonan, se analiza por los peritos informáticos, para en su caso, elaborar un informe, hasta su aportación a fase de plenario, es en todo momento lo mismo, esto es, sin que sufra manipulaciones o alteraciones[299]. Esto es debido a que, los efectos electrónicos son fácilmente manipulables, por lo que, es mucho más importante, si cabe, garantizar la identidad, la integridad y la autenticidad, en el caso de la información contenida en esta clase de dispositivos, que en otros delitos, como en el caso de las infracciones contra la salud pública (art. 368 CP).

[298] STS 1215/2009, de 30 diciembre. Voto Particular de Marchena Gómez que, pese a tratarse de un voto particular, y en consecuencia, no tiene relevancia a los efectos de la sentencia, queremos hacer nuestro su criterio, al mantener que, "una vez grabada la conversación en el terminal custodiado por los agentes de policía, el fichero así generado no ha sido abierto con posterioridad y, en consecuencia, no ha sido expuesto a ningún tipo de modificación. El Tribunal que ha de valorar esa fuente probatoria ha de tener asegurado, en el plano tecnológico, que no se han suprimido fragmentos relevantes para conocer el alcance de los hechos o que no han sido excluidas conversaciones que el agente responsable considera intrascendentes jurídicamente y que, sin embargo, pueden no serlo. En definitiva, resulta indispensable que el sistema garantice que después de cada conversación interceptada por los agentes facultados se procede al sellado tecnológico del archivo de sonido, con el fin de salvaguardar su integridad, excluyendo cualquier riesgo de manipulación".

[299] LEAL MEDINA, J. "Ruptura de la cadena de custodia y desconexión con las fuentes de prueba supuestos concretos, reflexiones que plantea*…"* O.P. Cit; RUBIO ALAMILLO, J. "Conservación de la cadena de custodia de una evidencia informática*…"* O.P. Cit.

Por otro lado, los efectos tecnológicos pueden ser aportados al proceso penal por los particulares, sin embargo, puede suscitar dudas sobre el respeto a la cadena de custodia. En este caso, los efectos tecnológicos podrán ser entregados a las Fuerzas y Cuerpos de Seguridad del Estado mediante la oportuna denuncia, para que si éstos, lo encontraran necesario, someter a análisis, o bien, aportarlos directamente al procedimiento penal junto con un informe particular pericial informático, que además, podrá ser sometido a la fe pública del notario.

En otro orden de ideas, como establece la norma procesal (art. 588 octies LECrim), el Ministerio Fiscal o la Policía Judicial podrán requerir, durante un periodo máximo de noventa días, prorrogable una sola vez hasta ciento ochenta días, 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. De igual modo, el requerido vendrá obligado a prestar su colaboración y a guardar secreto, bajo apercibimiento de incurrir en delito de desobediencia (art. 556 CP). De esta manera, la ley faculta a la Policía Judicial y al Ministerio Fiscal, poder requerir la conservación de los datos tecnológicos que obran en poder de las empresas prestadoras de servicios de la información, hasta que la autoridad judicial convalide el mencionado requerimiento, todo ello, como garantía para el buen de la investigación.

II. DISPOSICIONES ESPECÍFICAS

Una vez explicada las disposiciones comunes que resultan de aplicación a todas las medidas tecnológicas, seguidamente pasaremos a exponer, cada diligencia de investigación específica previstas en la Ley de Enjuiciamiento Criminal, lo cual, tiene gran importancia a efectos de averiguar la comisión y participación de hechos delictivos, en especial, los delitos informáticos y tecnológicos.

1) Interceptación de las comunicaciones telefónicas y telemáticas

El estudio de la medida de interceptación de las comunicaciones telefónicas y telemáticas se ha divido en varios apartados, en los cuales, comenzaremos con una introducción sobre el secreto de las comunicaciones, seguidamente analizaremos, el concepto y naturaleza jurídica de las mismas, los aspectos específicos regulados en la Ley de Enjuiciamiento Criminal, para continuar, con una de las partes más importantes de la obra, la incorporación al proceso de datos electrónicos de tráfico o asociados, proseguiremos observando, el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, y terminaremos con algunas particularidades observadas de la jurisprudencia y/o doctrina, relacionadas con esta clase de medida de investigación tecnológica.

a) Introducción secreto de las comunicaciones

Nuestra Constitución española de 1978, establece el secreto de las comunicaciones en el art. 18.3[300]. De esta manera, el bien constitucionalmente protegido es la libertad de las comunicaciones[301], el cual, comprende cualquier medio utilizado, tanto telemático como

[300] Sobre los antecedentes históricos y jurídicos del derecho fundamental del secreto de las comunicaciones, véase a SOLOZÁBAL ECHAVARRÍA, J. J. *Los derechos fundamentales en la Constitución española de 1978. Ayer*. Asociación de Historia Contemporánea. Editorial Marcial Pons. Madrid. Núm. 34. 1999. Págs. 217-241.

[301] Señalan, DE URBANO CASTRILLO, E. "El derecho al secreto de las comunicaciones*"*. La Ley. Madrid. 2011; ELVIRA PERALES, A. *El derecho al secreto de las comunicaciones telefónicas a golpe de jurisprudencia. Estudios sobre la Constitución Española: homenaje al profesor Jordi Solé Tura, Vol. 2)*. 2008. Editorial del Congreso de los Diputados. Madrid. Págs. 1.143-1.154; MURILLO DE LA CUEVA, P. L. *Notas sobre el derecho fundamental al secreto de las comunicaciones*. *Constitución, estado de las autonomías y justicia constitucional: libro homenaje al profesor Gurmesindo Trujillo.*

telefónico o de cualquier otra clase que la tecnología pudiera desarrollar. Sin embargo, la norma constitucional detalla los medios en el que podrán realizarse las comunicaciones (postal, telegráfica y telefónica), si bien, se trata una enumeración meramente demostrativa[302], lo cual, habrá que inferir que, la protección constitucional se extiende a todos los medios de comunicación modernos conocidos, como el correo electrónico, mensajes de móvil, mensajería instantánea como *WhatsApp*, etc.

De igual modo, como afirma Espín Templado, *el secreto de las comunicaciones constituye una garantía de la vida privada, en el sentido de preservar al individuo en un ámbito de actuación libre de injerencias de terceros y, en especial, de los poderes públicos[303]*, de tal forma que, como veremos posteriormente, no se podrán realizar injerencias en las comunicaciones, sin la intervención de la autoridad judicial.

En otro orden de ideas, nuestro Tribunal Constitucional mantiene que, el concepto de «secreto» tiene un carácter «formal»[304], esto es, el secreto es inviolable

---

Editorial Tirant lo Blanch. Valencia. 2005. Págs. 661-686; ESQUIROL ZULOAGA, I. *El derecho fundamental al secreto de las comunicaciones postales y telegráficas. Marco legal del derecho. La prueba en el proceso penal.* Revista General de Derecho. 2000. Págs. 437-504, que, el bien constitucionalmente protegido del derecho fundamental al secreto de las comunicaciones es la libertad de las comunicaciones.

[302] Ponen de manifiesto, FERNÁNDEZ SEGADO, F. *El Sistema Constitucional Español.* Dykinson. O.P. Cit. Págs. 228-231; DE ESTEBAN, J. Y GONZALEZ-TREVIJANO, P. J. *Tratado de Derecho Constitucional II.* Servicio de Publicaciones. Facultad de Derecho. Universidad Complutense de Madrid. Madrid. 2004. Págs. 135-140, que, la enumeración de medios que pueden ser objeto de la interceptación de las comunicaciones es meramente demostrativa, pudiendo abarcar también otros medios tecnológicos no contemplados expresamente en la Constitución.

[303] ESPÍN TEMPLADO, E. *Derecho Constitucional*. *Volumen I. El ordenamiento constitucional. Derechos y deberes de los ciudadanos.* Ediciones Tirant Lo Blanch. Valencia. 2007. Págs. 242-243.

[304] Afirma RODRÍGUEZ LAINZ, J. L. "Sobre la naturaleza formal del derecho al secreto de las comunicaciones dimensión constitucional e histórica*"*. Diario La Ley. Núm. 7.647. 2011, que, "la idea de la concepción formal de la protección que brinda el secreto de las comunicaciones a éstas, como garantía a ultranza de que la comunicación en sí misma y los elementos externos que forman su cortejo técnico no se verán afectados por injerencia ajena alguna si no se cuenta con el consentimiento del interlocutor o una resolución judicial que la ampare, no ha sido, pese a la opinión de algún autor, algo preestablecido que se remonte a la génesis natural de los derechos humanos tenidos como tales por el común de los pensadores

independientemente de su contenido, de modo que, la protección constitucional alcanza a los mensajes con un contenido íntimo, pero también, cuando es totalmente insignificante, de manera que, el Alto Tribunal procede a realizar una presunción *iure et iure*, pues se trata de un hecho que no admite prueba en contrario, que las comunicaciones son siempre secretas. Además, en la emisión de un mensaje, primeramente, la afectación se produce en el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE), pero dependiendo del contenido del mensaje, podrá incidir también, en la intimidad de los sujetos intervinientes (art. 18.1 CE)[305].

De igual modo, la protección constitucional alcanza a cualquier sujeto público o privado ajeno a la propia comunicación[306], sin embargo, el secreto de las comunicaciones, como cualquier derecho fundamental no es absoluto, sino que podrá ser restringido mediante resolución judicial[307]. Ahora bien, el tratamiento constitucional del derecho a la intimidad (art. 18.1 CE) no puede ser equiparable con el secreto de las comunicaciones (art. 18.3 CE), toda vez que, mientras que en este último, de forma expresa, se establece en el precepto constitucional la necesaria habilitación judicial para su injerencia, en

---

y sistemas políticos modernos". Los mismos argumentos son abordados en, MISMO AUTOR. "Los límites a la dimensión formal del derecho al secreto de las comunicaciones*"*. Diario La Ley. Núm. 7669. 2011.

[305] STC 114/1984, de 29 de noviembre (F.J. 7º).

[306] STC 123/2002, de 20 mayo (F.J. 5º).

[307] Destacando este aspecto, RODRÍGUEZ RUBIO, C. *La injerencia en el derecho al secreto de las comunicaciones a través de la regulación de las medidas de investigación tecnológica*. Revista Europea de Derechos Fundamentales. Núm. 28. 2016. Págs. 267-285; LÓPEZ-BARAJAS PEREA, I. *La protección del derecho al secreto de las comunicaciones en la investigación penal. (Constitución y democracia: ayer y hoy: libro homenaje a Antonio Torres del Moral, Vol. 2).* Editorial Universitas. Madrid. 2012. Págs. 1651-1667; DE LOS ÁNGELES SÁEZ BELTRÁN, M. *La restricción al derecho fundamental al secreto de las comunicaciones telefónicas. (Derecho, historia y universidades estudios dedicados a Mariano Peset, Vol. 2).* Editorial Universidad de Valencia. 2007. Págs. 583-590; GONZÁLEZ SOLER, O. E. *Aspectos constitucionales de algunas diligencias sumariales que afectan a los derechos a la intimidad y al secreto de las comunicaciones entradas domiciliarias. Comunicaciones postales y telefónicas*. Cuadernos de Derecho Judicial. Núm. 15. 2003. Págs. 91-164; FRANCISCO FÁBREGA RUIZ, C. *Secreto de las comunicaciones y proceso penal*. La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 4. 1997. Págs. 1187-1190.

cambio, en la intimidad, al no establecerse dicha obligatoriedad, el Tribunal Constitucional[308] viene admitiendo que, para determinados casos y con la suficiente y precisa habilitación legal, la Policía Judicial, pueda realizar prácticas que constituyan una injerencia leve en la intimidad de las personas.

b) Concepto y naturaleza jurídica de la interceptación de las comunicaciones telefónicas y telemáticas

Seguidamente se va a examinar la naturaleza jurídica de la interceptación de las comunicaciones, si bien, como el objeto de la injerencia recae en medios telefónicos y telemáticos, primeramente, debemos definirlos. De esta manera, el concepto de telefónica no trae grandes dificultades, pues de acuerdo con el diccionario de la RAE consiste *en lo relativo a telefonía,* de modo que, esto último, lo define como un *sistema de comunicaciones telefónicas,* es decir, perteneciente a teléfono, entendido como *conjunto de aparatos e hilos conductores con los cuales se transmite a distancia la palabra y toda clase de sonidos por la acción de la electricidad*[309]. De igual modo, el diccionario de María Moliner define telefonía como *técnica y actividad relacionadas con el teléfono,* y en consecuencia, teléfono es un *sistema de telecomunicación por medio de cables u ondas electromagnéticas, aplicado a la transmisión de sonidos,* así como *cada uno de los aparatos, receptores y trasmisores a la vez, instalados en la red telefónica*[310]. No obstante, el término telemático es más amplio, por lo que, resulta más necesario, si cabe, acudir al diccionario de la RAE para despejar toda duda, de tal forma que, se define como la *aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computarizada*[311], de igual manera, el diccionario de María Moliner lo describe como el *conjunto de técnicas y servicios que*

[308] STC 281/2006, de 9 octubre (F.J. 2º).

[309] Vista la definición en http://dle.rae.es.

[310] Para la definición de telefonía y teléfono, véase MOLINER, M. *Diccionario del uso español*. Editorial Gredos S.A.U. Madrid. 2007. Pág. 2.838.

[311] Vista la definición en http://dle.rae.es.

combinan las telecomunicaciones con la informática[312], lo cual, supone que el vocablo estudiado hace referencia a la informática y a las telecomunicaciones, o dicho de una manera más técnica, consiste en la transmisión, almacenamiento y procesado de cualquier clase de información contenida en sistemas informáticos, como datos, voz o imagen, pero también, comprende las comunicaciones por correo electrónico, mediante mensajes multimedia de voz o imagen, mensajes de texto, etc. Una vez realizada estas definiciones, cabe concluir que, la interceptación de las comunicaciones telefónicas y telemáticas, consiste en realizar una actividad de control y de injerencia en el ámbito privado por parte de la fuerza instructora, con habilitación expresa judicial, para la investigación de hechos delictivos, el cual, podrá recaer en medios telefónicos, pero también, en sistemas informáticos o de telecomunicaciones.

Llegados a este punto, para poder entender correctamente la naturaleza jurídica de la interceptación de las comunicaciones telefónicas y telemáticas, resulta necesario diferenciar fuente de medio de prueba, de tal forma que, aquella es todo elemento que contenga información significativa para el proceso, como por ejemplo un testigo o un perito, mientras que medio es la manera a través de la cual, dicha información es introducida en el proceso penal, como sucede con los interrogatorios de los acusados, en las declaraciones testificales o en los informes periciales[313]. Una vez realizada dicha aclaración, la interceptación de las comunicaciones se trata de una fuente de prueba para la investigación de delitos, donde lo relevante a estos efectos son, las personas o los interlocutores que mantienen una conversación o transmiten mensajes, mientras que, la forma de introducirlo al proceso penal normalmente será como documento, pues el soporte donde se conserva dicha información, como los discos utilizados para almacenar la comunicación, la transcripción de las conversaciones, etc, tiene la consideración de documento, con arreglo a lo dispuesto en el art. 26 código penal, en cumplimiento de la

[312] Para el concepto de telemático, véase MOLINER, M. *Diccionario del uso español*. Editorial Gredos S.A.U. Madrid. 2007. Pág. 2.839.

[313] BANACLOCHE PALAO, J. y ZARZALEJOS NIETO, J., *Aspectos Fundamentales de Derecho Procesal Penal*. La Ley. Madrid. 2011. Págs. 273-288; RIFÁ SOLER, J. M. *Fuentes, medios y actos de prueba. Apreciación y valoración de la prueba en el Proceso Penal*. Estudios Jurídicos. Ministerio Fiscal. Núm. 1. 2003. Págs. 13-54; CORTÉS DOMÍNGUEZ, V. *Capítulo I. Concepto y objeto de la prueba. (La prueba).* Editorial Tirant Lo Blanch. 2017. Págs. 19-55.

jurisprudencia mayoritaria[314]. Sin embargo, también podrá ser introducido en el proceso penal de otras formas, como la pericial en el supuesto de que un grupo experto en informática o de telecomunicaciones perteneciente a la Policía Judicial hubiera elaborado un informe, o bien, mediante la elaboración de un informe forense sobre fonética para identificar las voces, pero también la testifical, mediante la declaración de los agentes actuantes en sede judicial dando su versión sobre la comunicación intervenida.

c) Aspectos específicos regulados en la Ley de Enjuiciamiento Criminal

Seguidamente vamos a exponer las disposiciones específicas contenidas en la Ley de Enjuiciamiento Criminal que regulan la medida de interceptación de las comunicaciones telefónicas y telemáticas, y en concreto, los presupuestos (art. 588 ter a. en relación con el art. 579.1 LECrim.), el ámbito objetivo de la medida (art. 588 ter b. LECrim.), el ámbito subjetivo de las intervenciones: cuestión especial de la afectación a tercero no investigado (art. 588 ter c. LECrim.), la solicitud u oficio (art. 588 ter d. LECrim.), el control de la medida (art. 588 ter f. LECrim.), la duración y prórroga de la medida (art. 588 ter g. y h. LECrim.), el acceso de las partes a las grabaciones (art. 588 ter i. LECrim.) y el deber de colaboración (art. 588 ter e. LECrim.).

a´. Presupuestos

El Juez, al adoptar una medida de interceptación de las comunicaciones, como ya nos hemos referido en las disposiciones generales, debe observar sobre el cumplimiento de los principios rectores (art. 588 bis.a. LECrim: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad), pero además, de forma específica para esta clase de diligencia, deben respetarse unos presupuestos legales necesarios para su validez (art. 588 ter. a. LECrim)[315], si bien, la norma no exige la concurrencia de todos,

[314] STS 283/1988, de 2 de febrero; STS 511/1999, de 24 marzo (F.D. 1º).

[315] Con carácter general, véase, SANCHÍS CRESPO, C. "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 125. 2017; VILLANUEVA TURNES, A. *Las comunicaciones electrónicas su encuadre constitucional y la autorización judicial como requisito para su intervención. (FODERTICS 5.0: Estudios sobre Nuevas Tecnologías y Justicia).* Editores: Editorial Comares. Granada. 2016. Págs. 287-296; ALONSO SALGADO, C. *Una cuestión de garantías. La interceptación de las*

sino que, con que concurra uno, será suficiente para que la medida de injerencia sea ajustada a Derecho. De esta manera, la autorización judicial que acuerde la medida deberá hacer constar los principios rectores[316], pero además, únicamente se podrá adoptar para la investigación de los siguientes grupos de delitos:

1.º *Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión* (art. 579.1. 1.º por remisión del art. 588 ter a. LECrim).

La fórmula elegida por el legislador para la elección de que delitos pueden ser investigados mediante la adopción de una medida de injerencia en las comunicaciones es la cuantitativa, es decir, podrán ser objeto de interceptación los delitos castigados con pena en abstracto con un límite máximo de, al menos, tres años de prisión, lo cual, supone que se incluyen numerosos delitos considerados menos graves, esto es, con pena de prisión de tres meses hasta cinco años (art. 33.3 CP). De esta manera, cabe advertir que, como se ha mencionado, la pena máxima de prisión de tres años es en abstracto, o lo que es lo mismo, habrá que atender al rango punitivo del delito, de tal forma que,

---

comunicaciones telefónicas de la Ley de Enjuiciamiento Criminal a la propuesta de nuevo Código procesal penal. (Processulus: estudios sobre derecho procesal). Editores: Editorial Comares. Granada. 2015. Págs. 127-136; ALONSO SALGADO, C. *El largo camino hasta la Ley Orgánica 13/2015 algunos aspectos relevantes en relación a la interceptación de las comunicaciones telefónicas. (FODERTICS 4.0: estudios sobre nuevas tecnologías y justicia: IV Fórum de expertos y jóvenes investigadores en derecho y nuevas tecnologías, celebrado en la Facultad de Derecho de Salamanca, en 2015)*. Editores: Editorial Comares. Granada. 2015. Págs. 95-105.

[316] Acerca de la necesaria intervención judicial para la adopción de una medida de intervención en las comunicaciones y el contenido que debe comprender la autorización, en concreto, la autorización judicial deberá contener un juicio de proporcionalidad sobre la medida, véase DOMINGO MONFORTE, J. "La intervención judicial de las comunicaciones*"*. Actualidad Jurídica Aranzadi. Núm. 896. 2014. Pág. 10; ROMERO PAREJA, A. *"*Intervención de las comunicaciones*"*. Diario La Ley. Núm. 7816. 2012; MISMO AUTOR. "Secreto de las comunicaciones; su intervención judicial*"*. Revista Jurídica del Notariado. Núm. 80. 2011. Págs. 253-284; RODRÍGUEZ LAINZ, J. L. "Peculiaridades de la intervención judicial de comunicaciones electrónicas…" O.P. Cit; GIMENO SENDRA, J. V. "La intervención de las comunicaciones…" O.P. Cit; NADAL GÓMEZ, I. "La intervención de las comunicaciones telefónicas*"*. Tribunales de Justicia: Revista Española de Derecho Procesal. O.P. Cit. Págs. 45-66; MORENO CASTILLO, M. A. "La intervención de las comunicaciones telefónicas y la interceptación de comunicaciones escritas, telegráficas y electrónicas como medios de prueba en el nuevo código procesal penal*"*. Revista de Derecho. Núm. 1. 2002. Págs. 173-200.

pueden ser objeto de la medida tipos penales con pena mínima de muy poca entidad, como por ejemplo delito de estafa (arts. 248 y 249 CP) que se castiga con pena de prisión de seis meses a tres años de prisión o delito de lesiones (art. 147 CP) con pena de prisión de tres meses a tres años o multa, etc. De este modo, el criterio elegido por el legislador es cuantitativo, si bien, pese a ser el criterio más sencillo a efectos prácticos para determinar la gravedad de la pena, lo cierto es que, la jurisprudencia de nuestro Tribunal Supremo, viene manteniendo que, un hecho delictivo puede ser considerado grave, no tanto por la pena en abstracto a imponer, sino también en atención a otros criterios como el bien jurídico protegido o la trascendencia social del hecho[317]. Por este motivo, como seguidamente veremos, se han regulado otros presupuestos que pueden darse, para acordar una diligencia de investigación de intervención en las comunicaciones. Por último, la medida únicamente puede acordarse para delitos dolosos, de manera que, se excluyen todas las formas de imprudencia contenidas en el código como presupuesto para su adopción.

2.º *Delitos cometidos en el seno de un grupo u organización criminal* (art. 579.1. 2.º por remisión del art. 588 ter a. LECrim).

De esta manera, otro presupuesto para la adopción de una diligencia de intervención de las comunicaciones es que fuera para la investigación de un delito cometido en el seno de una organización (art. 570.1 bis CP) o grupo (art. 570.1 ter CP) criminal[318], todo ello, con arreglo a la definición dada en la reforma penal implementado con la LO.5/2010[319].

[317] STS 513/2014, 24 de junio (F. D. 1º).

[318] BRETONES ALCARAZ, F. J. "La criminalidad organizada en nuestro Código Penal, tratamiento anterior y posterior a la LO 5/2010 y LO 1/2015*"*. Diario La Ley. Núm. 8613. 2015; VERA SÁNCHEZ, J. S. *Organización y grupo criminal. Asociación ilícita (arts. 515-521; 570 bis, ter y quater) (Manual de derecho penal. Parte Especial. Doctrinan y jurisprudencia con casos solucionados. Tomo 1).* Editorial Tirant lo Blanch. Valencia. 2015. Págs. 784-794; VELASCO NÚÑEZ, E. "Crimen organizado organización y grupo criminal tras la reforma del Código Penal en la LO 5/2010*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 86. 2011. Pág. 1; CARRETERO SÁNCHEZ, A. "La organización y el grupo criminal en la reforma del Código Penal*"*. Diario La Ley. Núm. 7560. 2011.

[319] Art. único. 143 y 144 de la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal («BOE» núm. 152, de 23 de junio de 2010).

De esta manera, como advierte nuestro Tribunal Supremo, para la *organización criminal* se exige, la agrupación de, al menos, tres personas para la comisión del delito, que exista una una actuación planeada, bien con carácter estable, bien por tiempo indefinido, se produzca el desarrollo de una tarea concertada y coordinada, así como, se trate de un reparto funcional de cometidos puestos al servicio del delito[320], mientras que, para el *grupo criminal* se precisa de la unión o agrupación de más de dos personas con la finalidad de cometer de forma concertada delitos, sin embargo, se diferencia de la organización en la estabilidad y el reparto de tareas, esto es, puede permanecer estable cierto tiempo en función del tipo de infracción criminal a que se oriente su actividad delictiva, pero carece de una estructuración organizativa[321]. No obstante, como también mantiene nuestro Tribunal Supremo, el proceso penal se trata de un hecho de *cristalización progresiva*, que se verifica de forma paulatina, en función del resultado de las diligencias de investigación realizadas[322]. De esta manera, podría suceder que, en fase incipiente de la investigación se adopte una interceptación de las comunicaciones en base a la existencia de una organización o grupo criminal, mientras que una vez practicadas determinadas diligencias se llegara a observar que se trata de una mera codelincuencia o coparticipación, esto es, la unión o agrupación de personas en la actividad delictiva sin tener la consideración de organización o grupo criminal, de tal forma que, la consecuencia sería que la medida acordada quedaría sin sustento legal. Sin embargo, la aplicación del presupuesto de organización o grupo criminal no habrá de determinar la nulidad de la diligencia, por el mero hecho de que no quede acreditado a lo largo de la investigación dicha circunstancia. Por su parte, la solicitud u oficio del Ministerio fiscal y de la Policía Judicial deberá contener los elementos que fundamenten la medida, en concreto los indicios para creer que se trata de una organización o grupo criminal. En consecuencia, la medida de interceptación de las comunicaciones basadas en este presupuesto tendrán validez, cuando en el momento de su adopción existan evidencias, exteriorizadas en la petición policial o fiscal, pese a que a medida que avanza la investigación quede en entredicho la organización o grupo criminal, en

[320] STS 112/2012, 23 de febrero (F. D. 4º).

[321] STS 714/2016, 26 de septiembre (F.D. 12º).

[322] Acerca de la *"cristalización progresiva",* véase STS Núm. 385/2011, 5 de mayo. O.P. Cit. y STS Núm. Núm. 412/2011, 11 de mayo. O.P. Cit.

cambio, podrá declararse la nulidad de la medida cuando carezca la solicitud, y por ende la autorización judicial, de evidencias claras de la existencia de esa comisión plural y concertada del delito, o bien, cuando la resolución no se ajuste a los principios rectores, en particular la especialidad y proporcionalidad[323].

3.º *Delitos de terrorismo* (art. 579.1. 3.º por remisión del art. 588 ter a. LECrim).

Siguiendo la tradición histórica de política criminal española, así como a consecuencia de los recientes ataques terroristas que están acaeciendo en occidente, el legislador ha incluido el terrorismo como presupuesto para la adopción de una medida de interceptación de las comunicaciones. Como en el supuesto precedente, se diferencian las organizaciones de los grupos terroristas, si bien, resulta de aplicación lo mencionado sobre las organizaciones y grupos criminales (art. 571 CP con la remisión a los arts. 570.1 bis 570.1 ter ambos del CP), por lo que nos remitimos a ello. Por otro lado, la norma procesal no hace mención alguna a las organizaciones y grupos terroristas, seguramente debido a que una inmensa actividad terrorista se comete por los denominados "lobos solitarios", de tal forma que, el presupuesto para la adopción de esta medida comprende toda clase de fines terroristas (arts. 571 a 580 CP según la redacción dada por la L.O. 2/2015, de 30 de marzo), esto es, tanto el individual como el cometido por la agrupación o unión de personas con estructuración organizativa.

En relación con el presupuesto para la investigación del delito de terrorismo mediante la interceptación de las comunicaciones, cabe traer a colación, el régimen extraordinario contemplado en la Constitución española. De esta manera, el art. 55.2 CE viene a establecer que, una Ley Orgánica desarrollará con carácter excepcional, la suspensión,

[323] Examinan MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*... O.P. Cit. Págs. 219-221, la problemática de acordar una diligencia de intervención en las comunicaciones basada en la investigación de un delito cometido en el seno de una organización o grupo criminal, y posteriormente, se aprecia que no existía dicha delincuencia organizada, de tal forma que, como dice expresamente: "La admisión del hecho innegable de que lo que se insinúa como una organización en la fase inicial de investigación puede quedar luego degradado a un simple fenómeno de autoría plural, no es incompatible con la exigencia reforzada al Fiscal o, en su caso, a las Fuerzas y Cuerpos de Seguridad del Estado, de que la afirmación acerca de la concurrencia de un grupo u organización delictivos, cuente con elementales puntos de apoyo, por más que éstos participen de la naturaleza provisional que es propia de la fase incipiente de investigación."

durante el plazo máximo de setenta y dos horas, los derechos fundamentales a la inviolabilidad del domicilio (art. 18.2 CE), el secreto de las comunicaciones (art. 18.3 CE), así como, la detención preventiva (art. 17.2 CE), para la investigación de actuaciones cometidas por bandas armadas o elementos terroristas (esto habrá interpretarlo en organizaciones, grupos terroristas y delitos de terrorismo, pues la expresión banda armada fue suprimida en virtud de la L.O. 5/2010 de reforma del código penal). Debido a lo cual, la reforma procesal implementada con L.O. 13/2015 vino a desarrollar el mandato constitucional, al establecer que, por razón de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas (se mantiene la expresión banda armada, pese a ser una redacción dada en virtud de la L.O. 13/2015, de 5 de octubre) y existan razones fundadas que hagan imprescindible la medida, podrá ordenar el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, la intervención en las comunicaciones telefónicas o telemáticas, debiendo dar traslado al Juez competente[324] en el plazo de veinticuatro horas para su revocación o confirmación (art. 588.3 ter d. LECrim.). Dicho lo anterior, se debe examinar un problema observado, en concreto, como hemos visto anteriormente, la Constitución española establece en el art. 55.2 CE que, determinados derechos fundamentales pueden ser suspendidos excepcionalmente a instancias de órganos políticos para la investigación de delitos de terrorismo. De igual modo, la norma procesal penal hace alusión a que, podrá acordarse *el conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación* (art. 588.2.d. ter d LECrim.). Además, el art. 588.3 ter d. LECrim. que regula este régimen extraordinario, viene a decir expresamente que, *la medida prevista en los apartados anteriores de este artículo,* por lo que, hipotéticamente nada impediría que, en caso de urgencia y para delitos de terrorismo, el ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad pueda acordar la intervención de los mencionados datos de trafico asociados o no asociados. Por su parte, jurisprudencia mayoritaria mantiene que, los datos asociados o metadatos afectan especialmente a la intimidad personal del art. 18.1 CE y/o a la protección de datos o autodeterminación

[324] Con arreglo al artículo primero del Real Decreto-ley 3/1977, de 4 de enero, *sobre competencia jurisdiccional en materia de terrorismo*, en relación con D.T. de la Ley Orgánica 4/1988, de 25 de mayo, *de Reforma de la Ley de Enjuiciamiento Criminal*, el órgano jurisdiccional competente serán los Juzgados Centrales de Instrucción de la Audiencia Nacional.

informativa del art. 18.4 CE[325], de manera que, poca incidencia tienen en los derechos fundamentales expresamente mencionados en el art. 55.2 CE, esto es, la inviolabilidad del domicilio del art. 18.2 CE y el secreto de las comunicaciones del art. 18.3 CE. Por este motivo, bajo nuestro punto de vista, existe una desproporcionalidad en las atribuciones legales a favor de los órganos del ejecutivo aludidos, puesto que, la intervención de los datos asociados, que en muchas ocasiones, si cabe, será más importante conocer esta información que el contenido de la propia comunicación, no tienen incidencia en los derechos fundamentales que pueden ser suspendidos con arreglo al mencionado art. 55.2 CE. Además, autores como Velasco Nuñez[326], vienen afirmando que, pese a que esta situación extraordinaria de suspensión de derechos fundamentales pudiera tener amparo constitucional, lo cierto es que, al existir siempre operativo un Juzgado Central de Guardia en la Audiencia Nacional, resulta innecesario otorgar una facultad de esta índole a órganos políticos, toda vez que, el Ministerio Fiscal o la Policía Judicial podrían solicitar en cualquier momento al Juzgado de Guardia una medida de injerencia en las comunicaciones.

4º *Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación* (art. 588 ter a. *in fine* LECrim).

Un gran número de delitos informáticos tienen penas de prisión relativamente poco elevadas, como por ejemplo la posesión de material pornográfico (art. 189.5 CP), sin embargo, resulta evidente que la única manera de poder combatir estas infracciones es mediante la utilización por parte del Estado de las mismas armas[327]. Por este motivo, se ha incluido como presupuesto para acordar una medida intervención de las comunicaciones, *la investigación de delitos cometidos a través de instrumentos*

[325] STS 740/2017, 16 de noviembre (F.D. 1º); STS 774/2016, 19 de octubre (F.D. 5º).

[326] Así, VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs. 100-101, viene a criticar por innecesaria la intervención política en la restricción de derechos fundamentales al amparo del comentado art. 588.3 ter d. LECrim.

[327] Expone VIVÓ CABO, S. "La globalización del delito: ciberdelincuencia*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 132. 2018, que, para combatir la ciberdelincuencia, los Estados deben utilizar las mismas armas tecnológicas.

informáticos, todo ello, con independencia de la pena que le pudiera corresponder. De igual modo, seguramente pensando en los avances tecnológicos que pudieran surgir, se incluye, además, *los delitos cometidos a través de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*.

Sin embargo, como afirma Rodriguez Lainz[328], no todo delito cometido a través de las nuevas tecnologías justifica su investigación mediante la adopción de una medida de interceptación de las comunicaciones, sino que deberá someterse a un juicio de proporcionalidad, de tal forma que, únicamente se justificará la medida, para aquellos delitos que superen un mínimo de gravedad, pero además, cuando no existan otras medidas menos gravosas, pero igualmente útiles para el esclarecimiento de los hechos. Así, en este contexto, se debe mencionar a título ejemplo, el delito de tenencia de pornografía infantil (art. 189.5 CP), el cual, lleva aparejada una pena relativamente escasa (tres meses a un año de prisión o con multa de seis meses a dos años), si bien, prácticamente la única manera de investigar esta clase de delitos será acordando medidas restrictivas de derechos fundamentales, como la interceptación de las comunicaciones telemáticas o la aprehensión de dispositivos.

b´. Ámbito objetivo de la medida (art. 588 ter b. LECrim.)

El ámbito objetivo de la medida de interceptación de las comunicaciones hace referencia a todo lo que puede ser materia de conocimiento con esta diligencia por parte del Estado. De esta manera, como nos hemos referido anteriormente, puede ser objeto de injerencia, la tradicional comunicación telefónica, es decir, el contenido de la conversación realizada por teléfono, pero también, cualquier otro medio o sistema de comunicación telemática, lógica o virtual[329], como por ejemplo el texto del correo

[328] Advierte RODRÍGUEZ LAINZ, J. L. *"*II. La Autorización Judicial Para la Concesión de una Intervención de Comunicaciones Electrónicas. Presupuestos legales [artículos 588 bis a) y 588 bis b)]. La interceptación de las comunicaciones telefónicas y telemáticas en el Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal de 5 de diciembre de 2014*"*. Diario La Ley. Núm. 8465… O.P. Cit, que, no todo delito cometido a través de la red, justifica a que el Estado pueda acordar una medida de intervención en las comunicaciones telemáticas, sino que se deberá realizar una ponderación exhaustiva de los principios rectores con carácter previo a su adopción.

[329] Ponen de manifiesto, CRESPO BARQUERO, P. *Intervenciones judiciales en materia de comunicaciones telefónicas e internet. (Problemas actuales del proceso penal y derechos fundamentales)*.

electrónico, mensajes de móvil (SMS), etc. Sin embargo, la práctica forense demuestra que, con frecuencia, para evitar ser descubiertos, los delincuentes eluden decir o escribir comentarios que pudiera incriminarles. Por este motivo, la información proporcionada por el contenido de la conversación puede resultar menos útil para la investigación, que los datos que pudieran ser generados con motivo de aquella. Debido a lo cual, el objeto de la medida puede ser también, la intervención de los datos electrónicos de tráfico o asociados a la comunicación, pero también los datos que se produzcan independientemente del establecimiento de la comunicación (art. 588.2 ter b. LECrim)[330]. De esta manera, los datos asociados que menciona la norma procesal, tiene su origen en la Directiva 2002/58/CE (art. 2.b) *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*[331], en la cual, viene a establecer que, son todos aquellas informaciones derivadas de una comunicación o a efectos de la facturación de la misma. De este modo, el Tribunal Europeo de Derechos Humanos, en la pionera sentencia del caso *Malone contra el Reino Unido*, fue la primera vez que se ponía de manifiesto que, los datos asociados a la comunicación[332] pueden afectar a la intimidad, y en consecuencia, debían

---

Editorial Universidad de Deusto. Bilbao. 2010. Págs. 55-104; TORRALBA MENDIOLA, E. C., ROCA I JUNYENT, M. *Derecho a la intimidad: el secreto de las comunicaciones e Internet (Régimen jurídico de internet).* Editorial Wolters Kluwer. Madrid. 2001. Págs. 181-200, que, la intervención de las comunicaciones puede recaer en medios telefónicos, aunque también en medios telemáticos, como conversaciones mantenidas a través de la red.

[330] Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas. «BOE» Núm. 70, de 22 de marzo de 2019. Conclusiones. *3.ª "*Las resoluciones que acuerden la interceptación de comunicaciones telefónicas o telemáticas deberán precisar expresamente si la medida se extiende solo al contenido de la comunicación o incluye también algún dato de tráfico o asociado o algún dato producido con independencia de la comunicación, fundamentando conforme a los principios rectores establecidos en la Ley la procedencia de incluir cada uno de esos datos*".*

[331] «DOCE» 201, de 31 de julio de 2002, 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 (Directiva sobre la privacidad y las comunicaciones electrónicas).

[332] STEDDHH, de 2 de agosto de 1984, Caso de Malone contra el Reino Unido (párrafo 84).

ser merecedores también, de una especial protección. Sin embargo, dicha resolución se refería a los datos de facturación de la comunicación telefónica, toda vez que, aún no se conocía técnicamente las comunicaciones electrónicas o telemáticas modernas. En otro orden de ideas, la conservación de datos relativos a las comunicaciones electrónicas viene regulado por la Ley 25/2007, de 18 de octubre[333] que, a su vez, ha sido la consecuencia de la transposición al derecho interno de la Directiva 2006/24/CE[334], sin embargo, como después se analizará profusamente, la norma comunitaria ha sido declarada nula por el Tribunal de Justicia de la Unión Europea, lo cual, ha supuesto un debate doctrinal y jurisprudencial sobre su validez.

Asimismo, puede ser objeto de intervención la información proporcionada por los terminales sin que se haya producido una concreta comunicación, como por ejemplo la geolocalización. En definitiva, las empresas operadoras de telecomunicaciones manejan numerosos datos de los usuarios, normalmente para la facturación del servicio, de tal forma que, los poderes públicos pueden recabarlos en una investigación. Debido a lo cual, el Juez instructor deberá ponderar el hecho delictivo con el grado de injerencia que será sometido el investigado, para lo cual, la resolución habilitante deberá contener con exactitud la extensión de la medida, toda vez que, no es lo mismo a los efectos de

[333] Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*. «BOE» Núm. 251, de 19 de octubre de 2007. Han abordado la mencionada norma, véase, GONZÁLEZ LÓPEZ, J. J. *Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (Derecho y nuevas tecnologías. Vol. 2).* Editorial Universidad de Deusto. Bilbao. 2011. Págs. 347-362; MISMO AUTOR. *Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.* Derecho y Nuevas Tecnologías. Editorial Universidad de Deusto. Bilbao. 2010. Pág. 61; GONZÁLEZ LÓPEZ, J. J. "Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*"*. Revista General de Derecho Procesal. Núm. 16. 2008.

[334] «DOUE» 105, de 13 de abril de 2006, Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

afectación de los derechos fundamentales, conocer el contenido de la conversación que los datos asociados o la geolocalización del mismo.

c´. Ámbito subjetivo de las intervenciones: cuestión especial de la afectación a tercero no investigado

El ámbito subjetivo de la medida de interceptación hace referencia a que personas pueden sufrir la injerencia en las comunicaciones por parte del Estado. De esta manera, con carácter general el sujeto pasivo de la medida es el investigado, pudiendo ser objeto de intervención los terminales[335] o medios de comunicación que habitual u ocasionalmente sean utilizados por el investigado (art. 588.1 ter b. LECrim), esto es, puede estar dirigida sobre el terminal del que el investigado sea titular, como de aquel otro que pudiera ser utilizado por el mismo, como meramente usuario. Cabe advertir que, se justifica la extensión de la medida incluso a terminales que sean utilizados esporádicamente por el investigado, toda vez que, con frecuencia, los delincuentes, se sirven de diversos terminales o con diferentes titularidades para evitar ser descubiertos. De este modo, se prevé la posibilidad de extender la injerencia en las comunicaciones a terminales o sistemas pertenecientes a terceros en los siguientes supuestos: a) siempre que el sujeto investigado se sirva de aquella para transmitir o recibir información; b) el titular colabore con el investigado o se beneficie de su actividad; o bien, c) cuando el dispositivo sea utilizado maliciosamente por terceros, sin conocimiento de su titular (art. 588 ter c. LECrim.), como por ejemplo mediante el acceso remoto a terminales, sin que se percate de ello su legítimo titular.

[335] Advierte RODRÍGUEZ LAINZ, J. L. "Identificación del terminal y sujeto pasivo en la intervención judicial de comunicaciones". Diario La Ley. Núm. 6585. 2006, que, en la medida de intervención de las comunicaciones el sujeto pasivo es el investigado, si bien, se puede extender a terceros cuando exista justa causa, y en concreto, afirma que, "si la norma procesal habilita el lícito acceso a comunicaciones en las que participa la persona investigada, nos estaría diciendo que podrían ser objeto de injerencia, en un principio, cualesquiera comunicaciones, y cualquiera que fuera el medio o terminal empleado por el sujeto pasivo de la medida. Pero el nudo gordiano de la cuestión no debe encontrarse en tal extensión, como norma de máximos, sino en la aplicación concreta de tal permisividad legal, y, más específicamente, la implicación de los principios constitucionales de proporcionalidad, idoneidad, excepcionalidad y necesidad de la medida a la hora de definir su verdadero alcance".

De esta forma, al tratarse de personas ajenas a la investigación, ya sean por unos hechos desconocidos por su titular, o bien, por la anuencia con el investigado, la resolución judicial habilitante, deberá realizar una motivación reforzada sobre la injerencia en las comunicaciones. No obstante, cuando el investigado se valiera de un terminal ajeno con el consentimiento de su titular, dicha acción podría dar lugar a responsabilidad penal en concepto de, al menos, como cómplice (art. 29 y 63 CP).

En cualquier caso, resulta necesario que, siempre que sea conocido, se haga constar tanto en la solicitud u oficio del Ministerio Fiscal o de la Policía Judicial (art. 588.2.1º. bis b LECrim.), como en la posterior autorización judicial (art. 588.3.a. bis c LECrim.), la identidad del investigado, así como de cualquier otro afectado por la medida, si bien, nuestros tribunales[336] vienen manteniendo que, la falta de concreción en los datos de identidad de los sujetos no es óbice para cuestionar la legitimidad de la medida.

Por otro lado, con carácter excepcional, podrán ser intervenidos los terminales no solo del investigado, sino también de la víctima, de tal forma que, la norma procesal (art. 588.2 ter b LECrim.) positiviza la jurisprudencia de nuestro Tribunal Constitucional[337], al contener la posibilidad de intervenir las comunicaciones de la víctima, cuando sea previsible un grave riesgo para la vida o su integridad. De hecho, esta facultad puede ser de gran utilidad, por ejemplo, en desapariciones o secuestros de personas, como sucediera en el asunto públicamente conocido de la desaparición de Diana María

[336] STC 150/2006, 22 de mayo (F.J. 3º); STC 104/2006, de 3 de abril (F.J. 5º); STS 712/2012, 26 de septiembre (F.D. 2º); STS 309/2010, 31 de mayo (F.D. 13º).

[337] STC 145/2014, de 22 de septiembre (F.J. 3º).

Quer[338], en el cual, se interceptaron las comunicaciones, así como se hallaron sus datos asociados, en especial la geolocalización, con el fin de dar con su paradero[339].

d´. Solicitud u oficio

De esta manera, dentro de las disposiciones comunes se regula de forma genérica el contenido mínimo de la solitud u oficio del Ministerio Fiscal o la Policía Judicial de la autorización judicial para la adopción de las medidas restrictiva de derechos fundamentales (art. 588 bis b LECrim.), sin embargo, como ha sido examinado *supra*, nos remitimos a lo mencionado sobre dicha cuestión. De igual modo, de forma específica para la diligencia de interceptación de las comunicaciones telefónicas y telemáticas, deberá contener también, ciertas particularidades relacionadas con esta medida, concretamente los siguientes extremos: *la identidad del número abonado, del terminal o de la etiqueta técnica, la identificación de la conexión objeto de la intervención y los datos necesarios para identificar el medio de telecomunicación de que se trate* (art. 588.1 ter d. LECrim.). Por este motivo, para que el contenido de la petición de la medida de intervención de las comunicaciones sea completo, la Fiscalía y la Policía deberán de cumplir ambos preceptos de la ley rituaria criminal. De la misma forma, como nos hemos referido cuando exponíamos la petición de la autorización judicial dentro de las disposiciones comunes, nos encontramos ante una regulación, que bien podría entenderse como un *precepto-formulario[340]*, esto es, los solicitantes deberán

[338] Así, en un asunto mediático, la prensa muestra una información en relación a la intervención de las comunicaciones de la víctima, en especial, los datos de tráfico asociados de geolocalización, a los efectos de averiguar su paradero. Véase. "La investigación busca en los últimos veinte minutos del móvil de Diana Quer*"*. Diario La Voz de Galicia. 7 de septiembre de 2017; "Desbloquean el móvil de Diana Quer: alguien intentó acceder a él hasta en siete ocasiones*"*. Diario Faro de Vigo. 6 de julio de 2017.

[339] Sírvase de ejemplo, el procedimiento de diligencias previas Núm. 669/2016 seguido ante el Juzgado de 1ª Instancia e Instrucción Núm. 1 de Ribeira (A Coruña), donde se acuerda la intervención de las comunicaciones de la víctima para descubrir aspectos relevantes a la investigación.

[340] Afirman, MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 231-232, que, la regulación legal sobre la petición de autorización judicial, se asemeja a un formulario que los funcionarios solicitantes deben cumplimentar.

cumplimentar al menos, las exigencias mencionadas en las normas procesales, como si de un formulario se tratara, todo ello, para facilitar la labor de los funcionarios.

Además, la solicitud u oficio deberá determinar la extensión de la medida, el cual, podrá tener por objeto alguno de los siguientes extremos, a saber, el registro y la grabación del contenido de la comunicación, esto es, si se trata de audio, texto, imagen, etc, con indicación de la forma o tipo de comunicaciones a las que afecta, es decir, si está relacionada con la telefonía o con medios telemáticos, el origen y destino al momento de realizarse la comunicación, la geolocalización, o bien, si el conocimiento se extiende a otros datos asociados o no asociados pero de valor añadido como por ejemplo el tráfico de llamadas emitidas y recibidas, la identificación de los titulares de los números de teléfono, etc, y en todo caso, deberán hacer constar los datos concretos que habrán de ser obtenidos (art. 588.2 ter d. LECrim.).

e´. Control de la medida

Siguiendo con el análisis de la medida de interceptación de las comunicaciones, en cumplimiento del art. 588 bis g. LECrim, dentro de las disposiciones comunes que regula el control de las medidas tecnológicas, la Policía Judicial pondrá a disposición del Juez de instrucción, con la periodicidad que éste determine y en los soportes digitales distintos, la transcripción de los pasajes de interés y las grabaciones íntegras realizadas. Además, para garantizar la autenticidad e integridad de la información de los soportes aportados por la Policía Judicial, deberán indicar el origen y destino de cada una de ellas, así como, se asegurarán, mediante un sistema de sellado o firma electrónica que la información volcada desde el ordenador central a los soportes digitales no ha sido alterada (art. 588 ter f. LECrim.). De esta manera, la norma procesal hace referencia a que los sistemas informáticos desde que comienzan a funcionar, están produciendo rutinas, de tal forma que, su contenido se está modificando continuamente. Por este motivo, para garantizar que la información volcada desde el ordenador central, (que, en el caso español, el sistema de escuchas se realiza a través de SITEL -Sistema Integrado de Interceptación de Telecomunicaciones-)[341], a los soportes digitales, no han

[341] SITEL (Sistema Integrado de Interceptación de Telecomunicaciones) es un sistema de escuchas telefónicas dependiente del Ministerio de Interior, que es utilizado por la Policía Judicial, en concreto, la Policía Nacional, la Guardia Civil y el Servicio de Vigilancia Aduanera que, además, comparte los equipos informáticos con el CNI (Centro Nacional de Inteligencia). De igual modo, la STS 250/2009, de

sido alterados, para lo cual, se deberá proceder al encriptado mediante algoritmos matemáticos, denominada la técnica como *hashing*[342], que también es utilizada en la firma electrónica. De este modo, mediante una serie de dígitos o algoritmos se permite reconocer la identidad entre el ordenador central (SITEL) y los soportes digitales (CD, DVD, etc. donde se graban los audios o las imágenes intervenidas) y se vuelca la información, puesto que, ambas numeraciones deben coincidir. De esta forma, cualquier inexactitud en la numeración supone la alteración entre los contenidos, o dicho de otro modo, con esta técnica, hace posible, comparar en todo momento la existencia de alteraciones, y en el supuesto que la hubiera, habría que descartar el material del acervo probatorio del proceso penal. Debido a lo cual, se garantiza la autenticidad e integridad de la información, de manera que, desde su obtención, hasta su aportación a fase de plenario, pasando en su caso, por los peritos encargados de su análisis, no ha sido alterado, esto es, se asegura el respeto a la cadena de custodia[343] tecnológica.

---

13 marzo (F.D. 1º) se viene a explicar el mencionado sistema. Por su parte, los autores que se reseñan a continuación analizan también SITEL: RUIZ DORADO, M., VIDAL MARÍN, T. *Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de Reforma de la Ley de Enjuiciamiento Criminal*… O.P. Cit. Págs. 135-162; RODRÍGUEZ LAINZ, J. L. "SITEL nuevas tendencias, nuevos retos…" O.P. Cit; MISMO AUTOR. "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas…" O.P. Cit. FERNÁNDEZ RODRÍGUEZ, J. J. "La intervención de las comunicaciones digitales a propósito del sistema SITEL…" O.P. Cit. Págs. 61-76.

342 PEREIRA I PUIGVERT, S. *Sistema de "hash" y aseguramiento de la prueba informática. (FODERTICS II: hacia una justicia 2.0)*… O.P. Cit. Págs. 75-83.

343 LEAL MEDINA, J. "Ruptura de la cadena de custodia y desconexión con las fuentes de prueba supuestos concretos, reflexiones que plantea…" O.P. Cit; RUBIO ALAMILLO, J. "Conservación de la cadena de custodia de una evidencia informática…" O.P. Cit; GARCÍA MATEOS, J. A. *Cadena de custodia vs mismidad*. *(La prueba electrónica, validez y eficacia procesal)*… O.P. Cit. Pág. 130; FIGUEROA NAVARRO, M. C. *La cadena de custodia en el proceso penal*… O.P. Cit; RICHARD GONZÁLEZ, M. *La cadena de custodia en el proceso penal español*… O.P. Cit; DEL POZO PÉREZ, M. *La cadena de custodia*. *Tratamiento jurisprudencial*… O.P. Cit. De igual modo, la STS 1215/2009, de 30 diciembre… O.P. Cit, y en concreto, el Voto Particular formulado por Marchena Gómez, adherido por Maza Martín, vienen a exponer las garantías para respetar la cadena de custodia, en los mismos términos que lo mencionado en el texto principal.

f´. Duración y prórroga de la medida

Las medidas tecnológicas, como establece las disposiciones generales, tendrán la duración que se determine su regulación específica (art. 588 bis e. LECrim.), de manera que, acudiendo a las normas reguladoras sobre la diligencia de investigación de intervención en las comunicaciones teléfonicas o telemáticas (art. 588 ter g. LECrim), tendrán una duración máxima de tres meses, siendo el *dies a quo,* desde la fecha de la autorización judicial, independientemente de cuando comience a ser efectiva la misma[344]. Además, podrá ser prorrogada por períodos sucesivos, nunca superiores a tres meses, pero si inferiores, de tal forma que, la práctica habitual de los juzgados es prorrogar cada mes, y todo ello con un plazo máximo de dieciocho meses. De igual modo, para justificar la solicitud de la prórroga, la Policía Judicial deberá aportar la transcripción de los pasajes de las conversaciones más relevantes, con la finalidad de que el Juez pueda, decidir sobre el mantenimiento de la medida, pudiendo éste, además, con carácter previo de ser acordada, solicitar aclaraciones, mayor información, o requerir el contenido íntegro de las conversaciones (art. 588 ter h. LECrim)[345].

En otro orden de ideas, con frecuencia, los delincuentes para dificultar que las comunicaciones puedan ser interceptadas, suelen cambiar de terminales o de número de teléfono, en este caso, será necesaria autorización judicial para ampliar o modificar la medida a esos nuevos terminales. Sin embargo, el plazo máximo referido de dieciocho meses debe interpretarse que, únicamente es aplicable para cada investigado, en una misma causa, independientemente de que pudiera haber utilizado distintos terminales, durante la vigencia de la medida. De igual modo, cuando en un procedimiento penal se

[344] STC 68/2010, de 18 de octubre (F.J. 2º); STC 26/2006, de 30 de enero (F.J. 9º); STS 504/2015, de 24 de julio (F.D. 1º).

[345] FUENTES SORIANO, O. *Medio de investigación tecnológica y Problemas probatorios. (El proceso penal. Cuestiones fundamentales)*… O.P. Cit. Págs. 253-385; VILLAR FUENTES, I. *Lección 6. Actos de investigación limitativos de derechos fundamentales. (Lecciones breves de derecho procesal penal*). Editorial Comares. Granada. 2017. Págs. 63-72; VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015...* O.P. Cit. Pág. 104; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 263-266.

intervengan las comunicaciones del investigado, y cese la medida, por haber transcurrido el plazo, sin haberse acordado su prórroga, o bien, al desaparecer las circunstancias que justificaron su adopción, sin embargo, con posterioridad, se vuelve a reanudar, como por ejemplo debido a que se han encontrado nuevos hechos que evidencien que el delincuente ha retomado la actividad delictiva, habrá que estar al cómputo general, de tal forma que, una vez iniciado el nuevo plazo, se deberá deducir el plazo transcurrido anterior, no pudiendo superar entre ambos, el cómputo máximo de dieciocho meses. A mayor abundamiento, cabe advertir que, como la interceptación de las comunicaciones se produce en pieza separada y secreta (art. 588 bis d. LECrim.), mientras esté vigente ésta, no son de aplicación los plazos generales de instrucción (art. 324.1 LECrim.); a esto, hay que añadir que, *las diligencias de investigación acordadas con anterioridad al transcurso del plazo o de sus prórrogas serán válidas, aunque se reciban tras la expiración del mismo* (art. 324.2 LECrim.)[346].

g´. El acceso de las partes a las grabaciones

Para que las partes privadas (acusación particular o popular y defensa) puedan tener conocimiento del contenido del material intervenido, se precisa el alzamiento del secreto, y el cese en una misma causa de la vigencia de todas ellas (art. 588.1 ter i. LECrim.). Evidentemente, el secreto de la pieza separada tiene como finalidad evitar que, la diligencia de injerencia en las comunicaciones pierda eficacia, es por ello que, hasta que subsista una sola medida en una misma causa que afecte a alguno de los investigados, deberá mantenerse la reserva de la información. Sin embargo, expirada la última medida de interceptación, alzado el secreto, tanto de la pieza separada, como del genérico por los motivos expuestos en la ley (art. 302 LECrim.), se deberán hacer entrega a las partes privadas (puesto que el Ministerio Fiscal tiene acceso desde el inicio), copia de las grabaciones y de las transcripciones realizadas, momento en el cual, comenzará una fase contradictoria, donde las partes, en el plazo fijado por el Juez, podrán solicitar la inclusión de aquellas comunicaciones que entiendan relevantes y hayan sido excluidas, resolviendo el mismo sobre su exclusión o incorporación a la causa (art. 588.2 ter i. LECrim.). Además, cuando no sean relevantes con el objeto de la

[346] Art. único de la Ley 2/2020, de 27 de julio. «BOE» núm. 204, de 28 de julio de 2020, por la cual, se viene a implementar la reforma del art. 324 LECrim.

investigación, habrá de excluir de la entrega, los pasajes donde aparezcan aspectos de la vida íntima de las personas, debiéndose hacer constar de modo expreso esta circunstancia. Así, el tratamiento para las grabaciones íntimas de los investigados resulta ser similar al tradicional sistema implantado por el Ministro de Gracia y Justicia el Alonso Martínez en la Ley de Enjuiciamiento Criminal de 1882[347] para la apertura de la correspondencia escrita y telegráfica, de tal forma que, el Juez aparta la que haga referencia a los hechos de la causa, mientras que, la que no esté relaciona será entregada al procesado (arts. 586 y 587 de la LECrim.). Seguidamente, se produce una fase procesal contradictoria, donde las partes pueden solicitar que, se excluyan de la causa extremos irrelevantes, en especial pasajes con contenido íntimo, o en su caso, que se incluyan conversaciones que a su entender sean beneficiosas para sus intereses, y en vista de ello, el Juez decidir sobre su pertinencia.

Una vez transcurrido el plazo fijado por el Juez de alegaciones, se producirá la preclusión sobre la inclusión o exclusión de los pasajes no introducidos por las partes en el debate contradictorio mencionado[348], siendo el momento procesal oportuno para la selección de los contenidos en la fase de instrucción[349]. Sin embargo, al incidir en los derechos fundamentales consagrados en el art. 18 CE, se debería flexibilizar esta cuestión, permitiendo su discusión en momentos posteriores, como en la fase intermedia con los escritos de calificación provisional (arts. 649 a 658 LECrim. para el juicio ordinario, mientras que para el procedimiento abreviado los arts. 781 y 784 LECrim.), o bien, en el trámite de cuestiones previas al comienzo de la vista en los procedimientos

[347] Gaceta de Madrid, martes, 3 de octubre de 1882, Núm. 276, Tomo IV, págs. 17-22.

[348] MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento* Criminal *en 2015.* O.P. Cit. Págs. 271-281.

[349] Respecto al trámite contradictorio dirigido a seleccionar o impugnar los pasajes de la intervención de las comunicaciones que constan en las actuaciones, véase VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015…* O. P. Cit. Págs.105-106; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015…* O.P. Cit. Págs. 271-274; GÓMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Derecho Jurisdiccional III, Proceso Penal)*. O. P. Cit. Págs. 224-225.

abreviados (art. 786.2 LECrim.), o como cuestiones de previo pronunciamiento en el juicio ordinario (arts. 666 a 678 LECrim.)[350].

Aunque se trate de una problemática procesal que surge principalmente en fase plenaria, se encuentra estrechamente relacionado con el tratamiento procesal de la reproducción de las grabaciones realizadas que constan en las actuaciones. De esta manera, una vez entregadas las copias de las grabaciones a las partes, transcurrido el plazo del incidente sobre la selección del contenido (art. 588.2 ter i. LECrim), cabe preguntarse sí, es necesario a los efectos probatorios reproducir las cintas[351]. De este modo, el Tribunal Supremo[352] ha venido entendiendo que, una vez alzado el secreto y expirada la medida, no es necesario proceder a la audición de las grabaciones en fase de instrucción, pero tampoco, en la fase de juicio oral, en el momento de la práctica de la prueba. De esta forma, las grabaciones o "*cintas*" deberán ser custodiadas por el Letrado de la Administración de Justicia con todas las garantías, para ello, se deberán transcribir los pasajes más importantes, debiendo el Letrado de la Administración de Justicia cotejar su contenido, y conservar las grabaciones originales. Además, la transcripción de los

[350] STS 247/2010, de 18 marzo, el tribunal *a quo* resolvía sobre la validez en fase preliminar del juicio oral de unas determinadas pruebas obtenidas, si bien, tras su práctica, declararía que, gran parte de las pruebas eran nulas, por verse afectados los derechos fundamentales, y en concreto, el secreto de las comunicaciones y la intimidad.

[351] Sobre la necesariedad de la reproducción de las grabaciones o cintas, GÓMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Derecho Jurisdiccional III, Proceso Penal)*. Editorial Tirant Lo Blanch. Valencia. 2015. Págs. 225; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 274-276, si bien, este último, viene a afirmar que, "y es preciso reconocer que, en esta materia, como en tantas otras, la jurisprudencia no ha seguido una corriente uniforme, hasta el punto de detectarse una evolución en la que las resoluciones más recientes —éstas sí, con un alto grado de consolidación- nada tienen que ver con el nivel de exi¬gencia de los primeros pronunciamientos. Desde una obligada audición de los contenidos a los que pretende atribuirse valor probatorio a un criterio mucho más flexible en el que la no reproducción de esas grabaciones —en el caso de que se trate de conversaciones telefónicas- se percibe como una práctica habitual no censurable (cfr. SSTS 646/2014,8 de octubre; 250/2014, 14 de marzo; 538/2001, 30 de mar¬zo y 1954/2000, 1 de marzo)*"* (Pág 275).

[352] STS 195/2014, de 3 de marzo (F.D. 5º).

pasajes tendrá la consideración a los efectos de prueba de documento (art. 26 CP), lo cual, supone que podrán tenerse por reproducidas[353], sin que sea necesaria su audición, aunque se deberá permitir a las partes debatir sobre su contenido[354]. Sin embargo, no faltan ejemplos en la jurisprudencia[355] que interpretan que, las grabaciones para que sean consideradas como prueba de cargo suficiente, deberán ser introducidas en el debate contradictorio del plenario, ya sea con la audición directa del contenido, mediante la lectura de la diligencia documental donde se transcribe la grabación, o bien, a través de las declaraciones practicadas en juicio, en especial, las testificales de los agentes intervinientes en las escuchas. Además, el momento procesal para que las partes puedan solicitar la audición de las cintas en el juicio oral es en la fase intermedia con los escritos de calificación provisional (art. 728 LECrim)[356], toda vez que, como se sabe es, con dicho trámite, cuando las partes proponen la práctica de la prueba que quieran hacer valer para el acto de la vista, todo ello, sin perjuicio de las excepciones relativas a los careos de los testigos, las propuestas por el Tribunal o las propuestas en el propio acto por las partes (art. 729 LECrim)[357]. De lo mencionado hasta el momento, se desprende que, la jurisprudencia mantiene que, deberán reproducirse las grabaciones, o bien, introducirlas en el juicio, de alguna forma válida en Derecho, a fin de originar en la vista, bajo los principios de inmediación, contradicción y oralidad[358], debate

[353] STC 26/2010, de 27 abril (F.J. 5º), así, se viene a otorgar validez a la forma procesal de tener por reproducida la documental consistente en la transcripción de los pasajes.

[354] STS, de 5 febrero 1988 (F.D. 6º), aquí, se dice que, se debe permitir debate contradictorio de las partes en la transcripción del contenido de los pasajes de la grabación.

[355] STC 121/1998, de 15 junio (F. J. 5º).

[356] Abordan el contenido de los escritos de calificaciones, MUÑOZ CUESTA, J. *¿Es posible proponer prueba después del escrito de acusación o defensa en el procedimiento por sumario ordinario?* Repertorio de Jurisprudencia Aranzadi. Núm. 7. 2006. Págs. 21377-21380; MALUENDA MARTÍNEZ, A. *Contenido del escrito de acusación en el Procedimiento Abreviado.* Iuris: Actualidad y práctica del derecho. Núm. 193. 2013. Págs. 23-24, y en concreto, vienen a afirmar que, de ordinario, se trata del momento procesal para la solicitud de las pruebas a practicar en el plenario.

[357] STS 511/1999, de 24 marzo (F.D. 1º).

[358] STS 211/1995, de 17 febrero (F.D. 5º) y STS 584/1995, de 28 abril (F.D. 4º).

contradictorio entre las partes[359]. Sin embargo, cuando la grabación no suscitara controversia, resulta innecesaria su audición en el plenario, bastando pues, que se tenga por reproducida. De igual modo, se podrá solicitar la audición de aquellos fragmentos que se consideren más relevantes, debiendo permanecer las grabaciones íntegras bajo custodia judicial por si fuera necesario proceder a su cotejo[360].

Asimismo, la norma procesal establece como garantía que, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones, el juzgado deberá notificar a las personas intervinientes en las comunicaciones interceptadas pero ajenas a la causa penal, el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, teniendo el derecho, además, de solicitar la entrega de las grabaciones o las transcripciones, a excepción de que se vea afectado el derecho a la intimidad de terceros o resulte perjudicial a los fines del proceso (art. 588.3 ter i. LECrim.). Esta regulación, pretende evitar una práctica poco deseable que en ocasiones, ha realizado la Policía Judicial, que consiste en, solicitar a la autoridad judicial una medida de interceptación de las comunicaciones para la investigación de un delito grave, para lo cual, en el oficio se hace constar una lista de números de teléfono del investigado, pero a estos, se añaden otros teléfonos, que nada tienen que ver con la actividad delictiva investigada, y así, pueden intervenir las comunicaciones de otras personas con el plácet judicial. En cualquier caso, este tratamiento garantista de la intervención de las comunicaciones a terceros, será de difícil aplicación por los juzgados, dada la complejidad en averiguar y comunicar a todos los terceros no investigados que han sido objeto de una medida restrictiva de derechos fundamentales, así como, en contadas ocasiones, los juzgados dedicarán recursos para dicho fin, salvo circunstancias excepcionales, como personas de interés público o que el propio interesado expresamente lo solicite.

---

[359] Indican, DE URBANO CASTRILLO E. *Las nuevas exigencias de los principios de contradicción, oralidad, inmediación y publicidad*. Revista del Poder Judicial. Núm. Extra 19. 2006. Págs. 151-176 y BUENO DE MATA, F. *La práctica de la prueba electrónica en sede judicial ¿vulneración o reforzamiento de principios procesales?* Diario La Ley. Núm. 8332. 2014, que, se deberán reproducir las grabaciones, o bien, introducirlas en el juicio, de alguna forma válida en Derecho, a fin de originar en la vista, debate contradictorio, bajo los principios de inmediación, contradicción y oralidad.

[360] STS 972/2010, de 29 septiembre (F.D. 3º), expone lo innecesario de oir la totalidad de las cintas.

h´. Deber de colaboración

Por último, en relación con la diligencia de investigación de interceptación de las comunicaciones telefónica y telemática es preciso añadir el deber de colaboración que, se le exige a toda empresa prestadora de servicios de telecomunicaciones, o incluso, persona física que contribuya a facilitar las comunicaciones a través de cualquier dispositivo, están obligados a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados la asistencia y colaboración precisas para facilitar la ejecución de la medida (art. 588.1 ter. e. LECrim.)[361]. De esta manera, la base constitucional del deber de colaboración aludido, procede del art. 118 CE, al establecer en el mismo, la obligación de cumplimiento de todas las resoluciones judiciales firmes, así como, de prestar colaboración cuando fuera requerido por los órganos jurisdiccionales en el curso del proceso. De igual modo, las empresas operadoras de telecomunicaciones son adjudicatarias de una concesión otorgada por la Administración Pública para explotar el servicio (regulado en la Ley 9/2014, de 9 de mayo, *General de Telecomunicaciones*[362]), lo cual, hace que se establezca entre ellas, una relación jurídica de sujeción especial donde el adjudicatario está inmerso en una organización administrativa, respecto de la cual, se encuentra en una situación de dependencia con las instituciones públicas, materializándose entre otras cuestiones, en la obligación de prestar al Juez, el Ministerio Fiscal o los agentes de la Policía Judicial designados, la ejecución técnica de la medida (arts. 39 y 40 LGT).

[361] Sobre el deber de colaboración de las empresas prestadoras de los servicios de telecomunicaciones con la Administración de Justicia, con arreglo a la legislación procesal, véase, con carácter general, ENCINAR DEL POZO, M. A. y otros. *Ley de Enjuiciamiento Criminal con jurisprudencia sistematizada*. Editorial Tirant Lo Blanch. Valencia. 2017. Pág. 878; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*... O.P. Cit. Págs. 286-336; VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs.101-103; GÓMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Derecho Jurisdiccional III, Proceso Penal)*… O.P. Cit. Págs. 225-226.

[362] Ley 9/2014, de 9 de mayo, *General de Telecomunicaciones.* «BOE» Núm. 114, de 10 de mayo de 2014.

Así, las operadoras de servicios de telecomunicaciones, además de la exigencia del deber de secreto genérico respecto de las comunicaciones realizadas por sus usuarios (art. 39.1 LGT), se les impone también, la obligación de guardar secreto sobre el contenido del material intervenido, así como, de colaborar con los poderes públicos en una investigación (art. 588.2 e. LECrim.), y en caso contrario, aunque no lo diga expresamente la norma procesal, podrán incurrir en el delito de revelación de secretos cometido por funcionario público (art. 417 CP), al ser considerado como tal, de acuerdo con el art. 24.2 del CP, que establece que, se considerará funcionario público todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas, en este caso, en virtud del requerimiento judicial de ejecución técnica de la medida (art. 24.2 CP). De igual modo, el incumplimiento de cualquier deber de colaboración por la omisión del requerimiento efectuado por los poderes públicos, podrá suponer que incurran estas empresas, en la comisión del delito de desobediencia (art. 556 CP).

Por otro lado, como hemos estudiado, la medida de interceptación de las comunicaciones puede alcanzar también, a los datos de tráfico asociados o no asociados (art. 588.2.d. ter d. LECrim.), de esta manera, el deber de colaboración examinado, podrá extenderse igualmente a estos datos. Por este motivo, seguidamente vamos a examinar la incorporación al proceso de los datos electrónicos de tráfico o asociados, si bien, dada su importancia, así como, su problemática sobre su validez, hemos decidido dedicar un apartado específico a desarrollar dicha cuestión que será abordada en el epígrafe siguiente.

d) Incorporación al proceso de datos electrónicos de tráfico o asociados

Como hemos mencionado anteriormente, la medida de interceptación de las comunicaciones puede comprender también, los datos electrónicos de tráfico o asociados que obran en poder de las empresas prestadoras de servicios de telecomunicaciones. De esta manera, los datos de tráfico asociados a las comunicaciones pueden ser de gran valor para las autoridades para esclarecer la actividad delictiva. De igual modo, los datos de tráfico o asociados, son informaciones relacionadas con un proceso comunicativo, si bien, al margen del contenido de la propia comunicación, de tal forma que, no se vería afectado el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE), en el cual, la Constitución española expresamente

refiere que, únicamente pueden restringirse mediante resolución judicial. En cambio, los datos de tráfico inciden en la intimidad personal (art. 18.1 CE) y/o protección de datos o autodeterminación informativa (18.4 CE)[363] que, en caso, no exige expresamente nuestra Constitución para su injerencia la intervención judicial. Sin embargo, nuestro legislador ha preferido conferir a estos datos el máximo nivel de protección, al exigir que, únicamente pueden ser cedidos para su incorporación al proceso con autorización judicial (art. 588.1 ter j. LECrim.)[364]. De este modo, toda empresa prestadora de servicios de comunicación, o en su caso, particulares que faciliten la comunicación solo podrán ceder datos de tráfico o asociados de sus usuarios o clientes, mediante autorización judicial, para lo cual, los agentes facultados de la Policía Judicial podrán solicitar al Juez competente que recabe la información que conste en los archivos automatizados de los prestadores de servicios, pero únicamente será acordada cuando el conocimiento de los datos sean indispensables para la investigación. Además, se podrá solicitar la 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 (art. 588.2 ter j. LECrim.), como por ejemplo, vincular un terminal móvil o varios, en el lugar de la comisión del delito, buscar números de teléfonos en una zona geográfica concreta, en una franja de tiempo determinado, para ver la coincidencia con el momento de la comisión del delito, conjuntamente con ello, cruzar datos con otra localización en otra fecha donde se cometió un delito similar, con el objeto de conocer la existencia de alguna vinculación entre ellos, etc. En cualquier caso, la autorización judicial deberá determinar el alcance, fijando que datos deben ser objeto de cesión. Sin embargo, al tratarse de una injerencia menor que no afecta a informaciones relacionadas con el derecho al secreto de las comunicaciones (art. 18.3 CE), como el mensaje o contenido

[363] STS 740/2017, 16 de noviembre (F.D. 1º) y STS 400/2017, 1 de junio (F.D. 2º).

[364] Para la cesión de los datos de tráfico, nos remitimos entre otros, TEJADA DE LA FUENTE, E. *Capítulo II. La conservación de datos informáticos con fines de investigación criminal: requisitos y condiciones para la su incorporación al proceso penal. (Investigación tecnológica y derechos fundamentales).* Editorial Aranzadi. Navarra. 2017. Págs 123-145; VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs. 106-108; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 286-304, afirman que, será necesaria adoptar una resolución judicial al efecto.

de la comunicación o la identidad subjetiva de los interlocutores, vienen otorgando validez nuestros Tribunales[365] a ciertas medidas de investigación injerentes en el derecho a la intimidad acordadas por mera providencia, esto es, sin motivación alguna o con motivación sucinta.

De esta forma, como venimos exponiendo se establece que, mediante autorización judicial, se podrá requerir para su incorporación al proceso penal, los datos asociados a la comunicación que posean las empresas prestadoras de servicios de telecomunicaciones por motivos comerciales, esto es, informaciones que les sirve a éstas, para la facturación del servicio (llamadas entrantes o salientes, duración, titulares de la línea, geolocalización, etc.), o bien, *en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas* (art. 588.1 ter j. LECrim.). Por este motivo, la norma procesal debe ser completada con la legislación sobre retención de datos, esto es, con la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[366], que a su vez, derivaba de la transposición al derecho interno español, de la Directiva 2006/24/CE, de 15 de marzo, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*[367] *y por la que se*

[365] Sírvase de ejemplo, algunas resoluciones judiciales que acuerdan injerencias en la privacidad acordadas mediante simple providencia: STS 187/2015, 14 de abril (F.D. 5º) y STC 123/2002, 20 de mayo (F.J. 7º).

[366] En relación con la Ley 25/2007, de 18 de octubre, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*, BOE 251 de 19 de octubre de 2007, así, ORMAZÁBAL SÁNCHEZ, G. "Los deberes de conservación de datos por parte de los operadores de telecomunicaciones y su aportación al proceso mediante requerimiento judicial*"*. Diario La Ley. Núm. 7054-7056. 2008, viene afirmando que, "la exclusión absoluta de los procesos civiles, laborales y contencioso-administrativos que parece deducirse de la letra del precepto constituye, sin duda, una grave consecuencia que puede condenar al fracaso numerosas pretensiones ejercitadas fuera del proceso penal y que, por tanto, merece ser objeto de algún comentario. Antes de ello, es preciso examinar la reciente sentencia del TJUE, de 29 enero 2008, en la que se contiene un pronunciamiento sobre la adecuación al Derecho europeo de la normativa española que consagra la referida limitación a las causas penales de los deberes de conservar y comunicar datos por requerimiento judicial*"*.

[367] DOUE 105, de 13 de abril de 2006.

modifica 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*[368]. Llegados a este punto, conviene dedicar unas líneas a exponer, por las razones que después se explicarán, las normas comunitarias mencionadas. En concreto, la Directiva 2002/58/CE[369], establece que, los Estados miembros podrán adoptar medidas legislativas, para que, por motivos de seguridad o de investigación y persecución de delitos (art. 15), puedan obligar a las empresas operadoras de estos servicios conservar datos electrónicos de tráfico (art. 5 y 6) y/o los datos de localización (art. 9) de sus clientes durante un plazo limitado. Además, con arreglo a la norma comunitaria estudiada, los datos de tráfico son *cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma* (2.b), mientras que, los datos de localización son, de igual modo *cualquier dato tratado en una red de comunicaciones electrónicas* que también, *indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público* (2.c), de manera que, se trata de toda información vinculada a un proceso de comunicación como puede ser la identificación de los interlocutores, el número de usuario, la duración de la llamada, la geolocalización de los mismos, etc. Por su parte, la Directiva 2002/58/CE tiene carácter potestativo, esto es, se deja a los Estados miembros optar sobre si desean o no, que su derecho interno contenga una legislación restrictiva en las libertades comunicativas, de tal forma que, como no es preceptiva su transposición, el Estado español nunca aprobaría ley alguna sobre esta materia. Posteriormente, la Unión Europea aprobaría la Directiva 2006/24/CE[370] que

[368] DOUE 201, de 31 de julio de 2002.

[369] DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J. *Las obligaciones de los prestadores de servicios de internet a partir de la Directiva 2002/58/CE. Derecho Penal informático…* O.P. Cit. Págs. 255-257; HERRÁN ORTIZ, A. I. *La nueva Directiva europea 2002/58/CE sobre privacidad y comunicaciones electrónicas (XVIII Encuentros sobre Informática y Derecho, 2003-2004)*… O.P. Cit. Págs. 77-92.

[370] Respecto a la Directiva 2006/24/CE, AGUILERA MONTENEGRO, C. "Repercusiones de la transposición de la Directiva 2006/24/CE al ordenamiento español y su incidencia en el derecho al secreto de las comunicaciones*"*. Diario La Ley. Núm. 8140. 2013, afirma que, "debe hacer reflexionar al legislador, a la hora de transponer las directivas comunitarias a la legislación interna… por ser distintas

contenía las bases para que los Estados miembros regularan sobre las medidas que debían adoptar para que las empresas prestadoras de servicios de telecomunicaciones, por un plazo no superior a dos años y nunca inferior a seis meses (art. 6), conservaran datos de tráfico, de localización y los necesarios para identificar al abonado o usuario, en concreto los datos de identificación del origen o destino de la comunicación, la fecha, hora, duración, el tipo o el equipo de comunicación de los usuarios y la localización del equipo de comunicación móvil (art. 5). De este modo, con arreglo a regulación contenida en la Directiva 2006/24/CE, las operadoras de telecomunicaciones debían conservar los datos privados de todos los usuarios de internet y telefonía, independientemente de su finalidad, incluso, en caso de incumplimiento, podría acarrear para éstas, responsabilidades administrativas y penales (art. 13). Además, la norma comunitaria vino a conferir como plazo hasta el 15 de septiembre de 2007 (art. 15) para que los Estados miembros transpusieran al derecho interno su contenido, de tal forma que, en España se materializaría de acuerdo con la mencionada Ley 25/2007[371], *de conservación de datos.*

De esta manera, la ley española, en cumplimiento de la Directiva 2006/24/CE, viene a establecer la obligación de las empresas operadoras de servicios de telecomunicaciones de retener y conservar determinados datos de sus usuarios para, previa autorización

las diversas legislaciones*"*. Por su parte, RODRÍGUEZ LAINZ, J. L. "Reflexiones en torno al informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)*"*. Diario La Ley. Núm. 7706. 2011, dice expresamente que, *ha quedado patente que la necesidad de revisión y reforma de la Directiva 2006/24/CE alcanza el nivel, si no de lo imperioso, al menos de lo conveniente.* De igual modo, REDACCIÓN DIARIO LA LEY. "Luces y sombras de la Directiva de conservación de datos de telecomunicaciones*"*. Diario La Ley. Núm. 7636. 2011, se advierte que, "lo cierto es que la Comisión Europea no es la única institución que se ha mostrado crítica con la Directiva 2006/24, de conservación de datos, sino también las autoridades de protección de datos. Éstas opinan que no se encuentra suficientemente limitada la conservación de datos ni se ofrecen garantías suficientes sobre la forma en que se almacenan los datos, se accede a ellos y se utilizan*"*.

[371] En relación a la Ley 25/2007, véase con carácter general, GONZÁLEZ LÓPEZ, J. J. "Comentarios a la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*"*. Revista General de Derecho Procesal. Núm. 16. 2008; CUBERO MARCOS, J. I, ABERASTURI GORRIÑO, U. "Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos*"*. Revista Española de Derecho Constitucional. Año núm. 28. Núm. 83. 2008. Págs. 175-197.

judicial, ponerlos a disposición de los agentes facultados de la Fuerzas y Cuerpo de Seguridad del Estado, de los funcionarios de la Dirección Adjunta de Vigilancia Aduanera cuando realicen funciones de Policía Judicial y del personal del Centro Nacional de Inteligencia (art. 6 Ley 25/2007)[372]. Además, pueden ser objeto de conservación únicamente los datos de tráfico, de localización y los necesarios para identificar al abonado o usuario registrado, de tal forma que, se excluye, todo aquel que corresponda al contenido propio de las comunicaciones (art. 1 y 3 Ley 25/2007). De igual modo, se establece un plazo de conservación de los datos de todos los usuarios por doce meses, pudiendo ser reglamentariamente aumentado o reducido hasta un máximo de dos años o un mínimo de seis meses (art. 5.1 Ley 25/2007), sin perjuicio, del periodo de bloqueo previsto en la Ley Orgánica de Protección de Datos (art. 32 de la L.O. 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*[373], en relación con el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[374] *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*). De esta forma, cuando las empresas de telecomunicaciones reciban un requerimiento judicial de cesión de datos, de acuerdo con la autorización adoptada a tal efecto, tendrán la obligación en el plazo que expresamente establezca el mismo, de poner a disposición de los agentes facultados, o dicho de otro modo, del personal de Policía Judicial o CNI designados para su tratamiento, la información solicitada, incurriendo para el caso de incumplimiento, en responsabilidad administrativa sancionadora o penal (art. 10 Ley

[372] Mantiene ALVAREZ HERNANDO J. Y CAZURRO BARAHONA. V., *Practicum. Protección de datos. 2016*. Editorial Aranzadi. Pamplona. 2015. Págs. 102-105, que resulta necesaria autorización judicial para la cesión de datos de tráfico, de tal forma que, la forma de proceder será entregando la información a la Policía Judicial, o en caso, a los miembros del CNI.

[373] Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*. «BOE» Núm. 294, de 6 de diciembre de 2018. De este modo, el art. 32 de la L.O. 3/2018, regula el bloqueo de datos cuando proceda su rectificación o supresión que, en su caso, quedarán a disposición exclusiva de los Jueces y Tribunales, el Ministerio Fiscal o las Administraciones Públicas, para la exigencia de posibles responsabilidades derivadas de su tratamiento y por el solo plazo de prescripción que se establezca en las mismas.

[374] DOUE Núm. 119, de 4 de mayo de 2016. Págs. 1-88.

25/2007). Así, la norma excluye la posibilidad de los usuarios (art. 9 L. 25/2007) de ejercer los derechos de acceso y cancelación contenidos en la Ley Orgánica de Protección de Datos (arts. 13 y 15 L.O. 3/2018 y arts. 15 y 17 Reglamento UE 2016/679), de tal forma que, las operadoras de telecomunicaciones se les prohíbe informar a sus usuarios sobre qué datos son cedidos, así como, denegarán cualquier solicitud de cancelación.

Una vez examinado el régimen jurídico, de conformidad con las normas españolas y comunitarias, que venían a establecer la obligación de las empresas prestadoras de servicios de telecomunicaciones de conservar determinados datos de sus usuarios, para su cesión a requerimiento judicial, venimos a desarrollar un problema de gran calado suscitado sobre esta materia. De esta manera, el inconveniente surge a raíz de la declaración de nulidad[375] de la Directiva 2006/24/CE mediante la Sentencia del

[375] En relación con la declaración de nulidad de la Directiva 2006/24/CE, con carácter general, VON DANWITZ, T. "Conservación de datos generados o tratados en comunicaciones electrónicas en relación con la prestación de estos servicios TJ Gran Sala, S 8 abr. 2014*"*. La Ley Unión Europea, mes 15, 2014. Págs. 44-45; *El TJUE declara la disconformidad a Derecho de la Directiva 2006/24 de conservación de datos (Tribunal de Justicia de la Unión Europea, Sala Gran Sala, Sentencia de 8 abr. 2014, Asunto C-293/2012).* Repertorio Mensual de Jurisprudencia. Núm. 6. 2014. Pág. 5. Asimismo, BALLESTEROS MOFFA, L. A. "La difícil situación de la Ley 25/2007 de conservación y cesión de datos de tráfico y localización en las comunicaciones electrónicas: la «tala» de su base comunitaria y los desfavorables vientos desde sus homólogas europeas*"*. Revista Aranzadi de Derecho y Nuevas Tecnologías. Núm. 44. 2017, afirma que, "la invalidez de la Directiva 2006/24/CE por incompatibilidad con el principio de proporcionalidad plantea indefectiblemente su repercusión sobre las Leyes de transposición y, en particular, sobre la LCD. La cual se ha mantenido con una mínima modificación técnica de sus arts. 6.2, 7.3, 10 y ap. 5 de la Disp. adic. única, por parte de la Disp. final cuarta de la LGT, que ha precisado la cesión de datos a los agentes facultados e incluido mayores exigencias de control de los datos por las empresas conforme a un específico régimen sancionador*"*. Por su parte, 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. Núm. 8308. 2014, mantiene que, "las legislaciones internas, al amparo de la resucitada posibilidad de regular excepciones al estricto régimen de tratamiento y conservación de datos relativos a las comunicaciones, pueden dar forma y contenido a cada uno de los déficits de normatividad de los que adolece la Directiva 2006/24/CE. En definitiva: una norma nacional que, dictada dentro del margen de lo facultado por el art. 15.1 Directiva 2002/58/CE, hiciera frente a las necesidades de definición normativa que están detrás de la no superación del juicio de proporcionalidad y necesidad de aquélla, quedaría ajena sin duda a las consecuencias de la declaración de invalidez decretada por la STJUE de 8 de abril de 2014". Del mismo modo, GARCÍA DE

Tribunal de Justicia (Gran Sala), de 8 de abril de 2014, que venía a resolver dos cuestiones prejudiciales[376], la primera formulada por la Corte Suprema de Irlanda[377] (asunto C-293/12), y la segunda interpuesta por el Tribunal Constitucional de Austria[378] (asunto C-594/12)[379]. De esta forma, los órganos jurisdiccionales de los Estados europeos, plantearon al Tribunal de Justicia Europeo la validez de la Directiva 2006/24/CE, al consultar sí la norma europea respetaba el principio de proporcionalidad, toda vez que, la acción de la Unión Europea podría exceder de lo estrictamente necesario para alcanzar los objetivos de los Tratados (art. 5.4 TUE), así como, si la norma comunitaria objeto a debate, atentaba contra los derechos fundamentales respecto de las comunicaciones de la vida privada y familiar (art. 7 Carta de los Derechos Fundamentales de la Unión Europea), de la protección de datos de carácter personal (art. 8 Carta), de libertad de expresión y de información (art. 11 Carta).

Pues bien, los argumentos esgrimidos en la sentencia (apartados 31, 34, 35 y 36) pueden resumirse en que, la obligación de conservación de los proveedores de servicios de

---

PABLOS, J. F. "La invalidez de la Directiva europea sobre conservación de datos*"*. Revista Aranzadi de Derecho y Nuevas Tecnologías. Núm. 35. 2014. Págs. 23-42, entiende que, "la Ley española 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, al transponer estrictamente la Directiva 2006/24/CE, declarada inválida por el TJUE, ha de modificarse de acuerdo a lo señalado por el TJUE en la sentencia comentada de 8 de abril de 2014. Así, la futura reforma deberá establecer unas reglas claras y precisas que regulen la conservación de datos y el acceso a los mismos por las autoridades competentes, al mismo tiempo que garanticen a los particulares, cuyos datos se han conservado, las garantías suficientes referentes a la protección eficaz de sus datos personales contra riesgos de abuso o utilización ilícita".

[376] Art. 267 del Tratado de Funcionamiento de la Unión Europea: *El Tribunal de Justicia de la Unión Europea será competente para pronunciarse, con carácter prejudicial: a) sobre la interpretación de los Tratados; b) sobre la validez e interpretación de los actos adoptados por las instituciones, órganos u organismos de la Unión.*

[377] Corte Suprema de Irlanda, en inglés, "*High Court of Ireland"*.

[378] Tribunal Constitucional de Austria, en alemán, "*Verfassungsgerichtshof"*.

[379] STJUE, de 8 de abril de 2014. En los asuntos acumulados C-293/12 y C-594/12, en el fallo dispone la nulidad de la Directiva 2006/24/CE.

comunicaciones de datos de sus usuarios incide directamente en los derechos de protección de la vida privada en las comunicaciones y a la protección de datos. Además, esta decisión, coincide con la jurisprudencia mayoritaria de los tribunales españoles[380], que como hemos visto anteriormente, vienen afirmando que, los datos asociados o metadatos relacionados con la comunicación afectan a la intimidad personal (art. 18.1 CE) y/o protección de datos o autodeterminación informativa (18.4 CE). Sin embargo, la propia sentencia europea justifica la injerencia en los derechos fundamentales, cuando fuera por razones de interés general, la seguridad pública, la prevención de delitos y la lucha contra la delincuencia, en especial, la delincuencia organizada o el terrorismo, debiendo armonizar las intromisiones de acuerdo con el principio de proporcionalidad (apartados 38, 41, 42, 43, 44 y 45). Ciertamente, como continúa exponiendo la sentencia, la obligatoriedad de conservación de datos puede ser admisible para la lucha contra la delincuencia grave, pero en cambio, no resulta justificada para cualquier clase de actuación (apartado 51), de hecho, las restricciones en la protección de datos y en la privacidad deben realizarse sin sobrepasar los límites de lo estrictamente necesario (apartado 52). De este modo, se debe tener en cuenta que, la Directiva 2006/24/CE es aplicable a todos los medios de comunicación electrónicos, comprende todos los abonados y usuarios registrados, lo cual, en definitiva, supone una injerencia en los derechos fundamentales de prácticamente toda la población europea (apartado 56). Además, la Directiva comprende de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción alguna en relación con la lucha contra los delitos graves (apartado 57). A esto hay añadir que, la norma comunitaria se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento es delictivo. También, al no contener excepción alguna en su aplicación, afecta incluso a personas cuyas comunicaciones pueden estar sujetas al secreto profesional (apartado 58). De igual modo, no se restringe la conservación a datos referentes a un período temporal, zona geográfica o a un círculo de personas concretas que puedan estar implicadas en un delito grave (apartado 59), ni tampoco, el acceso a los datos conservados no se supedita a un control previo realizado por un órgano jurisdiccional, o

[380] Traemos a colación la STS 740/2017… O.P. Cit. (F.D. 1º) y STS 400/2017… O.P. Cit. (F.D. 2º), de modo que, vienen a afirmar que, los datos asociados o metadatos inciden en la intimidad y/o protección de datos o autodeterminación informativa.

bien, por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización sea lo estrictamente necesario para la prevención, detección o enjuiciamiento de delitos (apartado 62). En conclusión, los argumentos citados por el TJUE hacen que la Directiva 2006/24 sea declarada nula (apartado 71), por constituir una injerencia de gran magnitud y especial gravedad en los derechos fundamentales (apartado 65), en concreto en la privacidad en las comunicaciones y en la protección de datos (apartado 69), toda vez que, el legislador de la Unión Europea no habría respetado el principio de proporcionalidad.

Ahora bien, la declaración de nulidad de la Directiva 2006/24 por la sentencia del TJUE de 8 de abril de 2014 que ha sido examinada ¿podría afectar a la ley (L. 25/2007) de derecho interno español que la transpone? Dicha cuestión, como ahora veremos, no se responde fácilmente. De hecho, nos encontramos ante la situación compleja, toda vez que, como venimos exponiendo, la norma europea ha sido declarada nula por el T.J.U.E, pero en cambio, la ley española que transpuso las disposiciones de aquella es válida dentro de nuestro territorio. Cabe advertir que, la jurisprudencia reiterada del T.J.U.E.[381] mantiene que las sentencias dictadas al resolver una cuestión prejudicial, tienen efecto *erga omnes*, es decir, la interpretación sostenida en la resolución de una cuestión prejudicial debe ser seguida por el conjunto de órganos jurisdiccionales de los distintos Estados de la Unión Europea, en todos los asuntos en los cuales se invoque el texto interpretado, teniendo efectos vinculantes para todos los Estados miembros tanto de la declaración de invalidez de un acto emanado de un órgano de la U.E. como de la interpretación que se haga por el T.J.U.E. en su resolución, lo cual, hace que se garantice la aplicación uniforme del Derecho europeo. De esta manera, en el hipotético caso de aceptar estas afirmaciones, se podría llegar a la conclusión que, al tratarse de una sentencia dictada por el T.J.U.E, que además, sus efectos se extienden a todos los Estados miembros, la ley española debería ser excluida de nuestro ordenamiento

[381] STJUE, de 6 de marzo de 2003 (Asunto *Kaba*, causa C-466/00), en el párrafo 40 establece el carácter obligatorio de las sentencias prejudiciales del TJUE. Así, en el mismo sentido, SANZ HERMIDA, Á. M. *Las cuestiones prejudiciales. El Tribunal de Justicia de la Unión Europea. Instituciones y Derecho de la Unión Europea Instituciones de la Unión Europea. Volumen I.* Editorial Tirant lo Blanch. Valencia. 2015. Págs. 520-524.

jurídico. Sin embargo, nuestros tribunales[382] mantienen que la declaración de nulidad de la Directiva 2006/24/CE, no supone la automática invalidez de la Ley que la traspone al derecho interno, toda vez que, según sus argumentaciones, la sentencia hace pronunciamientos que son respetados en la ley (judicialidad de la medida, medidas de seguridad a adoptar, plazo que coincide con el indicado por el Abogado General en sus conclusiones, etc.), de tal modo que, se hace una adecuada interpretación de la ley española conforme las normas europeas, así como, no puede considerarse que la transposición esté subordinada a la Directiva, como lo está, del reglamento a la ley. Además, la institución española que tiene encomendada la facultad de poder declarar la nulidad de normas con rango de ley es nuestro Tribunal garante de la Constitución, mediante el recurso o cuestión de inconstitucionalidad (arts. 31, 35 y 39 LOTC)[383], o bien, podría plantearse una cuestión prejudicial ante T.J.U.E. (art. 267 TFUE)[384], como en el caso sueco (Sentencia del T.J.U.E, Gran Sala, de 21 de diciembre de 2016), o incluso, estrechamente relacionado con esta materia, la cuestión prejudicial planteada por la Sección Cuarta de la Audiencia Provincial de Tarragona[385], que serán ambas

[382] STS 768/2015, 23 de noviembre (F.D. 7º) y STS 470/2015, 7 de julio (F.D. 1º).

[383] Sobre la cuestión de incosntitucionalidad, PACHECO GALLARDO, M. "Cuestión de inconstitucionalidad". Diario La Ley. Núm. 8771. 2016, señala que, "es prerrogativa, exclusiva e irrevisable del órgano judicial".

[384] Con carácter general, véase AGUSTÍ MARAGALL, J. *La cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (Derecho Social de la Unión Europea: aplicación por el Tribunal de Justicia).* Editorial Francis Lefebvre. Madrid. 2018. Págs. 123-156; CALVO SALINERO, R. y PASTORIZA VÁZQUEZ, J. S. *La cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (La revisión de actos en materia tributaria).* Editorial Thomson Reuters-Lex Nova. 2016. Págs. 993-1044; IZQUIERDO SANS, C. *La cuestión prejudicial ante el TJUE. (Lecciones de jurisdicción social).* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 865-886; JIMENO BULNES, M. *La cuestión prejudicial. (El sistema jurisdiccional de la Unión Europea).* Editorial Thomson Reuters Aranzadi. Navarra. 2013. Págs. 173-210.

[385] Abordan, TEJADA DE LA FUENTE, E. y ZARAGOZA TEJADA, J. I. "Apuntes a la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona frente a la Ley 25/2007". Revista Aranzadi Doctrinal. Núm. 9. 2018, la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona, si bien, será objeto de análisis posteriormente.

objeto de análisis posteriormente. En cualquier caso, como mantiene Vázquez Seco[386], hasta que el legislador europeo desarrolle una nueva norma que sustituya la Directiva 2006/24/CE o el legislador español adecue la norma a los mandatos europeos, para la validez de la utilización de los datos conservados al amparo de la Ley 25/2007, deberán de cumplirse los siguientes requisitos que, además son exigencias consagradas por la jurisprudencia del Tribunal Constitucional[387], de tal forma que, son los necesarios para proporcionar una justificación constitucional objetiva y razonable a la injerencia en el derecho a la intimidad, a saber: *1. La existencia de un fin constitucionalmente legítimo. 2. Que la medida limitativa del derecho esté prevista en la Ley (principio de legalidad). 3. Que se acuerde mediante una resolución judicial motivada. 4. Que se respete el principio de proporcionalidad que a su vez y se concreta en las tres siguientes condiciones: a) Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); b) 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). c) 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).*

Otra interpretación sobre la declaración de nulidad de la Directiva 2006/24/CE sería volver a implantar la normativa europea anterior, esto es, la Directiva 2002/58/CE, de 12 de julio. Sin embargo, cabe recordar que, la norma europea establecía, de forma potestativa, la obligación de conservar datos, es decir, los Estados miembros podían optar sobre si deseaban implantar esta normativa, y para el hipotético caso de que fuera acogida, se fijaba que, las restricciones en los derechos fundamentales únicamente podrían realizarse, por razones de seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos (art. 15.1

[386] Advierte VÁZQUEZ SECO, L. "Ponencia sobre la retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. Análisis de la sentencia del tribunal de justicia de la unión europea de 8 de abril de 2014 en los asuntos acumulados C-293/12 Y C594/12*"*, publicado en www. Fiscal.es, que, hasta que el legislador español adecue la norma a los mandatos europeos, se deberán cumplir los requisitos constitucionales para la validez de la utilización de los datos conservados al amparo de la Ley 25/2007.

[387] Sobre las exigencias jurisprudenciales aludidas en el texto, STC 23/2014, de 13 de febrero (F.J. 2º).

2002/58/CE)[388]. De este modo, al amparo de la norma europea mencionada, el legislador español podría imponer la obligación a los operadores de telecomunicaciones de conservación y cesión de datos, pero únicamente con la finalidad de seguridad y persecución de hechos delictivos.

En otro orden de ideas, con posterioridad a la sentencia del TJUE, de 8 de abril de 2014 que declara la nulidad de la Directiva 2006/24, se aprobaría la Ley 9/2014, de 9 de mayo *de General de Telecomunicaciones*, si bien, el legislador lejos de enmendar esta situación de inseguridad jurídica, en el precepto que hace mención a la conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, se remite *in toto* a la ley 25/2007 (art. 42 de la Ley 9/2014), como dejando entender que la ley objeto de controversia resulta plenamente vigente.

Tal y como se había avanzado, el Tribunal de Suecia (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo[389]) planteó una cuestión prejudicial[390] sobre

[388] Pone de manifiesto, RODRÍGUEZ LAINZ, J. L. "La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones*"*. Diario La Ley. Núm. 8901. 2017, que, la Ley 25/2007, debería cumplir los límites establecidos en el art. 15.1 de la 2002/58/CE, esto es, la conservación de datos de tráfico por razones de seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos.

[389] *Kammarrätten i Stockholm*.

[390] En relación con las peculiaridades de la sentencia del TJUE de 21 de diciembre de 2016 sobre la validez de la norma de conservación de datos de tráfico del Estado de Suecia, y en consecuencia, su incidencia con nuestra Ley 25/2007, COLOMER HERNÁNDEZ, I. "Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016*"*. Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute. Sepin Editorial Jurídica. Madrid. 2018. Págs. 767-781. Así, RODRÍGUEZ LAINZ, J. L. "La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones…*"* O.P. Cit. afirma que, "hemos de asumir que si la razón de ser de la declaración de no conformidad con el Derecho de la Unión descansa en la vulneración de alguno de los derechos reconocidos en la Carta de Derechos Fundamentales de la Unión Europea —CDFUE—, con incuestionable efecto directo al igual que los Tratados, tal efecto irradiante afectaría de lleno a la norma nacional de transposición, que no podría encontrar como sustento un art. 15.1 de la Directiva 2002/58/CE que es interpretado a la luz del respeto de tales derechos fundamentales. A falta de una regulación adaptada a tales nuevos pronunciamientos, y debiendo considerarse, dadas las circunstancias, inoperante acudir al fácil expediente del planteamiento de una cuestión prejudicial para obtener un pronunciamiento

su sistema legal de conservación de datos relativos a las comunicaciones, para su posible utilización en el ámbito de la investigación criminal, de forma similar a nuestra Ley 25/2007. Dicha cuestión fue resuelta mediante la decisión de la Gran Sala de 21 de diciembre de 2016[391], en la cual, se acordaba que, la existencia de una normativa nacional que regulase el acceso de las autoridades nacionales competentes a los datos conservados, sin establecer límites en cuanto a la lucha contra la delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos se conserven en el territorio de la Unión (apartado 125 de la sentencia), se opone a la normativa europea vigente sobre esta materia (art. 15.1 de la Directiva 2002/58), así como conculca con los derechos fundamentales a la privacidad personal y familiar (art. 7 de la Carta UE), protección de datos (art. 8 de la Carta UE) y libertad de expresión y de información (art. 11 de la Carta UE).

De acuerdo con ésta decisión, se podría sacar la conclusión que, la ley española resulta inaplicable, al consistir en una norma nacional que, pese a contener un control del órgano jurisdiccional, no restringe la conservación de datos para la persecución de delitos graves y, tampoco exige que los datos se conserven en el territorio de la UE, lo cual, haría que nos encontráramos ante una situación jurídica anómala, pues se trata de una ley formalmente vigente, puesto que no ha existido declaración expresa de nulidad ni ha sido derogada por ninguna ley posterior, mientras que materialmente inaplicable, con arreglo a los argumentos de las resoluciones estudiadas del TJUE (en concreto, las SSTJUE de 8 de abril de 2014 y de 21 de diciembre de 2016). Por otra parte, se podría colmar la deficiencia legislativa que venimos estudiando, mediante la regulación contenida en la norma procesal penal relativa al deber de colaboración de los prestadores de servicios de telecomunicaciones (art. 588 ter e, k, l y m LECrim.), si

---

que no podría ser otro que el reflejado en la sentencia de 21 de diciembre de 2016, dada la clara analogía entre la legislación española y en concreto la sueca, no nos queda, lege data, otra opción que la de aprovechar las potencialidades de conservación/preservación singular de datos y cesión de los mismos de fuentes diversas a la defenestrada Ley 25/2007, que actualmente prevé la nueva regulación de las llamadas medidas de investigación tecnológica de la LECrim*"*.

[391] S.T.J.U.E., de 21 de diciembre de 2016. Asuntos TELE2 SVERIGE AB y otros, acumulados C-203/15 y C-698/15.

bien, pese a ser poco exhaustiva, al faltar aspectos relevantes como el plazo de duración o la concreción de los datos objeto de conservación, puede proporcionar cierta cobertura legal a la obligación de conservación de datos. No obstante, otra cuestión a tener en cuenta si mantenemos esta última tesis es, que validez tienen los datos conservados por las operadoras, entre el período comprendido entre el 8 de abril de 2014 que acordaba la nulidad de la Directiva 2006/24 mediante la sentencia del TJUE, y el 6 de diciembre de 2015 con la entrada en vigor de la reforma procesal penal implementada con la L.O. 13/2015, de 5 de octubre[392], en la cual, se instauraba el deber de colaboración aludido *supra*, toda vez que, los datos obtenidos dentro del periodo mencionado podrían carecer de sustento legal[393].

Una posible solución para la conservación de datos de tráfico o asociado, respetando la normativa y jurisprudencia europea, sería la emisión por la autoridad judicial de una orden de retención o de congelación de datos, de la misma manera que sucede en el régimen establecido para el bloqueo de datos en la rectificación o supresión conforme la Ley Orgánica de Protección de datos (art. 32 L.O. 3/2018 en relación con el Reglamento UE 2016/679, de 27 de abril de 2016)[394]. De esta manera, el Juez podría autorizar el bloqueo de los datos, el cual, se ejecutaría desde la fecha de emisión de la orden de interceptación, frente a determinadas personas y para una concreta investigación

[392] Así, la disposición final cuarta de la L.O. 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* («BOE» Núm. 239, de 6 de octubre de 2015), establece que, la entrada en vigor se producirá a los dos meses de su publicación en el «Boletín Oficial del Estado».

[393] Advierten, MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 189-193, de la problemática de la validez de la conservación y cesión de datos desde el periodo comprendido entre la declaración de nulidad de la Directiva 2006/24/CE y la entrada en vigor de la reforma procesal implementada por la L.O. 13/2015.

[394] Con carácter general acerca de la forma de proceder en el ejercicio del derecho de rectificación o supresión conforme la normativa de protección de datos (art. 32 L.O. 3/2018), BERROCAL LANZAROT, A. I. "El derecho de supresión de datos o derecho al olvido en el Reglamento General de Protección de Datos*"*. Revista General de Legislación y Jurisprudencia. Núm. 1. 2017. Págs. 7-71; ÁLVAREZ CARO, M. *El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas*. *(Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad).* Reus. Madrid. 2016. Págs. 227-240.

criminal. En este sentido, se podría aplicar el art. 588 octies de la LECrim. que regula la orden de conservación de datos, sin embargo, hace mención a que el Ministerio Fiscal o la Policía Judicial puedan requerir a cualquier persona física o jurídica la conservación y protección de datos, teniendo el Juez hasta ciento ochenta días para convalidar dicha actuación, lo cual, podría suscitar una grave controversia al tratarse de una medida sin un control judicial efectivo desde el primer día.

En cualquier caso, resulta evidente que, el ordenamiento jurídico español tiene actualmente grandes deficiencias en la regulación sobre la conservación y cesión de datos, por lo que el legislador debería satisfacer las necesidades observadas, dictando una ley que se adaptara a los mandatos comunitarios que han sido objeto de estudio.

Estrechamente relacionado con lo que venimos exponiendo, la Sección Cuarta de la Audiencia Provincial de Tarragona, ha planteado una cuestión prejudicial ante T.J.U.E. en el asunto C-207/2016, en la cual, interesaba un pronunciamiento, más centrado en el acceso a los datos informáticos almacenados por las empresas operadoras de telecomunicaciones en la prestación de sus servicios, con ocasión, de una investigación penal, que en la validez de la normativa nacional sobre el acceso de las autoridades nacionales a los datos conservados por dichas empresas[395], como en el caso del Tribunal Sueco. De esta manera, el Juzgado de Instrucción de Tarragona mediante auto de 5 de mayo de 2015, vino a denegar un oficio de la Policía Judicial, que solicitaba, en aplicación de la Ley de conservación de datos (art. 1 de la L.25/2007) y la Ley de Enjuiciamiento Criminal (art. 588 ter j. LECrim.), autorización judicial para recabar de las compañías telefónicas, información sobre las tarjetas SIM que pudieran haber sido utilizadas en un dispositivo móvil arrebatado mediante robo con violencia. De tal forma que, la Policía Judicial pretendía obtener, durante los diez días inmediatamente posteriores a la sustracción, información sobre las tarjetas SIM que pudieran haber sido insertadas en el terminal robado, así como, la identidad de las personas titulares de las mismas. Debido a la denegación de esta diligencia de investigación, el Juzgado de Instrucción acordaría el sobreseimiento y archivo de las actuaciones por falta de autor

[395] Así, TEJADA DE LA FUENTE, E. y ZARAGOZA TEJADA, J. I. "Apuntes a la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona frente a la Ley 25/2007…*"* O.P. Cit. exponen de forma detallada el iter procesal de la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona, si bien, únicamente queda aquí apuntado.

conocido (art. 641.2 LECrim.). Seguidamente, los autos de denegación de diligencia de investigación y sobreseimiento y archivo de las actuaciones, fueron recurridos por el Ministerio Fiscal en apelación, cuyo conocimiento vino a corresponder a la Sección Cuarta de la Audiencia Provincial de Tarragona, si bien, decidieron plantear el 14 de abril de 2016 una cuestión prejudicial ante el T.J.U.E. (Asunto C-207/16), en el sentido de preguntar si la gravedad del delito investigado ha de valorarse en atención a la pena prevista para el delito en cuestión o si el mismo, además, ha de presentar unos especiales niveles de gravedad y, en su caso afirmativo, cuál debería ser el umbral mínimo de la pena para justificar la injerencia. De esta forma, como establece la Directiva 2002/58/CE, los Estados miembros pueden adoptar, medidas legislativas para conservar los datos durante un plazo limitado, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas (art. 15.1 de la mencionada Directiva). Dicho lo anterior, la cuestión se resolvería mediante la sentencia del T.J.U.E. de la Gran Sala de 2 de octubre de 2018[396], en aplicación de la Directiva 2002/58/CE (puesto que como decimos, la declaración de nulidad de la Directiva 2006/24/CE supone volver a implantar la normativa europea anterior), de modo que, habría que interpretar que, el acceso de las autoridades públicas a los datos que permitan identificar, por ejemplo, a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal, que dicho acceso deba restringirse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, en la lucha contra la delincuencia grave. De esta manera, el T.J.U.E. viene a decidir que, el acceso a los datos conservados por las compañías de teléfonos que pretendía realizar la Policía Judicial mediante autorización judicial en aplicación de nuestra ley nacional de conservación de datos (art. 1 L.25/2007), así como la Ley de Enjuiciamiento Criminal (art. 588 ter j. LECrim.) es conforme a Derecho de la Unión Europea, esto es, con arreglo a la vigente Directiva 2002/58/CE. En conclusión, parece indicar esta resolución que, nuestra legislación sobre la conservación y cesión de los datos electrónicos de tráfico o

[396] S.T.J.U.E. de 2 de octubre de 2018, en el asunto C-207/16.

asociados por parte de las empresas prestadoras de los servicios de telecomunicaciones, respeta la Directiva 2002/58/CE, si bien, pese a que la norma española prevea como garantía para la cesión de los datos la intervención judicial (arts. 6 y 7 L. 25/2007), no contempla restricción alguna en la conservación, en concreto, debería cumplir los límites establecidos en el art. 15.1 de la Directiva 2002/58/CE, esto es, la conservación por razones de seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos, ya que, por el contrario, se aplica para todos los ciudadanos españoles que tengan dispositivos electrónicos, de tal forma que, a nuestro modo ver, esta regulación excede del espíritu de la Unión Europea, y en consecuencia, el Estado español debería adaptar su legislación a los mandatos comunitarios examinados en la presente obra.

e) Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad

La norma procesal contiene una regulación específica, dentro de las disposiciones sobre la intervención en las comunicaciones telefónicas y telemáticas, que tienen por finalidad, obtener los datos necesarios para la identificación de los usuarios o titulares de los terminales o los dispositivos de conectividad, que pudieran haberse utilizado en la comisión de delitos. Sin embargo, la peculiaridad de esta normativa es que, cuando la obtención de los datos no incida en la propia comunicación, se permite al Ministerio Público o los agentes facultados de la Policía Judicial poder acceder a dicha información, directamente, sin precisar de autorización judicial.

Seguidamente, se examinará la regulación sobre la identificación del número IP (art. 588 ter k. LECrim.), los terminales mediante captación de códigos con aparatos específicos (art. 588 ter l. LECrim.), así como, conocer los titulares a través de sus números de teléfono o de cualquier otro medio de comunicación, o bien, el número de teléfono o los datos identificativos cuando conozcan a los titulares (art. ter m. LECrim.).

a´. Identificación mediante número IP

En relación a la primera de las cuestiones expuestas, resulta necesario explicar que, la dirección IP (acrónimo de *Internet Protocol)* consiste en una secuencia de cuatro series de números únicos que identifican un dispositivo conectado en una determinada red,

esto es, a través de la dirección IP se puede conocer en qué red se encuentra el dispositivo (normalmente un ordenador) y a su vez, cuál es el equipo utilizado (ejemplo de dirección IP 79.147.36.228). Además, las direcciones IPs pueden ser dinámicas, esto es, cuando cada vez que un dispositivo se conecta a internet, dentro de una cantidad de direcciones IPs disponibles, el proveedor le asigna una dirección aleatoria (el método más utilizado de distribución es mediante el servidor DHCP -*Dynamic Host Configuration Protocol*-), pero también, las direcciones IP pueden ser fijas o estáticas, es decir, cuando la secuencia numérica asignada para el dispositivo es siempre la misma. Una vez realizada esta breve exposición sobre las direcciones IPs, cabe mencionar que, las operadoras de telecomunicaciones a los efectos de facturación del servicio, obran en su poder datos relacionados con sus clientes, entre otros, los datos del titular de la conexión a Internet, domicilio de la instalación o el lugar donde se factura el servicio, datos del medio de comunicación utilizados, los relacionados con la forma de pago del servicio como el número de cuenta del titular, teléfonos de contacto, tecnología de la conexión a Internet y datos técnicos asociados (ADSL, RDSI, Frame Relay, Cable, Satélite, Red Conmutada básica, velocidad de conexión …), y por supuesto, las direcciones IPs[397] asignadas en un momento determinado.

Pues bien, cuando en el ejercicio de las funciones de prevención y descubrimiento de delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada y no constara la identificación y localización del equipo o del dispositivo correspondiente ni los datos de identificación personal del usuario, deberán solicitar al Juez de instrucción que requiera a las operadoras de servicios de telecomunicaciones la cesión de aquellos datos que permitan la identificación y localización del terminal y la identificación del sospechoso (art. 588 ter k. LECrim.). Sin embargo, la Policía Judicial no precisa de autorización judicial para detectar y utilizar direcciones IPs de los usuarios de la red, de tal forma que, cuando desee que la secuencia numérica se especifique en una concreta persona o en su terminal y/o averiguar su localización, o dicho de otro modo, cuando en una investigación los agentes facultados de la policía deseen vincular el IP con una determinada persona, o

[397] Afirma PÉREZ BES, F. "La ciberseguridad como legitimación para el tratamiento de direcciones IP*"*. Revista de Privacidad y Derecho Digital. Núm. 5. 2016. Págs. 27-69, que, las direcciones IP son datos que obran en poder de las empresas de telecomunicaciones.

necesiten identificar o localizar el terminal o el dispositivo de conectividad utilizados, deberán solicitar del Juez que requiera a las operadoras de telecomunicaciones para que cedan los datos que obran en su poder. De esta forma, la dispensa de plácet judicial para detectar y utilizar las direcciones IPs por la Policía Judicial, se debe a que, éstas son públicas en la red, pues todo usuario puede obtener la secuencia numérica de terceros de una forma sencilla. De esta manera, la norma procesal dispone (art. 588 ter k. LECrim), lo que venía siendo jurisprudencia consolidada del Tribunal Supremo, pues veía afirmando que, la Policía Judicial puede rastrear lo que es público en internet, del mismo modo que, cualquier persona puede obtener la dirección de IP mediante la utilización de programas o páginas web específicas, o en su caso, interactuando con los usuarios en la red. Por este motivo, también se permite a la Policía Judicial, identificar las IPs por sus propios medios, reservando la intervención judicial para recabar de las operadoras de telecomunicaciones[398] los datos que permitan reconocer al usuario o identificar y localizar el terminal[399].

[398] En este sentido, la STS 680/2010, 14 de julio (F.D. 2º) y STS 739/2008, de 12 noviembre (F.D. 4º) "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"*;* Por su parte, la STS 292/2008, 28 de mayo (F.D. 9º) "el I.P. no identifica la persona del usuario, lo que hace necesario para conocer el número del teléfono y titular del contrato la autorización judicial". También, la STS 16/2014, 30 de enero (F.D. 2º) refiere en los mismos términos.

[399] En relación con la identificación de la policía judicial de la IP, RODRÍGUEZ LAINZ, J. L. "Acceso policial a información sobre atribución de IP dinámicas, Comentario a la STEDH del caso Benedik v. Eslovenia*"*. Diario La Ley. Núm. 9.241. 2018, señala que, "la norma nacional pudiera ser tildada de carente de un concreto control judicial generador de posibles situaciones de abuso, cuando la información obtenida por la vía del rastreo más o menos sistemático de concretas redes P2P no llegara a ser participada a la autoridad judicial, es un riesgo al que podríamos enfrentarnos ante un eventual recurso ante el Tribunal de Estrasburgo. La dinámica de investigación de grupos de delitos tecnológicos suele partir, como ya anticipáramos, de la necesidad de atribuir a una misma IP un número considerable de hashs de contenido conocidamente ilícito para actuar contra quienes pudieran estar detrás de tal intercambio; y ello por la sencilla razón de que así se evitan conexiones erróneas que pudieran tener como única razón de ser el nombre asignado a un concreto archivo de video o imágene. Ello genera lógicamente el almacenamiento y tratamiento de datos en principio sin un directo control judicial; aunque sea de datos en sí mismos anónimos, al ser expresión de una concreta IP que no puede ser relacionada por la policía con una identidad concreta como no sea recabando la correspondiente autorización judicial. Pero estos límites a lo que pudiera ser una tapadera de situaciones de abuso o arbitrariedad sí existen al día de hoy; aunque hayan de encontrarse en una norma externa a la LECRIM, más allá del sometimiento del art. 588

b´. Identificación de terminales mediante captación de códigos de identificación del aparato o de sus componentes.

En el marco de una investigación penal, si no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación, o de cualquier medio técnico que, sea apto para identificar el equipo de comunicación

---

ter k a los llamados principios rectores del 588 bis a de la LECRIM". Sin embargo, el MISMO AUTOR, "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas*"*. Diario La Ley. Núm. 7086. 2009, venía afirmando que, "la posición del Alto Tribunal al concluir de forma tajante que no se requiere autorización judicial para acceder a «... lo que es público y el propio usuario de la red es quien lo ha introducido en la misma»; considera igualmente que: «La huella de la entrada...[...]...queda registrada siempre y ello lo sabe el usuario». La autorización, en opinión del Alto Tribunal, quedaría reservada para desvelar la identidad que hay detrás de la utilización de determinada dirección IP relacionada con un concreto acceso público". De igual modo, mantiene ZARAGOZA TEJADA, J. I. "La investigación de la dirección IP tras la Reforma operada por Ley 13/2015*"*. Revista Aranzadi Doctrinal. Núm. 2. 2017. Págs. 359 – 377, que, "la concreción de dicha dirección IP puede determinarse bien dirigiendo directamente una petición a las entidades prestadoras de servicio o aquellas que faciliten la comunicación o bien como consecuencia de las propias labores de investigación realizadas por la policía judicial en orden a esclarecer el delito. En relación con este último supuesto, fue planteado ya cuando empezó a hacerse uso de este tipo de investigaciones la posible vulneración del derecho al secreto de comunicaciones en los supuestos en los que era la propia policía judicial la que conseguía la dirección IP valiéndose de rastreos extrajudiciales en fuentes abiertas. En concreto, se planteaba una posible vulneración del artículo 3 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación que exigía, para la cesión de estos datos y con carácter general, una autorización judicial previa. Al respecto, resulta necesario remarcar que la jurisprudencia de la Sala Segunda ha sido bastante reiterada en el sentido de considerar que la obtención de las direcciones IP derivadas de los rastreos realizados en redes sociales, foros abiertos de internet o redes P2P es una técnica perfectamente válida y que no implica vulneración de derecho fundamental alguno. Así, la STS 236/2008 determina que "los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma". En el mismo sentido, MAEZTU LACALLE, D. *La identificación del titular de una dirección IP. Problemática en aplicación de la ley 25/2007, de conservación de datos. (El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito)*. Editorial La Ley. Madrid. 2012. Págs. 241-330.

utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones (art. 588.1 ter l. LECrim.). De esta manera, la Policía Judicial puede tener grandes dificultades para averiguar que dispositivos o que líneas telefónicas están siendo utilizadas para la actividad delictiva, pues como se ha mencionado, los delincuentes, para evitar ser descubiertos, pueden cambiar con frecuencia los terminales móviles, o bien, utilizar terceras personas para que figuren como titulares, o incluso, con carácter general, ignorar la verdadera identidad de los sospechosos. Por este motivo, la norma procesal permite que, la Policía Judicial pueda realizar libremente operativos de seguimiento o vigilancia, con el objeto de, detectar con artificios técnicos números de teléfono de los investigados, pero sin acceder al contenido de la comunicación, para una vez obtenido los datos necesarios, poder solicitar al Juez la interceptación de las comunicaciones telefónicas o telemáticas (art. 588.2 ter l. LECrim.). En consecuencia, se viene a plasmar la jurisprudencia reiterada de nuestro Tribunal Supremo[400], que venía manteniendo que, cuando por otros medios no haya sido posible obtener el número de abonado, puede la Policía Judicial, mediante artificios técnicos como el denominado *IMSI/IMEI-Catcher*, averiguar los códigos de identificación del aparato de telecomunicación, como la numeración IMSI o IMEI[401]. De esta manera, cabe preciar

[400] Entre otras, la STS 249/2008, 20 de mayo (F.D. 4º) y STS 40/2009, de 28 enero (F.D. 1º).

[401] En relación a la captación del IMSI por la policía judicial, SÁNCHEZ SISCART, J. m. "A vueltas con el secreto de las comunicaciones. Algunos supuestos críticos en la jurisprudencia de la Sala 2.ª del Tribunal Supremo*"*. Diario La Ley. Núm. 7338. 2010, señala que, "la captación del IMSI fue obtenida por los agentes de policía, sin contar con autorización judicial, mediante la utilización de un escáner en las proximidades del usuario. Una vez averiguado, se solicitó a los respectivos operadores, con autorización judicial expresa, la identificación de los números de teléfono que se correspondían con esos IMSI y la intervención telefónica de esos números de teléfonos… la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia". Por su parte, RODRÍGUEZ LAINZ, J. L. "Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas…" O.P. Cit, afirma que, "el número de IMSI, acogido al estándar ITU E.212, se compone de un total de hasta 13 dígitos; los tres primeros se corresponden al código del país (MCC), los dos siguientes al código de la red móvil (MNC), y los diez últimos contienen la identificación de la estación móvil (MS o mobile station). Por tanto, quien accede a los dígitos de un número IMSI no puede conocer directamente el número de terminal telefónico asociado a éste, que por definición es único, aunque quepa la posibilidad técnica de relacionar dos números de teléfono a una sola tarjeta SIM". Asimismo, vienen a examinar la validez de la obtención por parte de la Policía Judicial de la numeración

que, la numeración IMSI (acrónimo de *International Mobile Subscriber Identity* -Identidad Internacional del Abonado a un Móvil-), responde al código único que identifica a las tarjetas SIM (acrónimo de *Subscriber Identity Module* -Módulo de Identificación del Suscriptor), esto es, tarjeta utilizada en los teléfonos móviles para almacenar información del usuario que es necesaria para ser identificado en la red, mientras que, la numeración IMEI (acrónimo de *International Mobile Station Equipment Identity* -Identidad Internacional de Equipo Móvil-), corresponde al número de identificación de un dispositivo móvil, que al conectarse a la red, se envía a la operadora de telecomunicaciones, para proporcionar información del servicio a los efectos de su facturación (conexión a la red, lugar donde se encuentra el terminal, titular del servicio, etc.). De esta forma, la Policía Judicial mediante la utilización de aparatos, como el *IMSI–Catcher,* puede obtener los números de identificación de las operadoras de telecomunicaciones, como la tarjeta SIM que se inserta en el teléfono móvil para asignar un número de abonado o MSISDN (acrónimo de *Mobile Station Integrated Services Digital Network* -Estación Móvil de la Red Digital de Servicios Integrados RDSI-), de manera que, la forma de proceder es, instalando el aparato (*IMSI–Catcher*) en algún lugar oculto, para que una antena capte la señal de los terminales próximos, simulando el comportamiento de la red GSM (acrónimo de *Global System for Mobile communications* -Sistema Global para las Comunicaciones Móviles-), con la finalidad de obtener la numeración IMSI, para una vez extraído el código de identificación de la tarjeta SIM, podrán solicitar al Juez intervenir las comunicaciones telefónicas o telemáticas del sospechoso.

De igual modo, de acuerdo con la tecnología existente en cada momento, la Policía Judicial sin acceder al contenido de las comunicaciones, podrá utilizar cualquier otro artificio que permita identificar el equipo utilizado o la tarjeta de acceso a la red de

---

IMSI, véase, igualmente, NICOLÁS ROLÓN, D. "Intercepción de metadatos de comunicaciones por teléfonos móviles. El IMSI-Catcher y su regulación en el ordenamiento procesal penal alemán*"*. Revista de Estudios de la Justicia. Núm. 27. 2017. Págs. 61-79; GUDÍN RODRÍGUEZ-MAGARIÑOS, F. "Legalidad de los mecanismos de barrido policial que permiten obtener los números IMEI/ IMSI de las tarjetas de telefonía móvil*"*. Revista General de Derecho Procesal. Núm. 18. 2009; MUÑOZ CUESTA, J. "Obtención mediante escáner por guardias civiles y sin autorización judicial del número de identidad internacional del abonado móvil (IMSI) de teléfonos móviles con tarjeta prepago. Comentario a la STS, Sala 2ª, de 20 de mayo de 2008*"*. Repertorio de Jurisprudencia Aranzadi. Núm. 13. 2008. Págs. 13-17.

telecomunicaciones, como por ejemplo para obtener el número de identificación del terminal móvil puesto por el usuario (PIN acrónimo de *Personal Identification Number* o Número de Identificación Personal) o por la operadora de telefonía para desbloquear el código introducido erróneamente por el usuario (PUK acrónimo de *Personal Unlocking Key* o Clave Personal de Desbloqueo)[402]. Además, cuando la Policía Judicial se dirija al tribunal, la propia solicitud u oficio deberá hacer constar expresamente que se han obtenido los datos mediante artificios técnicos, debiendo resolver el órgano jurisdiccional de forma motivada sobre la concesión o denegación de la medida (art. 588.2 *in fine* ter l. LECrim.). Por último, se debe advertir que, el uso de aparatos técnicos para obtener códigos de identificación, como expresamente alude la norma procesal, únicamente puede ser realizada por la Policía Judicial, de tal forma que, nunca puede ampliarse la legitimación a personas particulares, o bien, detectives privados, especialmente debido a que, con arreglo a la Ley de Seguridad Privada (arts. 10.2, 37.4 Ley 5/2014, de 4 de abril, *de Seguridad Privada*), se proscribe de su actividad para la investigación de delitos perseguibles de oficio[403].

c´. Identificación de titulares o terminales o dispositivos de conectividad.

Otra cuestión a tener en cuenta es que el Ministerio Fiscal y la Policía Judicial (art. 588 ter m. LECrim.), dentro del ejercicio de sus funciones, cuando tuvieran en su poder el números de teléfono o de cualquier otro medio de comunicación, y pretendan conocer la identidad del titular, o bien, conozcan la identidad del titular, y pretendan averiguar su

[402] Señala RODRÍGUEZ LAINZ, J. L. "Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones..." que, "el número PIN es por ello la consecuencia de la culminación de un procedimiento de asociación; en el que en sí mismo no intervendría sino por mor de esta relación que se hace entre el dispositivo físico, a través del número IMSI, y la información que sobre el número PIN se conserva en las bases de datos de Blackberry. Esta relación sería bastante similar al comportamiento del número de abonado de destino de una llamada telefónica. La autenticación en este caso se realiza precisamente por la compartición con los números IMEI/IMSI, y la correlación que se establece entre el segundo dato y el número de abonado asignado a la tarjeta SIM portadora del número IMSI".

[403] La STS 908/2016, 30 de noviembre (F.D. 5º) determina que la "L. 5/2014 de 4 de abril, prohíben a los detectives privados investigar delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza".

número de teléfono o los datos identificativos de cualquier medio de comunicación, sin necesidad de recabar autorización judicial, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia a la autoridad (art. 556 CP)[404]. De esta manera, como nos hemos referido anteriormente, el Ministerio Fiscal y la Policía Judicial no precisarán de plácet judicial para la averiguación de determinados datos de las operadoras de telecomunicación, en concreto, aquellos que comprendan los datos generados y almacenados en un registro, así como de la información relativa a la facturación del servicio[405], esto es así, debido a que no están vinculados a un proceso comunicativo, o dicho de otro modo, no inciden en el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE). De esta manera, el art. 588 ter m. LECrim. parece contradecir lo dispuesto en la Ley 25/2007 sobre la conservación de datos relativos a las comunicaciones electrónicas que, como hemos visto anteriormente, exige autorización judicial (arts. 6 y 7 de la Ley 25/2007) para la cesión de los datos conservados por las empresas de telecomunicaciones sobre la identidad del usuario o su número de teléfono relacionada con una comunicación (art. 3.1.a) y b) de la Ley 25/2007). Sin embargo, no debe confundirse, pues la diferencia entre ambas regulaciones estriba, en que los datos que precisan de autorización judicial, son aquellos relacionados con una comunicación, esto es, los datos de tráfico o asociados que están conservados por éstas empresas relativos a los titulares o número de teléfono de llamadas entrantes o salientes que han efectuado los usuarios, en cambio,

[404] Advierten VEGAS TORRES, J. *Las medidas de investigación tecnológica (Nuevas tecnologías y derechos fundamentales en el proceso)*... O.P. Cit. Págs. 21-47; VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015*... O.P. Cit. Pág. 109; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. ... O.P. Cit. Págs. 325-331; SAIZ GARITAONANDIA, A. *Algunas notas sobre telefonía móvil y derecho al secreto de las comunicaciones en supuestos de detención. (El derecho procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños)*. Tirant lo Blanch. Valencia. 2012. Págs. 1173-1186, sobre la necesaria autorización judicial para conocer la titularidad de un número de teléfono, o bien, conociendo la filiación de la persona, conocer su número de teléfono, todo ello, siempre que no sean datos relacionados con un proceso comunicativo.

[405] Acerca del listado de llamadas, la STS 459/1999, de 22 marzo (F.D. 2º), STS 1086/2003, de 25 julio (F.D. 3º) y STS 1231/2003, de 25 septiembre (F.D. 8º).

cuando se pretenda conocer el titular de un número de teléfono, o bien, conociendo la filiación de la persona, saber cuáles son sus números de teléfono, podrán ser obtenidos directamente por la Fiscalía o la Policía Judicial, pues como venimos exponiendo, no están relacionados con un proceso comunicativo. De igual modo, la exoneración de autorización judicial para la averiguación de estos datos se produjo con arreglo a la reforma procesal implementada con la L.O. 13/2015, de 5 de octubre (art. único. 14. de la mencionada L. O.), de tal forma que, en el hipotético caso que se afirme que existe un conflicto entre ambas regulaciones, se deberá resolver, en favor de ésta última, de conformidad con las normas generales sobre la vigencia de las leyes (art. 2.2 C.C.[406]). Además, la reforma procesal se produjo mediante una Ley Orgánica (art. 81 CE) que, como es sabido, está reservada entre otras cuestiones, para derechos fundamentales y precisa de mayoría absoluta de los miembros del Congreso de los Diputados en una votación final para su aprobación.

f) Algunas particularidades observadas de la jurisprudencia y/o doctrina

Dada su importancia, hemos decidido dedicar un epígrafe a examinar algunas particularidades observadas en la jurisprudencia y/o doctrina, relacionadas con la interceptación en las comunicaciones telefónicas y telemáticas, y en concreto, las singularidades del correo electrónico, mensajería instantánea, redes sociales, *chats, blogs, SMS y* MMS, la grabación de conversaciones propias, así como, la intervención de las comunicaciones entre familiares.

a´. El correo electrónico, mensajería instantánea, redes sociales, chats, blogs, SMS y MMS.

El uso extendido entre la población de servicios de comunicación electrónica, ha determinado que, con frecuencia, la actividad delictiva transcurra por estas nuevas tecnologías. Por este motivo, los poderes públicos no pueden quedar al margen de este fenómeno, en vista de que, en ocasiones, la averiguación del delito y el descubrimiento

[406] Art. 2.2 del CC: *Las leyes sólo se derogan por otras posteriores. La derogación tendrá el alcance que expresamente se disponga y se extenderá siempre a todo aquello que, en la ley nueva, sobre la misma materia sea incompatible con la anterior. Por la simple derogación de una ley no recobran vigencia las que ésta hubiere derogado.*

del delincuente transcurre por conocer la información proporcionada por estos servicios de comunicación. Sin embargo, toda injerencia en los derechos fundamentales, se debe realizar con todas las garantías, para lo cual, nuestros tribunales han ido trazando las ideas principales que deben regir para su tratamiento en el ámbito judicial. De esta forma, vamos a examinar seguidamente, la jurisprudencia más relevante sobre el correo electrónico[407], mensajería instantánea[408] (*Facebook Messenger, Skype, Line, Hangouts, Telegram, Whatsapp, Wechat, etc.)*, redes sociales[409] (*Facebook, Instagram, Tuenti, LinkedIn, Twitter, Spotify, Badoo, Weibo*, etc.), *chats*[410] o *blogs*, servicio de mensajes cortos (SMS o *Short Message Service*)[411] y sistema de mensajería multimedia (MMS o *Multimedia Messaging Service*)[412]:

a´.1 El correo electrónico

- Derechos fundamentales afectados según la jurisprudencia

Como en toda comunicación, en los correos electrónicos inciden en distintos derechos fundamentales, en concreto, el secreto de las comunicaciones (art. 18.3 CE), la

[407] Correo electrónico o *e-mail* es un servicio de red que permite a los usuarios enviar y recibir mensajes electrónicos.

[408] Mensajería instantánea o IM es un servicio de comunicación entre personas que permite enviar mensajes de texto en tiempo real, a través de dispositivos conectados a una red, de tal forma que, los más habituales utilizados actualmente son: *Facebook Messenger, Skype, Line, Hangouts, Telegram y Whatsapp.*

[409] Red Social es una plataforma digital de comunicación global que pone en contacto a un gran número de usuarios.

[410] "*Chats"* o charla es un servicio de comunicación que permite conversar por escrito de manera instantánea entre dos o más personas conectadas a la red. De esta manera, el *chat* puede ser público, esto es, cuando cualquier persona puede participar en el mismo, o bien, privado, cuando el acceso está restringido a determinadas personas.

[411] SMS o *Short Message Service* es un servicio de telefonía móvil que permite enviar mensajes cortos de texto.

[412] MMS o *Multimedia Messaging Service* es un servicio de mensajería de telefonía móvil que permite enviar o recibir contenidos multimedia, como fotografías, sonidos o videos.

intimidad (art. 18.1 CE) o la protección de datos o autodeterminación informativa (art. 18.4 CE), si bien, como veremos, dependerá del estado en que se encuentre el mensaje, para que afecte a un derecho o a otro, y en consecuencia, determinará el tratamiento legal que será de aplicación en cada caso. De esta manera, cabe precisar que, hay tres momentos del proceso comunicativo en un correo electrónico, a saber, la transmisión del mensaje, el almacenamiento en el servidor y el acceso del usuario al mismo, esto es, la transmisión se inicia cuando se remite el mensaje, y finaliza cuando el receptor accede al contenido de la comunicación. De este modo, cuando el mensaje ha sido remitido, pero aún, no ha sido abierto y leído por el destinatario, el proceso comunicativo se encuentra en curso, por lo que, el derecho afectado es, al menos, la inviolabilidad de las comunicaciones (art. 18.3 CE), y en consecuencia, cualquier acceso al contenido del correo electrónico precisa, con arreglo a la norma constitucional, de autorización judicial. Sin embargo, cuando los mensajes, han sido 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 propio de la inviolabilidad de las comunicaciones, pues se ha visto culminado el proceso comunicativo, y en consecuencia, la información contenida en el mensaje es susceptible de protección en el ámbito de la intimidad, de tal forma que, como decimos, la Constitución en este caso, no exige expresamente para su injerencia el plácet judicial, por lo que, su protección es de una intensidad inferior a la reservada para el derecho al secreto de las comunicaciones. Por esta razón, precisar cuando el acceso afecta a la intimidad (art. 18.1 CE), o bien, alcanza también, al secreto de las comunicaciones (art. 18.3 CE), tiene relevancia, para determinar el régimen constitucional aplicable[413]. De este modo, como ya nos hemos referido, la intervención en las comunicaciones siempre requiere de resolución judicial, mientras que, para la intimidad (art. 18.1 CE), excepcionalmente se ha admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal, la Policía Judicial pueda realizar

[413] Afirma ROMEO CASABONA, M. C. "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de la red". Revista Aranzadi de Derecho y Nuevas Tecnologías. Núm. 10. 2006. Págs. 15-33; MISMO AUTOR. "La protección penal de la intimidad y de los datos personales los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable". Estudios Jurídicos. Ministerio Fiscal. Núm. 2. 2003. Págs. 73-104, que, la incidencia de los derechos fundamentales en los mensajes de correo electrónico dependerá de donde se encuentre el proceso comunicativo.

determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, como practicar inspecciones, reconocimientos o intervenciones corporales leves[414], siempre y cuando se respeten los principios de proporcionalidad y razonabilidad[415]. Por su parte, en el mismo sentido, Delgado Martín[416] diferencia varios escenarios del proceso comunicativo de los correos electrónicos a los efectos de su incidencia en los derechos fundamentales. De esta manera, la primera comprende la información almacenada en el servidor, esto es, sin entrar a conocer el contenido propio del mensaje, como por ejemplo los datos de la agenda o lista de usuarios, en este caso, cualquier injerencia afectaría a la intimidad (art. 18.1 CE), y la protección de datos o autodeterminación informática (art. 18.4 CE). Por el contrario, cuando el mensaje se encuentra en proceso de transferencia, es decir, se trata de un proceso comunicativo en curso, debido a que, el mensaje aún no ha sido recibido por el destinatario, o bien, habiéndose enviado y recibido, todavía no lo ha abierto el receptor, en este supuesto, la comunicación no se habría perfeccionado, y en consecuencia, el derecho fundamental conculcado sería la inviolabilidad de las comunicaciones (art. 18.3 CE). De igual modo, el último escenario engloba, cuando el emisor ha redactado el mensaje pero aún no lo ha enviado, por ejemplo guardándolo en el borrador del servidor, o bien, el receptor del mensaje lo ha abierto y permanece almacenado en el servidor como leído (en este caso, habría que presumir que se ha producido la lectura del contenido con la simple apertura del mensaje), en esta ocasión, no se ha iniciado, o ha finalizado el proceso de comunicación, por lo que, el derecho fundamental que se vería afectado sería la intimidad (art. 18.1 CE).

Así, como es sabido, el concepto de «secreto» tiene un carácter «formal» sobre lo comunicado, esto es, la condición «formal» del secreto de las comunicaciones, hace que se presuma (*iuris et de iure*) que es «secreto» el mensaje, aunque el contenido de la

[414] STC 207/1996, de 16 de diciembre (F.J. 4º).

[415] STC 142/2012, de 2 de julio: (F.J. 10º).

[416] Sobre la descripción de los distintos escenarios posibles de los mensajes de correo electrónico, en relación a su incidencia en los derechos fundamentales, véase, DELGADO MARTÍN, J. "Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos*"*. Diario La Ley. Núm. 8202. 29 de noviembre de 2013.

comunicación pertenezca o no, al ámbito de lo personal, lo íntimo o lo reservado, y en consecuencia, la protección constitucional se extiende al contenido del mensaje, independientemente de su incidencia en la esfera íntima de los interlocutores[417].

Una vez realizada las anteriores puntualizaciones, traemos a colación las afirmaciones de Marchena Gómez[418], el cual, mantiene que, en el servidor del correo electrónico se encuentran diversas clases de mensajes, como son los enviados, recibidos, los eliminados que permanecen en la papelera de reciclaje, los abiertos, los no leídos, etc. Por esta razón, dada la variedad, obligar a determinar en qué estado se encuentra cada mensaje, para fijar que derecho fundamental se vería afectado, y en consecuencia, establecer el tratamiento constitucional aplicable a los efectos de exigir plácet judicial, resulta totalmente desproporcionado. De manera que, mantiene el autor que, tanto si el mensaje incide en el secreto de las comunicaciones (art. 18.3 CE), como en la intimidad (art. 18.1 CE), y en su caso, en la protección de datos o autodeterminación informativa (art. 18.4 CE), únicamente podrá ser autorizada la injerencia mediante resolución judicial. De hecho, el tratamiento igualitario para todos los mensajes, independientemente del derecho fundamental afectado, se justifica, aparte de otorgar garantías a las intromisiones de los poderes públicos, además por razones prácticas, pues resultaría de gran complejidad discernir en cada momento en qué estado se encuentra la comunicación para determinar la exigencia o no, de intervención judicial. En consecuencia, los argumentos aducidos por el autor llevan a concluir que, cualquier injerencia efectuada en los mensajes de correo electrónico sin mandamiento judicial produce la ilicitud de la prueba por haberse obtenido violentando los derechos o libertades fundamentales (art. 11.1 LOPJ).

[417] La STC 114/1984, de 29 de noviembre (O.P. Cit), refiere al carácter formal del contenido de la comunicación.

[418] En relación a necesaria autorización judicial para acceder a la información de los correos electrónicos, independientemente del derecho fundamental que se vea afectado, véase, MARCHENA GÓMEZ, M. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones Jurídicas… O.P. Cit. Págs. 304-310; MISMO AUTOR. "Dimensión jurídico-penal del correo electrónico*"*. Estudios jurídicos. 2007.

- Empresas prestadoras de servicios de correo electrónico

Las empresas prestadoras de servicios de telecomunicaciones, como hemos visto, están obligadas a prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial la asistencia y colaboración precisas para facilitar el cumplimiento de la medida de intervención de las telecomunicaciones, en concreto, lo que interesa aquí es, la posibilidad de que los jueces puedan acudir a éstas compañías, para obtener información sobre las cuentas de correo electrónico de los usuarios, puesto que ostentan la obligación de dar cumplimento al requerimiento, so pena de incurrir en delito de desobediencia (art. 588 ter e. LECrim.). Sin embargo, como mantiene Velasco Nuñez[419], con frecuencia las cuentas de correo electrónico son gestionadas por sociedades erradicadas en países extranjeros, normalmente en Estados Unidos (por ejemplo, *Gmail* de la empresa *Gloogle* en California, *Outlook* o *Hotmail* de *Microsoft* en Washington, Yahoo! de *Verizon Communications Inc.* en California y Nueva York.), que además, suelen ser las utilizadas en la actividad delictiva, entre otras cuestiones, por ser gratuitas. Por este motivo, los datos de los usuarios que obran en poder de estas sociedades norteamericanas se encuentran almacenados en servidores fuera del territorio nacional, por lo que, para recabar dicha información, se precisa realizar la solicitud mediante Comisión Rogatoria Internacional (art. 276 a 278 LOPJ)[420]. No obstante, como decimos, al encontrarse las empresas, así como sus servidores en territorio estadounidense, se aplica la legislación propia del país (*Electronic Communications Privacy Act of* 1986 –ECPA-, 18 U.S.C. § 2510-22). De esta manera, cuando la autoridad judicial española necesite acceder a la información contenida en esos servidores para esclarecer algún hecho delictivo, deberá requerir dicha información a través de auxilio judicial mediante la emisión de una Comisión Rogatoria Internacional,

[419] Alude VELASCO NUÑEZ, E. *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 99-102, a la dificultad de requerir información a las empresas prestadoras de servicios de cuentas de correo electrónicos erradicadas en Estados Unidos.

[420] Respecto a Estados Unidos, se aplicará también, el *Tratado de Asistencia Jurídica Mutua en Materia Penal entre el Reino de España y los Estados Unidos de América*, hecho en Washington el 20 de noviembre de 1990 («BOE» Núm. 144, de 17 de junio de 1993) y el *Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de América*, firmado el 25 de junio de 2003 (DO L 181/34 de 19 de julio de 2003).

que además, deberá ser traducida al idioma de origen, para una vez recibida, si es aceptada, la autoridad norteamericana ejecutará la medida requiriendo a las empresas para que retengan o conserven los datos de los usuarios investigados, y finalmente, se remitirá a España la información obtenida. No obstante, el trámite normalmente puede dilatarse bastante en el tiempo, piénsese en el largo periodo que puede llegar a tardar, desde que se realiza la solicitud, hasta que se envía a España la información, produciendo en ocasiones situaciones que impiden o dificultan la efectividad de la medida. Por este motivo, la transmisión y ejecución de las Comisiones Rogatorias pueden realizarse, para supuestos de urgencia, a través de la Organización Internacional de Policía –INTERPOL[421]- (art. 15.5 *Convenio Europeo de Asistencia Judicial en Materia Penal*, hecho en Estrasburgo el 20 de abril de 1959[422]), mediante el sistema de comunicaciones entre las Oficinas Centrales Nacionales, esto es, el organismo que conecta a las policías nacionales con la red mundial de INTERPOL. De esta forma, la solicitud, adoptando la forma de resolución judicial motivada, en el sentido de explicar detalladamente la necesidad de obtener los datos para la investigación criminal, se remite a la Oficina Central española, gestionada por la Policía Judicial, para su remisión a través de INTERPOL, a su homólogo del país de destino. Sin embargo, en el caso estadounidense, su Oficina Central Nacional únicamente conceden información para la investigación de delitos graves o muy graves, pero además, excluyen cualquier remisión de datos relacionados con delitos que pudieran afectar a la libertad de expresión por conculcar con la Constitución estadounidense (Primera Enmienda de 15 de diciembre de 1791), como por ejemplo, injurias (art. 208 CP) o calumnias (art. 205 CP) cometidas a través de Internet. Otro argumento que suelen utilizar para la denegación de información es, con arreglo al art. 3 del Estatuto de la Organización Internacional de Policía Criminal –INTERPOL- de 1956, el cual, establece la prohibición de la INTERPOL de intervenir en cuestiones o asuntos de carácter político, militar, religioso o racial. Además, con carácter general, Estados Unidos no proporciona datos de las cuentas de correo electrónico cuando sean para la investigación de delitos cometidos

[421] RAYÓN RAMOS, M. "Organización Internacional de Policía Criminal INTERPOL*"*. Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 42. 1998. Págs. 111-137.

[422] Ratificado por España el 14 de julio de 1982 y publicado en el «BOE» núm. 223, de 17 de septiembre de 1982.

fuera de su territorio nacional. De este modo, en el supuesto de que la investigación delictiva afecte a los intereses norteamericanos, la petición por las autoridades judiciales españolas deberá ser exhaustiva, en la cual, deberá justificar las razones de su solicitud y los preceptos concretos infringidos del Código Penal español, todo ello, con la traducción al inglés. De esta manera, una vez recibida la Comisión Rogatoria Internacional, las autoridades norteamericanas, darán traslado al fiscal para que informe sobre los indicios de criminalidad, debiendo realizar en su escrito, un juicio de probabilidad o ponderación *("probable cause"*) sobre los hechos, y finalmente, el Juez norteamericano resolverá sobre la pertinencia de la medida. Para el hipotético caso de que el Juez aceptara la diligencia, se incoaría paralelamente una investigación en territorio norteamericano, toda vez que, en caso contrario, no podría dirigirse a la compañía proveedora del servicio. En conclusión, solicitar información a las compañías norteamericanas de gestión de cuentas de correo electrónico por las autoridades judiciales españolas resulta una tarea ardua, y prácticamente imposible de que se llegue a materializar.

Sin embargo, el trámite para obtener información sobre correos electrónicos de compañías prestadoras de servicios en la Unión Europea (como por ejemplo *GMX Mail* de la compañía *United Internet AG* en Alemania, *OpenMailBox* en Francia, etc.) es distinto al norteamericano, pues, con arreglo a la normativa comunitaria aplicable (art. 19 del *Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea*, hecho en Bruselas el 29 de mayo de 2000[423]), los Estados miembros deberán garantizar que otro Estado miembro pueda acceder directamente a los sistemas de servicios de telecomunicaciones que operen a través de una pasarela en su territorio, todo ello, a los efectos de intervenir las comunicaciones de una persona que se halle dentro de sus límites fronterizos. Por este motivo, las autoridades competentes de un Estado miembro, en el seno de una investigación penal, de acuerdo con la regulación de su Derecho nacional aplicable, tendrán derecho, siempre que se halle la persona investigada en ese Estado miembro, a llevar a cabo la intervención por mediación de un proveedor de servicios designado que se encuentre en su territorio, sin la participación del Estado miembro en que se encuentre la pasarela. Además, con arreglo a la Ley 23/2014, de 20 de noviembre, *de reconocimiento mutuo de resoluciones penales en la*

[423] Publicado en DOUEC Núm. 197 de 12 de julio de 2000 y BOE Núm. 247 de 15 de octubre de 2003.

Unión Europea[424], modificada por la Ley 3/2018, de 11 de junio[425], que venía a transponer la Directiva 2014/41/CE de 3 de abril de 2014, *relativa a la orden europea de investigación en materia penal*[426] permite emitir una resolución judicial denominada orden europea de investigación (OEI) de un Estado miembro para llevar a cabo medidas de investigación en otro Estado miembro (arts. 2.2.i. y 186 de la L. 23/2014, en relación con el art. 1.1 Directiva 2014/41/CE*)*, de tal forma que, un Estado miembro puede emitir una orden europea de investigación (OEI) para la intervención de telecomunicaciones en el Estado miembro cuya asistencia técnica se requiera (art. 202 L. 23/2014, en relación con el art. 30 Directiva 2014/41/CE), debiendo reconocer la autoridad de ejecución la OEI sin requerir otra formalidad, y se asegurará de que se ejecute de la misma manera y bajo las mismas circunstancias que si la medida de investigación de que se trate hubiera sido ordenada por una autoridad del Estado de ejecución (art. 206 L. 23/2014, en relación con el art. 9 Directiva 2014/41/CE), salvo que la autoridad de ejecución decida invocar alguno de los motivos de denegación del reconocimiento o de la ejecución de la OEI (arts. 205.1, 207 y 209 en relación con el art. 11 Directiva 2014/41/CE). De este modo, obtener información sobre los usuarios de cuentas de correo electrónico de empresas erradicadas en Estados de la Unión Europea, será mucho más accesible que en el caso norteamericano, pues, la autoridad judicial española, de acuerdo con la legislación mencionada, podrá dirigirse directamente a éstas, para recabar la información que sea necesaria en el seno de una investigación penal.

Por otro lado, es posible que, las empresas que gestionan las cuentas de correo electrónico tengan sede en España (por ejemplo, Microsoft Ibérica, Google España o Yahoo Iberia), de tal forma que, los juzgados pueden requerir directamente a sus filiales españolas información sobre sus usuarios. Sin embargo, estas sociedades no suelen proporcionar todos los datos requeridos, toda vez que, normalmente los servidores se encuentran fuera de nuestras fronteras, por lo que, en aplicación de su legislación nacional (en el ejemplo anterior, la legislación norteamericana), negarán la solicitud, o

[424] «BOE» Núm. 282, de 21 de noviembre de 2014.

[425] «BOE» Núm. 142, de 12 de junio de 2018.

[426] Publicada en el DOUE el 1 de mayo de 2014 L 130/1.

bien, la contestación será incompleta. Por este motivo, cuando los órganos jurisdiccionales necesiten recabar mayor información de los usuarios, como acceder al contenido de los correos electrónicos, deberán necesariamente tramitarla, mediante Comisión Rogatoria Internacional para países internacionales, o bien, emitir una orden europea de investigación (OEI) para países comunitarios.

- Intervención de un correo electrónico

Seguidamente vamos a exponer sucintamente la forma habitual de proceder en la intervención de los correos electrónicos del investigado. De esta manera, una vez acordada la autorización judicial habilitante[427], la Policía Judicial se dirige al proveedor del servicio (ISP)[428], pues es el encargado de permitir la remisión y recepción de los correos electrónicos del usuario, para que proporcionen la información necesaria para su intervención, como la identificación del usuario, la determinación del punto de red donde el proveedor suministra el servicio, el protocolo de acceso a mensajes de Internet (IMAP) o de oficina de correo (POP), etc. Una vez recibida la información con los datos necesarios, se configura el servidor, para que los equipos policiales de investigación encargados de esta operación, también puedan recibir el mensaje, de tal forma que, se duplica el correo electrónico, para que, además de recibir el mensaje en la cuenta del investigado, sea recibido también en la cuenta habilitada por el agente, sin que se percate de esta situación, la persona objeto de la medida. A continuación, la Policía Judicial[429] aportará al Juez los mensajes de correos electrónicos que contengan información relacionada con la investigación penal, o bien, el contenido íntegro de las conversaciones intervenidas (arts. 588 bis g, ter f, ter h. LECrim). Además, el Juez

[427] Advierte GARCIMARTIN MONTERO, R. *Interceptación de comunicaciones telefónicas o telemáticas, Los medios de investigación tecnológicos en el proceso penal*. Editorial Thomson Reuters Aranzadi. Navarra. 2018. Págs. 98-100, de las especialidades procedimentales en la interceptación de comunicaciones telefónicas o telemáticas, en especial, la intervención judicial.

[428] Proveedor de Servicios de Internet (ISP o "*Internet Service Provider"*) es la empresa que conecta a los usuarios de Internet a través de diferentes tecnologías como DSL, cable módem, GSM, dial-up, etc.

[429] Explica, como hemos mencionado en el texto, BAYONA PÉREZ, J. L. "La Guardia Civil y las nuevas tecnologías de la información…" O.P. Cit Págs. 35-46, la forma de actuar por la Policía Judicial, en la ejecución de una medida de interceptación de las comunicaciones telemáticas.

habrá de seleccionar los mensajes intervenidos, conservando en la causa únicamente aquellos que sean relevantes, descartándose pues, los que afecten a la intimidad del investigado o de terceros (art. 586 LECrim.).

- Incorporación al proceso penal y prueba de los correos electrónicos

La forma habitual de incorporar al proceso los correos electrónicos es mediante la impresión en papel del mensaje, sin embargo, en este caso, pueden ser fácilmente manipulados, de tal forma que, se alteren las identidades de los destinatarios o se modifiquen las fechas de emisión o recepción del mismo, pues se puede crear *a doc* un mensaje falso, con apariencia de veracidad, pero en cambio se presenta como original, pues ha salido del buzón con forma de auténtico. Piénsese por ejemplo, lo sencillo que es, cambiar la fecha y hora del dispositivo para que aparezca en la impresión un momento temporal erróneo, o bien, crear cuentas falsas de correo para que parezca que el mensaje ha sido enviado por otra persona, etc. Por este motivo, la incorporación al proceso penal de los correos intervenidos se deberá realizar respetando todas las garantías, a fin de asegurar la autenticidad del mensaje e identidad del emisor y receptor. De este modo, los correos electrónicos obtenidos tienen la consideración de fuente de prueba, para ello, pueden ser incorporados al proceso penal de dos maneras: aportados por alguno, o por los dos interlocutores (emisor o receptor), o bien, aquellos obtenidos tras haberse acordado judicialmente una medida de investigación válida en Derecho, como la intervención en las comunicaciones telemáticas (art. 588 ter y siguientes LECrim.)[430], así como, otras diligencias que serán objeto de estudio más adelante, como la entrada y registro domiciliario con aprehensión de equipos informáticos (art. 588 sexies y siguientes LECrim.) o registro remoto de ordenadores (art. 588 septies y siguientes LECrim.)[431].

[430] GARCÍA RUIZ, J. M. "Correo electrónico y proceso penal". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 3. 2003. Págs. 1687-1697.

[431] Acerca de las distintas diligencias de investigación que pueden ser utilizadas por la Policía Judicial para conocer el contenido de los equipos informáticos, véase, RICHARD GONZÁLEZ, M. "La investigación y prueba de hechos y dispositivos electrónicos". Revista General de Derecho Procesal. Núm. 43. 2017, entre otras medidas, el registro de dispositivos masivos de información o el registro remoto de ordenadores.

Habiendo dicho lo anterior, para que un correo electrónico pueda alcanzar valor probatorio en un proceso penal, deberá ser aportado en su momento procesal oportuno y en la forma establecida en la ley[432]. Sin embargo, la regulación contenida sobre esta materia es inexistente, por lo que, la práctica habitual es que se aporten mediante la presentación de una fotocopia o impresión del mensaje, de tal forma que, se trata de una prueba documental[433], pues la información consta en un documento. En otras ocasiones, el Letrado de la Administración de Justicia, o bien, un Notario, pueden transcribir el contenido de los correos electrónicos, dando fe de su coincidencia con el documento original, sin embargo, los fedatarios públicos únicamente acreditan la coincidencia del documento aportado con aquel mostrado en el dispositivo, pero no garantizan la autenticidad del mismo.

Retomando lo que venimos afirmando al inicio sobre que los correos electrónicos pueden ser fácilmente manipulables, en especial, cuando son aportados al proceso mediante la impresión en formato papel, cabe mencionar que, con carácter general, no

[432] Afirma RUBIO ALAMILLO, J. "El correo electrónico como prueba en procedimientos judiciales*"*. Diario La Ley. Núm. 8.808. 2016, que, "debido a la facilidad, puesta de manifiesto en este artículo, con la que se puede alterar o falsificar un correo electrónico o, sencillamente, incumplir los protocolos procesales que garanticen la cadena de custodia, integridad e inmutabilidad de la prueba a lo largo del proceso, el perito informático, en este tipo de procedimientos, juega un papel fundamental". Por su parte, MARTÍNEZ DE CARVAJAL HEDRICH, E. "Valor probatorio de un correo electrónico*"*. Diario La Ley. Núm. 8.014. 2013, mantiene que, "por regla general, cuando una parte considera que dispone de un correo electrónico de especial relevancia para el caso lo aporta impreso, tal y como se genera al pulsar la opción de «imprimir» del programa de gestión de correos utilizado. La realidad es que el valor intrínseco de dicha prueba es prácticamente nulo y queda a expensas de que la otra parte no lo impugne ya que, caso de hacerlo, difícilmente se puede defender su legitimidad sin el adecuado soporte técnico. Esta carencia de fuerza probatoria se debe a que lo que se aporta en una copia impresa del correo y, como tal, es extremadamente sencillo generar documentos de texto con una apariencia idéntica, por lo que se genera una duda razonable sobre su autenticidad". En el mismo sentido, véase, GAVILÁN LÓPEZ, J. "Correos electrónicos y SMS como prueba*"*. Iuris: Actualidad y Práctica del Derecho, Núm. 167. 2012. Págs. 30-33; FUENTES SORIANO, O. *El valor probatorio de los correos electrónicos. (Justicia penal y nuevas formas de delincuencia)*. Editorial Tirant lo Blanch. Valencia. 2017. Págs. 183-210.

[433] Destaca BERRO, L. "El correo electrónico como prueba documental*"*. Revista de Derecho y Tribunales. Núm. 18. 2012. Págs. 175-190, que el correo electrónico es una prueba eminentemente documental.

habrá de tenerlos por falsos, sino que dependerá su valor probatorio, de la actitud impugnatoria que adopte alguna de las partes, así como, del resto acervo probatorio obrante en las actuaciones. De esta manera, cuando alguna de las partes proceda a la impugnación de los mensajes, por ejemplo, alegando la falsedad o manipulación fraudulenta, quien haya aportado el documento, le incumbe acreditar la veracidad, mediante algún medio válido en Derecho, como el interrogatorio de los acusados, testificales, periciales informáticas, o incluso, indicios que permitan llegar a la conclusión de la autenticidad de los *emails*. De este modo, la mejor forma para garantizar la veracidad o autenticidad de los correos electrónicos es con la elaboración de un informe pericial informático[434]. Sin embargo, la pericial informática resulta ser una prueba muy compleja, lenta y costosa, toda vez que, para que sea realizada con todas las garantías, se deben analizar minuciosamente los dispositivos utilizados en la comunicación, así como respetar la cadena de custodia. Por este motivo, cuando no se discuta la autenticidad, sino el valor probatorio de su contenido, bastará con la utilización de cualesquiera otros medios probatorios tradicionales, como el interrogatorio de los acusados o testificales, esto es, la declaración del sujeto que haya tenido contacto directo o de referencia sobre el mensaje (lo normal será que declare el emisor o el receptor del correo electrónico, o bien, el agente de policía judicial que haya intervenido en la interceptación de las comunicaciones). También, documentales, con la presentación de documentos públicos (el acta notarial o del Letrado de la Administración de Justicia que constate el mensaje) o privados (fotocopias o soportes electrónicos como un CD o DVD que contenga archivos con *emails*), o incluso, como prueba por indicios que permita al juzgador dar validez a los correos electrónicos

[434] Acerca de la prueba pericial informática, como mejor manera de garantizar la veracidad o autenticidad de los correos electrónicos, véase, RICHARD GONZÁLEZ, M. "La investigación y prueba de hechos y dispositivos electrónicos*"*. Revista General de Derecho Procesal. Núm. 43. 2017; VELASCO NUÑEZ E., *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 53-55; 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. Núm. 7329. 2010; MAGRO SERVER, V. "La prueba pericial informática. La utilización de los medios de prueba informáticos en el proceso penal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 33. 2006. Págs. 107-115; LÓPEZ-SILVES MARTÍNEZ, A. *Pericial informática*. Estudios de Derecho Judicial. Núm. 71. 2005. Págs. 259-292.

aportados al proceso. En este sentido, como mantiene nuestro Tribunal Supremo[435], cuando exista impugnación sobre la autenticidad de cualquiera de las conversaciones realizadas mediante correo electrónico y que fueron aportadas en la causa mediante documentos impresos, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria, y en tal caso, será indispensable la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido. Debido a lo cual, la prueba pericial informática resultará imprescindible para garantizar la autenticidad de la comunicación realizada a través de los correos electrónicos, toda vez que, se alcanza la adveración del mismo con la práctica de dicha prueba.

Una vez expuesta la importancia de esta prueba, aunque será objeto de análisis posteriormente en un capítulo dedicado de forma genérica a ella, cabe dedicar unas líneas a explicar la prueba pericial informática específica de correos electrónicos. De este modo, el correo electrónico permite a los usuarios enviar y recibir mensajes electrónicos, de tal forma que, como en toda comunicación, existen dos partes diferenciadas, el emisor y el receptor, si bien, en el caso del *email*, coincide con los datos de encabezamiento del mismo, pero además, en el cuerpo del mensaje aparece el contenido de la comunicación, en consecuencia, cuando se imprime en papel, se presenta en el documento toda esta información. Sin embargo, como decimos, los datos pueden ser manipulados, para lo cual, la mejor manera de comprobar la autenticidad del mensaje es mediante el examen técnico del ordenador que haya participado en el proceso comunicativo, de modo que, pueda ser corroborado el recorrido del mensaje desde su emisión, pasando por los diversos servidores que hayan participado, hasta su recepción por el destinatario, mostrando también la huella cronológica del correo, esto es, las direcciones IP a través de las cuales ha pasado, así como la fecha y la hora del mismo. Por su parte, lo más importante del contenido informático de un correo electrónico es el encabezamiento, pues encierra los datos necesarios reales para identificar la huella cronológica del mensaje, con ello, se pueden extraer los datos originales para identificar a los usuarios emisor y destinatario, las direcciones IP del recorrido el mensaje, lo cual, hace posible averiguar incluso la geolocalización, el número ID del correo o código único que identifica cada mensaje, así como la fecha y

[435] STS Núm. 300/2015… O.P. Cit. (F.D. 4º).

hora de la emisión y recepción del mensaje. En definitiva, la mejor manera de conocer la autenticidad del mensaje es mediante el acceso al equipo informático, para lo cual, habrá que realizar un análisis comparativo entre la información contenida en los datos del encabezamiento del correo electrónico impreso en papel con los datos obtenidos del dispositivo electrónico, y en consecuencia, elaborar un informe pericial informático al efecto.

a´.2 Otros servicios de comunicación: mensajería instantánea (*Facebook Messenger, Skype, Line, Hangouts, Telegram, Whatsapp, Wechat*, etc.), sistema de mensajería multimedia (MMS o *Multimedia Messaging Service*)

- Características generales de la mensajería instantánea

La mensajería instantánea (*Facebook Messenger, Skype, Line, Hangouts, Telegram, Whatsapp, Wechat, etc.)* permite la comunicación bidireccional como multidireccional entre usuarios mediante la utilización de dispositivos móviles o *Smartphone*, pero también, puede ser utilizada por otros dispositivos electrónicos como ordenadores o *tablets*, en la cual, hace posible transmitir en tiempo real principalmente mensajes de texto, aunque es posible además, realizar videoconferencias, enviar fotografías, mensajes de voz (VOIP) o captaciones de video, compartir contactos o la ubicación donde se encuentra el terminal[436], etc. La diferencia principal con los correos electrónicos es que la información transmitida no se conserva en un servidor externo, ni con carácter general, precisa acceder a una sesión para establecer la comunicación, sino que los datos permanecen en los dispositivos electrónicos utilizados por los usuarios. De este modo, los proveedores del servicio de mensajería instantánea, que se encargan de gestionar sus aplicaciones o *software*, tienen por objeto facilitar la comunicación entre los usuarios, para lo cual, aplican determinados protocolos de seguridad que garantizan el cifrado de la información. Por este motivo, la información que únicamente podrá facilitar el proveedor del servicio será la relacionada con los datos de tráfico generados en la conversación, esto es, la identidad de los usuarios, número de teléfono o IP, origen o destino del mensaje, hora, fecha, duración de la comunicación, etc. En cambio,

[436] Sobre las cuestiones técnicas aludidas en el texto acerca de las aplicaciones de mensajería instantánea, en especial, el *Whatsapp*, RODRÍGUEZ LAINZ, J. L. "Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones*"*. Diario La Ley. Núm. 8831. 2016.

cuando se pretenda intervenir las comunicaciones para acceder al contenido del mensaje emitido en tiempo real, habrá que acudir a un *software* específico que permita descifrar o desencriptar los protocolos. Sin embargo, la interceptación de las comunicaciones no podrá referirse a conversaciones que hayan tenido lugar en el pasado, pues el contenido del mensaje no se almacena en servidor alguno[437]. Por este motivo, el Juez no podrá dirigirse a la empresa proveedora del servicio a los efectos de requerir los mensajes que hayan sido enviados y recibidos, sino que la única manera de poder acceder a dichos mensajes será con la intervención directa de los dispositivos utilizados por los comunicantes.

- Mensajería instantánea como prueba en el proceso penal

Los mensajes instantáneos utilizados por los usuarios pueden ser llevados al proceso penal para acreditar hechos, de tal forma que, tienen la consideración de prueba electrónica o digital[438], toda vez que, se trata de información producida, almacenada o transmitida en un medio electrónico, lo cual, hace que puedan tener valor probatorio. De igual modo, como se ha mencionado para los correos electrónicos, puede incorporarse la información en el proceso penal mediante algún medio válido en Derecho, siendo la manera habitual, la aportación al proceso como prueba documental, esto es, como documento en formato papel de los mensajes o "pantallazos", aunque nada impediría ilustrar al tribunal de otra forma, como por ejemplo mediante la elaboración de un informe pericial, o bien, con la declaración de los encartados o testificales, que hayan tenido contacto con el dispositivo electrónico donde se haya efectuado la comunicación. Sentado lo anterior, cabe realizar una serie puntualizaciones relacionadas con la

[437] En relación a los proveedores de los servicios de mensajería instantánea, en especial, el *WhatsApp*, véase, MOLINA PÉREZ TOMÉ, S. y SÁNCHEZ VALDEÓN, M. *Cifrado de WhatsApp y aportación de prueba. (La prueba electrónica: validez y eficacia procesal)*. Editorial Juristas con Futuro. Desafíos Legales. Madrid. 2016. Pág. 104; MAEZTU LACALLE, D. *¿Puede WhatsApp (u otro prestador de servicios de comunicaciones) certificar el contenido de una comunicación? (La prueba electrónica: validez y eficacia procesal).* Editorial Juristas con Futuro. Desafíos Legales. Madrid. 2016. Pág. 98.

[438] Con respecto a la prueba electrónica, DELGADO MARTÍN, J. "La prueba electrónica en el proceso penal*"*. Diario La Ley. Núm. 8167. 2013, lo define como "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio*",* lo cual, incluiría también, los mensajes instantáneos.

obtención e incorporación[439] de los mensajes instantáneos en el proceso penal. De esta manera, se podrá obtener la información contenida en los *software* de mensajería instantánea mediante la adopción de alguna medida restrictiva de derechos fundamentales, en concreto, con la intervención de las comunicaciones telemáticas (art. 588 ter LECrim.), o bien, con alguna otra diligencia que serán objeto de análisis posteriormente, como el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.) o registro remotos sobre equipos informáticos (art. 588 sexies LECrim.).

En este sentido, como advierte nuestro Tribunal Supremo[440], existe un derecho al "*entorno virtual*", que integraría toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos, de tal forma que, el sacrificio en este derecho, supone, como en la inviolabilidad de las comunicaciones y la intimidad, que sea mediante plácet judicial. De esta manera, la incorporación al proceso penal de datos o informaciones relacionadas con los mensajes remitidos o recibidos a través de un *software* de mensajería instantánea, deben realizarse a través de algún medio válido en Derecho. En este sentido, dada las peculiaridades técnicas de esta clase de mensajería, pues las piezas de convicción se encuentran en dispositivos informáticos o tecnológicos, tales como teléfonos inteligentes (*smartphone*), *tablets*, ordenadores,

[439] Afirma DELGADO MARTÍN, J. "La prueba de Whatsapp*"*. Diario La Ley. Núm. 8605. 2015, que, "para avanzar en la forma de acreditar el contenido de mensajes de WhatsApp debemos distinguir tres fases comunes a toda prueba electrónica o digital: 1. Obtención de la prueba: se refiere al acceso a las fuentes de la prueba electrónica, es decir, a la obtención de la información o datos por las partes (o por la autoridad pública en el proceso penal) antes de su aportación al proceso. 2. Incorporación al proceso de la información o datos obtenidos que sean relevantes para la acreditación de hechos. 3. Valoración de la información o datos por el Juez o Tribunal de enjuiciamiento*"*. En el mismo sentido, BUENO DE MATA, F. *Diligencias de investigación tecnológicas para la obtención y aportación de mensajes de whatsapp, snapchat o telegram (Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática: Salamanca, 19-21 de octubre 2016. Vol.1)*. Editorial Ratio Legis. Salamanca. 2016. Págs. 251-263, expone la forma de proceder para obtener e incorporar al proceso los mensajes de *Whatsapp*.

[440] Sobre el derecho al entorno virtual, la STS 97/2015, 24 de febrero (F.D. 4º), STS 342/2013, de 17 de abril y STS 204/2016, 10 de marzo (F.D. 11º) y STS 508/2017, 4 de julio (F.D. 1º).

etc, habrá que adaptar los formatos e instrumentos para que pueden tener acceso al proceso penal a través de algún medio de prueba previsto en el ordenamiento procesal, y en concreto, como decimos, lo habitual será que adopte la forma de documento, pues como en el caso de los correos electrónicos, su incorporación al proceso puede realizarse mediante la impresión en formato papel de los mensajes o "pantallazos", pero también, en otras ocasiones, la aportación podrá ser a través del propio documento electrónico (por ejemplo adjuntar una memoria USB -"*pendrive*"-, DVD, CD-Rom, etc.), pues también se considera documento, con arreglo al art. 26 del CP, o incluso, se podrá aportar el propio dispositivo o terminal para su examen por el tribunal (por ejemplo entregar al juzgado el *smartphone* o *tablet* con la conversación mantenida vía *WhatsApp)*.

Además, se podrá incorporar al proceso penal la información a través de un informe pericial realizado por un técnico en informática o en telecomunicaciones, o bien, por otros medios de prueba como la declaración de los procesados (art. 385 LECrim.) o interrogatorio de testigos (art. 410 LECrim.), mediante el testimonio que puedan realizar sobre los mensajes enviados o recibidos. En cualquier caso, nada impediría que, para una mejor acreditación de los hechos, pueden utilizarse varios medios probatorios en el mismo proceso penal.

En conclusión, la mejor manera de acreditar unos hechos relacionados con la mensajería instantánea sería aportando el dispositivo para que fuera examinado por el tribunal, si bien, como la conversación puede ser bidireccional o multidireccional (ejemplo grupos de *WhatsApp*), podrá incorporarse cualquier terminal que haya participado en la conversación. A la vez, los mensajes pueden aportarse con la transcripción escrita en documento privado en formato papel o electrónico, o bien, público, con un acta notarial con la transcripción del contenido de la conversación[441]. Conjuntamente a esto, el Letrado de Administración de Justicia deberá someterlo al cotejo, de tal forma que, garantice que el contenido del dispositivo corresponde con la transcripción. Sin embargo, cuando esto no fuera suficiente, debido a que alguna parte impugne la

[441] Examina RIPOLL SOLER, A. "El acta notarial perfecta de comunicaciones por Whatsapp*"*. Revista Boliviana de Derecho. Núm. 19. 2015. Págs. 404-425, la posibilidad de recoger en un acta notarial los mensajes de *Whatsapp*, con arreglo a la legislación española.

autenticidad y/o de integridad con argumentos sólidos (por ejemplo que ha existido manipulación o que la identidad ha sido suplantada), como en el caso estudiado de los correos electrónicos, se *desplazara la carga de la prueba hacia quien pretenda aprovechar su idoneidad probatoria,* de modo que, *será indispensable en tal caso la práctica de una prueba pericial*[442] *que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*[443]. Sin perjuicio con lo mencionado anterioremnte, podrá someterse también a declaración a los testigos o encartados, para que expongan los hechos sobre los mensajes enviados o recibidos[444].

---

[442] Sobre la aplicación de mensajería instantánea de *whatsapp* como medio probatorio en el proceso, todo ello, a raíz de la sentencia del TS Núm. 300/2015 que venimos analizando, véase, GARZÓN, M. J. "Los «pantallazos» de los mensajes «whatsapp» como medio de prueba en el proceso laboral. A propósito de la Sentencia del Tribunal Superior de Justicia de Galicia, de 28 de enero de 2016…*"* O.P. Cit. Págs. 177-183; BUENO DE MATA, F. "La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica…*"* O.P. Cit.; MISMO AUTOR. *La validez de los "screenhots" o "pantallazos" como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo. (Los desafíos de la justicia en la era post crisis)…* O.P. Cit. Págs. 141-152; MISMO AUTOR. *Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª), de 19 de mayo de 2015 (ROJ: STS 2047/2015)…* O.P. Cit. Págs. 322-324; RODRÍGUEZ LAINZ, J. L. "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea propósito de la STS, Sala 2.ª, 300/2015, de 19 de mayo…*"* O.P. Cit.

[443] STS 300/2015, 19 de mayo (O.P. Cit), sobre los "pantallazos" como prueba en el proceso penal. Dicha doctrina jurisprudencial ha sido asumida en las resoluciones judiciales que se mencionan a continuación: STS 754/2015, 27 de noviembre; SAN 37/2015, 12 de junio; SAP de Barcelona (Sección 20ª) 379/2017, 9 de mayo; SAP de La Rioja (Sección 1ª) 111/2017, 5 de octubre; SAP de Sevilla (Sección 4ª) 437/2017, 22 de septiembre; SAP de Sevilla (Sección 4ª) 437/2017, 22 de septiembre; SAP de Soria (Sección 1ª) 47/2018, 21 de mayo; SAP de Valencia (Sección 4ª) 276/2017, 25 de abril.

[444] Señala CUAIRÁN, J. "La aportación de WhatsApps como medio de prueba en el procedimiento penal*"*. Diario La Ley. Núm. 9219. 2018, que, "los mensajes de WhatsApp son perfectamente utilizables como medio de prueba en un procedimiento penal —debiendo estarse al principio de libre valoración de la prueba por parte del Juez, junto con el resto de pruebas practicadas, en virtud del art. 741 LECrim.—, dada la configuración técnica actual de este servicio de mensajería no es posible garantizar, sin lugar a la duda razonable, la autenticidad de las conversaciones ni la integridad de su contenido, si no es mediante el cotejo de todos los terminales intervinientes en la conversación". Por su parte, DELGADO MARTÍN, J. "La prueba del whatsapp*"*. O.P. Cit, afirma que, "quien se enfrente a la prueba de un mensaje o

a´.3 Redes sociales

Las redes sociales[445] (ejemplo *Facebook, Instagram, Tuenti, LinkedIn, Twitter, Spotify, Badoo, Weibo*, etc.) son plataformas tecnológicas que permiten a sus usuarios a través de sus correspondientes perfiles, vincularse entre sí, creando sistemas cruzados e interactivos de generación y difusión de información. Una vez realizada esta aclaración, seguidamente vamos a examinar desde la perspectiva de la jurisprudencia, la problemática suscitada sobre el uso de estas plataformas en el ámbito laboral[446], si bien, aunque se trate de un asunto que concierne principalmente a la jurisdicción social, lo

---

conversación de WhatsApp no solamente ha de ser consciente de los riesgos de manipulación y/o suplantación, sino que también debe analizar con detenimiento las diferentes posibilidades de proposición de medios probatorios, teniendo en cuenta la posición procesal que eventualmente puede adoptar la parte contraria". En el mismo sentido, véase, SANJURJO RÍOS, E. I. "Las conversaciones de WhatsApp como objeto de investigación y prueba en el proceso penal*"*. Justicia: Revista de Derecho Procesal. Núm. 1. 2017. Págs. 503-528; MIRÓ MORROS, D. "Las comunicaciones a través del aplicativo "whatsapp" como prueba*"*. Actualidad jurídica Aranzadi. Núm. 934. 2017. Págs. 7-7; ARRABAL PLATERO, P. *El whatsapp como fuente de prueba. (El proceso penal: cuestiones fundamentales).* Editorial Tirant lo Blanch. Valencia. 2017. Págs. 351-362.

[445] Sobre que las redes sociales pueden ser un instrumento para la actividad delictiva, véase, PRIETO, S. "Delitos y redes sociales*"*. La Ley Penal. Núm. 112. La Ley 1259/2015; ALONSO GARCÍA, J. *Derecho penal y redes sociales*. Derecho Penal y Redes Sociales. Editorial Aranzadi. Navarra. 2015; LLORIA GARCÍA, P. *Delitos y redes sociales los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al «sexting»)*… O. P. Cit. Pág. 3; NIETO MARTÍN, A. y MAROTO CALATAYUD, M. "Las redes sociales en internet como instrumento de control penal tendencias y límites*"*. Revista de Derecho Penal y Criminología. Núm. 1. 2013. Págs. 93-130; LLORIA GARCÍA, P. *Intimidad y redes sociales ¿cómo alcanzar la tutela penal? (Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías).* Editorial Universidad de Valencia. 2011. Págs. 467-475.

[446] Con carácter general, acerca del uso de las redes sociales en el ámbito laboral, véase, NAVARRO SERRANO, A. "Redes Sociales y Libertad de Expresión: ¿puede un trabajador criticar a su empleadora, fuera del centro y jornada de trabajo, y ser sancionado por ello?*"* Revista Aranzadi Doctrinal Núm. 8/2016; SELMA PENALVA, A. "La información reflejada en las redes sociales y su valor como prueba en el proceso laboral análisis de los últimos criterios jurisprudenciales*"*. Revista General de Derecho del Trabajo y de la Seguridad Social. Núm. 39. 2014; GRANDE, C. y GORDILLO, C. "El uso de las redes sociales en la jurisprudencia social*"*. Actualidad Jurídica Aranzadi Núm. 855/2013; CALVO GALLEGO, J. "TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales*"*. Revista Doctrinal Aranzadi Social. 2012.

cierto es que, como veremos, se pueden extraer ideas para su aplicación al ámbito penal. De esta manera, la situación es, el uso de las redes sociales por el trabajador en su jornada laboral, puede ser causa de despido disciplinario, si bien, para que el despido pueda ser declarado procedente, debe existir una especial gravedad del hecho y que constituya un incumplimiento grave y culpable de las obligaciones asumidas por el trabajador (art. 54 ETT), para lo cual, el empleador habrá de haber informado adecuadamente al trabajador sobre los límites en el uso de los medios tecnológicos y las consecuencias jurídico laborales de su incumplimiento (sanción o despido). Además, el empleador ostenta el poder de dirección sobre el trabajador (art. 5.c. ETT), es decir, puede realizar un control efectivo en el cumplimiento de sus instrucciones (art. 20.3 del ET), y en caso de incumplimiento, incluso tiene la facultad para imponer sanciones (art. 58.1 del ET). Esto es debido a que las empresas pueden ser responsables penalmente (art. 31 bis CP implementado con la L.O. 5/2010, de 22 de junio), o bien, civilmente, por culpa *in vigilando o in eligendo* (art. 1903 CC), por las acciones ilícitas cometidas por sus empleados. No obstante, el aludido poder de dirección del empleador, tiene sus restricciones cuando incida en el derecho fundamental a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE). Sin embargo, en el caso de las redes sociales que, los datos se encuentran publicados en un contexto de espacio abierto y de amplia difusión, pues los usuarios libremente pueden acceder a la información a través de la red, debido a lo cual, difícilmente afecta las intromisiones en la esfera más íntima de las personas. De esta manera, lo importante es analizar la admisibilidad de las pruebas obtenidas desde las redes sociales por parte del empleador, pues, teóricamente no se verían afectados los derechos fundamentales[447]. Sin embargo, cuando el acceso tecnológico se produzca en la vida privada del trabajador, dicha libertad se restringe a la hora de obtener pruebas para su aportación a juicio, de tal forma que, como recuerda el

[447] STC 241/2012, de 17 de diciembre (F.J. 3º y 7º) y STC 170/2013, de 7 de octubre (F.J. 4º y 5º) dispone que "la acción empresarial de fiscalización no ha resultado desmedida respecto a la afectación sufrida por la privacidad del trabajador".

Tribunal Europeo de Derechos Humanos en el asunto Barbulescu contra Rumania[448], la comunicación electrónica debe ser protegida en cuanto que forma parte del ejercicio de una vida privada, siendo cuestión distinta, cuáles son los límites que pueden establecerse a su ejercicio[449]. De este modo, de acuerdo con la comentada sentencia del TEDDHH, las comunicaciones efectuadas desde el lugar de trabajo por los instrumentos tecnológicos proporcionados para desempeñar su actividad laboral están protegidas por los derechos fundamentales a la vida privada y de correspondencia (art. 8 Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[450]), salvo

[448] La STEDDHH, asunto Barbulescu contra Rumania, de 5 septiembre 2017 (Párrafo 116) dispone que *"*el derecho laboral tiene características específicas que deben tenerse en cuenta. La relación entre una empresa y su empleado es una relación contractual, acompañada de derechos y obligaciones especiales, y caracterizada por una relación legal de subordinación. Se rige por su propio sistema jurídico, que es claramente distinto del sistema general de relaciones entre individuos*…"*

[449] Con carácter general acerca de la doctrina Barbulescu, véase, SÁNCHEZ DEL OLMO, V. "El impacto (divergente) de la doctrina Barbulescu en las resoluciones de instancia comentarios a las sentencias 341/2017 y 737/2017 de los Juzgados de lo Social de Madrid n. 19 y n. 33*"*. Trabajo y Derecho: Nueva Revista de Actualidad y Relaciones Laborales. Núm. 45. 2018. Págs. 123-134; CANO GALÁN, Y. "La licitud de la prueba obtenida mediante el control del correo electrónico corporativo: aplicación de la doctrina del asunto Barbulescu II*"*. Diario La Ley. Núm. 9194. 2018; LÓPEZ DE LA FUENTE, G. *Poder de control empresarial y limitación de derechos fundamentales de los trabajadores a propósito de la STEDH de 12 de enero de 2016, Barbulescu contra Rumanía (Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute)*. Sepin Editorial Jurídica. Madrid. 2018. Págs. 455-469; MOLINA NAVARRETE, C. "De Barbulescu II a López Ribalda ¿que hay de nuevo en la protección de datos de los trabajadores?*"* Revista Derecho del Trabajo. Núm. 19. 2018. Págs. 121-130; "TEDH (Gran Sala) Caso Barbulescu contra Rumania. Sentencia de 5 septiembre 2017*"*. Revista Aranzadi de Derecho y Nuevas Tecnologías. Núm. 46. 2018; GARCÍA GONZÁLEZ, R. L., y PASTOR MERCHANTE, J. "Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral: una reflexión tras la sentencia del TEDH de 12 de enero de 2016 en el caso Barbulescu*"*. Diario La Ley. Núm. 8715. 2016; GUDÍN RODRÍGUEZ-MAGARIÑOS, F. "El derecho al respeto a la intimidad telemática versus la sentencia «Barbulescu», del Tribunal Europeo de Derechos Humanos: consecuencias en el orbe penal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 118. 2016.

[450] Resolución de 5 de abril de 1999, de la Secretaría General Técnica, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de

que el trabajador sea informado por anticipado de la extensión y de la naturaleza de la vigilancia, de manera que, sea plenamente conocedor que, el empleador tiene acceso a sus comunicaciones. Esto resulta predicable también, a las comunicaciones efectuadas desde una plataforma de redes sociales que, como decimos, se originan en un contexto de espacio abierto en la red.

No obstante, el derecho laboral tiene un régimen jurídico propio que, lo diferencia de otras ramas del Derecho, pues coexiste una relación de subordinación entre el empresario y el trabajador, de tal forma que, los Estados disponen de un amplio margen de apreciación para fijar la regulación del marco de actuación en el que deberá desenvolverse la vida laboral del trabajador en el ámbito de la empresa, con respeto a las reglas sobre utilización de comunicaciones electrónicas.

Una vez examinado en el ámbito laboral sobre la admisibilidad de las pruebas electrónicas en el proceso obtenidas por el empleador, se pueden extraer las siguientes conclusiones para su aplicación al proceso penal. De este modo, cuando los datos publicados se encuentren en un contexto de espacio abierto y de amplia difusión, como sucede habitualmente en las redes sociales, toda información obtenida podrá ser incorporada libremente al proceso penal, por el contrario, cuando el acceso al contendido de la red social sea restringido o limitado a pocas personas (por ejemplo, con una clave de acceso), entrará en juego la protección a la intimidad (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE). De esta manera, la diferencia con el régimen jurídico laboral que, el empresario podía realizar injerencias en la privacidad del trabajador, cuando informara por anticipado de la vigilancia en los medios tecnológicos proporcionados para desempeñar su actividad, así como de las consecuencias del uso inadecuado del mismo, en la jurisdicción penal, al no existir una relación de subordinación como en el ámbito social, toda intromisión no consentida que incida en la intimidad, o bien, en el secreto de las comunicaciones, deberá realizarse con todas las garantías, para lo cual, habrá de estar respaldada con una autorización judicial habilitante[451]. En este caso, nos remitimos a lo expuesto en la parte del presente trabajo

marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983. «BOE» Núm. 108, de 6 de mayo de 1999.

[451] Afirman RODRÍGUEZ ÁLVAREZ, A. *Proceso penal y redes sociales aportación por las partes de la información contenida en ellas (El proceso penal cuestiones fundamentales)*. Editorial Tirant lo Blanch.

sobre la obtención e incorporación de los correos electrónicos y la mensajería instantánea, en especial, a la jurisprudencia de nuestro Tribunal Supremo sobre los "pantallazos"[452].

a´.4 Chats, foros y blogs

El *chats* o charla es una comunicación escrita entre dos o más personas realizada de manera instantánea mediante el uso de un *software* conectado a la red, pero además, el *chats* puede ser abierto, cuando se realiza de forma pública y cualquier persona puede intervenir en el mismo, pero también puede ser cerrado, cuando el acceso es privado y restringido a determinadas personas, esta distinción es importante por los motivos que después se examinarán.

Los usuarios de los *chats,* con frecuencia, utilizan apodos, *nicks* o pseudónimos que puede dificultar su identificación. De igual modo, la principal característica de estas aplicaciones es que los datos no se almacenan en los terminales, sino que se encuentran en los propios servidores de los *chats*. Una vez examinado de forma sucinta en qué consisten los *chats,* cabe mencionar que, los abiertos, al ser de libre acceso e intervienen numerosos usuarios, cualquier intromisión no plantea problemas en los derechos fundamentales, en especial, el secreto de las comunicaciones (art. 18.3 CE), de tal forma que, el conocimiento e incorporación al proceso penal no precisa de plácet judicial, pues bastará con la aprehensión y aportación mediante alguna forma válida en Derecho, siendo la forma habitual como documento impreso en formato papel. Por su parte, los *chats* cerrados, al tratarse de una comunicación bidireccional privada, cualquier intromisión no consentida por el titular, requiere recabar autorización judicial, pues incide directamente en el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE), y en su caso, en la intimidad (art. 18.1 CE). No obstante, para obtener los datos de tráfico o asociados a una comunicación de los *chats* abiertos y cerrados, como por ejemplo proceder a la identificación y localización de los equipos informáticos a través de la dirección IP (art. 588 ter k LECrim.), será necesario plácet judicial, con

2016. Págs. 339-348; SÁEZ-SANTURTÚN PRIETO, M. "La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 de mayo de 2015…" O.P. Cit, que, los mensajes en redes sociales pueden ser aportados como prueba en el proceso penal.

[452] STS 300/2015, O.P. Cit.

arreglo a las disposiciones contenidas en la ley procesal penal (art. 588 ter j LECrim.), así como la Ley de conservación de datos (arts. 6.1 y 7 L. 25/2007).

A su vez, resulta necesario reseñar que, los foros de internet son sitios de discusión en línea, donde los usuarios publican mensajes alrededor de un tema, de tal forma que, nada impediría que estas personas exteriorizaran manifestaciones con contenido ilícito, como por ejemplo enalteciendo o justificando públicamente el terrorismo (art. 578 CP)[453]. Este delito, como es sabido, se castiga la conducta consistente en enaltecer o justificar públicamente los delitos de terrorismo o de sus participantes, o bien, actos que entrañen descrédito, menosprecio o humillación a las víctimas o sus familiares (art. 578.1 CP)[454], sin embargo, tendrá la pena carácter agravatorio, cuando se realice el hecho mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información (art. 578.2 CP)[455]. De este modo, el enaltecimiento o justificación pública del terrorismo comporta que, la acción se realiza contra un colectivo difuso, esto es, sin identificar a ninguna persona en concreto, sino que se proyecta sobre personas que pertenecen a un determinado grupo, mientras que, realizar actos que entrañan descrédito, menosprecio o humillación de las víctimas o sus familiares, se produce un ataque dirigido contra personas concretas, es decir, afecta directamente en un bien jurídico de la víctima, en particular, a su propia dignidad.

[453] Sobre los foros públicos utilizados para enaltecer o justificar el terrorismo, véase, SAN 3/2010, de 2 de marzo (F.J. 1º) y SAN 21/2014, 29 de mayo.

[454] En relación al delito de enaltecimiento y justificación del terrorismo, con carácter general, véase, CARUSO FONTÁN, M. V. "Los límites a la libertad de expresión en la Constitución y en las normas penales (especial referencia a la problemática del delito de apología en el terrorismo)". Revista Penal. Núm. 20. 2007. Págs. 32-49; MISMO AUTOR. "El delito de apología del terrorismo en la legislación penal española". Cuadernos de Doctrina y Jurisprudencia Penal. Año 11. Núm. 20-21. 2006. Págs. 399-421; CAMPO MORENO, J. C. "El enaltecimiento o justificación de los delitos terroristas o de sus autores". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 1. 2001. Págs. 1751-1755.

[455] Sobre el delito tecnológico de enaltecimiento del terrorismo, véase, STS 846/2015, 30 de diciembre (F.D. 4º), STS 95/2018, 26 de febrero (F.D. 1º) y STS 52/2018, de 31 de enero (F.D. 1º).

De esta manera, la infracción habrá de realizarse de forma pública, sin embargo, el tipo básico del apartado primero se circunscribe a la difusión de apología en un acto público ante la concurrencia de personas, mientras que el tipo agravado del apartado segundo, se refiere a las acciones cometidas en medios de comunicación de masas o en la red, por ejemplo, en redes sociales como *tuitter*, *facebook*, canal *youtube*, etc.[456]. Cabe precisar que, el presente trabajo principalmente examina el delito de enaltecimiento o justificación pública del terrorismo cometido a través de las nuevas tecnologías, si bien, ésta conducta integra también la acción del tipo básico (art. 578.1 CP), o dicho de otro modo, la diferencia entre uno y otro, únicamente estriba, en el medio tecnológico utilizado para cometer la acción, debido a lo cual, para una mejor comprensión, hemos decidido realizar su exposición de forma conjunta.

De esta forma, autores como Correcher Mira[457] critican el tipo penal de enaltecimiento al terrorismo (art. 578 CP), toda vez que, según su opinión, conculca con la protección constitucional a la libertad de expresión (art. 20 CE), de modo que, su tipificación coaccionaría la libre expresión de opiniones, así como, su castigo sería desproporcionado[458]. Sin embargo, para entrar a valorar dicha cuestión, se precisa realizar una ponderación a los límites de la libertad de expresión, de tal forma que,

[456] Acerca del "ciberterrorismo" cometido a través de redes sociales, véase, POVEDA CRIADO, M.A., TORRENTE BARREDO B. "Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista*"*. Opción: Revista de Ciencias Humanas y Sociales. Núm. Extra 8. 2016. Págs. 509-518, en el cual, el autor.

[457] Critica, CORRECHER MIRA, J. *Delito de enaltecimiento del terrorismo y humillación a las víctimas tras la reforma de la lo 2/2015 en materia de delitos de terrorismo*. Revista General de Derecho Penal. Núm. 27. 2017, el delito de analtecimiento y humillación al terrorismo por conculcar con el derecho fundamental a la libertad de expresión, así como por tener unas penas aperejadas muy elevadas.

[458] Sobre las críticas a la tipificación del delito de enaltecimiento al terrorismo, véase, RODRÍGUEZ PUERTA, M. J. "¿Dónde está el límite a la libertad de expresión? El discurso del odio y el delito de enaltecimiento del terrorismo y humillación a las víctimas STS de 18 enero 2017". Revista de Derecho y Proceso penal. Núm. 46. 2017. Págs. 311-316; GALÁN MUÑOZ, A. "¿Leyes que matan ideas frente a las ideas que matan personas? Problemas de la nueva represión de los mecanismos de captación terrorista tras la reforma del Código penal de la LO 2/2015". Revista de Derecho Penal y Criminología. Núm. 15. 2016. Págs. 95-138; GADEA ALDAVE, G. "La libertad de expresión en el marco jurídico español referente al uso de internet con fines terroristas*"*. Opción: Revista de Ciencias Humanas y Sociales. Núm. Extra 2. 2015. Págs. 333-356.

habrá de discernir cuándo lo inaceptable se convierte en delictivo, de manera que, como contrapunto a dichas afirmaciones, se encuentra el Tribunal Supremo al sostener que, nos encontraríamos ante una manifestación del discurso del odio, que incita a la violencia a través del enaltecimiento de actividades terroristas, por lo que, no quedaría amparada la conducta dentro del contenido constitucionalmente protegido del derecho a la libertad de expresión[459].

Sin entrar a valorar más en dichas polémicas, nuestros tribunales vienen afirmando que se exige como elemento subjetivo el dolo, esto es, se perfecciona el tipo con el conocimiento de los elementos que definen el delito, es decir, tener plena conciencia y voluntad de que se está difundiendo un mensaje con contenido que evoque acciones violentas terroristas, pero además, resulta superfluo en términos de tipicidad el móvil o las razones de dichos mensajes[460].

En otro orden de ideas, cuando se traten de delitos cometidos a través de las nuevas tecnologías de la información y la comunicación, el tribunal de forma accesoria, tendrá la obligación de acordar la retirada de los contenidos. Sin embargo, cuando los hechos fueran cometidos por medio de internet o de servicios de comunicaciones electrónicas, el tribunal podrá primeramente ordenar la retirada de los contenidos o servicios ilícitos, pero también subsidiariamente, cuando la medida resulte proporcionada con la gravedad de los hechos o la difusión sea exclusiva o preponderantemente de contenidos ilícitos, podrá ordenar a los prestadores de servicios de alojamiento web o *hosting* que retiren el contenido, a los motores de búsqueda como *Google*, *Bing* o *Yahoo!*, etc. que supriman los enlaces, o bien, a los proveedores de servicios de comunicaciones electrónicas como *Telefónica*, *Vodafone*, *Orange*, etc. que impidan el acceso (art. 578.4 CP), pero además, incluso pudiendo adoptar todas éstas medidas de forma cautelar por el juzgado de instrucción competente (art. 578.5 CP en relación con el art. 13 LECrim).

---

[459] STS 335/2017, 11 de mayo (F.D. 4º) dispone que la "alabanza o justificación de acciones terroristas, no merecen la cobertura de derechos fundamentales como la libertad de expresión (art. 20 CE) o la libertad ideológica (art. 16 CE), pues el terrorismo constituye la más grave vulneración de los derechos humanos de la comunidad que lo sufre*"*.

[460] STS 4/2017, 18 de enero (F.D. 2º) dispone que la conducta contenida en el art. 578 del CP sólo puede ser cometida de forma dolosa.

Por último, está previsto un agravamiento de las penas, cuando los hechos ocasionen objetivamente una alteración grave para la paz pública, creen un sentimiento grave de inseguridad o temor a la sociedad (art. 578.3 CP).

Despues de realizar está aclaración y continuando la explicación en la materia objeto de estudio, cabe mencionar que, lo habitual será que los foros sean de libre acceso, así como la información contenida se aloja en servidores de la propia plataforma, y no en los dispositivos de los usuarios, por lo que, en este caso, ninguna afectación en los derechos fundamentales se produce, cuando la Policía Judicial accede y obtiene dicha información por sus propios medios, sin embargo, como en el supuesto mencionado anteriormente, cuando los foros tengan partes cerradas, no públicas, o bien, se precise recabar los datos asociados o trafico relativos a una comunicación, en especial, localizar e identificar la dirección IP, será necesaria la intervención judicial.

De la misma manera, los *blogs* o diarios en la red, se caracterizan por su condición mixta entre una página *web* y un *log*, esto es, un registro secuencial de un archivo o base de datos, por lo que, consisten en páginas abiertas al público que se actualizan periódicamente con entradas donde los usuarios (*bloggers*) muestran sus opiniones o hacen comentarios sobre un asunto concreto. De este modo, la información se encuentra en un servidor vinculado al usuario (*blogger*), así como, la empresa prestadora del servicio es la que posee los datos del *blog*. Como en los casos estudiados anteriormente, el carácter público de estas plataformas, hace que cualquier persona pueda acceder al contenido[461], y en consecuencia, nada impediría que la Policía Judicial pueda obtener dicha información sin precisar de la intervención judicial[462]. En cambio, cuando necesiten recabar información reservada alojada en el servidor, o bien, pretendan obtener los datos electrónicos de tráfico o asociados a la comunicación, será necesario solicitar autorización judicial.

[461] VELASCO NUÑEZ E., *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 144-148.

[462] SAN 3/2018, 18 de enero (F.D. 2º); SAP de Madrid (Sección 16ª) Núm. 123/2017, 24 de febrero (F. D. 2º), en las cuales, se pone de manifiesto que, los datos públicos de los blogs no precisan de plácet judicial.

a´.5 Servicio de mensajes cortos (SMS o Short Message Service) y mensajes multimedia (MMS o Multimedia Messaging Service)

Los mensajes cortos de texto (SMS) son un servicio de telefonía móvil que permite enviar o recibir mensajes de texto, mientras que, el servicio de mensajería multimedia (MMS) hace posible también, la transmisión de contenidos multimedia, como sonido, video o fotos. Sin embargo, con la aparición de los *smartphones* o teléfonos inteligentes que permiten la instalación de aplicaciones con servicios de mensajería instantánea que hacen posible el mismo servicio, incluso con mejores prestaciones, ha ocasionado que los usuarios utilicen cada vez menos esta forma de comunicación. En cualquier caso, como se trata de un servicio de comunicación, que se encuentra activo en todos los terminales móviles, puede ser susceptible de ser utilizado para la actividad criminal, y en consecuencia, puede ser importante su intervención para la investigación de delitos. Piénsese, por ejemplo, en el *smishing*, esto es, suplantar la identidad cuando la vía del engaño se realiza a través de mensajes de texto (SMS).

Por este motivo, vamos a explicar brevemente como se intervienen las comunicaciones de los mensajes SMS y MMS, si bien, resulta muy similar que en el caso de los correos electrónicos[463], por lo que, nos remitimos a las consideraciones hechas sobre los mismos. De esta manera, cuando el interlocutor envía o recibe un SMS o MMS, el agente facultado de policía judicial duplica o monitoriza el mensaje en idénticas condiciones que el investigado, para ello, resulta necesaria la colaboración de la empresa prestadora del servicio de telecomunicaciones, para que proporcione los datos necesarios para su ejecución, para ello, habrá de recabar autorización judicial. De igual modo, cuando el proceso comunicativo se encuentre en curso, esto es, el emisor ha enviado el mensaje pero el receptor aún no lo ha leído, afecta al secreto de las comunicaciones (art. 18.3 CE), mientras que, cuando el mensaje se encuentra almacenado en el terminal, debido a que aún no se ha enviado, permaneciendo en la

[463] STS 884/2012, de 8 de noviembre (F.D. 2º) dispone que los SMS y MMS, son similares a los correos electrónicos.

bandeja de salida, o bien, recibido como leído, incide en la intimidad (art. 18.1 CE)[464], si bien, como decíamos para los correos electrónicos, a efectos prácticos y para otorgar garantías al proceso penal, independientemente de que derecho fundamental se encuentre afectado, las injerencias precisarán de autorización judicial, que además, tras la reforma procesal implementada en el 2015, vienen avalados estos argumentos, con arreglo a las disposiciones contenidas en la LECrim. (arts. 588.1 bis a, 588 bis c y 588 ter b de la LECrim.).

b´. Las grabaciones de conversaciones propias

Seguidamente vamos a examinar la jurisprudencia relacionada con el hecho de revelar ante la autoridad judicial una conversación telefónica donde participe uno mismo, aunque obtenida por uno de los interlocutores de forma subrepticia mediante alguna clase de aparato de captación de sonido. De esta manera, las personas privadas, con frecuencia, utilizan dispositivos tecnológicos con el fin de grabar conversaciones telefónicas, para después aportarla a juicio como medio probatorio de un hecho, pues, cabe preguntarse si, el material obtenido de esta forma, conculca con los derechos fundamentales al secreto de las comunicaciones (art. 18.3 CE), a la intimidad (art. 18.1 CE), o bien, a un proceso con todos las garantías y a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE), y en caso afirmativo, provocaría la nulidad de la prueba por ilicitud, y en consecuencia, se expulsaría del acervo probatorio (art. 11.1 LOPJ), todo ello, sin perjuicio de que también, se pudiera incurrir en un delito de interceptación de las telecomunicaciones o de utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido del art. 197.1 CP. Delito que, como se sabe, la acción típica consiste en interceptar las comunicaciones emitidas por cualquier medio de telecomunicación o señal telemática, como por ejemplo en el *iter* del proceso comunicativo captar correos electrónicos[465] o el texto remitido por mensajería

[464] STS 850/2014, 26 de noviembre (F.J. 9º) y SAP de Baleares (Sección 1ª) 20/2014, 18 de febrero (F.J. 2º) disponen que el derecho fundamental afectado es la intimidad, cuando el mensaje se encuentra almacenado en el terminal o en la bandeja de salida.

[465] Sobre el delito de interceptación de las comunicaciones de correos electrónicos, véase, POLAINO NAVARRETE, M. *Lecciones de derecho penal. Parte especial*… O.P. Cit. Págs. 231-254; PUENTE ABA, L. M. "Delitos contra la intimidad y nuevas tecnologías*"*. Eguzkilore: Cuaderno del Instituto Vasco

instantánea, mientras que, para imágenes o sonido, la conducta únicamente será punible cuando para ello se hayan utilizado artificios técnicos que permitan su grabación o captación, de tal forma que, escuchar detrás de la puerta o mirar a un vecino desde la ventana resulta irrelevante penalmente en tanto en cuanto no se registre mediante algún aparato técnico. De este modo, para considerar que ha existido una violación del secreto de las comunicaciones con incidencia penal, debe realizarse por un tercero ajeno a la propia comunicación, la captación del sonido o la imagen mediante la utilización de algún artificio técnico[466]. Además, la acción se consuma con la interceptación de las comunicaciones, no siendo suficiente la mera colocación de los artificios técnicos, si no han sido utilizados para dichos fines ilícitos.

Sin embargo, en relación con el secreto de las comunicaciones, nuestro Tribunal Constitucional viene manteniendo que[467], *no hay secreto de aquél a quien la comunicación se dirige, de igual modo, quien emplea durante su conversación telefónica un aparato que permita grabar lo que se está diciendo a otras personas presentes, no supone una violación del secreto de las comunicaciones. De este modo, quien graba una conversación de otros, independientemente de las implicaciones penales que pudiera conllevar, atenta al derecho del secreto de las comunicaciones, mientras quien graba una conversación con otro no viola el referido derecho*. *La norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros públicos o privados, pero ajenos a la comunicación misma.* Además, sigue afirmando que, *la imposición indiscriminada de una obligación de silencio al interlocutor es irrazonable y contradictoria*, toda vez que excedería de los *actos inherentes a la libre comunicación humana*. De igual modo, *los interlocutores en las comunicaciones telefónicas tienen el dominio de la comunicación, de forma que, por un lado, no está*

---

de Criminología. Núm. 21. 2007. Págs. 163-183; BOIX REIG, F. J. *Derecho penal. Parte especial.* Editorial Iustel. Madrid. 2016. Págs. 493-546.

[466] En relación con la captación de la imágen y sonido mediante un artificio técnico, véase, MUÑOZ MARÍN, A. "Secreto en las comunicaciones verbales*"*. CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 117. 2010. Pág. 193.

[467] STC 114/1984, de 29 de noviembre (F.J. 7º); STC 56/2003, de 24 de marzo (F.J. 3º); STC 81/1998, de 2 de abril (F.J. 2º), vienen a declarar que, las grabaciones de conversaciones realizadas por uno de los interlocutores no afectan a los derechos fundamentales.

sujeto a un deber de secreto de lo comunicado por el mero hecho de haber recibido la comunicación por uno de estos medios y, por otro, puede dar entrada en la comunicación a otras personas sin que éstas, que entran en la comunicación con el conocimiento y autorización —expresa o tácita— de uno de los interlocutores, estén tampoco violando el secreto de las comunicaciones. Cuestión distinta es la de las escuchas telefónicas realizadas sin que ninguno de los comunicantes lo conozca o lo autorice, lo que únicamente puede hacerse, sin violar el derecho fundamental mencionado, cuando media autorización judicial. De esta forma, el testigo de unos hechos puede declarar sobre lo que haya percibido por sus sentidos, de la misma manera que el receptor del mensaje puede narrar sobre el contenido del mismo, además, puede apoyar su testimonio con la grabación del sonido[468]. En el mismo sentido, el Tribunal Supremo[469] viene sosteniendo que, *el secreto de las comunicaciones se vulnera cuando un tercero no autorizado interfiere y llega a conocer el contenido de las que mantienen otras personas, no cuando uno de los comunicantes se limita a perpetuar, mediante grabación mecánica, el mensaje emitido por el otro. Aunque esta perpetuación se haya hecho de forma subrepticia y no autorizada por el emisor del mensaje y aunque éste haya sido producido en la creencia de que el receptor oculta su verdadera finalidad, no puede ser considerado el mensaje secreto e inconstitucionalmente interferido. Cosa completamente distinta es que el mensaje sea luego utilizado por el receptor de una forma no prevista ni querida por el emisor,* como por ejemplo que uno de los interlocutores incorpore la grabación al proceso penal. De lo mencionado anteriormente, debemos extraer que, de acuerdo con la jurisprudencia examinada, la incorporación al proceso penal de grabaciones con registros de conversaciones telefónicas efectuadas por uno de los interlocutores, aunque fuera de forma subrepticia y no autorizada por el otro emisor del mensaje, no vulnera el derecho constitucional al secreto de las comunicaciones[470].

[468] STS 883/1994, de 11 mayo (F.D. 3º); STS 208/2006, de 20 febrero (F.D. 1º), se dice que, el testigo habría efectuado una grabación de sonido de los hechos.

[469] STS 652/2016, 15 de julio (F.D. 8º).

[470] PERALS CALLEJA, J. *La grabación de las comunicaciones entre particulares medio de prueba en el proceso penal. La utilización de videocámaras de seguridad. (Investigación tecnológica y derechos fundamentales).* Editorial Aranzadi. Navarra. 2017. Págs. 247-284; ZOCO ZABALA, C. "La intervención

No obstante, debemos analizar cuando la conversación telefónica registrada tenga un contenido que incida en la esfera más íntima de las personas, esto es, se trate de una grabación realizada por alguno de los interlocutores, sea aportada como material probatorio a la autoridad judicial, pero el contenido afecte al derecho fundamental a la intimidad (art. 18.1 CE). De este modo, nuestros Tribunales[471] vienen sosteniendo que, las grabaciones realizadas de esta manera, tampoco vulneran el derecho constitucional a la intimidad, salvo casos excepcionales en que el contenido de la conversación afecte al núcleo íntimo de alguno de los interlocutores.

Cosa distinta es que, una conversación obtenida por los métodos descritos, sea utilizada como prueba de confesión de alguno de los intervinientes, de tal forma que, se aporte al proceso penal sin revestir las garantías que proporciona la intervención judicial, o en su caso, del Letrado de la Administración de Justicia que, con carácter previo a su declaración en el Tribunal, con la asistencia de abogado, advierten al investigado o acusado de los derechos que le asisten, y en particular, el derecho a no declarar contra sí mismo y a no confesarse culpable [arts. 118.1.h) y 520.2.b) de la LECrim. en relación con el art. 24.2 CE]. De esta manera, de acuerdo con la jurisprudencia[472] examinada, cabe distinguir dos situaciones; por un lado, cuando las grabaciones son captadas por un particular, y por otro, cuando las grabaciones son obtenidas por un agente de la autoridad, o bien, por un superior jerárquico en un entorno institucional. De este modo, cuando el registro telefónico se realiza por un particular interviniente en la comunicación, no vulnera el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE), sin embargo, se prescinde de calificar las manifestaciones realizadas por el encartado como confesión, sino que podrán ser incorporadas al proceso, pero como ratificación de las declaraciones de los demás intervinientes en la conversación, teniendo el mismo valor probatorio que el testimonio de referencia sobre las declaraciones vertidas por el encartado. Esto es así, debido a que,

---

judicial de las comunicaciones ¿privadas? regulación legal y nuevos escenarios tecnológicos*"*. Editorial Thomson Reuters Aranzadi. Navarra. 2014.

[471] STS 2190/2002, 11 de marzo (F.D. 1º); STS 178/1996, 1 de marzo (F.D. 1º); STS 2/1998, de 29 de julio (F.D. 10º).

[472] STS 517/2016, de 14 de junio (F.D. 3º) y STS 298/2013, 13 de marzo (F.D. 1º).

la confesión no reviste de las garantías mencionadas *supra*, es decir, con carácter previo, el Juez, y en su caso, por el Letrado de la Administración de Justicia, realiza la lectura de derechos, en presencia de su abogado. De esta forma, la grabación de conversaciones telefónicas realizadas por alguno de los interlocutores no puede considerarse confesión, en los términos referidos para la conformidad (arts. 655 y 787 LECrim), esto es, como forma anticipada de terminación del proceso, sino que, en todo caso, las cintas se aportarán al ramo probatorio, y serán apreciadas por el tribunal conforme los criterios generales valorativos. De esta manera, el registro de un particular de una conversación telefónica, en el cual, el otro interviniente admite haber cometido algún hecho delictivo, al igual que sucede con las manifestaciones espontáneas de un sospechoso realizadas ante la policía, y que después son negadas en la declaración oficial efectuada en sede policial o judicial, tendrán el valor de testimonio de referencia[473]. En este sentido, cabe precisar que, como mantienen nuestros Tribunales[474], el valor probatorio del testigo de referencia es disminuido, si bien, puede servir de fundamento para la condena cuando va acompañado de otras pruebas, mientras que, cuando sea la única prueba válida, no puede erigirse como suficiente para desvirtuar la presunción de inocencia. De la misma manera, se niega suplir un testimonio directo por el de mera referencia cuando ambos comparecen en juicio y declaran de forma discrepante ante el Tribunal[475]. Por este motivo, en el caso examinado, habría que dar preferencia a la declaración de los intervenientes en la conversación telefónica, que las propias cintas que registran dicha interlocución.

Por otro lado, cuando la grabación telefónica tiene por finalidad obtener una confesión extraprocesal arrancada de forma subrepticia, pero ésta, se encuentra en una posición de superioridad institucional, debido a que la ejecutan agentes de la autoridad, o bien, por superiores jerárquicos, se viene afirmando que, vulnera el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE), por lo que debe ser

[473] STS 16/2014, 30 de enero (F.D. 2º), sobre la declaración vertida ante la policía, será tenida en cuenta como testimonio de referencia.

[474] STC 68/2002, de 21 de marzo (F.J. 10º); STC 303/1993, de 25 de octubre (F.J. 7º); STS 597/2017, 24 de julio (F.D. 3º).

[475] STS 229/2016, 17 de marzo (F.D. 3º).

descartada del proceso, pues en caso contrario, incurrirían en nulidad probatoria con arreglo al art. 11.1 LOPJ[476].

Una vez analizada la incidencia en los derechos fundamentales, debemos puntualizar que, la primera premisa a tener en cuanta para considerar lícita la grabación entre particulares realizada por uno de los interlocutores es que habrá de ser un encuentro voluntario y libre. De este modo, cuando la persona ha sido grabada de forma que es conducida al encuentro utilizando argucias con la premeditada pretensión de hacerle manifestar hechos que pudieran ser utilizados en su contra, debe ser excluida del material probatorio del proceso penal. En consecuencia, será válida únicamente la grabación que sea obtenida de un encuentro libremente concertado entre ambos y que se acuda a la cita espontáneamente y sin condicionamientos de ninguna clase, pues la espontaneidad y la buena fe son requisitos condicionantes de su valoración. De igual modo, como viene afirmando nuestro Tribunal Supremo[477], quien fuerza y provoca una conversación ya no es posible situarse en el mismo plano, sino que, en cierto modo, se le arrancan o extraen de modo torticero sus manifestaciones, de tal forma que, deberá ser descartada toda práctica consistente en grabar una actividad delictiva que haya sido previamente provocada[478]. Nuestras afirmaciones pueden relacionarse con la jurisprudencia que diferencia, por un lado, el delito descubierto, esto es, el hecho delictivo que se hubiera cometido independientemente de la intervención por parte del agente en descubrir o registrar la actividad, pues pretende únicamente dar a conocer dicha situación, de aquel otro delito provocado, es decir, cuando la acción delictiva es cometida como consecuencia de la incitación realizada por quien quiere subrepticiamente captar el hecho perpetrado. Por esta razón, el registro de hechos descubiertos no trae consigo problema alguno de validez, mientras que la grabación de una actividad delictiva previamente provocada, vulnera el derecho a un proceso con todas las garantías (art. 24.2 CE), y en consecuencia, debe ser excluida del proceso penal.

[476] STS 298/2013, de 13 de marzo (F.J. 1º); STS 421/2014, de 16 de mayo (F.J. 3º).

[477] STS 311/2018, 27 de junio (F.D. 1º); STS 1066/2009, de 4 de noviembre (F.D. 4º).

[478] STS 713/1995, de 30 mayo (F.D 10º).

Por último, para garantizar la autenticidad e integridad del material, será necesario que, las partes pongan a disposición del Juzgado, las cintas íntegras y en soporte original (DVD, CD, PENDRIVE, etc.), todo ello, para evitar que se produzcan alteraciones, trucajes o montajes fraudulentos o simples confusiones, de tal forma que, el Juez pueda controlar de forma directa la validez de la fuente de prueba (art. 588 ter f. LECrim).

c´. Intervención en las comunicaciones entre familiares

Por último, es necesario abordar las soluciones que ha dado la jurisprudencia[479] en la intervención en las comunicaciones entre familiares, destacando las situaciones que se producen en el entorno o "*dimensión*" familiar, cuando existe un vínculo de parentesco. La cuestión que se suscita es si sus miembros ostenten algún privilegio o causa que pudiera justificar las eventuales injerencias en la privacidad. Como, por ejemplo, para descubrir los secretos, se utiliza algún artificio técnico de escucha, o bien, se accede a los mensajes de *whatsapp* o de correo electrónico mantenidos el familiar con un tercero. Sobre estas cuestiones, resulta necesario advertir que, todas personas son titulares de los derechos a la intimidad (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE), pues se tratan de derechos fundamentales básicos del ser humano, que tienen por objeto, proscribir las injerencias no deseadas en el ámbito de su privacidad. De hecho, como venimos estudiando, la invasión ajena en los espacios íntimos, cuya impenetrabilidad por terceros se establece "*erga omnes*", viene reservada a la intervención judicial, lo cual, deriva que no pueda dejarse dichas intromisiones al arbitrio de un particular.

Una vez realizadas estas aclaraciones, debemos distinguir las injerencias en la intimidad cuando existe una relación de parentesco, por un lado, las producidas en el vínculo conyugal o análoga relación de afectividad, y por el otro, las ocasionadas entre padres e hijos. De este modo, en lo que respecta a la relación entre cónyuges, no existe

[479] Con carácter general, sobre la dimensión del secreto de las comunicaciones y la intimidad en la relación entre familiares, y en especial, en el matrimonio y en padres a hijos menores de edad, véase, RODRÍGUEZ LAINZ, J. L. "El secreto de las comunicaciones en el Derecho de familia (control parental y valor probatorio de comunicaciones entre integrantes de un núcleo familiar)*"*. Revista de Derecho de Familia: Doctrina, Jurisprudencia, Legislación. Núm. 65. 2014. Págs. 25-52; RODRÍGUEZ LAINZ, J. L. "Sobre la dimensión privada y familiar del derecho al secreto de las comunicaciones*"*. Diario La Ley. Núm. 7598. 2011.

justificación alguna en que dentro del entorno o "*dimensión*" familiar[480], puedan realizar injerencias en la intimidad o el secreto de las comunicaciones, por el mero hecho de haber contraído matrimonio. Todavía más si cabe, la esfera privada de los cónyuges se acentúa, cuando se encuentran en plena crisis matrimonial, esto es, cuando van a iniciar los trámites de la separación o divorcio, o bien, se encuentran inmersos en un proceso de familia. Esto también es predicable, para las personas unidas en relación de análoga afectividad al matrimonio (unión de hecho o convivencia *more uxorio*). De esta forma, un cónyuge o persona con análoga relación de afectividad, no podrá realizar injerencias en las comunicaciones de su consorte, como por ejemplo, para descubrir infidelidades de su pareja, colocar subrepticiamente aparatos de interceptación y grabación de las conversaciones telefónicas o acceder a un sistema informático vulnerando las medidas de seguridad establecidas para impedirlo. Pues bien, en el hipotético caso que el cónyuge realizara injerencias en las comunicaciones o en la intimidad en la forma descrita, aunque ésta se produzca dentro del ámbito familiar, la conducta podrá ser subsumible en el delito de descubrimiento y revelación de secretos (arts. 197 y siguientes CP). No obstante, cuando los datos obtenidos por los cónyuges, violentando los derechos fundamentales, tuvieren por objeto, su incorporación a procesos judiciales, por ejemplo, en un procedimiento de divorcio, medidas paterno filiales, de violencia de género, etc. además, de incurrir en las responsabilidades penales aludidas *supra*, dichos registros o grabaciones deberán ser excluidas del acervo probatorio, por su ilicitud, con arreglo al art. 11.1 LOPJ.

Por otro lado, en lo concerniente a la relación entre padres e hijos, cabe mencionar que, los menores también son titulares de los derechos a la intimidad y al secreto de las comunicaciones (art. 4.1 de la Ley de Protección del Menor 1/1996[481]). De igual modo, los padres o tutores tienen la obligación de respetar estos derechos, y además, deberán de proteger a sus hijos frente a posibles ataques de terceros (art. 4.5 de la Ley de Protección del Menor 1/1996). Sin embargo, los progenitores y tutores son responsables civilmente de los daños y perjuicios causados por sus descendientes menores, según se

[480] Acerca de la *"dimensión familiar"*, véase, STS 694/2003, de 20 de junio (F.D. 5º) y STS, de 14 de mayo de 2001 (F.D. 2º).

[481] «BOE» Núm. 15, de 17 de enero de 1996.

desprende de las normas de derecho privado (art. 1903 CC párrafo II[482]), así como, de la Ley de Responsabilidad Penal del Menor que regula la responsabilidad solidaria de éstos, frente a las infracciones cometidas por sus hijos (art. 61.3 L.O. 5/2000[483]). En otro orden de ideas, como nos hemos referido en alguna ocasión en este trabajo, el secreto de las comunicaciones rige mientras se encuentra en curso el proceso de comunicación[484], una vez cesado éste, llegado el mensaje al receptor, la afectación podría recaer en la intimidad. Esta distinción es importante a los efectos de determinar el tratamiento constitucional aplicable, pues cuando se produce una afectación en la intimidad, no se supedita expresamente su injerencia a la intervención judicial[485].

En consecuencia, podemos extraer que, las intromisiones en el proceso comunicativo en curso afectan a la inviolabilidad de las comunicaciones, y aunque se trate de los padres respecto de sus hijos, cualquier injerencia requerirá de plácet judicial, pues en caso contrario, tiene su reflejo sancionador en el delito de descubrimiento y revelación de secretos (art. 197.1 CP). En el caso de que el acceso de los progenitores se produzca cuando el mensaje ha sido recibido y leído por el menor (por ejemplo, acceder al contenido de los mensajes *whatsapp*, correo electrónico, redes sociales, etc.), dicha situación incide en la intimidad del menor (art. 18.1 CE), y como venimos afirmando, para determinados supuestos, su intromisión no precisa de la intervención judicial. De esta manera, los progenitores son los titulares de la patria potestad concebida como función tuitiva respecto de sus menores, por lo que, el ordenamiento hace descansar en los padres las obligaciones de velar por sus hijos menores, debido a lo cual, el Estado no puede desposeerles de toda capacidad de control en casos de gravedad[486]. Por este

[482] «Gaceta de Madrid» Núm. 206, de 25 de julio de 1889.

[483] «BOE» Núm. 11, de 13 de enero de 2000.

[484] STS 342/2013, 17.3… O.P. Cit, STS 786/2015, 4.12… O.P. Cit, STS 859/2014, 26.11… O.P. Cit, se examinan la incidencia de los derechos fundamentales en un proceso comunicativo, a los efectos de determinar la intervención judicial.

[485] STS 777/2013, de 7 de octubre (F.D. 4º) dispone que "la intimidad no comporta automáticamente previa habilitación judicial inexcusable".

[486] STS 864/2015, 10 de diciembre (F.DD. 3º, 4º y 5º), la cual, ha sido ampliamente comentada en el cuerpo del presente trabajo, si bien, basta decir que, la resolución alude a que los menores de edad son

motivo, se debe ponderar el conflicto entre el derecho a la intimidad de los menores y la actuación de los progenitores en el ejercicio de la guarda y su deber de protección, y en su caso, resolver a favor de éste para casos justificados, como por ejemplo cuando el menor es víctima de delitos, pueda haber cometido él mismo algún ilícito penal que pueda dar origen a la responsabilidad civil solidaria de los padres (art. 61.3 L.O. 5/2000), o bien, el menor no tenga madurez suficiente para prestar por sí solo el consentimiento exigido en el código penal en las injerencias en su intimidad[487]. Cosa distinta es que, los hijos sean mayores de edad, salvo que se prorrogue por la declaración de incapacidad de los mismos (art. 171 CC), de esta forma, los padres pierden la obligación de velar por sus hijos, por lo que, será de aplicación lo mencionado anteriormente sobre los cónyuges, esto es, no podrán realizar injerencia alguna en la intimidad, pues en caso contrario, podrían incurrir en el delito de descubrimiento y revelación de secretos (art. 197 y siguientes del CP).

2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

La medida que va a ser objeto de análisis es las escuchas o filmación ambientales instrumentalizadas a través de la colocación de dispositivos técnicos en espacios públicos o privados, para captar mediante micrófonos conversaciones orales, o bien, grabar y filmar imágenes con cámaras de vídeo, todo ello, sin el conocimiento de los investigados. De esta manera, la diferencia principal con la medida estudiada

---

titulares de los derechos fundamentales a la intimidad y el secreto de las comunicaciones, sin embargo, en un proceso comunicativo, cabe diferenciar los mensajes que se encuentran en curso, en este caso, afecta al secreto de las comunicaciones, y toda injerencia debe realizarse con autorización de judicial, de aquellos otros mensajes que, han sido recibidos y guardados en el dispositivo, en este caso, se vería afectado la intimidad. En este último supuesto, se permite a los padres respecto de sus menores realizar intromisiones cuando sean por motivos justificados.

[487] La STS 864/2015 que ha sido mencionada *supra*, así como la Sentencia del Juzgado de lo Penal N°. 1 de Pamplona, Núm. 145/2017, de 29 mayo (F.D. 2º), viene a absolver a la madre que había instalado en el teléfono móvil de su hija un sistema de grabación, pues no tenía madurez suficiente para prestar por sí sola el consentimiento exigido por el código penal, resultando necesario que fuera completado por quienes ejercían su patria potestad, y en concreto, por su madre, titular de la patria potestad y de la guarda y custodia de la misma.

anteriormente de interceptación de las comunicaciones (art. 588 ter LECrim.), radica en que el sonido, o en su caso, las imágenes se obtienen de forma directa, esto es, sin que medie aparato de telecomunicaciones entre los interlocutores. Por su parte, la diligencia de captación y grabación de comunicaciones orales (art. 588 quater a hasta la e LECrim.) fue creada con arreglo a la reforma procesal penal implementada con la L.O. 13/2015. Aunque el ordenamiento jurídico procesal no regulaba esta medida, lo cierto es que, antes de la reforma del 2015, nuestros tribunales, con frecuencia, venían acordándola, pues aplicaban por extensión, la normativa reguladora sobre la interceptación de las comunicaciones (antiguo art. 579.2 LECrim)[488]. De hecho, el Tribunal Constitucional[489] y el Tribunal Europeo de Derechos Humanos[490] habían puesto de manifiesto en reiteradas ocasiones que, las medidas restrictivas de derechos fundamentales debían de indicar con suficiente claridad la extensión y las modalidades del ejercicio del poder de apreciación de las autoridades. Sin embargo, estas insuficiencias habían sido paliadas en gran parte por la jurisprudencia de los tribunales[491]. Como ya nos hemos referido en este trabajo, el Tribunal Constitucional acordaría en la sentencia 145/2014[492] que, la regulación existente hasta la fecha, se trataba únicamente de *intervenciones telefónicas, no a escuchas de otra naturaleza*, por lo que, no suponía un *defecto por insuficiencia de la ley, sino* que existía una *ausencia total y completa de ley*. Por este motivo, el Estado español no tuvo más remedio que modificar nuestra ley procesal para incluir otras medidas (art. único.15 L.O. 13/2015),

[488] Pone de manifiesto, ARAGONÉS SEIJO, S. "La ausencia de previsión legal para las escuchas en vehículos*"*. Diario La Ley. Núm. 8.570. 2015, la ausencia legal en la regulación de las medidas restrictivas de derechos fundamentales, con anterioridad a la reforma procesal implementada con arreglo a la L.O. 13/2015.

[489] STC 49/1999, de 5 de abril (F.J. 5º); STC 184/2003, de 23 de octubre (F.D. 6º) y la STC 26/2006, de 30 de enero (F.D. 5º).

[490] STEDDHH 842/1997, de 30 julio 1998 (asunto Valenzuela Contreras) y STEDDHH de 18 febrero 2003 (asunto Prado Bugallo contra España).

[491] STS 34/2003, de 22 de enero (F.D. 1º).

[492] STC Núm. 145/2014… O.P. Cit. (F.J. 7º).

como las escuchas o filmaciones ambientales[493] que, seguidamente será objeto de estudio. De esta forma, vamos a exponer la medida de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos regulada en nuestra norma procesal penal (art. 588 quater a hasta la e LECrim.), y en concreto, examinaremos los derechos fundamentales afectados con la diligencia, el contenido de la grabación de las comunicaciones orales directas, los presupuestos, la resolución judicial, el control, el cese y destrucción de los archivos. Por último, analizaremos algunas particularidades observadas en la jurisprudencia y/o doctrina.

a) Los derechos fundamentales afectados con la diligencia

Las escuchas o grabaciones ambientales son, sin duda, una de las medidas tecnológicas más invasivas reguladas en la LECrim, pues consiste en la obtención de sonido o imágenes, incluso en el domicilio, esto es, el lugar donde las personas desarrollan su vida íntima. Por este motivo, los derechos fundamentales afectados pueden ser el secreto de las comunicaciones (art. 18.3 CE), cuando se pretende obtener el sonido en una conversación mantenida, la intimidad personal y familiar (art. 18.1 CE), cuando se obtienen imágenes, pero también, la inviolabilidad domiciliaria (art. 18.2 CE), cuando fuera necesaria la entrada en el domicilio para la colocación del dispositivo técnico. Sin embargo, el alcance de la injerencia de la medida es graduable, es decir, no es lo mismo

[493] Con carácter general, en relación a la STC 145/2014, véase, OTAMENDI ZOZAYA, F. *Antecedentes y origen de la reforma A) La sentencia del Tribunal Constitucional 145/2014 (Las últimas reformas de la ley de enjuiciamiento criminal. Una visión práctica tras un año de vigencia)*… O.P. Cit. Pág. 95-148; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Pág. 194-198; LÓPEZ-BARAJAS PEREA, I. y LOZANO EIROA, M. "STC 145/2014, de 22 de septiembre de 2014, Vulneración del derecho al secreto de las comunicaciones: grabación sin garantías de conversaciones verbales mantenidas en dependencias policiales…" O.P. Cit. 5; NISTAL BURÓN, J. "La intervención de las comunicaciones verbales de los detenidos en dependencias policiales (A propósito de la Sentencia 145/2014, de 22 septiembre, de la Sala segunda del Tribunal Constitucional, dictada en el recurso de amparo número 6157-2010)…" O.P. Cit. Págs. 139-153; GONZÁLEZ MONJE, A. *Sentencia del Tribunal Constitucional (Sala Segunda), 145/2014, de 22 de septiembre (BOE núm. 261, de 28-X-2014) Intervención de comunicaciones en dependencias policiales*… O.P. Cit. Págs. 355-357; RODRÍGUEZ LAINZ, J. L. "Sobre la inconstitucionalidad de las vigilancias policiales mediante micrófonos ocultos (A propósito de la STC 145/2014, de 22 de septiembre)". Diario La Ley. Núm. 8438. 10 de diciembre de 2014… O.P. Cit.

el registro del sonidos, que además sean complementados con la obtención de imágenes, incluso en el domicilio del investigado, para lo cual, como veremos posteriormente, la autorización judicial deberá determinar el grado de afectación en la privacidad del investigado, por lo que, cuando fuera necesario acordar la injerencia en su máximo nivel, habrá que motivar suficientemente la decisión (art. 588 quater c. LECrim.).

b) El contenido de la grabación de las comunicaciones orales directas

La medida consiste en la posibilidad de acordar la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales en la vía pública, en otro espacio abierto, en el propio domicilio, o bien, en otro espacio cerrado, pero también, podrán ser complementadas con la obtención de imágenes (art. 588.1 quater a. LECrim.)[494]. De esta manera, cuando fuera necesario acceder a un domicilio o un espacio destinado al ejercicio de la privacidad, para la colocación del dispositivo técnico, habrá de contener la resolución judicial las razones de la procedencia de entrar en dichos lugares (art. 588.2 quater a. LECrim.), esto es así, debido a que el derecho fundamental afectado es la inviolabilidad domiciliaria (art. 18.2

[494] En relación a la medida de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, véase, ORDUNA NAVARRO, B. "Intervención de las comunicaciones orales mediante dispositivos electrónicos. Alcance de la reforma de la LECrim. LO 13/15, de 5 de octubre*"*. Diario La Ley. Núm. 9191. 2018; GOMEZ COLOMER, J. L. *Los actos de investigación garantizados (II): Modernos medios tecnológicos de investigación. Derecho jurisdiccional III: Proceso Penal*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 239-268; VELASCO NUÑEZ, E. *Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. (Investigación Tecnológica y Derechos Fundamentales. Comentarios a las modificaciones introducidas por la Ley 13/2015)*. Editorial Aranzadi. Navarra. 2017. Págs. 225 – 245; CEDEÑO HERNÁN, M. *Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos. (Nuevas tecnologías y derechos fundamentales en el proceso)*. Editorial Thomson Reuters Aranzadi. Navarra. 2017. Págs. 49-84; GOMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Los poderes del Estado. La organización territorial del estado. Volumen II)*. Editorial Tirant lo Blanch. Valencia. 2016. Págs. 239-268; CASANOVA MARTÍ, R. "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos*"*. Diario La Ley. Núm. 8674. 2016; VELASCO NÚÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal...* O.P. Cit. Págs. 110-114; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 336-355.

CE), y para su injerencia se precisa de autorización. No obstante, la entrada domiciliaria o en otro ámbito privado se realiza de forma instrumental, esto es, el acceso se produce como medio para la colocación de dispositivos, y no para realizar un registro, de manera que, la propia autorización judicial que acuerde la medida de escuchas ambientales, podrá contener las razones que justifican la instalación de los dispositivos. Por su parte, la escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes (art. 588.3 quater a. LECrim.), de tal forma que, habrá de inferir que, la utilización de cámaras ocultas viene subordinada a la captación del sonido, o dicho de otro modo, se permite la captación de sonido sin imágenes (colocación de micrófonos), pero en cambio, no se admite la grabación de imágenes sin el registro de audio (cámara oculta sin micrófono). De igual modo, se podrá autorizar las escuchas y filmación, o bien, únicamente la grabación de imágenes, en espacios públicos, la diferencia entre una y otra, será objeto de estudio más adelante. Sin embargo, el criterio de la Fiscalía[495] es que se puede autorizar la captación y grabación en lugares cerrados de imágenes sin sonido, toda vez que, vienen manteniendo que, el sonido supone una intromisión menor en los derechos del investigado, si bien, bajo nuestro punto de vista, dicho criterio es contrario a la ley, puesto que, el precepto no deja dudas de interpretación cuando dice que, las escuchas y grabación se podrá complementar con la obtención de imágenes.

Por otro lado, conforme las disposiciones generales aplicables a todas las medidas, la cual, viene a establecer que, la Policía Judicial se hará cargo de la intervención [arts. 588.2.5º bis b y 588.3.d) bis c. LECrim.], ello supone que habrá que interpretar que, la captación y registro con los dispositivos técnicos recae en la Policía Judicial, y en consecuencia, preferiblemente se deberá descartar su utilización por investigadores privados, como detectives o particulares, salvo que esté justificado para la investigación, como por ejemplo, colaboradores, confidentes de la policía o víctimas, si bien, su ejecución deberá estar bajo control judicial (piénsese en los confidentes o colaboradores de la policía que esconden micrófonos entre sus ropas, o bien, tienen por finalidad la colocación del dispositivo en un espacio privado, pues tienen acceso al mismo, todo ello

[495] Circular 3/2019, de 6 de marzo, de la Fiscal General del Estado, *sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos* (BOE Núm. 70 de 22 de marzo de 2019).

con el objeto de captar un encuentro[496]), salvo las excepciones comprendidas en la jurisprudencia sobre las grabaciones sonoras realizadas por particulares, o cámaras ocultas, cuando uno de los interlocutores sea el que registra la conversación, pues dichas cuestiones, serán objeto de análisis en el presente trabajo posteriormente.

c) Los presupuestos

La validez de la medida dependerá de la concurrencia de una serie de presupuestos legales[497], y en concreto que, la utilización del dispositivo técnico para la captación y grabación de sonido, o en su caso, la obtención de imágenes, habrá de estar vinculada a comunicaciones que puedan tener lugar en uno o varios encuentros concretos, para lo cual, habrá de atender a los indicios puestos de manifiesto por la investigación sobre cuya previsibilidad haga presumir que el investigado vaya a acudir al encuentro (art. 588.1 quater b. LECrim.)[498]. De lo mencionado anteriormente, puesto que la norma procesal no especifica plazo máximo alguno de duración y no debe interpretarse que es ilimitada[499], se deduce que, la medida está pensada para obtener la información de uno o varios encuentros puntuales, finalizado el mismo, procederá su cese (art. 588 quater e. LECrim.). De esta manera, podría ser necesario captar varios encuentros en fechas distintas, como por ejemplo cuando pueda preverse distintas reuniones de forma periódica, en este caso, colocar y retirar micrófonos o cámaras ocultas en cada

[496] STS 404/2018, de 13 de septiembre (F.D. 2º) y STS 309/2010, de 31 de marzo (F.D. 2º).

[497] Sobre los presupuestos legales para acordar una medida de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, véase, GOMEZ COLOMER, J. L. *Los actos de investigación garantizados (II)*… O.P. Cit. Págs. 239-268; VELASCO NÚÑEZ, E. *Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos*… O.P. Cit. Págs. 225 – 245; CEDEÑO HERNÁN, M. *Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos*… O.P. Cit. Págs. 49-84; BUENO DE MATA, F. *Comentarios críticos y reflexiones acerca de las últimas reformas procesales en materia de investigación tecnológica*… O.P. Cit. Págs. 549 – 572.

[498] Auto de la AP de Sevilla (Sección 1ª) 941/2016, 9 de noviembre (F.J. 1º).

[499] Pone de manifiesto, NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*... O.P. Cit. Págs. 902-909, que, la medida de escuchas ambientales no tiene una duración ilimitada, sino que, por su propia naturaleza, está pensada para encuentros concretos.

encuentro, podrá resultar difícil para la operatividad de la investigación, pero además, acceder en diversas ocasiones a espacios privados podría originar más riesgo de ser descubiertos. Por este motivo, el término "*colocar*" que alude el precepto legal (art. 588.1 quater a. LECrim.), podría considerarse sinónimo de "*activar*", de manera que, una vez colocados los dispositivos, se permite su activación cuando tenga lugar el encuentro, y una vez finalizado el mismo, se podrán desactivar hasta el próximo, pudiendo realizar este procedimiento tantas veces como fuera necesario, si bien, cada encuentro será necesaria la intervención judicial para la adopción de la activación, pues en caso contrario, la prueba obtenida podría ser declarada ilícita por violación de derechos fundamentales (art. 11.1 LOPJ), sin perjuicio que también, el agente de Policía Judicial encargado de su ejecución pudiera incurrir en un delito especial impropio de utilización de artificios técnicos de escuchas cometido por funcionario público (art. 536 CP)[500]. Como se sabe, para este delito, el sujeto activo solamente puede ser autoridad o funcionario público que intervenga en la investigación de causa por delito. De esta manera, la conducta consiste en interceptar las telecomunicaciones o captar la imagen y/o el sonido mediante la utilización de artificios técnicos, violentando las garantías constitucionales del secreto de las comunicaciones (art. 18.3 CE), o bien, legales (art. 588 bis y siguientes LECrim.), de tal forma que, carezca o sea incompleta la resolución judicial habilitante, pudiendo incluso agravarse las penas cuando exista divulgación o revelación de la información obtenida. De igual modo, cuando las interceptaciones en las comunicaciones sean cometidan por los mismos sujetos, prevaliéndose de su cargo, pero sin mediar causa por delito, se castigará con la misma pena prevista para el tipo básico (art. 197.1 CP) en su mitad superior y con inhabilitación para ejercer su cargo (art. 198 CP)[501].

Además, se establecen otros presupuestos para acordar la medida, en particular, cuando los hechos que estén siendo investigados sean constitutivos de alguno de los siguientes delitos: *dolosos castigados con pena con límite máximo de, al menos, tres años de*

[500] Sobre la tipicidad del art. 536 CP, véase, STS 250/2017, 5 de abril (F.D. 4º), STS 694/2008, 6 de octubre (F.D. 1º) STS 79/2012, de 9 de febrero (F.D. 10º) SAP de Guipúzcoa (Sección 1ª) 38/2000, 17 de febrero: (F.D. 5º).

[501] Sobre la tipicidad del art. 198 CP, véase, STS 509/2016, 10 de junio (F.D. 1º), STS 534/2015, 23 de septiembre (F.D. 1º), STS 525/2014, 17 de junio (F.D. 4º) y STS 1189/2010, 30 de diciembre (F.D. 4º).

prisión, cometidos en el seno de un grupo u organización criminal y delitos de terrorismo (art. 588.2.a. quater a. LECrim.). De esta manera, como se puede observar, coinciden prácticamente los mismos hechos delictivos que para acordar la diligencia de interceptación de las comunicaciones telefónicas y telemáticas, a excepción de los *cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación* (art. 588 ter a) y 579.1 LECrim.). Por tanto, la diferencia entre la captación de una conversación realizada a través de un sistema de telecomunicaciones, como el teléfono o el ordenador, de otra, realizada en abierto, esto es, escuchas ambientales, estriba en que ésta última, no puede ser autorizada para la investigación de delitos informáticos o tecnológicos. Esto tiene su justificación en que la diligencia de captación y grabación de comunicaciones orales está pensada para la investigación de delitos tradicionales y graves. Finalmente, la norma procesal prevé como último presupuesto que la autoridad judicial haga un juicio de ponderación sobre la utilización de los dispositivos técnicos, para ello, deberá determinar cuándo racionalmente la colocación de los mismos supone aportar datos esenciales de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor (art. 588.2.b) quater a. LECrim.).

d) La resolución judicial

La resolución judicial que acuerde la medida deberá contener, además de las exigencias establecidas en las disposiciones generales aplicables a todas las diligencias tecnológicas, que han sido estudiada *supra* (art. 588 bis c LECrim.), una mención concreta al lugar o dependencias, así como a los encuentros del investigado que van a ser sometidos a vigilancia (art. 588 quater c LECrim.). De esta manera, el Juez deberá justificar las razones que le llevan a adoptar la medida, para ello deberá realizar un juicio de ponderación sobre el sacrificio de los derechos fundamentales, debiendo además, efectuar una "motivación reforzada"[502], cuando se lleve a cabo en un lugar cerrado o en el domicilio. Sin embargo, aunque la norma procesal alude a que se deberá

[502] Afirma ALISTE SANTOS, T. J. "Algunos supuestos controvertidos en la motivación de resoluciones judiciales*"*. Diario La Ley. Núm. 7540. 2011, que, la motivación reforzada de las resoluciones judiciales estará dedicada para determinados supuestos que exista una mayor injerencia en los derechos fundamentales. En el mismo sentido, traemos a colación la STC 81/2014, de 28 de mayo (F. J. 3º) y la STC 97/2010, de 15 de noviembre (F. J. 2º).

especificar la ubicación espacial (*lugar o dependencias*), lo cierto es que, nada impediría que el dispositivo pueda ser portado por una persona a lo largo de un trayecto determinado (por ejemplo un agente encubierto, testigo, víctima, confidente o colaborador policial llevan un micrófono en un vehículo[503]), si bien, la exigencia legal hace referencia a que habrá que especificar el lugar, la ubicación y el contexto temporal, así como, determinar el/los encuentro/s sometidos a vigilancia, con el fin de controlar la medida y para que no pueda ser suplantada por otra realizada en fecha distinta.

e) El control de la medida

Al Juez de instrucción le incumbe examinar los presupuestos para la concesión de la medida, pero también le compete el control de las circunstancias de su ejecución (art. 588 bis g. LECrim.), para lo cual, la Policía Judicial pondrá a su disposición el soporte original o copia electrónica auténtica de las grabaciones e imágenes, pero además deberá ir acompañado de una transcripción de las conversaciones que considere de interés, debiéndose excluir la captación de conversaciones o imágenes que no tengan relación con el investigado, o bien, afecten a la esfera más íntima del mismo. De igual manera, a los efectos de control judicial, se exige que en el informe de la Policía Judicial se haga constar la identificación de los agentes que hayan participado en la ejecución y seguimiento de la medida, pero también, se pretende con ello, que puedan ser citados posteriormente en calidad de testigos, para prestar declaración sobre el resultado de la misma (art. 588 quater d. LECrim.)[504].

[503] Sobre la pertinencia de la adopción de la medida consistente en instalar en un vehículo un sistema de grabación de sonido, véase, Auto TSJ de Madrid 51/2018, 28 de junio (F.D. 7º), Auto AP de Barcelona (Sección 9ª) 370/2018, 3 de mayo y Auto AP Sevilla (Sección 1ª) 941/2016… O.P. Cit. (F.J. 1º).

[504] Ponen de manifiesto, VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Pág. 114, MISMO AUTOR "*Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.la prueba tecnológica"*. Diario La Ley. Núm. 8183. 2013 y MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015…* O.P. Cit. Pág. 352-353, que, el informe de la Policía Judicial deberá hacer constar la identificación de los agentes que hayan participado en la ejecución y seguimiento de la medida, si bien, con arreglo al art. 436 LECrim, cuando el testigo fuera miembro de las Fuerzas y Cuerpos de Seguridad en el ejercicio de sus funciones, será suficiente para su identificación el número de su registro personal (TIP) y la unidad administrativa a la que estuviere adscrito.

f) El cese de la diligencia y destrucción de los archivos

Debido a que la medida de escuchas y filmaciones ambientales no establece entre sus disposiciones un plazo de duración máximo, en aplicación de las disposiciones generales a todas las diligencias tecnológicas (art. 588 bis j. LECrim.), habrá que entender que, el cese de la medida se producirá cuando finalicen los encuentros previstos, o bien, resulte evidente que el encuentro no se va a celebrar. Además, como el objeto de la medida es registrar encuentros puntales, se exige nueva autorización judicial para la grabación de conversaciones o la captación de imágenes que puedan tener lugar en otros encuentros (art. 588 quater e. LECrim).

Por último, será igualmente de aplicación las disposiciones comunes que regulan la destrucción de los archivos de imagen o sonido (art. 588 bis k. LECrim.), de forma que, nos remitimos a la parte del presente trabajo que lo desarrolla, si bien, basta mencionar que, se ordenará el borrado y eliminación de los registros originales cuando termine el procedimiento mediante resolución firme, conservando una copia bajo custodia del Letrado de la Administración de Justicia, y en todo caso, se acordará la destrucción de las copias conservadas cuando hayan transcurrido cinco años desde la ejecución o prescripción de la pena, el sobreseimiento libre, o bien, la sentencia absolutoria firme, salvo que fuera necesario su conservación durante más tiempo a juicio del Tribunal.

g) Algunas particularidades observadas en la jurisprudencia y/o doctrina

Seguidamente vamos a examinar brevemente algunas particularidades observadas en la jurisprudencia y/o doctrina, sobre las escuchas y filmaciones ambientales, en concreto, los hallazgos casuales, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos entre particulares y la cámara oculta.

a´. El hallazgo casual.

El hallazgo casual de delitos ha sido estudiado anteriormente en el epígrafe dedicado a la interceptación de las comunicaciones, por lo que, nos remitimos al examen realizado sobre dicha cuestión. Por ello, nos centraremos en analizar los hechos delictivos descubiertos por casualidad en la ejecución de una medida de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, y en particular, el problema práctico que se plantea cuando se descubre otro delito no

comprendido en los presupuestos legales para su adopción (art. 588.2.a. quater a. LECrim.), esto es, cuando el nuevo delito hallado se sanciona con menor pena (*dolosos castigados con pena con límite máximo de, al menos, tres años de prisión)* o bien, de diferente materia (*en el seno de un grupo u organización criminal y delitos de terrorismo*). Será más frecuente que esta situación suceda en esta medida, pues los presupuestos legales para su adopción, como hemos visto anteriormente, son más restringidos que para otras diligencias de investigación contempladas en la LECrim. En este contexto, la solución que ha dado la jurisprudencia[505] para la situación descrita es que, *cuando los hechos descubiertos tengan conexión (art. 17 LECrim.) con los que son objeto de investigación, los hallazgos surtirán plenos efectos, mientras que, cuando los hallazgos causales no guardasen esa conexión con los causantes de la medida, si bien, aparentan una gravedad penal suficiente como para tolerar proporcionalmente su adopción, se estimarán como mera "notitia criminis" y se deducirá testimonio para que, siguiendo las normas de competencia territorial y en su caso las de reparto, se incoe el correspondiente proceso penal*. De este modo, podemos extraer las siguientes conclusiones: Así, cuando el delito descubierto casualmente sea conexo, no existirá violación al principio de especialidad, y en consecuencia, la autorización judicial inicial será suficiente para continuar con la investigación en el propio procedimiento incoado; en cambio, cuando la naturaleza del delito hallado, no tenga conexividad alguna con los hechos causantes de la habilitación judicial, habrá que atender al criterio de la gravedad del hecho para determinar que la medida acordada es proporcional, y en caso de que sea suficientemente gravosa, se estimará como revelación de la comisión de un hecho delictivo, para lo cual, habrá que deducir testimonio para iniciar un nuevo proceso ante el juzgado que corresponda. En consecuencia, cuando el delito descubierto no tenga conexividad, así como, tras realizar un juicio de proporcionalidad se determine que el hecho hallado es de poca entidad o gravedad, la medida restrictiva de derechos fundamentales no estará sujeta a los principios de especialidad ni proporcionalidad. Por tanto, la información obtenida sobre la nueva infracción no podrá ser utilizada en la propia causa, ni tampoco será motivo para incoar un nuevo procedimiento, lo cual, en nuestra opinión, viene a ser una garantía para los investigados.

[505] STS 372/2010, de 29 de abril (F.D. 7º) y STS 25/2008, de 29 de enero (F.D. 6º).

b´. La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos entre particulares.

Se trata de analizar la validez de las grabaciones ambientales realizadas subrepticiamente por un particular, con el objeto de su incorporación al proceso penal como prueba de la comisión de un hecho delictivo, si bien, advertir que, resulta de aplicación lo referido *supra* sobre las grabaciones de conversaciones propias dentro del epígrafe que desarrolla las intervenciones en las comunicaciones telefónicas y telemáticas, por lo que nos remitimos a lo mencionado sobre dicha cuestión. No obstante, basta recordar que, las grabaciones realizadas por uno de los interlocutores de la conversación, no vulnera el secreto de las comunicaciones (art. 18.3 CE), pues como pone de manifiesto nuestro Tribunal Supremo[506], *se debe distinguir entre grabar una conversación de otros y grabar una conversación con otros, de tal forma que, el secreto de las comunicaciones se vulnera cuando un tercero no autorizado interfiere y llega a conocer el contenido de las que mantienen otras personas, no cuando uno de los comunicantes se limita a perpetuar, mediante grabación, el mensaje emitido por el otro, aunque esta perpetuación se haya hecho de forma subrepticia y no autorizada por el emisor del mensaje y aunque éste haya sido producido en la creencia de que el receptor oculta su verdadera finalidad. Además, el secreto pierde su condición de tal, cuando ha sido exteriorizado por quien lo emite, de igual modo, no puede hablarse de interferido, porque lo ha recibido la persona a la que materialmente ha sido dirigido y no por un tercero que se haya interpuesto*. Tampoco cabe interpretar que exista, con carácter general, vulneración a la intimidad[507], cuando participa en el material grabado uno mismo, esto supone que, cuando el registro del sonido o imágenes sea especialmente

[506] La STS 45/2014, de 7 de febrero (F.D. 2º) y STS 1051/2009, 28 de octubre (F.D. 2º), vienen a distinguir entre grabar una conversación de otros y grabar una conversación con otros.

[507] Sobre la intervención de las comunicaciones telefónicas propias y sus implicaciones penales, véase, GUTIÉRREZ SANZ, M. R. "Denuncia sobre vulneración del derecho a la intimidad personal y a la propia imagen al utilizar grabación de imagen y voz del acusado sin autorización judicial previa (TS 2ª S 977/1999, de 17 junio)". Tribunales de Justicia: Revista Española de Derecho Procesal. Núm. 5. 2000. Págs. 637-641. Sin embargo, en la línea que venimos afirmando, la grabación realizada por un particular no vulnera la intimidad ni ningún otro derecho fundamental, por lo que, no procede sancionar la conducta como delito, salvo que fuera especialmente atentatorio a la intimidad.

atentatorio contra la intimidad del otro (ideología, religión, creencias, salud, origen racial o vida sexual), en este caso, se podría incurrir en responsabilidad penal por delito de descubrimiento y revelación de secretos (art. 197 CP).

Como decíamos anteriormente, el presupuesto para determinar la validez de las *grabaciones de conversaciones privadas entre dos personas realizadas por una de ellas sin conocimiento ni consentimiento de la otra parte* dependerá que el encuentro sea *voluntario y libre*, de modo que, *la espontaneidad y la buena fe son requisitos condicionantes de su valoración, porque cuando se fuerza y provoca una conversación ya no es posible situarla en el mismo plano*[508].

Por otro parte, como exponíamos al analizar esta cuestión, el particular que pretenda incorporar la grabación al proceso penal, deberá poner a disposición del tribunal el material, para lo cual, será necesario aportar las cintas íntegras y en soporte original (DVD, CD, PENDRIVE, etc.), todo ello para que el Juez pueda garantizar la integridad y la autenticidad del mismo[509].

c´. La cámara oculta

Estrechamente relacionado con la medida de grabación y obtención de imágenes que venimos estudiando, tenemos el uso de las cámaras ocultas, de este modo, se trata de analizar esta técnica desde la jurisprudencia, cuando se realiza por el periodismo para

[508] Sobre la licitud si el encuentro es voluntario y libre, véase, STS 652/2016, 15 de julio (F.D. 8º), STS 311/2018, 27 de junio (F.D. 1º) y STS 1066/2009. O.P. Cit.

[509] SAP de Madrid (Sección 2ª) 408/2017, de 19 de junio (F.D.3º) dispone que, será necesario poner a disposición del juez el material grabado, debiendo remitirse las cintas íntegras y en el soporte original. Asimismo, en relación con la sentencia mencionada, traemos a colación: ROSELL CORBELLE, A. "El valor de las grabaciones de los delatores ante el derecho de defensa (Reflexiones sobre el «Caso Guateque»)*"*. Diario La Ley. Núm. 9111. 2018; GONZALO LEÓN, F. "Impugnación del Recurso de Casación del Ministerio Fiscal contra la sentencia del 'Caso Guateque'. La ilicitud en el conocimiento de la 'notitia criminis' y su propagación al inicio y a los actos de investigación*"*. Trabajo en la Universidad Complutense de Madrid. 2018. Visto en http://eprints.ucm.es/47389/1/TFM.%20CASO%20GUATTEQUE%20PARA%20PUBLICACI%C3%93N.pdf.

hacer pública cierta actividad ilícita[510]. Nuestros Tribunales vienen afirmando que, la técnica de cámara oculta por el periodismo es un método invasivo en el derecho a la intimidad personal y familiar y a la propia imagen (art. 18.1 CE), por lo que, habrá que sopesar el uso del mismo, si bien, éste derecho puede ceder ante el derecho a la información (art. 20.1 CE), cuando se refieran a hechos con relevancia pública, tengan interés en el sentido de que sean noticiables, así como que dicha información sea veraz[511]. En consecuencia, se tendrá que realizar un juicio de ponderación sobre la colisión entre la intimidad y la información, y una vez superado éste, determinar qué derecho tiene prevalencia. Por su parte, en los reportajes periodísticos de "investigación" con cámara oculta, nuestro Tribunal garante de la Constitución[*512*] vino a adoptar la doctrina emanada del Tribunal Europeo de Derechos Humanos[513] sobre la "*expectativa razonable de privacidad*"[514], la cual, dependiendo del lugar donde se

[510] En relación con las cámaras ocultas, véase, BOIX REIG, F. J. y JAREÑO LEAL, A. *La protección jurisprudencial en los casos de grabación de la imagen con cámara oculta o sin consentimiento. Cuestiones sustantivas y procesales. (Nuevos conflictos sociales: el papel de la privacidad)*. Editores Iustel. Madrid. 2015. Págs. 201-218; BEL MALLÉN, J. I. *Derecho a la intimidad personal, uso de cámaras ocultas y otras amenazas a los derechos personales. (Libertad de expresión e información en Internet: amenazas y protección de los derechos personales).* Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 2013. Págs. 375-394; RUBIO TORRANO, E. "Grabación con cámara oculta, derecho a la intimidad y libertad de información*"*. Aranzadi Civil-Mercantil. Revista Doctrinal. Vol. 2. Núm. 1 (abril). 2012. Págs. 17-20; SAUX, E. I. "Afectación de derechos personalísimos por vía de la utilización de cámaras ocultas*"*. Revista Crítica de Derecho Privado. Núm. 8. 2011. Págs. 27-53.

[511] Sobre la ponderación del derecho a la intimidad personal y familiar y a la propia imagen (art. 18.1 CE), y a la información (art. 20.1 CE), traemos a colación, la STC 77/2009, de 23 de marzo (F.J. 2º).

[512] STC 12/2012, de 30 de enero (F.J. 5º), STC 24/2012, de 27 de febrero (F.J. 2º) y STC 74/2012, de 16 de abril (F.J. 2º).

[513] STEDDHH 552\2001, asunto P. G. y J. H. contra Reino Unido, de 25 septiembre 2001 y STEDDHH 50030\2003, asunto Peck contra Reino Unido, de 28 enero 2003.

[514] En relación con la doctrina de la "expectativa razonable de intimidad" emanada del TEDDHH, y que ha sido asumida por el TC, señala, RODRÍGUEZ LAINZ, J. L. "El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre*"*. Diario La Ley. Núm. 8122. 2013, que, la *"*idea de la expectativa razonable de privacidad suponía que la exteriorización de ese derecho o poder de exclusión se basara en un criterio de razonabilidad; en el sentido de no poder exigírsele ir más allá de lo que razonablemente pudiera tener en cuenta cualquier persona como forma de exteriorizar el ejercicio de

encuentre la persona, tendrá distintas manifestaciones de la vida privada protegible frente a intromisiones ilegítimas, o dicho de otro modo, cuando la persona se encuentre en un ámbito privado, al resguardo de la observación de terceros, sus manifestaciones pueden conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores, mientras que, cuando se encuentra en un ámbito público, cualquier persona podría observarla, pero además, podría captar o gravar con algún dispositivo técnico sus actividades. Por este motivo, no puede albergar expectativas de intimidad, cuando se participa en actividades que por las circunstancias que le rodea, claramente pueden ser objeto de registro o de información pública. Así, a título de ejemplo, cuando una persona camina por una calle puede ser vista inevitablemente por cualquier otra persona que esté presente, pero también, puede ser filmada la misma escena por medios tecnológicos (piénsese en un guardia de seguridad observando por un circuito cerrado de televisión). En cambio, existe una expectativa a no ser escuchado u observado por terceras personas, cuando un individuo se encuentra en un lugar específicamente ordenado a asegurar la discreción de la conversación (por ejemplo en el despacho donde se realizan consultas profesionales). Por su parte, la doctrina[515], en la línea de nuestro Tribunal Constitucional[516] vienen afirmando que, *la intromisión en los derechos fundamentales de terceros resultante del ejercicio de la libertad de información*

---

tal poder —dimensión positiva—. Por lo que supondría una extralimitación, y afectación a su derecho a la privacidad, cualquier acto de injerencia realizado por los poderes públicos o terceras personas con el que, conforme a la legislación vigente, el ciudadano no pudiera razonablemente contar —dimensión negativa—*"*. De igual modo, afirma GUERRERO PERALTA, O. J. "La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal*"*. Derecho Penal y Criminología. Vol. 32. Núm. 92. 2011. Págs. 42-72, que, "la expectativa razonable de intimidad se oponga a la noción de derecho fundamental a la intimidad, no quiere decir que no se pueda aplicar en otros ámbitos. A este respecto resulta interesante observar lo que ocurre en el contexto del derecho laboral español".

[515] Sobre la cámara oculta como método periodístico, y sus implicaciones en el derecho a la intimidad, afirma CRUZ GARCÍA, G. "El marco constitucional del ejercicio del periodismo de investigación con cámara oculta*"*. Diario La Ley. Núm. 8840, Sección Doctrina, 10 de octubre de 2016, que, "el uso de la cámara oculta por parte de los periodistas no es ilegítimo en todos los casos como así se ha demostrado a lo largo de este trabajo. Si bien sus limitaciones son más amplias en nuestro país que en el resto de países democráticos".

[516] Acerca de las argucias empleadas por el periodista para grabar su comportamiento o actuación desinhibida, traemos a colación la STC 12/2012, de 30 de enero (FJ 6º)… O.P. Cit.

únicamente es legítima en la medida en que la afectación de dichos derechos resulte adecuada, necesaria y proporcionada para la realización constitucional del derecho a la libertad de información. Por lo tanto, allí donde quepa acceder a la información pretendida sin necesidad de colisionar con los derechos referidos, queda deslegitimada, por desorbitada o desproporcionada, aquella actividad informativa innecesariamente invasora de la intimidad o la imagen ajenos. Por este motivo, *la utilización de un dispositivo oculto de captación de la voz y la imagen se trata de un ardid o engaño que el periodista despliega simulando una identidad, para poder acceder a un ámbito reservado de la persona afectada con la finalidad de grabar su comportamiento o actuación desinhibida, provocar sus comentarios y reacciones así como registrar subrepticiamente declaraciones sobre hechos o personas, que no es seguro que hubiera podido lograr si se hubiera presentado con su verdadera identidad y con sus auténticas intenciones.*

Además, se debe reseñar que, cuando se graban imágenes con el método de cámara oculta, pero se emite en los medios de comunicación el rostro difuminado, pixelado o distorsionado del afectado, pero con ello no se impide reconocer completamente al mismo, ya sea por la voz, por su aspecto físico, o bien, por otros elementos accesorios, como el mobiliario o la localización, la intimidad protegida constitucionalmente también puede verse afectada[517]. En definitiva, aunque pueda ser la información de relevancia pública, habrá que armonizar los criterios establecidos por el Tribunal garante de la Constitución, de tal forma que, cuando este método intrusivo, pueda llevarse a cabo, por otra vía menos lesiva (por ejemplo, entrevistas), la cámara oculta, como forma de obtener información periodística, constituirá una ilegítima intromisión en el derecho fundamental a la intimidad (18.1 CE)[518].

No obstante, en alguna ocasión, el Tribunal Europeo de Derechos Humanos en el Caso *Haldimann* y Otros contra Suiza[519], ha puesto de relieve que, la injerencia en la vida

[517] STC 24/2012, de 27 de febrero… O.P. Cit. (FJ 3º), dispone que, el rostro difuminado si no impide reconocer plenamente al afectado, puede ser atentatorio a la intimidad.

[518] STC 25/2019, de 25 de febrero (F.J. 8º).

[519] STEDDHH 34\2015, asunto *Haldimann* y Otros contra Suiza, de 24 febrero 2015 (párrafo 66) dispone que, "el Tribunal considera, teniendo en cuenta las circunstancias del caso, que la injerencia en la vida

privada del sujeto realizada con el método de filmación periodística de video oculto no es suficientemente grave, como para superponerse al interés público de la información ofrecida por los periodistas, si bien, en el asunto referido, la decisión tomada por el tribunal se basaba en que la persona afectada no se trataba de una figura pública, la imagen y la voz había sido distorsionada, por lo que se presentaba de forma anónima, así como, la entrevista no se había grabado en las oficinas o en otros locales comerciales, sino en una sala expresamente preparada por los periodistas con cámaras de video[520].

Una vez realizado, un breve análisis de la jurisprudencia sobre las cámaras ocultas como método periodístico, cabe preguntarse si, las imágenes obtenidas por el profesional de la información pueden servir como fuente de prueba en el proceso penal. De esta manera, nuestro Tribunal Supremo[521] examinando la jurisprudencia mencionada anteriormente, llega a la conclusión que, no se puede afirmar que, *la utilización de una cámara oculta conlleve, siempre y en todo caso, una vulneración de los principios y derechos que*

---

privada del agente, que renunció a expresarse sobre la entrevista, no es de una gravedad tal que deba pasar por alto el interés del público por la información de las malas prácticas denunciadas en el sector de los seguros*"*.

[520] Con carácter general, acerca del empleo de cámaras ocultas como método periodístico, y su incidencia en los derechos fundamentales, véase, BELADIEZ ROJO, M. "Cámaras ocultas y periodismo: una perspectiva constitucional*"*. Revista General de Derecho Constitucional. Núm. 28. 2018; VIDAL LÓPEZ, P. "¿Qué ha dicho realmente el TEDH sobre las cámaras ocultas?" Actualidad Jurídica Aranzadi. Núm. 937. 2018. Pág. 13; PÁRAMO Y DE SANTIAGO, C. "Libertad de expresión e información en reportaje con cámara oculta emitido en televisión. Comentario a la STS de 23 de noviembre de 2017*"*. CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 204. 2018; DE LUNA Y JIMÉNEZ DE PARGA, P. "El delito de escarnio y el uso de la cámara oculta en los reportajes de investigación*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 123. 2016; CRUUZ GARCÍA, G. "El marco constitucional del ejercicio del periodismo de investigación con cámara oculta*"*. Diario La Ley. Núm. 8841. 2016; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal.* Editorial SEPIN. Madrid. 2016… O.P. Cit. Págs. 158-170; JIMÉNEZ SEGADO, C. y PUCHOL AIGUABELLA, M. "La cámara oculta frente a los derechos a la intimidad y a la propia imagen (Comentario a la STS, Sala 1ª, Pleno, 1233/2008, de 16 de enero de 2009)". Diario La Ley. Núm. 7152. 2009.

[521] Sobre la utilización de cámara oculta, traemos a colación la STS 793/2013, de 28 octubre, en aplicación de la STC 12/2012, de 30 de enero… O.P. Cit. (F.D. 2º).

convergen en el proceso penal, sino que, *la licitud o exclusión de esa prueba sólo puede ser el desenlace lógico de un riguroso juicio de ponderación* por los órganos jurisdiccionales[522] *entre, la intimidad y a la propia imagen* (art. 18.1 CE) *y la posible existencia de un fin legítimo*, en especial, el derecho a la información de las personas (art. 20.1 CE), pero además, habrá que respetar los *principios de proporcionalidad, necesidad y racionalidad*[523].

En otro orden de ideas, la función de las Fuerzas y Cuerpos de Seguridad del Estado es investigar los delitos para descubrir y detener a los presuntos culpables y ponerlos a disposición judicial [arts. 11.1.g) L.O. 2/1986 en relación con el 126 CE]. De igual modo, la seguridad pública es competencia exclusiva del Estado (art. 1.1 L.O. 2/1986), pero además, la Policía Judicial depende orgánicamente del Ministerio del Interior y funcionalmente de los Jueces, Tribunales o Ministerio Fiscal (art. 31 L.O. 2/1986). Por su parte, la Constitución reconoce, en aras del interés de todos en conocer los hechos de actualidad que puedan tener trascendencia pública, la libre comunicación y recepción de información veraz [art. 20.1.d) CE], de tal manera que, los sujetos de este derecho son el medio difusor de la información, o los profesionales del periodismo, pero también, la colectividad y cada uno de sus miembros en su conjunto[524]. Asimismo, el periodismo tiene la función de materializar el principio de publicidad, esto es, los actos procesales sean presenciados o conocidos por terceros, de forma que, comporta un medio de fiscalizar la conducta de los poderes públicos. Por su parte, en ocasiones el periodismo ha servido para descubrir actividades ilícitas, incluso relacionadas con altos cargos de la

[522] Auto AP de Madrid (Sección 16ª) 516/2012, de 22 junio, vino a adoptar el sobreseimiento y archivo de las actuaciones, al declarar nulas las pruebas consistentes en una grabación realizada con cámara oculta, y su posterior difusión en medios de comunicación, al entender que, haciendo un juicio de ponderación entre derecho de información *versus* intimidad, había que dar preferencia a este último.

[523] FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J. A. "La cámara oculta en el proceso penal*"*. Revista penal. Núm. 38. 2016. Págs. 85-106; VELÁZQUEZ VIOQUE, D. "Validez de la prueba obtenida mediante cámara oculta ¿cambio de paradigma?*"* Iuris: Actualidad y Práctica del Derecho. Núm. 177. 2012. Págs. 36-39.

[524] STC 168/1986, 22 de diciembre (F.J. 2º), pone de manifiesto el derecho a la libre comunicación y recepción de información veraz del art. 20.1.d) CE recae en el medio difusor de la información, o los profesionales del periodismo, aunque también en la colectividad en su conjunto.

política (por ejemplo, en el caso Grupos Antiterroristas de Liberación –GAL-)[525]. Sin embargo, a diferencia de las Policía Judicial que, como nos hemos referido, depende orgánicamente del Ministerio del Interior y funcionalmente de la autoridad judicial y fiscal, el periodista tiene una relación de dependencia con el medio al que presta servicio, de modo que, con frecuencia, su labor puede ir orientada más, a fines económicos que propiamente informativos (por ejemplo ratios de audiencia, sensacionalismo, etc.), por lo que, con carácter general, habría que descartar la investigación periodística, como método de descubrir hechos delictivos.

3. Captación de imágenes en espacios y lugares públicos

Seguidamente vamos a examinar la medida consistente en permitir a la Policía Judicial, obtener y grabar por cualquier medio técnico, imágenes del investigado, esto es, sin precisar de autorización judicial, cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos (art. 588.1 quinquies a. LECrim.)[526]. Por ello, se debe diferenciar, por un lado, la captación y grabación de sonido, acompañada o no de imágenes, en espacios públicos, que ha sido

[525] El caso Grupos Antiterroristas de Liberación (GAL), vino a consistir que, tras la investigación periodística sobre los GAL realizada en el Diario 16, se presentó a la opinión pública la organización, fuentes de financiación e implicaciones políticas de los GAL, de tal forma que, se descubrió, la "guerra sucia" utilizada por el Gobierno español para combatir el terrorismo de ETA, lo cual, dio origen a actuaciones judiciales. En relación a esto, traemos a colación la STS 2/1998, de 29 de julio y la Sentencia del Tribunal Europeo de Derechos Humanos (Sección Tercera), en el asunto Vera Fernández-Huidobro c. España, 6 de enero de 2010.

[526] Con carácter general, sobre la medida de captación de imágenes en espacios y lugares públicos, véase, GARCIA MARCOS, J. *Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización*… O.P. Cit. Págs. 285 – 325; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*… O.P. Cit. Págs. 909-913; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Págs. 114-116; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 355-360; 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*… O.P. Cit.; GÓMEZ COLOMER, J. L. *Diligencia de filmación de lugares públicos*… O.P. Cit. Págs. 204-206.

estudiado en el epígrafe anterior (párrafos 1 y 2 del art. 588 a quater LECrim.), que como decíamos precisaba de autorización judicial, de aquella otra medida que ahora estudiamos, la cual, faculta a la Policía Judicial para registrar con videocámara o tomar imágenes fotográficas en espacios públicos, esto es, sin captar audio o sonido, que en este caso, no requiere de la intervención judicial para su adopción (art. 588.1 quinquies a. LECrim.). Esto es debido a que, como decíamos anteriormente, las *expectativas razonables de privacidad*[527] en la vía pública son diferentes del que se espera de un espacio donde se desenvuelve la esfera íntima de las personas, y en consecuencia, el grado de injerencia puede ser menos intenso en estos casos[528]. No obstante, aunque la Policía Judicial por su propia iniciativa pueda tomar imágenes de espacios públicos, sin necesidad de recabar autorización judicial, nada impediría a que este, pudiera acordarla también, como medida de investigación.

En otro orden de ideas, a los efectos de determinar cuándo se exige autorización judicial, debemos interpretar que se entiende por "*lugares o espacios públicos*" que refiere el art. 588.1 quinquies a. LECrim. Por su parte, nuestro Tribunal Constitucional no siempre ha considerado domicilio a todo espacio cerrado, pues en determinados supuestos se ha prescindido del oportuno plácet judicial para espacios cerrados, como por ejemplo en locales destinados a almacén de mercancías[529], un bar y un almacén[530], unas oficinas de una empresa[531], los locales abiertos al público o de negocios[532]. De

[527] Sobre la doctrina de la "expectativa razonable de privacidad", véase, STC 170/2013, 7 de octubre (F.D. 5º), STS 239/2014, 1 de abril (F.D. 2º) y STS 610/2016, 7 de julio (F.D. 1º).

[528] En la conclusión primera de la circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, *sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización*. «BOE» Núm. 70, de 22 de marzo de 2019, dispone que, "la captación de imágenes por la Policía Judicial en lugares o espacios públicos no afecta a ninguno de los derechos fundamentales del art. 18 CE", mientras que "las grabaciones obtenidas por medio de sistemas de videovigilancia pueden afectar al contenido del derecho fundamental a la protección de datos de carácter personal".

[529] STC 228/1997, de 16 de diciembre (F.J. 7º).

[530] STC 283/2000, de 27 de noviembre (F.J. 2).

[531] Auto TC 171/1989, de 3 de abril (F.J. 2).

[532] Auto TC 58/1992, de 2 de marzo (F.J. 2).

igual modo, el art. 588 quater a. LECrim, el cual, ha sido estudiado en el epígrafe anterior, hace mención a "*la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados*". De todo ello, debemos interpretar que, no podemos confundir los lugares abiertos o cerrados, pues aluden estrictamente al espacio físico, de aquellos otros con una mayor dimensión, como los públicos o privados, que hacen referencia al lugar donde las personas desarrollan o no su vida íntima[533]. Es por ello que, cuando la norma procesal refiere a "*espacios públicos*" debemos situarlo en esta segunda, es decir, aquellos lugares donde las personas no desenvuelven acciones en la esfera privada, no ejercen su libertad más íntima o no tienen la consideración de domicilio o espacios asimilados. Por esta razón, nuestros tribunales[534] han permitido la captación de imágenes por la Policía Judicial sin autorización judicial en garajes cerrados, cafeterías, gasolineras, etc.

Por último, la norma procesal establece que podrán grabarse a terceras personas distintas del investigado, cuando la vigilancia no pueda realizarse sin reducir de forma relevante su utilidad o cuando existan indicios fundados de la relación de dichas personas con el investigado o bien con los hechos objeto de la investigación (art. 588.2 quinquies a. LECrim.).

a) Algunas particularidades observadas en la jurisprudencia y/o doctrina: grabaciones realizadas por videocámara.

Nos vamos a detener en analizar brevemente el uso de videocámaras en espacios públicos, como fuente de prueba tecnológica en el proceso penal, para lo cual, examinaremos la legislación y jurisprudencia aplicable. Como hemos estudiado anteriormente, la Policía Judicial puede a su propia iniciativa registrar imágenes en lugares públicos, si bien, debemos distinguir, por un lado, la grabación para un momento puntual, de aquella otra fija que se instala como videovigilancia, pues en este caso, habría que proceder al tratamiento de los datos personales, y por tanto, podría

[533] Acerca del espacio público o privado, esto es, lugar donde las personas desarrollan o no su vida íntima, véase, STC 22/1984, de 17 de febrero; STC 137/1985, de 17 de octubre; STC 10/2002, de 17 de enero.

[534] SAP de Madrid (Sección 29º) 152/2019, de 22 de febrero (F.D. 1º) y SAP de Madrid (Sección 23º) 272/2017, de 5 de mayo (F.D. 3º).

conculcar con el derecho fundamental del art. 18.4 de la CE. En consecuencia, las grabaciones realizadas por la Policía Judicial en la vía pública[535] para un momento preciso estarían legitimadas, con arreglo al art. 588 quinquies a de la LECrim, si bien, la colocación de cámaras de video vigilancia fijas[536] necesitan de mayores garantías, pues, como decimos, incide en el derecho fundamental a la protección de datos (art. 18.4 CE)[537]. La Ley Orgánica 4/1997 de 4 de agosto, *por la que se regula la utilización de*

[535] STS 124/2014, 3 de febrero (F.D. 3º), STS 485/2013, 5 de junio (F.D. 1º), STS 433/2012, 1 de junio (F.D. 9º) y STS 180/2012 de 14 de marzo (F.D. 2º) disponen que se considera "legítima y no vulneradora de derechos fundamentales la filmación de escenas presuntamente delictivas que suceden en espacios o vías públicas".

[536] Con carácter general, acerca de la colocación de video vigilancia fijas, véase, DE LA IGLESIA CHAMARRO, A. *Videovigilancia, espacio público y derechos fundamentales. (Conflictos de derechos fundamentales en el espacio público)*. Editorial Marcial Pons. Madrid. 2017. Págs. 37-70; PÉREZ CAMBERO, R. "Videovigilancia en el ámbito público*"*. Actualidad Administrativa. Núm. 1. 2017; FERNÁNDEZ GARRIDO, J., LANDÍN LÓPEZ, E. "Videovigilancia regularización y nueva doctrina del tribunal constitucional*"*. Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 139. 2016. Págs. 59-78; DURÁN SILVA, C. *Videovigilancia y derecho a la intimidad. (FODERTICS II: hacia una justicia 2.0)...* O.P. Cit. Págs. 169-177; PÉREZ-CRUZ MARTÍN, A.-J. *Videovigilancia entre la seguridad y la libertad. (Derecho, eficacia y garantías en la sociedad global: Liber Amicorum I en honor de María del Carmen Calvo Sánchez).* Editorial Atelier. Madrid. 2013. Págs. 315-329; DE LA IGLESIA CHAMARRO, A. *Videovigilancia y espacio público. (Derechos y espacio público: Cátedra de amparo de derechos y libertades)*. Editorial Universidad de Oviedo. 2013. Págs. 29-59; DE LA IGLESIA CHAMARRO, A. *Reflexiones sobre videovigilancia y obstaculización al libre ejercicio de derechos. (Constitución y democracia: ayer y hoy: libro homenaje a Antonio Torres del Moral. Vol. 2)*. Universitas Editorial. Madrid. 2012. Págs. 1989-2010.

[537] Afirma BERMEJO BOSCH, R. "Análisis en la doctrina administrativa de la Agencia Española de Protección de Datos en relación con el tratamiento de imágenes a través de sistema de vídeovigilancia*"*. Revista Aranzadi de derecho y nuevas tecnologías. Núm. 25. 2011. Págs. 61-80, que, "los sistemas de videovigilancia tienen como finalidad, en principio, garantizar la seguridad de personas, bienes y recursos, si bien permiten la grabación, captación, transmisión, conservación y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real. No obstante, en el momento en que las imágenes constituyen datos de carácter personal entra en juego la aplicación de la normativa en materia de protección de datos, la cual se encargará de establecer los límites necesarios para que, sin dejar de garantizarse el fin perseguido -la seguridad-, se respeten los derechos que asisten a las personas titulares de los datos que puedan ser objeto de tratamiento a través de los sistemas de videovigilancia. De este modo, se hace necesario establecer un elenco de obligaciones a los responsables de ficheros de videovigilancia en aras de garantizar los principios fundamentales que la Ley Orgánica 15/1999, de 13 de

videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos[538], permite a la policía, previa autorización administrativa (art. 3 L. O. 4/1997)[539], la grabación de

diciembre, de Protección de Datos de Carácter Personal 1 (en adelante LOPD) establece como pilares esenciales del derecho fundamental a la protección de datos de carácter personal". Por su parte, mantiene, FRÍAS MARTÍNEZ, E. "Los sistemas de videovigilancia la protección de datos y sus efectos en el proceso penal*"*. Diario La Ley. Núm. 7396. 2010, que, "la imagen de una persona y su voz es un dato de carácter personal relativo a la intimidad y privacidad, conceptos no coincidentes necesariamente en su contenido, y que el derecho a la protección de datos de carácter personal es un Derecho Fundamental. Pero como tal derecho no es de carácter absoluto, sino que ha de ceder ante determinados supuestos, pero siempre con un mínimo de garantías y siempre de modo proporcional y necesario. Con objeto de regular el modo en el que deben captarse y tratarse imágenes de personas a través de cualquier medio, cámaras, circuitos cerrados, webcam, etc., se aprobó la Instrucción 1/06 de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, quedando únicamente excluidas las imágenes que un particular pueda captar en su vida privada".

[538] Respecto a la L.O. 4/1997, «BOE» Núm. 186, de 5 de agosto de 1997, véase, BARCELONA LLOP, J. *A propósito de la Ley Orgánica 4/1997, de 4 de agosto, llamada de videovigilancia*. Actualidad administrativa. Núm. 13. 1998. Págs. 205-215; GONZÁLEZ URDÍNGUIO, A. y GONZÁLEZ GUTIERREZ DE LEÓN, M. A. "La videovigilancia en el sistema democrático español, análisis y crítica de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos*"*. Revista de la Facultad de Derecho de la Universidad Complutense. Núm. 89. 1998. Págs. 105-124.

[539] Afirma DURÁN SILVA, C. "Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 126. 2017, que, "la videovigilancia preventiva, se encuentra legalmente prevista en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y cuerpos de Seguridad del Estado en lugares públicos (en adelante, LOV) pudiendo desarrollarla los miembros de las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos, abiertos o cerrados, y por las empresas de seguridad privada, quienes podrán instalar videocámaras en establecimientos abiertos al público, e, incluso, en locales privados, pudiendo tales imágenes acceder al eventual y posterior proceso siempre que no invadan espacios estrictamente íntimos, como por ejemplo, los aseos"; Por su parte, señala ETXEBERRIA GURIDI, J. F. *Videovigilancia y su eficacia en el proceso penal. (El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito)*. Editorial La Ley. Madrid. 2012. Págs. 331-377, que, *"*entre las disposiciones extraprocesales podríamos resaltar especialmente la LO 4/1997, de 4 de agosto, reguladora de la utilización de videocámaras por las FF y CC de Seguridad en lugares públicos. Esta LO es de suma importancia porque contiene una serie de criterios consagrados por la jurisprudencia con motivo de la videovigilancia y porque algunos de los mismos son proyectables al empleo de la videovigilancia en el proceso penal. Pese a su naturaleza extraprocesal*"*; De igual modo, mantiene RODRÍGUEZ LAINZ, J. L. "Las grabaciones de videocámaras de seguridad como

imágenes y sonidos de forma sistemática y continuada en lugares públicos, abiertos o cerrados, con el fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos e infracciones relacionados con la seguridad pública (art. 1.1 L. O. 4/1997); si bien, precisará el tratamiento de las imágenes y el sonido conforme a la Ley 3/2018 de Protección de Datos (art. 2.2 L. O. 4/1997).

No obstante, aunque la norma examinada permita también la captación de sonido en espacios públicos con una simple autorización administrativa, lo cierto es que, habrá que entender que ha sido superada por la regulación contenida en la norma procesal (apartados 1 y 3 del art. 588 quater a. LECrim.), que exige para ello el oportuno plácet judicial.

En este contexto, cabe preguntarse, si los particulares pueden obtener imágenes como fuente de prueba en el proceso penal. Así, se permite con carácter general, a la seguridad privada tomar imágenes a través de sistemas de cámaras o videocámaras, fijas o móviles, en el interior de los edificios, de las instalaciones o propiedades a proteger (art. 41.1 de 4 de abril, *de Seguridad Privada*[540]), así como, excepcionalmente, previa

---

fuente probatoria en el proceso penal*"*. Diario La Ley. Núm. 7921. 2012, que, "la instalación y uso de videocámaras de seguridad por parte de fuerzas y cuerpos de seguridad viene regulada por la LO 4/1997, de 4 de agosto, por la que se regula el uso de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, desarrollada por el RD 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la LO 4/1997, de 4 de agosto. La ley se desarrolla en una estructura orgánica en la que se define su ámbito material, las finalidades legítimas a las que están destinados dichos instrumentos de vigilancia, los derechos de los ciudadanos que han de ser objeto de especial respeto, y en general los trámites administrativos para su instalación y normal funcionamiento". En el mismo sentido y en relación con L.O. 4/1997, véase, NAVAJAS RAMOS, L. "La prueba videográfica en el proceso penal su valor y límites para su obtención*"*. Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. 12. 1998. Págs. 147-170; ANDRÉS RIVAS, L. F. "Videovigilancia y policía*"*. Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 139. 2016. Págs. 79-89; DÍEZ RIPOLLÉS, J. L. *El control de los espacios públicos mediante cámaras de videovigilancia (Un derecho penal comprometido: libro homenaje al Prof. Dr. Gerardo Landrove Díaz)…* O.P. Cit. Págs. 309-362; CEREZO DOMÍNGUEZ, A. I., DÍEZ RIPOLLÉS, J. L. "La Videovigilancia en las zonas públicas: su eficacia en la reducción de la delincuencia*"*. Boletín Criminológico. Núm. 121. 2010.

[540] «BOE» Núm. 83, de 5 de abril de 2014.

autorización administrativa, se permite tomar imágenes con fines de seguridad privada en los espacios públicos (art. 42.2 L. 5/2014)[541], para lo cual, la monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal (L.O. 3/2018), y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima (art. 42.5 L. 5/2014). De igual modo, cuando las grabaciones se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, podrán ser aportadas, de propia iniciativa o a requerimiento de las Fuerzas y Cuerpos de Seguridad, para cual, habrá que respetar los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales (art. 42.4 L. 5/2014).

Por su parte, la línea que mantiene la jurisprudencia al respecto[542], admite realizar filmaciones a los particulares[543], o en su caso, a detectives privados, en los espacios públicos, siempre que no sean filmaciones continuadas y tengan como finalidad su utilización exclusiva como fuente de prueba en un proceso judicial (por ejemplo, la grabación con teléfonos móviles o cámaras móviles en la comisión de un hecho delictivo), mientras que, para la instalación de video vigilancia fija, únicamente se permite en espacios privados, cuando medie consentimiento de su titular, así como, se cumpla con la normativa reguladora sobre el tratamiento de datos de carácter personal (L.O. 3/2018), puesto que las grabaciones de cámaras de seguridad fija en la vía pública

[541] STS 124/2014, 3 de febrero (F.D. 3º) dispone que "el material fotográfico y videográfico obtenido en el ámbito público y sin intromisión indebida en la intimidad personal o familiar tiene un valor probatorio innegable".

[542] STS 1154/2011, 12 de enero (F.D. 1º) y STS 4/2005, 19 de enero (F. D. 1º).

[543] Sobre filmaciones realizadas por los particulares, véase, DE LA IGLESIA CHAMARRO A. *Las garantías de los derechos fundamentales frente a los dispositivos de videovigilancia utilizados por particulares (Derecho y nuevas tecnologías).* Editorial Universidad de Deusto. Bilbao. 2011. Págs. 25-36; DE LA IGLESIA CHAMARRO, A. *Las garantías de los derechos fundamentales frente a los dispositivos de videovigilancia utilizados por particulares. (Derecho y nuevas tecnologías).* Editorial Deusto, D. L. Bilbao. 2010. Pág. 2.

queda descartada, sin perjuicio de que hipotéticamente pudieran obtener autorización administrativa que ha sido mencionada anteriormente[544].

En definitiva, se debe aceptar que, cuando se cumplan con los presupuestos legales y jurisprudenciales examinados, esto es, respetando todas las garantías aludidas, se podrán incorporar al proceso penal, como fuente de prueba, filmación de imágenes[545], ya sean registradas en espacios públicos como privados.

4. Intervención de las comunicaciones en los calabozos en dependencias policiales y en centros penitenciarios: mención especial a las comunicaciones entre el abogado o procurador y su cliente

Vamos a examinar a continuación, la intervención de las comunicaciones en los centros penitenciarios y en los calabozos en dependencias policiales, pues a efectos de este trabajo, resulta imprescindible conocer las escuchas como medida de investigación tecnológica, para lo cual, haremos especial alusión a las comunicaciones entre abogado y procurador y su patrocinado dentro de estas instituciones. De esta manera, con carácter previo, conviene explicar que, las personas que se encuentran internas en centros penitenciarios o bien, detenidas bajo custodia policial, surge una relación jurídica de sujeción especial[546] con la Administración Pública[547]. De forma que, el

[544] SAN (Sala de lo Contencioso-Administrativo) de 10 febrero 2011 (F.J. 2º) dispone que "las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende". En el mismo sentido, véase, MAGRO SERVET, V. "La instalación de cámaras de videovigilancia en hogar/local con vista exterior por cuestiones de seguridad y su afectación a la normativa de protección de datos". CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 172. 2015. Págs. 109-120.

[545] Acerca de la grabación de videovigilancia como prueba en el proceso penal, véase, DAMIÁN MORENO, J. "Reflexiones sobre la reproducción de imágenes como medio de prueba en el proceso penal (a propósito de la llamada videovigilancia)". Revista Vasca de Derecho Procesal y Arbitraje. Vol. 9. Núm. 2.1997. Págs. 237-246; MISMO AUTOR. "Reflexiones sobre la reproducción de imágenes como medio de prueba en el proceso penal (a propósito de la llamada videovigilancia)". Anales de la Facultad de Derecho: Revista Jurídica de la Universidad de León. Núm. 1. 1997. Págs.103-113.

[546] En relación a la sujeción especial en centros penitenciarios, véase, CERVELLÓ DONDERIS, V. *La relación jurídica penitenciaria. La relación de sujeción especial y sus consecuencias (Derecho Penitenciario)*. Editorial Tirant Lo Blanch. Valencia. 2016. Págs. 140-143.

interno se integra en una institución preexistente que proyecta su autoridad sobre quienes integran en ella, para lo cual, se debe garantizar y velar por la seguridad y el buen orden regimental del centro. Así, conlleva en la necesidad de ajustarse a las normas de régimen interior reguladoras de la vida del establecimiento, pero además, la situación jurídica mencionada también resulta de aplicación para las relaciones entre el detenido y los agentes de policía que lo custodia.

Las personas privadas de liberad pueden tener restringidos algunos derechos fundamentales, como el deambulatorio (art. 19 CE) o el sufragio universal (art. 23.1 CE), pero otros no tienen por qué verse afectados como los derechos de los condenados a prisión del art. 25.2 CE[548]. En particular, lo relevante a los efectos del presente trabajo es que, no se pueden producir injerencias en el secreto de las comunicaciones (art. 18.3 CE) para personas privadas de libertad[549], salvo razones justificadas y, como veremos posteriormente, cumpliendo los presupuestos y garantías legales contenidos en la norma procesal penal y penitenciarias. Así, para velar por la seguridad de los centros penitenciarios, se permiten tomar distintas medidas de carácter administrativo, como por ejemplo que los funcionarios de prisiones realicen registros o cacheos[550] (art. 23 de la

[547] Acerca de que el interno de un centro penitenciario está respecto a la Administración en una relación de sujeción especial, traemos a colación la STC 74/1985, de 18 de junio (F.J. 2º), la STC 175/2000, de 26 de junio (F.J. 2º), STC 140/2002, de 3 de junio (F.J. 4º) y STC 119/1996, de 8 de junio (F.J. 4º).

[548] Sobre la incidencia en los derechos fundamentales de las personas privadas de libertad, véase, LÓPEZ MELERO, M. *Los derechos fundamentales civiles y sociales de los internos en centros penitenciarios y su libertad*. Anuario de la Facultad de Derecho. Núm. 8. 2015. Págs. 157-186; SUBIJANA ZUNZUNEGUI, I. J. "Los derechos fundamentales de las personas privadas de libertad y la doctrina del Tribunal Constitucional*"*. Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. Extra 12. 1998. Págs. 167-186; GARCÍA MORILLO, J. "Los derechos fundamentales de los internos en centros penitenciarios*"*. Revista del Poder Judicial. Núm. 47. 1997. Págs. 23-60.

[549] STC 128/1997, de 14 de julio (F. D. 4º), STC 175/1997, de 27 de octubre (F.D. 2º), STC 200/1997, de 24 de noviembre (F.D. 2º), STC 188/1999, de 25 de octubre (F.D. 5º), STC 175/2000, de 26 de junio (F.D. 3º) y STC Núm. 170/1996… O.P. Cit. (F.D. 4º), disponen que "los internos en un Centro Penitenciario son también titulares del derecho al secreto de las comunicaciones (art. 18.3 C.E.)".

[550] Con carácter general, sobre los registros y cacheos de los internos en centro penitenciario, véase, DE VICENTE MARTÍNEZ, R. "Registros y cacheos en el ámbito penitenciario*"*. Revista de Derecho y Proceso Penal. Núm. 22. 2009. Págs. 31-50.

Ley Orgánica 1/1979, de 26 de septiembre, *General Penitenciaria*[551]), pero también, pueden ejecutar medidas restrictivas en las comunicaciones orales y escritas, de tal forma que, mediante resolución motivada del Director del establecimiento, dando cuenta a la autoridad judicial competente (Juez de Vigilancia en el caso de penados o a la autoridad judicial de la que dependa si se trata de detenidos o presos –Juzgado de Instrucción o tribunal que conozca del enjuiciamiento–) pueden intervenir las comunicaciones de los internos (art. 51.5 LOGP y el art. 43 del Real Decreto 190/1996, de 9 de febrero, *por el que se aprueba el Reglamento Penitenciario*[552]).

Igualmente, como ya se ha estudiado en los epígrafes anteriores, el Juez puede autorizar para la investigación delictiva, las medidas de interceptación de las comunicaciones (art. 588 ter LECrim.) y escuchas ambientales en lugares cerrados (art. 588 quater LECrim.), por lo que, conforme a la legislación procesal comentada, se podrían acordar también la intervención de los teléfonos que utilizan los internos para comunicarse (arts. 51.4 LOGP y 47 R. D. 190/1996), o bien, instalar dispositivos de escuchas en los calabozos de dependencias policiales, en los locutorios habilitados para visitas (arts. 13 LOGP, 48 y 216 R. D. 190/1996), o celdas (arts. 19 LOGP, 13 y 14 R. D. 190/1996) en centros penitenciarios.

Una vez examinado que, con arreglo a la legislación penitenciaria y procesal se pueden producir injerencias en las comunicaciones de los internos y detenidos, cabe preguntarse si, también pueden ser objeto de estas intromisiones, las comunicaciones realizadas entre el abogado y su patrocinado, pues vienen protegidas constitucionalmente por el derecho de defensa, así como de asistencia letrada y a no declarar contra sí mismo (art. 24.2 CE)[553]. De esta manera, cuando la información proporcionada por el cliente a su

[551] «BOE» Núm. 239, de 5 de octubre de 1979.

[552] «BOE» Núm. 40, de 15 de febrero de 1996.

[553] Afirma MARTÍNEZ RUIZ, J. "Reflexiones de urgencia motivadas por la desconcertante aplicación procesal de la intervención de las comunicaciones orales directas en el ámbito penitenciario, con especial atención a las comunicaciones abogado-cliente*"*. Diario La Ley. Núm. 7376. 2010, que, "el apartado 2 del citado art. 51, tras ordenar que «las comunicaciones de los internos con el Abogado defensor o con el Abogado expresamente llamado en relación con asuntos penales y con los Procuradores que los representen, se celebrarán en departamentos apropiados», articula un régimen específico de suspensión e intervención, en cuya virtud, «no podrán ser suspendidas o intervenidas salvo por orden judicial y en los

supuestos de terrorismo»". Por su parte, mantiene, NISTAL MARTÍNEZ, J. "La libertad de las comunicaciones con el abogado defensor como garantía del derecho a la defensa*"*. Diario La Ley. Núm. 7383. 2010, que, "solamente en casos de terrorismo se puede suspender el derecho de los internos en los centros penitenciarios a la comunicación confidencial con sus abogados defensores, en la medida en que la orden de intervención está amparada en una Ley Orgánica —art. 51.2 LOGP— de lo contrario se afectaría directamente al derecho a la libertad y a la igualdad, porque quien está en prisión debe gozar del derecho de defensa igual que quien está en libertad, sin que su confinamiento se convierta en un medio privilegiado de investigación contra él a costa, precisamente, de su defensa. Y esto ha de ha de ser así, aunque la comunicación pueda versar sobre temas ajenos a la defensa jurídica del interno, porque ese es un riesgo que forma parte de la propia naturaleza del derecho al secreto de las comunicaciones en el art. 18.3 CE, dado su carácter formal en el sentido de que se predica de lo comunicado, sea cual sea su contenido". Por elcontrario, entiende, ARRIBAS LÓPEZ, E. "Algo más sobre la intervención de comunicaciones de los internos con sus abogados la voluntad del legislador*"*. Diario La Ley. Núm. 7436. 2010, que, "ni siquiera la autoridad judicial esté legitimada para decretar la intervención de las comunicaciones de los internos con sus abogados. Sostenemos, por el contrario, que debe estar normativamente contemplada —como, de hecho, pensamos que lo está— la posibilidad de que esa intervención pueda producirse; lo contrario sería crear un espacio completamente blindado e inmune a cualquier tipo de actuación, y ello, insistimos, por sus graves consecuencias en determinados casos, ni es razonable, ni puede asumirse desde un punto de vista político-criminal. Finalmente, no por defender lo anterior se nos escapa la gravedad y trascendencia de una decisión como la de intervenir las comunicaciones de las personas presas o penadas con sus abogados defensores. La afectación de la intimidad personal y del derecho de defensa (arts. 18.1 y 24.2 CE) es evidente. Por eso, la decisión interventora debe estar rodeada de todas las garantías posibles y adoptarse con toda la prudencia, proporcionalidad y requisitos que se consideren necesarios, pero debe poder adoptarse, y debe hacerse, por quien únicamente puede teniendo en cuenta las reglas básicas de un Estado de Derecho: los órganos jurisdiccionales"; En el mismo sentido, traemos a colación, RODRÍGUEZ ÁLVAREZ, A., GARCÍA MONTEAGUDO, A. *La intervención de las comunicaciones telefónicas y telemáticas entre el abogado y el investigado. (FODERTICS 6.0: los nuevos retos del derecho ante la era digital)*. Editorial Comares. Granada. 2017. Págs. 195-206; LÓPEZ-BARAJAS PEREA, I. *El secreto de las comunicaciones con el abogado defensor en la nueva sociedad de la información. (Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal -I Internacional-, La Coruña, 2 y 3 de junio de 2011).* Edit. Universidad de La Coruña. 2012. Págs. 517-530; MARTÍNEZ ALARCÓN, M. L. "El derecho al secreto de las comunicaciones de los internos en establecimiento penitenciario con sus representantes legales*"*. Revista Española de Derecho Constitucional. Año núm. 31. Núm. 92. 2011. Págs. 141-167; JUANATEY DORADO, C. "La intervención de las comunicaciones de los internos con sus abogados defensores en el ámbito penitenciario, doctrina del Tribunal Constitucional*"*. Revista General de Derecho Penal. Núm. 15. 2011; BAUTISTA SAMANIEGO, C. "La intervención de las comunicaciones del abogado defensor en centro penitenciario*"*. Iuris: Actualidad y Práctica del Derecho. Núm. 156. 2011. Págs. 16-23; PELAYO JIMÉNEZ, R. C. "Intervención de las comunicaciones entre

abogado es utilizada como fuente de prueba, la defensa del acusado queda prácticamente anulada, en consecuencia, las garantías del proceso penal quedarían menoscabadas. Por este motivo, las comunicaciones entre los encartados y sus abogados, con carácter general, deben ser confidenciales, pues así lo pone de manifiesto la Unión Europea en el art. 4 de la Directiva 2013/48/UE[554] *sobre el derecho a la asistencia de letrado en los procesos penales*. Sirviendo como base esta normativa comunitaria, al transponer al derecho interno la misma, los arts. 118.4 y 520.7 LECrim. vienen a establecer que *todas las comunicaciones entre el investigado o encausado y su abogado tendrán carácter confidencial,* para lo cual, el Juez deberá ordenar la eliminación de la grabación o la entrega al destinatario de la correspondencia detenida, cuando las conversaciones o comunicaciones con los operadores jurídicos hubieran sido captadas o intervenidas durante la ejecución de alguna medida restrictiva de derechos fundamentales[555].

No obstante, conviene precisar que cuando se constate *la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal,* la norma procesal permite restringir la confidencialidad de las comunicaciones entre el abogado y su cliente, todo ello, *sin perjuicio de lo dispuesto en la Ley General Penitenciaria* (art. 118.4 y 520.7 LECrim.), en la cual, establece que únicamente podrán intervenirse estas comunicaciones mediante *autorización judicial y en los supuestos de terrorismo* (art. 51.2 LOGP y 48.3 del Reglamento). Es por ello que, la legislación

---

abogado y cliente, intromisión legítima en el derecho a la defensa*"*. Actualidad jurídica Aranzadi. Núm. 795. 2010. Págs. 1-6.

[554] Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, *sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad* («DOUE» Núm. 294, de 6 de noviembre de 2013), en el art. 4 dispone que, "los Estados miembros respetarán la confidencialidad de las comunicaciones entre los sospechosos o acusados y sus letrados".

[555] Sobre las comunicaciones del abogado con su cliente reguladas en los arts. 118.4 y 520.7 LECrim, véase, MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 104-108.

procesal y penitenciaria comentada, permite realizar injerencias en las comunicaciones entre el operador jurídico y su patrocinado, cuando existan indicios de la comisión de algún delito del propio abogado, o bien, cuando se trata de un supuesto de terrorismo.

Estrechamente relacionado con lo anterior, traemos a colación la sentencia del Tribunal Supremo[556], por la cual, se condenaba en única instancia al Magistrado-Juez titular del Juzgado Central de Instrucción nº 5 de la Audiencia Nacional[557]. Dada su importancia en relación con lo que venimos exponiendo, seguidamente vamos a realizar un breve resumen de los hechos que tuvieron lugar. De esta manera, en el seno de una investigación por delitos fiscales, blanqueo de capitales, falsedad, cohecho, tráfico de influencias y asociación ilícita, mediante auto de fecha 19 de febrero de 2009, el Magistrado-Juez adoptaría como medida de investigación tecnológica de observación de las comunicaciones que mantuvieran los abogados con su cliente en el Centro Penitenciario Madrid V (Soto del Real), y en concreto, la aludida resolución establecía el siguiente tenor literal: "*la observación de las comunicaciones personales que mantengan los citados internos con los letrados que se encuentran personados en la causa u otros que mantengan entrevistas con ellos, y con carácter especial, las que mantengan con el letrado D. José Antonio López Rubal, previniendo el derecho de defensa, en el Centro Penitenciario en que se encuentran, o cualesquiera otros donde se trasladen, con la coordinación de la Dirección de dichos Centros, así como de forma general con la Dirección General de Instituciones Penitenciarias, debiendo la Unidad encargada de la investigación disponer los medios necesarios para llevar a cabo dicha intervención en los citados Centros, por un periodo comprendido desde el 19.02.09*

[556] STS 79/2012, de 9 de febrero.

[557] Sobre el procedimiento penal por los delitos de prevaricación (art. 446.3º CP) e interceptación de las comunicaciones o utilización de artificios técnicos de escuchas por funcionario público, mediando causa por delito (art. 536, párrafo primero CP) cometido por el ex Magistrado-Juez titular del Juzgado Central Nº 5 de la Audiencia Nacional, véase, MARTÍNEZ ALARCÓN, M. L. "Sobre la condena por prevaricación del magistrado Baltasar Garzón por la intervención de las comunicaciones autorizada con ocasión de la instrucción de la Sala de lo Penal del Tribunal Supremo de 9 de febrero de 2012". Estudios de Deusto: Revista de la Universidad de Deusto. Vol. 60. Núm. 1. 2012. Págs. 273-301; JESÚS DOLZ LAGO, M. "Condena del Juez Garzón por las «escuchas del caso Gürtel*"*. Diario La Ley. Núm. 7889. 2012; MONTERO HERNANZ, T. "La intervención de comunicaciones en el ámbito penitenciario. A propósito de las escuchas del caso Gürtel*"*. Diario La Ley. Núm. 7335. 2010.

hasta el 20.03.09 (ordinal segundo parte dispositiva)*"*. Posteriomente, en fecha 20 de marzo de 2009, volvería a adoptar un segundo auto, en el que se ordenaba que continuase con la grabación de las escuchas, acordando la prórroga de las intervenciones, en el cual, se decía expresamente: *"Ordenar la Prórroga de la observación de las comunicaciones personales que mantengan los citados internos con los letrados que se encuentran personados en la causa u otros que mantengan entrevistas con ellos, previniendo el derecho de defensa, en el Centro Penitenciario en que se encuentran, o cualesquiera otros donde se trasladen, con la coordinación de la Dirección de dichos Centros, así como de forma general con la Dirección General de Instituciones Penitenciarias, debiendo la Unidad encargada de la investigación disponer los medios necesarios para llevar a cabo dicha intervención en los citados Centros, por un periodo comprendido desde el 20.03.09 hasta el 20.04.09"* (ordinal segundo parte dispositiva). Finalmente, en fecha 27 de marzo de 2009 dictaría nuevo auto en el que acordaba *"excluir de esta pieza las transcripciones de las conversaciones mantenidas entre los imputados Francisco Correa Sánchez, Pablo Crespo Sabaris y Antoine Sánchez y sus letrados y que se refieran en exclusiva a estrategias de defensa*". De este modo, como hemos examinado anteriormente, la legislación penitenciaria permite intervenir las comunicaciones de los internos, mediante *autorización judicial y en los supuestos de terrorismo* (art. 51.2 LOGP y 48.3 del Reglamento), y aunque en el momento de acordarse los autos por el Juzgado Central Nº 5 de la Audiencia Nacional (19.02.2009 y 20.03.2009), la norma procesal no contenía regulación alguna sobre las intervenciones entre los abogados y sus clientes, pues la inclusión de los arts. 118.4 y 520.7 LECrim. se produciría bastante después, con arreglo a la L.O. 13/2015, de 5 de octubre, lo cierto es que, nada impediría acordar alguna medida restrictiva de los derechos fundamentales, para investigar también la actividad ilícita de abogados, pues éstos, no ostentan prerrogativas o patente de corso para la comisión de delitos. De forma que, la adopción de la diligencia únicamente se podía acordar para la investigación de delitos cometidos por el abogado o de terrorismo, si bien, este último queda descartado, pues como decimos, se pretendía averiguar y descubrir delitos de corrupción. Sin embargo, el auto de autorización judicial de la medida y su prórroga que acordaba la medida de injerencia en las comunicaciones alcanzaba al letrado personado *en la causa u otros que mantengan entrevistas con ellos*, de suerte que, se intervenían las comunicaciones de todos los abogados que tuviera el investigado, pero además, de tantos otros que pudiera tener el mismo en el futuro. Por este motivo, la sentencia objeto

de estudio, vino a concluir que, existía un atentado contra el derecho de defensa, pues la medida no se limitaba a investigar a un abogado concreto que pudiera haber participado en una actividad ilícita, sino que, con ello, se impedía la confidencialidad entre el investigado y de cualesquiera otros abogados que pudieran tener el mismo, como dando a entender que, todos los operadores jurídicos pudieran ser potenciales delincuentes. En consecuencia, se condenaría al mismo a un delito de prevaricación (art. 446.3º CP) en concurso aparente de normas (artículo 8.3 CP) con un delito de interceptación de las comunicaciones o utilización de artificios técnicos de escuchas por funcionario público, mediando causa por delito (art. 536, párrafo primero CP), pues las resoluciones fueron acordadas a sabiendas de ser injustas, toda vez que la condición de Juez es de técnico en Derecho, de tal forma que, se le presume conocedor del Derecho y de la ciencia jurídica «*iura novit curia*» (STS 79/2012. F.D. 6º), así como, en los autos de 19 de febrero de 2009 y de 20 de marzo de 2009 con la *inclusión de la cláusula previniendo el derecho de defensa,* y en el auto de 27 de marzo de 2009 acordando excluir *las transcripciones de las conversaciones mantenidas entre los imputados y sus letrados y que se refieran en exclusiva a estrategias de defensa,* revelan que sabía que sus resoluciones afectarían a este derecho[558].

5. Utilización de dispositivos o medios técnicos de geolocalización

a) Introducción

Seguidamente vamos a examinar la medida tecnológica de utilización de dispositivos o medios técnicos de seguimiento y localización (art. 588 quinquies b. LECrim.), o también conocidas como "balizas", lo cual, tiene su importancia a los efectos de conocer el lugar donde se encuentra el investigado. Lo que puede ser de gran utilidad

[558] STS 79/2012, de 9 de febrero… O.P. Cit. (F.D. 2º) dispone que, "el acusado sabía cuáles eran las consecuencias necesarias de las dos resoluciones que dictó. La inclusión de la cláusula previniendo el derecho de defensa, dejando a un lado su efectividad, revela que sabía que su resolución afectaría a este derecho. El propio tenor literal de los autos lo acredita, al referirse a todos los letrados personados y a otros que mantengan entrevistas con los internos, lo cual, gramaticalmente, al no establecerse excepción alguna, afecta a todos los personados, estén imputados o no, y por lo tanto, existan, o no existan, contra ellos indicios de actividad criminal, y a todos los letrados que se personen en el futuro, con independencia de su identidad, y nuevamente con independencia de que existan o no indicios de actividad criminal contra ellos".

para el esclarecimiento de algún hecho delictivo. Sin embargo, no debemos confundir las "balizas" con la geolocalización, como dato asociado a una comunicación que permite identificar la localización de un terminal móvil (art. 3.1.f) Ley 25/2007) que, como hemos estudiado anteriormente, se tratan de datos conservados por las operadoras de telecomunicaciones, y que pueden ser cedidos con el oportuno plácet judicial [arts. 588.2 ter b, 588.2.c) ter d, 588 ter e. y 588 ter j. LECrim. y 6.1 y 7 Ley 25/2007][559].

La medida que ahora analizamos consiste en la instalación de un dispositivo técnico que, durante un plazo determinado, permite conocer la localización geográfica del investigado (art. 588 quinquies b. LECrim.), de forma que, la geolocalización de los terminales móviles mediante los datos asociados a una comunicación ha sido estudiado dentro del epígrafe dedicado a la interceptación de las comunicaciones telefónicas o telemáticas.

Una vez realizada las aclaraciones oportunas, cabe mencionar que, la tecnología permite la utilización de diferentes medios técnicos, que hacen posible con gran exactitud conocer la ubicación de las personas u objetos, de tal forma que, las "*balizas*" atienden a la idea de un dispositivo electrónico oculto que genera información sobre la localización, y que, a través de las señales que emite, permite realizar un seguimiento remoto de determinado objeto a través de un dispositivo receptor. Las "*balizas*" pueden

[559] En relación a la geolocalización como medida de investigación penal, véase, PEREZ GIL, J. *Los datos sobre localización geográfica en la investigación penal. (Protección de datos y proceso penal)*. Edit. La Ley. 2013. Págs. 491-571; LÓPEZ JIMÉNEZ, D. CARLOS DITTMAR, E. *Internet móvil y geolocalización, nuevos retos para la privacidad en la era digital. (La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica)*. Editorial Thomson Reuters Aranzadi. 2013. Págs. 519-542; PEREZ GIL, J. *Nuevas técnicas de obtención de información: intervención de comunicaciones, datos de localización, obtención de pruebas electrónicas, videovigilancia. El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento. (El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito)*. La Ley. Madrid. 2013. Págs. 255-328; VÁZQUEZ ROMERO, R. *De geolocalización y práctica probatoria, condenados a encontrarse. (La prueba electrónica: validez y eficacia procesal)*. Editorial Juristas con Futuro. Madrid. 2016. Pág. 116, de modo que, todos ellos, vienen a diferenciar entre las "balizas" de localización y seguimiento, de la geolocalización como dato asociado a una comunicación.

ser de diferentes clases, de las cuales, las más frecuentes son los que se detallan a continuación[560]:

- El sistema global de navegación por satélite (*Global Navigation Satellite System* –GNSS-), son un grupo de satélites que transmiten señales para determinar el posicionamiento y localización del dispositivo, de tal forma que, permiten determinar las coordenadas geográficas y la altitud de un punto dado como resultado de la recepción de señales provenientes de dichos satélites.

- El sistema de posicionamiento global (*Global Positioning System* –GPS-) es un sistema que también mediante la utilización de satélites, permite determinar con una alta precisión la posición de un objeto[561].

---

[560] Acerca de la tecnología que se puede aplicar en las "balizas", véase, PEDRAZ PENALVA, E. *Protección de Datos y Proceso Penal*. Editorial La Ley. Madrid. 2010. Págs. 307-354.

[561] Afirma RODRÍGUEZ LAINZ, J. L. "GPS y balizas policiales*"*. Diario La Ley. Núm. 8416. 2014, que, "el GPS es en sí un dispositivo de almacenamiento masivo de datos; con una alta capacidad de conservación, especialmente cuando le añadimos o introducimos una tarjeta de memoria. Como tal dispositivo, puede tener capacidad para conservar infinidad de datos e informaciones. Con solo adentrarnos en la finalidad propia del dispositivo, es decir: la gestión de localización geográfica del terminal y el apoyo a la navegación por rutas preestablecidas o en modo de navegación libre; un concienzudo análisis de la información que se conserva nos permitiría realizar un perfil de hábitos de personalidad de su usuario, que incluso nos facilitaría llegar a conclusiones sobre auténticos datos sentibles". Asimismo, continúa afirmando el MISMO AUTOR. "Los dispositivos electrónicos de posicionamiento global (GPS) en el Proceso Penal*"*. Diario La Ley. Núm. 7945. 2012, que, "bajo el acrónimo GPS (Global Positioning System) se esconde un universo tecnológico que ha revolucionado nuestra propia forma de vida en pocos años. El sistema de posicionamiento se nutre de momento de una red de 24 satélites denominada NAVSTAR. La interactuación del mayor número posible de satélites con aparatos receptores, dispositivos electrónicos de posicionamiento, que han venido a ser denominados comercialmente GPS, permiten localizar la prácticamente exacta ubicación del receptor en cualquier punto del planeta, y bajo cualquier condición meteorológica. La tecnología GPS, implementada con la futura interoperatividad del sistema Galileo, opera a través del espectro radioeléctrico, valiéndose de radiofrecuencias habilitadas y reservadas específicamente para tal menester; de suerte que cualquier receptor puede acceder libremente a ellas, y valerse de la información que facilitan los satélites, a modo de balizas, para permitir su localización". Por su parte, mantiene VELASCO NÚÑEZ, E. "Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.la prueba tecnológica*"*. Diario La Ley. Núm. 8183. 2013, que, "una de las aplicaciones que hoy en día incorporan

- Los sistemas de localización en tiempo real (*Real-Time Locating System* –RTLS-) son sistemas que monitorizan la posición de un elemento móvil mediante la utilización de tecnología de alta frecuencia, siendo lo habitual, la comunicación por radiofrecuencia, aunque también algunos sistemas usan tecnologías ópticas (infrarrojas) o acústicas (ultrasonido) alternativamente o conjuntamente con la radiofrecuencia.

- Los sistemas de identificación por radiofrecuencia (*Radio Frequency Identification* –RFID-) son sistemas que permiten el almacenamiento y recuperación de datos remotos mediante la utilización de dispositivos denominados etiquetas, tarjetas o transpondedores, de tal forma que, con la colocación de estos dispositivos de pequeño tamaño hace posible transmitir a través de sus antenas la identidad de un objeto (similar a un número de serie único) mediante ondas de radio.

- La localización por sistema global para las comunicaciones móviles (*Global System for Mobile communications* –GSM-) se trata de una tecnología utilizada por las empresas operadoras de telefonía móvil, el cual, hace posible determinar, con cierta precisión, donde se encuentra físicamente un terminal. De este modo, las estaciones base (*Base Transceiver Station* –BTS-) que disponen de equipos con transmisores y receptores de radio, hacen posible, la conexión entre los usuarios de telefonía móvil, de tal forma que, acudiendo a los datos proporcionados por estas estaciones (BTS), será posible conocer con precisión la localización del terminal donde está emitiendo o recibiendo la señal de comunicación. Por su parte, el uso habitual de la tecnología GSM es para proporcionar conexión a los usuarios de telefonía, de tal forma que, estas empresas utilizan los datos de localización para fines comerciales o para determinar la tarifa aplicable. Sin embargo, lo importante aquí, será que la información proporcionada por la empresa de telefonía no corresponda a datos

---

muchos terminales telecomunicativos es el vulgarmente llamado GPS, de gran utilidad para el investigador en principio en el campo de la geolocalización (para conocer el posicionamiento, ubicación espacial y temporal exacta del receptor bajo cualquier condición meteorológica), pero también importante a la hora de obtener datos (distancias, horarios, kilometraje, itinerario, incidencias e infracciones en el tráfico, por ejemplo) importantes para la investigación". En el mismo sentido, traemos a colación, MISMO AUTOR, *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 287-293.

asociados a una comunicación, puesto que, en este caso, el régimen jurídico aplicable, como nos hemos referido, será el estudiado anteriormente.

Tras haber realizado una breve introducción, seguidamente vamos a examinar la regulación contenida en la Ley de Enjuiciamiento Criminal sobre la medida tecnológica de "balizas" de localización y seguimiento, y en concreto, la autorización judicial, en el cual, haremos una mención especial a los derechos fundamentales afectados por la diligencia, los supuestos de urgencia que hacen posible que se posponga la intervención judicial, así como, el deber de colaboración, la duración, el control de la medida y la destrucción de los archivos.

b) La autorización judicial: los derechos fundamentales afectados por la medida

Primeramente advertir que, la medida de utilización de dispositivos técnicos de seguimiento y de localización no supone una comunicación en el sentido referido en nuestra Constitución (art. 18.3 CE)[562], sino que incide en la capacidad de las personas en situarse en un punto geográfico con la convicción de que su localización no va a ser conocida y tratada por terceros, debido a lo cual, la afectación en los derechos fundamentales se produce en la intimidad personal (art. 18.1 CE), y en su caso, en la autodeterminación informativa o protección de datos personales (art. 18.4 CE). Por su parte, la afectación en la intimidad se produce debido a que el investigado se somete a un seguimiento minimizando el riesgo de ser descubierto, en relación con los seguimientos policiales convencionales[563]. De esta manera, la utilización de "*balizas*"

[562] C. 4/2019, de 6 de marzo, F.G.E, («BOE» Núm. 70, de 22 de marzo de 2019). O.P. Cit… en la conclusión novena, dispone que, "el conocimiento de datos de geolocalización del investigado a través de dispositivos técnicos supone una limitación de su derecho a la intimidad, pero no de su derecho al secreto de las comunicaciones. Como regla general, se trata de una limitación de baja intensidad, lo que deberá tener su reflejo en el juicio de proporcionalidad que se lleve a cabo en la resolución judicial que autorice la medida".

[563] En relación con la medida de seguimiento y localización por "balizas" realizada por la policía, afirma, VELASCO NÚÑEZ, E. "Tecnovigilancia, geolocalización y datos aspectos procesales penales*"*. Diario La Ley. Núm. 8338. 2014, que, "podríamos pensar que su uso no añade a las clásicas vigilancias policiales presenciales más que la ventaja de la reserva y el abaratamiento de costes y de medios, pues el GPS realiza tecnológicamente los seguimientos que antes debían hacer durante horas o días concretos funcionarios policiales o detectives privados, y que como se desarrollan sobre actividad desplegada en la

como método de *tecnovigilancia* no supone una comunicación (art. 18.3 CE), sino que despliega su injerencia en el ámbito del derecho a la intimidad (art. 18.1 CE), la Constitución española no exige expresamente el oportuno plácet judicial. En este sentido, el Tribunal Europeo de Derechos Humanos ha venido manteniendo que, la colocación de dispositivos de geolocalización por la policía no supone una injerencia en el secreto de las comunicaciones, sino que en todo caso, se vería afectado el derecho al respeto de la vida privada (art. 8.1 Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales), pues la finalidad de la utilización de la "*baliza*" es pretender observar los desplazamientos del investigado, por lo que guardaría relación con la cotidianeidad de la vida privada del mismo. Además, el TEDDHH viene a considerar que, la medida estará justificada y será proporcional para delitos de especial gravedad, como el terrorismo, pues para este caso, no existirá violación al derecho a la vida privada (art. 8.1 CEDH), y en consecuencia, se podrían utilizar los datos obtenidos de la "*baliza*" de seguimiento, sin necesidad de recabar autorización judicial, salvo que se estableciera otro criterio en las legislaciones internas de los Estados (art. 8.2 CEDH)[564].

---

calle, no afectan a la privacidad y son perfectamente legítimas desde una perspectiva meramente probatoria. Sin embargo, las balizas a veces penetran ámbitos privados (garajes, fincas particulares) de los que su sistema GPS puede aportar información que va más allá de la que podría aportar el vigilante sin mandamiento judicial, y si como dice la citada STS EE.UU. Katz vs. US, 389 US 347 (de) 1967: «lo que una persona conscientemente expone en público, aunque sea en su casa u oficina, no es objeto de protección (de la privacidad) por la 4.ª enmienda», parece lógico afirmar su contrario, predicándose que debe protegerse lo que uno se empeña «razonablemente» en excluir del conocimiento de los demás". En el mismo sentido, véase, RELLANO TOLEDO, W. *Cooperación internacional y TIC, geolocalización, cibercrimen y derechos fundamentales (FODERTICS 4.0: estudios sobre nuevas tecnologías y justicia: "IV Fórum de expertos y jóvenes investigadores en derecho y nuevas tecnologías, celebrado en la Facultad de Derecho de Salamanca, en 2015")*. Editorial Comares. Granada. 2015. Págs. 175-186; TORRE OLID, F. "Tecnología de geolocalización y seguimiento al servicio de la investigación policial. Incidencias sobre el derecho a la intimidad*"*. Revista de Derecho y Criminología. Núm. 2. 2012. Págs. 58-99.

[564] STEDDHH, de 2 de septiembre de 2010 (asunto Uzun Vs. Alemania), dispone en el párrafo 80 que, "la vigilancia por GPS del demandante, tal como se efectuó en las circunstancias del caso, era proporcional a los objetivos legítimos perseguidos y por lo tanto «necesarios en una sociedad democrática», en el sentido del artículo 8 párrafo 2".

Por su parte, nuestro Tribunal Supremo venía entendiendo que, la colocación de "*balizas*" de seguimiento no producía injerencias en la intimidad (art. 18.1 CE), pues según su criterio, se trataba de una diligencia de investigación, legítima desde la función constitucional que tiene la Policía Judicial en la averiguación del delito y descubrimiento y aseguramiento del delincuente (art. 126 CE), por lo que su colocación no suponía injerencias en los derechos fundamentales que exijan la intervención judicial[565], pues, aparte del secreto de las comunicaciones (art. 18.3 CE), tampoco afectaría a la inviolabilidad domiciliaria (art. 18.2 CE)[566] o a la libertad ambulatoria (art. 19 CE)[567]. De esta manera, nuestro Tribunal nomofiláctico, llegaría a afirmar que[568], *el uso de radiotransmisores (balizas de seguimiento GPS), no vulnera el derecho fundamental al secreto de las comunicaciones o supone una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo y una ponderación sobre dicha afectación constitucional*, si bien, cabe precisar que, la resolución aludida se refería a embarcaciones marítimas, por lo que no dejaba claro si era de aplicación también a transportes terrestres, como por ejemplo el vehículo conducido por el investigado.

Sin embargo, independientemente de todo lo comentado, la legislación procesal implementada mediante la reforma llevada a cabo por la Ley Orgánica 13/2015, de 5 de octubre[569], ha venido a otorgar las mayores garantías, de tal forma que, se establece la obligatoriedad de autorización judicial para la adopción de la medida de utilización de

[565] STS 562/2007, de 22 de junio (F.D. 2º) y STS 906/2008, de 19 de diciembre (F.D. 1º) disponen que, la colocación de baliza de seguimiento no afecta al derecho a la intimidad.

[566] STS 523/2008, de 11 de julio (F.D. 7º) dispone que la baliza de seguimiento y localización no afecta a la inviolabilidad del domicilio, pues "no consta que para situar el artilugio fuera necesario entrar en algún recinto que constituyera un domicilio de los previstos en los arts. 554 o 561 LECr".

[567] STS 55/2007, de 23 de enero (F.D. 6º) dispone que la colocación de baliza no produce injerencia en el derecho a la libertad ambulatoria y, en consecuencia, no precisa de autorización judicial.

[568] STS 798/2013, de 5 de noviembre (F.D. 11º) y STS 610/2016, 7 de julio (F.D. 1º).

[569] «BOE» Núm. 239, de 6 de octubre de 2015.

dispositivos de seguimiento o "*balizas*"[570] (art. 588.1 quinquies b. LECrim.)[571]. Sin embargo, la norma no específica qué clase de delitos pueden objeto de esta medida, por lo que, el Juez podrá acordarla para cualquier delito, siempre que concurran razones de necesidad y proporcionalidad. De igual modo, la propia resolución deberá concretar el medio técnico que va a ser utilizado (GNSS, GPS, RTLS, etc.) todo ello, a los efectos de control y para evitar cualquier confusión o posibles cambios en la información (art. 588.2 quinquies b. LECrim.).

c) Los supuestos de urgencia que hacen posible que se posponga la intervención judicial

Como hemos examinado anteriormente, la autorización judicial es necesaria para la utilización de dispositivos técnicos de localización y seguimiento o "*balizas*". Sin embargo, cuando concurran situaciones de urgencia, que hagan razonablemente temer que de no colocarse inmediatamente el dispositivo, podría verse frustrada la investigación, se permite a la Policía Judicial, la colocación del mismo, dando cuenta a la autoridad judicial a la mayor brevedad posible, y en todo caso, en el plazo máximo de veinticuatro horas, el cual, podrá ratificar, o bien, acordar el cese, en este último supuesto, la información obtenida carecerá de efectos en el proceso (art. 588.4 quinquies b. LECrim.). De esta manera, se pospone la intervención judicial por razones de urgencia, de tal forma que, tras la instalación del dispositivo técnico, en un breve plazo de tiempo, la Policía Judicial deberá remitir un oficio al Juez competente, informando de las razones que han llevado a la utilización de la "baliza", así como justificando los motivos de su colocación sin autorización judicial previa, el cual, deberá valorar la pertinencia de la medida, para lo cual, deberá dictar un auto ratificando o

[570] En relación a la medida de utilización de dispositivos o medios técnicos de seguimiento y localización, con arreglo a la reforma procesal implementada con la L.O. 13/2015, afirma, REYES LÓPEZ, J. I. "Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la LO 13/2015*"*. Revista Aranzadi Doctrinal. Núm. 4. 2016. Págs. 53-66 y el MISMO AUTOR, "El nuevo régimen jurídico de los dispositivos de geolocalización a partir de la ley orgánica 13/2015*"*. Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 135. 2016. Págs. 73-94, que, "cualquier artificio técnico de geolocalización que tenga una relación directa o indirecta con una persona y por lo tanto pueda afectar al derecho a la intimidad, exige indefectiblemente autorización judicial a partir del 6 de diciembre de 2015".

[571] Sírvase de ejemplo de la instalación de dispositivos de seguimiento y localización en vehículos mediando resolución judicial, SAP de Ciudad Real (Sección 2ª) Núm. 8/2019, 2 de abril (F.D. 1º).

cesando la medida. Esto es debido a que con frecuencia, en los seguimientos policiales será necesario la utilización de "balizas" de forma inmediata, pues si hubiera que esperar a que el Juez la acordara, seguramente perjudicaría a su efectividad (por ejemplo en una vigilancia o seguimiento físico se prevea que el vehículo o embarcación va a partir de forma inminente).

Ahora bien, a nuestro parecer, tal y como ya se ha manifestado la doctrina, dejar la intervención judicial para un momento posterior, puede originar "corruptelas" policiales en el sentido de que, puedan ser utilizadas las "balizas" de manera indiscriminada y remitir el oficio, únicamente cuando pretendan judicializar la medida. En cualquier caso, superando la tradicional jurisprudencia comentada *supra*, la cual, exoneraba del plácet judicial para la utilización de "balizas", el legislador ha despejado toda duda, exigiendo ahora autorización judicial, incluso con posterioridad a su colocación[572].

d) El deber de colaboración

De esta manera, los prestadores de servicios de telecomunicaciones o de servicios de la sociedad de la información, así como cualquier otra persona física o jurídica tienen la obligación de prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial, la asistencia y colaboración precisas para facilitar el cumplimiento de la medida de localización o seguimiento (arts. 588.3 quinquies b. en relación con el 588 ter e.

[572] Con carácter general, acerca de la exigencia de autorización judicial para la colocación de balizas de seguimiento, véase, NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*. Editorial Tirant lo Blanch. Valencia. 2017. Págs. 909-914; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Págs. 114-119; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 360-370; 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. Núm. 17. 2015; GÓMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización*… O.P. Cit. 2015. Págs. 228-230.

LECrim.), bajo apercibimiento de incurrir en delito de desobediencia (art. 556 CP)[573]. De este modo, como hemos estudiado *supra* en la introducción, las "balizas" pueden utilizar diferentes tecnologías, es por ello que, para ejecutar la medida podría ser necesaria la colaboración de empresas que prestan éstos servicios, por ejemplo en la localización mediante la tecnología GSM, en la cual, se pretenda realizar un seguimiento de un terminal móvil utilizado por el investigado, para lo cual, habría que acudir a la empresa operadora del servicio de telecomunicaciones para que mediante la información proporcionada por las estaciones base BTS, pueda averiguarse las coordenadas geográficas del dispositivo.

e) La duración, el control de la medida y la destrucción de los archivos

La medida de colocación de dispositivos técnicos de localización y seguimiento o "balizas" tendrá una duración máxima de tres meses a partir de la fecha de su autorización, pero excepcionalmente, cuando estuviera justificado a la vista de los resultados obtenidos, el Juez podrá acordar prórrogas sucesivas por el mismo o inferior plazo, hasta un máximo de dieciocho meses (art. 588.1 quinquies c. LECrim.). De este modo, el plazo ordinario máximo será de tres meses, pues la propia naturaleza de la medida hace que, lo habitual sea realizar un seguimiento para un momento puntual, y el plazo de duración mencionado sea más que suficiente para obtener los resultados esperados, si bien, cuando estuviera justificada la ampliación de la medida (por ejemplo una embarcación que tarda varios meses en realizar su recorrido marítimo), se podrá acordar un mayor sacrificio en la intimidad, todo ello, hasta el máximo referido.

Por otro lado, a los efectos de control de la medida, la Policía Judicial deberá entregar al Juez competente los soportes originales o copias electrónicas auténticas que contengan la información recogida cuando éste lo solicite y, en todo caso, cuando terminen las investigaciones (art. 588.2 quinquies c. LECrim.). A su vez, no se exige la transcripción de los datos obtenidos, como sucede en la medida de intervención en las comunicaciones (art. 588 ter f. LECrim.), pues, como cualquier seguimiento policial, lo normal será que, las alusiones a la utilización de la "baliza", se haga en el propio

[573] BERMÚDEZ GONZÁLEZ, J. A. *El deber de colaboración de particulares*… O.P. Cit. Págs. 473 - 508; RODRÍGUEZ LAINZ, J. L. "Las bases de datos comerciales relativas a las comunicaciones electrónicas como fuente probatoria en el proceso penal…" O.P. Cit.

atestado, pudiendo valerse, además, de algún informe pericial que explique la técnica utilizada para su ejecución. De la misma manera, la información obtenida deberá ser debidamente custodiada para evitar su utilización indebida, de tal forma que, esta alusión que hace la norma procesal (art. 588.3 quinquies c. LECrim.), puede interpretarse que, la diligencia objeto de estudio incide en la intimidad, pues en caso contrario, no se tomarían tantas precauciones.

Por último, la destrucción del material se verificará con arreglo al régimen general (art. 588 bis k. LECrim.), esto es, el Juez ordenará el borrado o eliminación de los registros originales una vez que se ponga término al procedimiento mediante resolución judicial firme, debiendo el Letrado de la Administración de Justicia custodiar[574] una copia durante 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, siempre que a juicio del Tribunal no fuera precisa su conservación por tiempo superior.

6. Entrada o registro domiciliario

a) Introducción

Primeramente, es necesario precisar que, aunque la diligencia de investigación de entrada o registro domiciliario no se trata de una medida tecnológica, y por tanto, teóricamente poco tendría que ver con el objeto del presente trabajo, lo cierto es que, hemos decido dedicar unas líneas a su análisis, pues los órganos jurisdiccionales, con frecuencia, acuerdan esta medida conjuntamente con el registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.), la cual, ésta última, indudablemente tiene incidencia con las nuevas tecnologías, si bien, será estudiada en el epígrafe siguiente.

De esta manera, la entrada y registro domiciliario viene regulada en la Ley de Enjuiciamiento Criminal, bajo la rúbrica *de las Medidas de Investigación Limitativas de*

[574] Sobre la custodia por el LAJ de las cintas o grabaciones, véase, ORTUÑO NAVALÓN, M. C. *Aspectos procesales de la prueba electrónica. Procesos penales. Garantías de conservación y custodia. (La prueba electrónica ante los tribunales)*... O.P. Cit. Págs. 101-103.

los Derechos reconocidos en el Artículo 18 de la Constitución (Título VIII), de acuerdo con la reforma implementada mediante la Ley Orgánica 13/2015, de 5 de octubre[575]. De esta forma, seguidamente vamos a examinar en el presente epígrafe los registros domiciliarios físicos, esto es, la entrada y registro en lugar cerrado (arts. 545 a 572 LECrim.), para continuar posteriormente analizando los registros virtuales del investigado, que vienen regulados dentro de las medidas tecnológicas creadas con arreglo a la reforma procesal implementada con la L.O. 13/2015, en concreto, el registro de dispositivos de almacenamiento masivo de información (arts. 588 sexies LECrim.) y los registros remotos sobre equipos informáticos (arts. 588 septies LECrim.).

b) Entrada y registro en lugar cerrado

Nuestra Constitución (art. 18.2 CE), viene a establecer que, únicamente se puede acceder o registrar un domicilio[576] cuando concurran los supuestos de consentimiento del titular, mediante autorización judicial o exista flagrancia delictiva[577]. Por este motivo, seguidamente analizaremos por separado los tres.

---

[575] «BOE» Núm. 239, de 6 de octubre de 2015.

[576] En relación con el registro domililiario, véase, GÓMEZ COLOMER, J. L. *Diligencia de entrada y registro en lugar cerrado…* O.P. Cit. Págs. 223-228; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada…* O.P. Cit. Págs. 719-785; MORENO CATENA, V. *Actos de investigación que afectan a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones…* O.P. Cit. Págs. 271-275; MARTÍN RÍOS, M. P. *Diligencia de entrada y registro en lugar cerrado. Nociones preliminares de derecho procesal penal para criminólogos…* O.P. Cit. 2017. Págs. 89-94; VÁZQUEZ IRUZUBIETA, C. *De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución. (Comentario a la Ley de Enjuiciamiento Criminal, actualizada por las Leyes 13/2015, y 41/2015, de 5 de octubre)*. Editorial VLex. Madrid. 2015. Pág. 455-480; PÉREZ GÓMEZ, R. "La diligencia de entrada y registro. Requisitos jurisprudenciales*"*. Revista de Derecho VLex. Núm. 138. 2015; DURÁN SILVA, C. "La diligencia de entrada y registro: su necesaria adaptación a la realidad actual. La reforma del proceso penal*"*. Edit. La Ley. 2013. Madrid. Págs. 351-421; FIGUEROA NAVARRO, M. C. "La obtención de pruebas mediante la entrada y registro en domicilio*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 91. 2012. Pág. 2.

[577] Con carácter general acerca de los presupuestos para acceder a un domicilio, véase, CABEZUDO BAJO, M. J. "El uso de las tecnologías en la entrada y el registro domiciliario. Cambio en su concepción tradicional y nuevos retos en la protección de los derechos fundamentales afectados*"*. Revista de Derecho Penal y Criminología. Núm. 15. 2016. Págs. 53-93; HERNÁNDEZ DOMÍNGUEZ, J. J. "Supuestos

a´. El consentimiento del titular

Se puede acceder o registrar un domicilio cuando su titular presta libre y voluntariamente consentimiento para ello (art. 545 LECrim. en relación con el art. 18.2 CE), si bien, podrá prestarse de forma expresa (por ejemplo, firmando un documento), pero también se admite tácita, cuando se presuma debido a que el titular exteriorice actos que revelen su consentimiento y no invoque el derecho fundamental a la inviolabilidad del domicilio (art. 551 LECrim.). Sin embargo, autores como López Barja de Quiroga[578], mantienen que los derechos fundamentales son de carácter indisponible, de tal forma que, deben respetarse, independientemente de su invocación, pues según el propio autor, la dispensa de los derechos consagrados en la Constitución, únicamente pueden prestarse mediante consentimiento expreso y tras ser informado el interesado de todas las consecuencias jurídicas de su decisión. Por este motivo, el consentimiento tácito o presunto debe interpretarse de forma restrictiva, de tal forma que, cuando exista cualquier duda, pues no constan inequívocamente actos propios de no oposición o de colaboración del titular, deberá de resolverse negativamente a la validez de la autorización[579].

---

constitucionales que posibilitan la entrada y registro en domicilio". Revista de Derecho Penal. Núm. 36. 2012. Págs. 97-115; CUCHI DENIA, J. M. *"*La diligencia judicial de entrada y registro, presupuestos constitucionales a la luz de la jurisprudencia*"*. Diario La Ley. Núm. 7354. 2010; GARRIDO LORENZO, M. A. *Derechos fundamentales y doctrina jurisprudencial. Especial referencia a la intervención de las comunicaciones telefónicas y a la diligencia de entrada y registro domiciliario*. Estudios Jurídicos. Ministerio Fiscal. Núm. 1. 2003. Págs. 417-468; RODRÍGUEZ FERNÁNDEZ, R. *La diligencia de entrada y registro como excepción al derecho fundamental de inviolabilidad domiciliaria. Presupuestos y requisitos...* O.P. Cit. Págs. 833-852; FERNÁNDEZ FERNÁNDEZ, J. C. *Entradas y registros domiciliarios, restricción al derecho de la inviolabilidad domiciliaria*. Estudios Jurídicos. Cuerpo de Secretarios Judiciales. Núm. 6. 2001. Págs. 407-442.

[578] Pone de manifiesto, LÓPEZ BARJA DE QUIROGA J., *Tratado de Derecho Procesal Penal…* O.P. Cit. Págs. 1899-1901, que, los derechos fundamentales son indisponibles, de tal forma que, para su dispensa se necesita prestar consentimiento expreso.

[579] STS 922/2010, de 28 octubre (F.D. 4º).

b´. Resolución judicial

Debido a que lo habitual será que el titular no preste consentimiento para acceder o registrar su domicilio, la mayoría de las veces se producirá con autorización judicial[580], incluso si fuera necesario con el auxilio de la fuerza (art. 568 LECrim.), aunque nada impediría a que fuera acordado el oportuno plácet judicial, mediando, además, consentimiento del titular.

c´. Flagrancia

La Constitución española, como nos hemos referido, viene a establecer que, las entradas o registros domiciliarios se practicarán con el consentimiento del titular o mediante autorización judicial, salvo flagrancia delictiva (art. 18.2 CE)[581], de tal forma que, ahora examinaremos esta última excepción. De este modo, el concepto de delito flagrante es definido por el autor Jacobo López Barja de Quiroga[582] *como todo hecho que pueda ser percibido directamente por los sentidos, siempre que se esté lesionando con inmediatez un bien jurídico protegido por el ordenamiento penal*, mientras que, *Julio Banacloche*

[580] MORALES MUÑOZ, E. *Diligencias de investigación en el proceso penal. La diligencia de entrada y registro. Tercer presupuesto: autorización judicial. Procedimiento para su práctica. Efectos de las entradas y registros domiciliarios inconstitucionales*. Boletín del Ministerio de Justicia. Año 61. Núm. 2037. 2007. Págs. 2107-2129; ROBLES ACERA, A. "La autorización judicial y el secretario en las entradas y registros domiciliarios*"*. Actualidad Jurídica Aranzadi. Núm. 43. 1992. Pág. 2; GUTIÉRREZ GONZÁLEZ, C. "Prueba ilícita. Entrada y registro sin previa autorización judicial*"*. Revista General de Derecho. Núm. 552. 1990. Págs. 6375-6391.

[581] En relación a la excepción de la flagrancia delictiva como criterio para entrar o registrar un domicilio, véase, MORALES MUÑOZ, E. *Diligencias de investigación: Registro domiciliario cuestiones generales y consentimiento titular. Situaciones de flagrancia*… O.P. Cit. Págs. 1841-1858; DE LUCCHI LÓPEZ-TAPIA, Y. "Entrada y registro en domicilio, concepto de domicilio y de delito flagrante (TS 2ª S 824/1999, de 19 mayo)*"*. Tribunales de Justicia: Revista Española de Derecho Procesal. Núm. 3. 2000. Págs. 387-390; ALONSO PÉREZ, F. "Concepto de delito flagrante y su relación con la diligencia de entrada y registro en lugar cerrado*"*. La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 6. 1998. Págs. 2253-2255.

[582] LÓPEZ BARJA DE QUIROGA J., *Tratado de Derecho Procesal Penal. Tomo II*… O.P. Cit. Pág. 1956.

Palao[583], se refiere al mismo, como aquel *requisito indispensable para la entrada en un domicilio sin la debida autorización que la situación de comisión del delito sea "evidente", entendiendo por tal lo que es cierto, claro, patente y sin la menor duda.* Asimismo, el Tribunal Constitucional[584] entiende por flagrancia como aquella *situación fáctica en la que el delincuente es "sorprendido" (visto directamente o percibido de otro modo) en el momento de delinquir o en circunstancias inmediatas a la perpetración del ilícito, por lo que la evidencia del delito y urgencia en la intervención policial están presentes en la inviolabilidad de domicilio proclamada en la Constitución, precepto que, al servirse de esta noción tradicional, ha delimitado un derecho fundamental y, correlativamente, la intervención sobre el mismo del poder público. Mediante la noción de "flagrante delito" la Constitución no ha apoderado a las Fuerzas y Cuerpos de Seguridad para que sustituyan con la suya propia la valoración judicial a fin de acordar la entrada en domicilio, sino que ha considerado una hipótesis excepcional en la que, por las circunstancias en las que se muestra el delito, se justifica la inmediata intervención de las Fuerzas y Cuerpos de Seguridad,* de la misma manera, nuestro Tribunal Supremo[585] viene afirmando que, *la flagrancia viene configurada por la evidencia sensorial del hecho delictivo que se está cometiendo o se acaba de cometer en el mismo instante de ser sorprendido el delincuente, siendo así conocida directamente tanto la existencia del hecho como la identidad del autor, percibiéndose al tiempo la relación de este último con la ejecución del delito y dándose evidencias patentes de tal relación,* pero además, continua diciendo que, se perfila con las siguientes notas específicas que lo caracterizan*: 1º inmediatez temporal: es decir, que se esté cometiendo un delito o que haya sido cometido instantes antes; 2º inmediatez personal: consistente en que el delincuente se encuentre allí en ese momento en situación tal con relación al objeto o a los instrumentos del delito que ello ofrezca una prueba de su participación en el hecho; y 3º necesidad urgente de actuación: de tal modo que la policía, por las circunstancias concurrentes en el caso concreto, se vea*

[583] BANACLOCHE PALAO, J. y ZARZALEJOS NIETO, J., *Aspectos Fundamentales de Derecho Procesal Penal…* O.P. Cit. Pág. 185.

[584] STC 341/1993, de 18 de noviembre (F.D. 8º).

[585] STS 631/2005, 16 de mayo, en el F.D. 2º se viene a definir el concepto de flagrancia, y además, alude a las notas que debe reunir.

impelida a intervenir inmediatamente con el doble fin de poner término a la situación existente impidiendo en todo lo posible la propagación del mal que la infracción penal acarrea, y de conseguir la detención del autor de los hechos, necesidad que no existirá cuando la naturaleza de los hechos permita acudir a la Autoridad judicial para obtener el mandamiento correspondiente.

Por su parte, la legislación procesal penal alude a la flagrancia delictiva en las disposiciones reguladoras del registro domiciliario, al establecer que, *los agentes de policía podrán proceder de propia autoridad a la inmediata detención de personas con mandamiento de prisión contra ellas, cuando sean sorprendidas en flagrante delito o cuando un delincuente, inmediatamente perseguido por los Agentes de la autoridad, se oculte o refugie en alguna casa o, en casos de excepcional o urgente necesidad, cuando se trate de presuntos responsables* relacionados con organizaciones o grupos criminales o terroristas, si bien, deberán dar cuenta inmediatamente al Juez, *con indicación de las causas que lo motivaron y de los resultados obtenidos en el mismo, con especial referencia a las detenciones que, en su caso, se hubieran practicado*, indicando además, *las personas que hayan intervenido y los incidentes ocurridos* (art. 553 LECrim). De igual modo, dentro de la regulación sobre el procedimiento para el enjuiciamiento rápido de determinados delitos, se alude a la flagrancia delictiva (art. 795.1.1ª LECrim.), de tal forma que, lo define como aquel delito *que se estuviese cometiendo o se acabare de cometer cuando el delincuente sea sorprendido en el acto. Se entenderá 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* (art. 795.1.1ª LECrim.), sin embargo, aquí flagrancia supone la forma del iniciar o incoar este procedimiento especial, por lo que, difícilmente será de aplicación para la medida de registro domiciliario, pues al afectar a un derecho fundamental, deberá tener un carácter más restrictivo[586].

[586] STS, de 29 marzo 1990 (F.D. 4º).

c) Algunas particularidades observadas en la jurisprudencia y/o doctrina: el hallazago casual

Como se ha mencionado en la parte del presente trabajo dedicada a las disposiciones comunes aplicables a las medidas tecnológicas, el principio de especialidad (apartado 1º y 2º del art. 588 bis a LECrim.) consiste en que la autorización judicial debe especificar el delito concreto objeto de investigación, de tal forma que, habrá que rechazar las intervenciones predelictuales o de prospección[587]. Sin embargo, el problema surge cuando habiéndose adoptado una medida restrictiva de derechos fundamentales para la investigación de un delito concreto se descubre otro distinto no amparado por la autorización judicial. De este modo, no existe justificación alguna para que el funcionario que se encuentre investigando unos hechos de apariencia delictiva cierre los ojos ante los indicios de delito que se presentasen a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial[588]. Por su parte, los agentes de policía tienen siempre el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuvieren conocimiento, practicando incluso las diligencias de prevención que fueran necesarias por razón de urgencia (art. 284 LECrim.)[589], por esta razón, nuestros tribunales vienen dando validez a los elementos probatorios de un determinado delito producido en el curso de una

[587] STS 510/2017, 4 de julio (F.D. 1º), STS 504/2015, de 24 de julio (F.D. 1º) y STS 168/2015, 25 de marzo (F.D. 1º).

[588] Con carácter general, acerca de los hallazgos casuales, véase, NADAL GÓMEZ, I. "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal…" O.P. Cit. Núm. 40. 2016; GARCÍA SAN MARTÍN, J. *El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal (Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas: memorias del Proyecto I.F.O. Illegal Flow Observation JUST/2011/ISEC/DRUGS/AG/3671)…* O.P. Cit. Págs. 309-319; GARCÍA SAN MARTÍN, J. "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal…*"* O.P. Cit. Pág. 10; RIVERO ORTIZ, R. "Hallazgos casuales en los delitos y faltas, nuevos pronunciamientos jurisprudenciales*"*. Diario La Ley. Núm. 7846. 2012; ECHARRI CASI, F. J. "Prueba ilícita, conexión de antijuridicidad y hallazgos casuales*"*. Revista del Poder Judicial. Núm. 69. 2003. Págs. 261-301.

[589] STC 41/1998, de 24 febrero (F.J. 33º), STS 103/2015, 24 de febrero (F.D. 5º), STS 17/2014, 28 de enero (F.D. 5º) y STS 423/2016, 18 de mayo (F.D. 6º).

investigación autorizada para otro delito distinto, cuando la autorización inicial haya reunido todos los requisitos exigibles para ser tenida como correcta[590].

Los hallazgos casuales ya han sido examinados anteriormente, si bien, hay que destacar que, para la medida de registro domiciliario, como veremos, tiene un régimen algo distinto que de otras medidas tecnológicas (arts. 588 bis i. y 579.3 bis LECrim.), como la intervención en las comunicaciones telefónicas y telemáticas. De este modo, como ya se ha analizado, la ley procesal penal con la redacción dada con arreglo a la L.O. 13/2015[591] viene a establecer que, en la diligencia de detención y apertura de la correspondencia escrita y telegráfica (art. 579 bis LECrim.), así como para las medidas tecnológicas, (arts. 588 bis i, por remisión al 579.3 bis LECrim.), entre las que se encuentra la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter LECrim.), para la continuación del delito casualmente descubierto se precisará de autorización judicial, para la cual, éste 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 (art. 579.3 bis LECrim.)[592]. Así, la denominada doctrina jurisprudencial, ahora regulada en la ley procesal, del "hallazgo casual", viene a establecer que, para las medidas de investigación aludidas *supra*, cuando se descubra un delito distinto al previsto en la autorización, precisará de una renovada resolución[593] que contenga los elementos delictivos nuevos y sorpresivos, con los razonamientos que sean precisos, para continuar legalmente con la misma. En cambio, cosa distinta sucede, cuando en la práctica de una diligencia de entrada y registro domiciliario se encuentran hechos delictivos distintos a los previstos en la autorización judicial habilitante. Así, la falta de autorización judicial para el delito nuevo descubierto, no comporta necesariamente la nulidad de la prueba, pues en terminología anglosajona, se produce un descubrimiento inevitable ("*discovery*

[590] STS 768/2007, 1 de octubre (F.D. 1º), STS 981/2003, de 3 julio (F.D. 2º) y STC 41/1998, de 24 febrero (F.J. 22º).

[591] «BOE» Núm. 239, de 6 de octubre de 2015.

[592] Sírvase de ejemplo, SAP de A Coruña (Sección 6ª) Núm. 24/2017, 17 de febrero (F.D. 3º).

[593] STS 681/2013, 23 de septiembre (F.D. 16º), STS 616/2012, 10 de julio (F.D. 2º) y STS 171/2015, 19 de mayo (F.D. 2º).

inevitable")[594]. Por su parte, recuérdese que el art. 18.2 de CE dispone que la entrada o registro domiciliario se podrá realizar con resolución judicial, salvo en caso de *flagrante delito.* Por este motivo, la jurisprudencia viene admitiendo que, cuando en la ejecución de esta clase de medida restrictiva de derechos fundamentales, se descubre un delito distinto, entraría en juego la excepción contenida en la *lex superior* de la *fragancia delictiva* (art. 553 LECrim. en relación con el art. 18.2 CE)[595], pues, producido el hallazgo casual, no estaríamos ante un cambio o novación del objetivo inicial del acto, sino ante una ampliación o adición al mismo, consecuencia de las evidencias casualmente descubiertas en una investigación judicial legítima. Así, para los descubrimientos casuales en los registros domiciliarios, la jurisprudencia viene admitiendo su validez y la adjudicación de valor probatorio, en aplicación de la regla de la *conexidad* (art. 17 LECrim)[596], o bien, de otros criterios como la *proporcionalidad*, siempre que la autorización y la práctica se ajuste a las exigencias y previsiones legales y constitucionales. De este modo, cuando se produce el descubrimiento de un delito sorpresivo será considerado proporcional la continuidad de la investigación sin precisar de una renovada autorización judicial, cuando el hecho delictivo sea considerado grave[597], si bien, como hemos examinado anteriormente, la gravedad del delito no se determina exclusivamente por la pena con la que el mismo se sanciona, sino también en atención a otros criterios, como el bien jurídico protegido y a la relevancia social de los hechos[598].

---

[594] Acerca del *discovery inevitable*, STS 805/2016, 27 de octubre (F.D. 2º), STS 300/2016, 11 de abril (F.D. 2º), STS 511/2015, 21 de julio (F.D. 4º) y STS 811/2012, 30 de octubre (F.D. 3º).

[595] Sobre la flagrancia, STS 885/2004, 5 de julio (F.D. 2º), STS 578/1995, de 28 abril (F.D. 4º), STS 616/2012, 10 de julio (F.D. 2º) y SAP de Madrid (Sección 2ª) 137/2018, 26 de febrero (F.J. 1º).

[596] Acerca de la regla de la conexidad de los arts. 17.5 y 300 LECrim, STS 423/2016, 18 de mayo (F.D. 6º), STS 103/2015, 24 de febrero (F.D. 5º), STS 102/2007, 16 de febrero (F.D. 1º), STS Núm. 103/2015… O. P. Cit (F.D. 5º), STS Núm. 17/2014… O. P. Cit (F.D. 5º) y STS Núm. 423/2016… O. P. Cit (F.D. 6º).

[597] STS 91/1999, de 1 febrero (F.D. 1º).

[598] En relación con la gravedad del delito, la STC Núm. 82/2002, de 22 de abril… O.P. Cit. (F.D. 2º), dispone que, no se determina exclusivamente por la pena con la que el mismo se sanciona, sino también, habrá que atender a otros criterios, como el bien jurídico protegido o la relevancia social de los hechos.

De lo mencionado, podemos extraer como conclusión que, cuando en la práctica de una medida de entrada y registro domiciliario se encuentren efectos o instrumentos que se refieran a conductas delictivas distintas, no quedarían fuera de la autorización judicial inicial que cubra dicha intromisión, pues nuestros tribunales vienen manteniendo que, para esta clase de medida, que se caracteriza por su realización en unidad de acto, una renovada autorización sería contraproducente en la ejecutabilidad de la misma, pero además, la justificación de dicha situación, la encontraríamos en el criterio constitucional de la flagrancia (arts. 553 LECrim. y 18.2 CE), aunque también se admiten otros, como la regla de la *conexidad* del art. 17 LECrim, teniendo en cuenta que no hay novación del objeto de la investigación sino simplemente "adición" a la misma, o bien, la *proporcionalidad*, esto es, cuando el delito hallado sea de suficiente gravedad, como para no dejarlo de investigar. En cambio, para la continuación de los delitos descubiertos casualmente en las medidas de detención y apertura de la correspondencia escrita y telegráfica (art. 579 LECrim.), así como tecnológicas (arts. 588 bis, ter quater, quinquies, sexies y septies LECrim.), como por ejemplo las escuchas telefónicas (art. 588 ter LECrim.) o directas con dispositivos electrónicos (art. 588 quinquies a. LECrim.), debido a que por su propia naturaleza hace que se presuponga una prolongación temporal en la ejecución de las mismas, se precisará, con arreglo a los arts. 579.3 bis. en relación con el art. 588 bis i. LECrim, de una ampliación de la autorización judicial habilitante inicial[599].

7. Registro de dispositivos de almacenamiento masivo de información

Tras haber examinado la medida de entrada y registro domiciliario, continuamos abordando las medidas tecnológicas reguladas en la LECrim. En lo relativo al registro de dispositivo masivo de información, como hemos advertido anteriomente, puede estar relacionada con la diligencia de registro domiciliario. Esto se debe a que, cuando las infracciones son cometidas a través de equipos informáticos, preferiblemente habrá que adoptar diligencias tendentes a su ocupación y el examen de sus contenidos[600], por lo que, habitualmente serán acordadas ambas a la vez.

[599] STS 17/2014, 28 de enero… O.P. Cit. (F.D. 5º).

[600] STS Núm. 811/2015… O.P. Cit. (F.D.1º), dispone que, para los delitos tecnológicos, habrá que adoptar preferiblemente medidas tendentes a la ocupación y examen de los equipos informáticos.

Por su parte, la medida objeto de estudio engloba a todo registro realizado sobre los ordenadores (portátiles o de sobremesa, unidad central de procesamiento –CPU-), instrumentos de comunicación telefónica o telemática (terminales móviles -*smartphone* o teléfono inteligente-, *tablets* o tabletas, dispositivos receptores con tecnología GPS -Sistema de Posicionamiento Global-, etc.), dispositivos de almacenamiento masivo de información digital (discos duros -interno o externo-, memoria USB, disco óptico -CD, DVD, BLU-RAY-) o repositorios telemáticos de datos (como la nube –*icloud, Dropbox, OneDrive*, etc.-). Así, comprende cualquier aparato, dispositivo o sistema que contenga información tecnológica o sea capaz de almacenar datos de los usuarios, aunque lo realmente importante para la investigación será obtener la memoria con la consecuente información para su posterior análisis, como la unidad de discos duro de los ordenadores o la memoria Flash o ROM de los *Smartphone* o *tablet*, junto a otros medios, como la memoria USB o discos ópticos (art. 588.1 sexies a. LECrim.)[601].

De esta manera, la protección jurídica de la información de los dispositivos electrónicos debe alcanzar a todo su contenido, de forma que, el acceso quede restringido a terceras personas, pues el titular decide con quien compartir sus datos. En consecuencia, los datos de esta clase de dispositivos se enmarcan en el ámbito de los derechos relativos a la vida privada del individuo del art. 18 CE, si bien, no todos los derechos se verán

[601] Con carácter general, sobre el registro de dispositivos masivos de información, véase, GARCÍA SAN MARTÍN, J. *Diligencias y medios de prueba. Diligencias Sumariales. Registro de dispositivos de almacenamiento masivo de información*… O.P. Cit. Págs. 265-266; GÓMEZ COLOMER, J. L. *Registro de dispositivos de almacenamiento masivo de información*… O.P. Cit. Págs. 262-263; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*… O.P. Cit. 2017. Pág. 916; FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J. Á. "El consentimiento del detenido al acceso a sus redes sociales y dispositivos de almacenamiento masivo de información*"*. La Ley Penal. Núm. 126. mayo-junio 2017; ZARAGOZA TEJADA, J. I. *El registro de dispositivos de almacenamiento masivo de la información. Investigación Tecnológica y Derechos Fundamentales*… O.P. Cit. Págs. 405 – 448; ZOCO ZABALA, C. *Intervención de las comunicaciones e intervención del ordenador*… O.P. Cit; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Págs. 119-121; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 371-372; FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J. A. *Diligencias de investigación. Registro de ordenadores. (Cuestiones actuales del Proceso Penal).* Ediciones Experiencia. Barcelona. 2015. Págs. 138-140.

afectados por igual, pues al contener información diversa, determinará su encaje en un derecho u otro. Así, los dispositivos tendrán información relacionada con el proceso comunicativo, de forma que, cuando se encuentre en curso la comunicación, pues la transmisión de lo comunicado aún no ha sido recibida por el destinatario, el derecho fundamental afectado será el secreto de las comunicaciones (art. 18.3 CE).

Ahora bien, en esta clase de medida de ocupación de dispositivos, difícilmente se verá afectado el derecho al secreto de las comunicaciones, pues el objeto no será intervenir propiamente el proceso comunicativo. Por esta razón, con frecuencia la injerencia se producirá en un proceso comunicativo consumado, esto es, se accederá a las transmisiones finalizadas (por ejemplo, correos electrónicos, mensajes de *Whatsapp*, etc.) por lo que la afectación producida normalmente encajará en el ámbito del derecho a la intimidad (art. 18.1 CE)[602]. Además, los dispositivos electrónicos contienen otros datos, como los técnicos o de otra clase, a saber, números de teléfonos, contactos, etc. que puedra incidir en la autodeterminación informativa o protección de datos (art. 18.4 CE).

Por su parte, nuestros tribunales han venido a realizar un tratamiento jurídico unitario de la información almacenada en los dispositivos electrónicos, de modo que, todos los datos (por ejemplo, los mensajes, imágenes, documentos, correos electrónicos, etc.), independientemente de su contenido, estarán protegidos, y cualquier injerencia deberá estar sujeta a todas las garantías. Así, se ha constituido lo que se ha venido a denominar el derecho al propio «entorno virtual o digital»[603], de suerte que, los sujetos que utilizan

[602] STC Núm. 123/2002… O.P. Cit. (F.D. 4º) y STC Núm. 70/2002… O.P. Cit. (F.D. 9º) disponen que "el 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".

[603] Acerca del derecho al «entorno virtual o digital», véase, RODRÍGUEZ LAINZ, J. L. *Sobre la influencia de la jurisprudencia del Tribunal Europeo de Derechos Humanos en la actual regulación legal del llamado "derecho al entorno virtual"*… O.P. Cit. Págs. 279-312; CADENA SERRANO, F. A. "El Derecho al Entorno Digital…" O.P. Cit; DELGADO MARTÍN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015…" O.P. Cit; DE LORENZO-CÁCERES APOLINARIO, J. A. *Entorno digital ¿involución de derechos?*… O.P. Cit. Págs. 325-332; GONZÁLEZ-CUÉLLAR SERRANO, N. *Garantías constitucionales de la persecución penal en el "entorno digital"*… O.P. Cit. Págs. 887-916.

dispositivos, además de tener expectativas de privacidad, tienen derecho a la exclusión del propio «entorno virtual», en el sentido de que el titular decide con quien compartir sus datos. En consecuencia, este derecho integraría 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. Debido a lo cual, surge entonces la necesidad de dispensar una protección jurisdiccional frente a las necesidades del Estado en averiguar el delito y descubrir al delincuente, por lo que, el derecho de exclusión del propio «entorno virtual» exige que la ocupación de un ordenador o dispositivo electrónico con el objeto de acceder a su contenido requiera, como decimos, de autorización judicial. De este modo, el órgano jurisdiccional ha de exteriorizar en sus razonamientos la necesidad de sacrificar, no solo el domicilio como sede física en el que se ejercen los derechos individuales, sino también aquellos otros derechos que convergen en la utilización de las nuevas tecnologías[604]. A esto hay que añadir que, cuando sea preciso acceder a un domicilio para ocupar los dispositivos, obviamente entrará en juego el derecho fundamental a la inviolabilidad domiciliaria del art. 18.2 CE.

Habiéndose realizado las anteriores puntualizaciones, seguidamente examinaremos la diligencia de investigación de registro de dispositivos de almacenamiento masivo de información (art. 588 sexies LECrim.)[605] que, como el resto de medidas tecnológicas,

[604] STS 204/2016, 10 de marzo (F.D. 11º), STS 426/2016, 19 de mayo (F.D. 7º), STS 97/2015, 24 de febrero (F.D. 4º) y STS 786/2015, 4 de diciembre (F.D. 1º).

[605] Con carácter general, en relación con la medida de de investigación de registro de dispositivos de almacenamiento masivo de información, véase, LÓPEZ-BARAJAS PEREA, I. "Nuevas tecnologías aplicadas a la investigación penal, el registro de equipos informáticos*"*. IDP: Revista de Internet, Derecho y Política. Núm. 24. 2017; GARCÍA MOLINA, P. *El registro, físico o remoto, de dispositivos de almacenamiento masivo de información y de equipos informáticos de abogados*… O.P. Cit. Págs. 121-135; FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J. A. "Registro de dispositivos de almacenamiento masivo de información*"*. Derecho: Revista Jurídica de la Universidad de Santiago de Compostela. Vol. 25. Núm. 2. 2016. Págs. 25-58; ZARAGOZA TEJADA, J. I. *El registro de dispositivos de almacenamiento masivo de la información. Investigación Tecnológica y Derechos Fundamentales*... O.P. Cit… 2017. Págs. 405 – 448; PALOP BELLOCH, M. "Registro de dispositivos de almacenamiento masivo de información…" Justicia: Revista de Derecho Procesal. Núm. 2. diciembre 2017. Págs. 443-490; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*.

fue creada mediante la L.O. 13/2015, tomando como base, la jurisprudencia comentada sobre el derecho al «entorno virtual o digital». Es por ello que, seguidamente analizaremos la necesidad de motivación individualizada (art. 588 sexies a. LECrim.), la autorización judicial (art. 588 sexies c. LECrim.) y el acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado (art. 588 sexies b. LECrim.), para terminar con la cuestión controvertida de los hallazgos casuales.

a) La necesidad de motivación individualizada

La medida de investigación objeto de estudio consiste en la ocupación y registro de la información tecnológica almacenada en cualquier continente electrónico, si bien, como se produce una afectación en los derechos mencionados anteriormente, la norma procesal exige autorización judicial con motivación individualizada[606], de tal forma que, 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 (art. 588.1 sexies a. LECrim.), todo ello, con plena sujeción a los principios

---

O.P. Cit... Págs. 914-925; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*. O.P. Cit… Págs. 119-129; RODRÍGUEZ ÁLVAREZ, A. *Diligencia de registro de dispositivos y "smartphones"…* O.P. Cit… Págs. 255-263; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. O.P. Cit…. Págs. 370-385.

[606] Sobre la necesaria resolución judicial individualizada para el acceso a los dispositivos electrónicos, afirma, VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs. 121-122, que, "muestra el legislador una cierta preocupación por esta doble motivación, en la consideración de que una cosa es acceder al domicilio -lo que afecta al derecho protegido en el art. 18.2 CE- y otra diferente, al contenido de la información tecnológica hallado en él -que afectaría más al derecho protegido en el art. 18.1 y 4-". De la misma manera, mantienen MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015…* O.P. Cit. Págs. 372-375, que, *"*la exigencia de que la resolución del instructor no sólo se centre en la justificación de los motivos que legitiman la entrada en el domicilio del imputado. Se hace preciso, además, que explicite las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.*"* En el mismo sentido, GOMEZ COLOMER, J. L. *Los actos de investigación garantizados (II): Modernos medios tecnológicos de investigación…* O.P. Cit. Págs. 263-264; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada…* O.P. Cit. Págs. 914-916; GIMENO BEVIÁ, J. *Medidas tecnológicas de investigación. Registros de dispositivos de almacenamiento masivo de información…* O.P. Cit.

rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad (art. 588.1 bis a. LECrim.). Sin embargo, lo que interesa examinar aquí es, la *necesitad de motivación individualizada* exigida en la ley, pues con ello, se pretende erradicar una práctica habitual que venían realizando nuestros tribunales[607] en la adopción de una diligencia de entrada y registro domiciliario, de tal forma que, cuando autorizaban dicha medida, se hacía extensiva también a todos aquellos soportes de información encontrados en la interior de la vivienda, por tanto, sin especificar el alcance a los dispositivos electrónicos y el grado de afectación a los derechos fundamentales. De esta manera, la norma procesal exige ahora que el Juez de instrucción exteriorice las razones que justifican la intromisión en cada uno de los distintos espacios de exclusión que el ciudadano define frente a terceros, en el sentido de que, cuando sea previsible encontrar dispositivos tecnológicos en la vivienda, la propia resolución judicial que acuerda la práctica de la diligencia de registro domiciliario, deberá contener una justificación específica sobre el acceso a dicha información. De igual modo, aunque lo habitual será que la autorización judicial de entrada y registro domiciliario contenga de forma individualizada los razonamientos precisos para acceder a los dispositivos encontrados en la vivienda, nada impediría que se realice dicha especificación en una resolución judicial distinta, esto es, acordar un auto *ad hoc* que legitime el registro de dispositivos de almacenamiento masivo de información. Esto se desprende cuando la norma procesal alude a que la incautación de dispositivos electrónicos, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido (art. 588.2 sexies a. LECrim.), de tal forma que, podría acordarse una autorización de registro domiciliario, y una vez aprehendidos los dispositivos, adoptar ulteriormente un auto permitiendo el registro de los mismos. Todo ello viene ocasionado, como ya nos hemos referido anteriormente que, los dispositivos configuran el derecho «entorno virtual o digital» de modo que, cualquier injerencia en los mismos exige una decisión

[607] STS 864/2015, 10 de diciembre (F.D. 7º) y STS 786/2015, 4 de diciembre (F.D. 1º) disponen que la nueva regulación implementada con la L.O. 13/2015 "pretende abandonar prácticas en las que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia". En cambio, las STS 1231/2003, 25 septiembre, STS 1086/2003, 25 julio, STS 1235/2002, 27 de junio y STS 316/2000, 3 de marzo, que, vienen a aplicar la legislación procesal anterior, y en consecuencia, en la práctica de un registro domiciliario, hacen constar la incautación de dispositivos electrónicos y ordenadores personales, si bien, fueron registrados sin acordar una resolución judicial individualizada.

debidamente motivada al efecto, pues queda expresamente proscrito cualquier autorización implícita o sobreentendida.

b) La autorización judicial

Primeramente, es necesario advertir que, la norma procesal no contiene enumeración alguna de delitos que pueden ser susceptibles de adopción de esta clase de medida, como sucede en otras diligencias tecnológicas, como por ejemplo la intervención en las comunicaciones telefónicas o telemáticas (arts. 588 ter a. y 579.1 LECrim.) o registros remotos sobre equipos informáticos (art. 588.1 septies a. LECrim.) de forma que, cualquier delito podrá ser investigado mediante el registro de dispositivos de almacenamiento masivo de información. De igual modo, serán de aplicación las disposiciones comunes a todas las medidas tecnológicas (art. 588 bis a LECrim.), de modo que, se exige autorización judicial para acceder a la información contenida en los dispositivos tecnológicos, para lo cual, el Juez deberá integrar un juicio de razonabilidad sobre la afectación de la medida en la privacidad del investigado, debiendo ponderar los principios rectores ya estudiados (art. 588 bis a LECrim.), en concreto, se deberá especificar el delito concreto investigado, evitando con ello ocupaciones prospectivas, conjugar la idoneidad, excepcionalidad y necesidad de la medida, así como se adoptará únicamente cuando sea proporcional, esto es, se prescindirá cuando ocasione graves perjuicios en los derechos de los investigados en relación con los posibles beneficios para la investigación.

Respecto a la regulación específica para esta clase de medida tecnológica, alude a que la resolución judicial habilitante deberá fijar los términos y el alcance del registro, de forma que, habrá que especificar el hecho delictivo concreto objeto de la medida. Además, el Juez podrá autorizar la realización de copias de los datos informáticos (art. 588.1 sexies c. LECrim.), así como, fijar 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 (art. 588.1 sexies c. LECrim.)[608].

[608] En relación a las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación en la práctica de una medida de registro de dispositivos, véase, LÓPEZ-BARAJAS PEREA, I. *Nuevas tecnologías aplicadas a la investigación penal, el registro de equipos informáticos*… O.P. Cit; AIGE MUT, Mª B. *La nueva diligencia de registro de dispositivos de almacenamiento masivo*… O.P. Cit

No obstante, la norma procesal no regula las cautelas necesarias o no sugiere mecanismo alguno para asegurar la integridad de los datos, por esta razón, seguidamente vamos a examinar la forma de proceder que, los tribunales[609] han ido diseñando para acceder a los datos tecnológicos con garantías, en especial, con la doctrina jurisprudencial de la cadena de custodia[610] de los efectos intervenidos. De este modo, como nos hemos referido en alguna ocasión, respetar la integridad de la cadena de custodia[611] supone garantizar que desde que se recogen los vestigios tecnológicos relacionados con el delito, hasta que llegan a concretarse como pruebas en el juicio oral, en su caso, pasando por las diferentes instituciones encargadas de estudiar, analizar o elaborar dictámenes periciales, tener la seguridad que no ha sufrido alteraciones o manipulaciones, esto es, en todo momento es lo mismo. Por este motivo, durante la práctica de un registro domiciliario fuera necesario acceder a la información contenida en los ordenadores o dispositivos electrónicos, a los efectos de garantizar que la información no sufre alteraciones, se deberá realizar alguna de estas dos posibilidades, la primera, realizar el volcado y clonado de la información en el momento de hacer el registro, o bien, la segunda, proceder a la ocupación para su registro en un momento posterior[612], para lo cual, se deberán precintar debidamente los dispositivos. En cualquiera de los dos supuestos, el Letrado de la Administración de Justicia, en su calidad de fedatario público judicial, deberá levantar acta, documentando en ella, las

---

Págs. 389-397; RODRÍGUEZ ÁLVAREZ, A. *Diligencia de registro de dispositivos y "smartphones"*… O.P. Cit Págs. 255-263; DELGADO MARTÍN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015*"*. Diario La Ley. Núm. 8.693. 2016.

[609] Acerca de la realización del volcado del contenido de los terminales, véase, STS 196/2017, 24 de marzo (F.D. 1º).

[610] Con carácer general, sobre la cadena de custodia, véase, RUBIO ALAMILLO, J. "Conservación de la cadena de custodia de una evidencia informática…" O.P. Cit; GARCÍA MATEOS, J. A. *Cadena de custodia vs mismidad*… O.P. Cit. Pág. 130.

[611] STS 581/2017, 19 de julio (F.D. 5º).

[612] STS 661/2017, 10 de octubre (F.D. 2º) dispone la posibilidad de autorizar judicialmente la ocupación y posterior registro de los dispositivos almacenadores de memoria informática y cualesquiera otros vinculados a soportes de esa naturaleza, o bien, proceder al volcado y clonado in situ, en el momento de hacer el registro a presencia del Letrado de la Administración de Justicia y del investigado.

operaciones realizadas en el registro, en la cual, habrá de hacer constar una lista con lo inspeccionado, o en su caso, con lo ocupado. Dicho lo anterior, cabe precisar que, salvo que los dispositivos constituyan el objeto o instrumento del delito (por ejemplo en el delito de pornografía infantil –art. 189 CP-), o existan otras razones que lo justifiquen (por ejemplo la falta de medios del juzgado), se deberá evitar la incautación de los dispositivos cuando puedan causar un grave perjuicio a su titular o propietario y sea posible obtener el volcado en condiciones que garanticen la autenticidad e integridad de los datos (art. 588.2 sexies c. LECrim.). Piénsese, por ejemplo, en el registro de una persona jurídica que tiene ordenadores con ficheros de clientes o proveedores, de tal forma que, su incautación seguramente supondrá la paralización de su actividad comercial, encaminando seguramente en el cierre empresarial.

Es por ello que, a continuación, se va a exponer brevemente la forma de proceder para garantizar que los efectos informáticos o electrónicos no sufren alteraciones o manipulaciones, puesto que, desde que comienzan a funcionar, incluso sin la voluntad del usuario, se están produciendo rutinas informáticas, que alteran continuamente el contenido de los mismos. Por este motivo, para garantizar la autenticidad e integridad del contenido de los dispositivos, resulta necesario, tanto si se realiza en la propia vivienda registrada, como si se deja para un momento posterior, congelar la información, para lo cual, habrá que realizar una imagen exacta, mediante la técnica del "*clonado"* o *"volcado"*, con el fin de que pueda ser sometido, en su caso, a cualquier comprobación pericial, mientras se conserva íntegro el original. El proceso de "*clonado"* consiste en la introducción de un *hardware* o aparato físico o externo que permita extraer los datos de los ordenadores, terminales móviles y otros dispositivos electrónicos (por ejemplo, mediante la utilización del *hardware UFED -Universal Forensic Extraction Device-*[613]), de manera que, se copia *bit* a *bit* el contenido del disco de origen en el disco de destino, y con ello no se altera la integridad del sistema. En consecuencia, habrá de descartar la utilización de cualquier *software* o elemento lógico

[613] Se alude al hardware utilizado por la Policía Judicial para realizar el volcado y clonado de la información de los dispositivos electrónicos, de modo que, hemos tomado como fuente: http://conexioninversa.blogspot.com/2010/11/hardware-forensics.html, en relación con: https://www.gdt.guardiacivil.es/webgdt/enlaces.php; https://www.policia.es/org_central/judicial/udef/bit_contactar.html.

introducido o instalado en el sistema (por ejemplo, con discos ópticos –CD, DVD o *Blu-Ray*-, memoria USB, etc.) para llevar a cabo el proceso de "*clonado"*, pues con esta técnica se producen alteraciones en las rutinas informáticas, en perjuicio de la conservación de los datos. Además, para garantizar la identidad entre el original y el "*clonado"*, habrá de proceder a codificar o encriptar mediante algoritmos matemáticos o *"hashing"*[614], también utilizado en la firma electrónica, el cual, hace posible que puedan ser ambos contrastados en cualquier momento. De este modo, mediante una serie de dígitos se hace posible reconocer la identidad de ambos soportes, puesto que los algoritmos siempre son idénticos, de hecho, cualquier inexactitud en la numeración, supone haber manipulado el contenido de los soportes. En este sentido, como mantiene Gudín Rodríguez-Magariños[615], al afirmar que, *la operación de clonado pretende tres efectos: la realización de un volcado parcial o total de la información, la identificación de dicha información mediante la técnica del "hashing" y la obtención de una copia exacta de la información extraída de los soportes electrónicos*. De igual forma, será conveniente verificar el momento exacto de la práctica del "*clonado"*, consignando los datos o circunstancias que determinan su realización (fecha, hora, intervinientes, circunstancias, etc.), así como identificar su contenido, para ello se constata su autenticidad e integridad mediante la codificación aludida con algoritmos "*hash"* u otro análogo, pues en definitiva, como sigue expresando Gudín Rodríguez-Magariños[616] *la forma de llevarse a efecto las operaciones de volcado requiere: la preservación del contenido mediante el bloqueo de escritura que impida modificar su contenido; identificar el contenido mediante el método de algoritmo hash u otro análogo; el clonado o realización de una imagen exacta que será objeto del examen pericial informático; y la constatación de la fecha, circunstancias e intervinientes que*

[614] PEREIRA I PUIGVERT, S. *Sistema de "hash" y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas "inaudita parte"...* O.P. Cit… Págs. 75-83.

[615] GUDÍN RODRÍGUEZ-MAGARIÑOS A.E. "Incorporación al Proceso del Material Informático Intervenido durante la Investigación Penal*"*. Boletín del Ministerio de Justicia. Revista núm. 2.163. 2014. Págs. 8-13.

[616] GUDÍN RODRÍGUEZ-MAGARIÑOS, A.E. "Incorporación al Proceso del Material Informático Intervenido durante la Investigación Penal..." O.P. Cit. Pág. 13.

participen en la realización de la diligencia, quedando documentado tales extremos por el secretario judicial.

En cambio, cabe precisar que, la presencia del Letrado de Administración de Justicia, no ha sido considerado por el Tribunal Supremo[617] como presupuesto de legitimidad de las operaciones de volcado o "*clonado*" de un ordenador o dispositivo, sin embargo, es perfectamente posible que, el Juez en su autorización habilitante, incluya como garantía adicional la presencia del Letrado de Administración de Justicia, pues como nos hemos referido anteriormente, será cada Juez, bajo su criterio, quien fije las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación (art. 588 sexies c. LECrim.).

Por su parte, el segundo escenario que hemos aludido anteriormente es que, cuando en un registro domiciliario los ordenadores o dispositivos electrónicos constituyan el objeto o instrumento del delito, de tal forma que, sea necesaria la incautación de los mismos, o bien, existan otras razones que lo justifiquen, por ejemplo sea un gran número de ordenadores o en esos momentos los agentes actuantes no tuvieran los medios técnicos necesarios para proceder al volcado, clonado y encriptado de la información, se procederá a la ocupación de los efectos tecnológicos, dejando para un momento posterior el registro. De este modo, para descartar toda duda sobre la integridad de los datos, se deben cumplir ciertas garantías, de suerte que, en el propio acto del registro donde se hayan ocupado ordenadores y otros dispositivos deberán ser precintados, para que puedan ser llevados a dependencias policiales para formar el atestado, o bien, se llevará a la sede judicial con la seguridad de que no han sido manipulados. Una vez realizado esto, se procederá al desprecinto de los dispositivos incautados, para lo cual, habrá que documentar su realización. Seguidamente, se procederá a realizar el volcado, el clonado y el encriptado de la forma descrita *supra*, es decir, con las condiciones técnicas necesarias para asegurar la autenticidad e integridad de los datos, en garantía de su preservación. De igual modo, cuando fuera necesario, se elaborará un dictamen pericial, con el análisis pertinente sobre las copias exactas o "clones" que, además, el informe resultante, habrá de remitirlo al juzgado para su unión a las actuaciones. Finalmente, verificadas las operaciones técnicas que sean precisas, los

[617] STS 116/2017, 23 de febrero (F.D 9º).

ordenadores, dispositivos y efectos tecnológicos intervenidos serán precintados nuevamente para su entrega al órgano jurisdiccional competente, quedando bajo su custodia, encargándose del depósito el Letrado de la Administración de Justicia (art. 459 LOPJ)[618], pues debe conservarse de forma íntegra para servir de una eventual pericia de contraste de su contenido.

Una vez examinada, la forma de actuar por nuestros tribunales para asegurar la integridad de los datos y las garantías de su preservación en el registro de dispositivos electrónicos masivos de información, podemos acudir también a la jurisprudencia del Tribunal Europeo de Derechos Humanos[619], en la cual, en los últimos años ha venido estableciendo una serie de reglas, extraídas incluso de las normas procesales de países de nuestro entorno como Austria, para que el acceso a la información se produzca respetando las garantías, de tal forma que, viene a establecer lo siguiente: *a) quien ocupa los locales en el que se realiza el registro deberá estar presente; b) deberá redactarse un informe al concluir el registro y la lista de objetos incautados deberá igualmente ser redactada; c) si el propietario se opone a la incautación de documentos o de soportes de datos, éstos deberán ser precintados y entregados al Juez que decidirá si los adjunta o no al sumario de instrucción; y d) además, en caso de un registro del despacho de un abogado, se requerirá la presencia de un representante del Colegio de Abogados.*

Siguiendo la estructura de la propia norma, seguidamente vamos a examinar otros aspectos regulados en el art. 588 sexies c. LECrim. de tal forma que, como el investigado a veces oculta para evitar ser descubierto en otros dispositivos documentos, archivos, fotografías, etc, se permite ampliar el registro a la información almacenada en sistemas informáticos diferentes, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este (art. 588.3 sexies c. LECrim.). De este modo, en el propio registro del dispositivo, se podrá acceder para llegar a la

[618] Acerca de la función del Letrado de la Administración de Justicia de depositario de las memorias de información obtenidas en los registros, véase, ORTUÑO NAVALÓN, M. C. Aspectos procesales de la prueba electrónica. Procesos penales. Garantías de conservación y custodia… O.P. Cit. Págs. 101-103.

[619] STEDDHH (asunto *Wieser* y *Bicos* Beteiligungen GmbH contra Austria), de 16 octubre 2007 (párrafo 60).

información deseada alojada en otro sistema, siempre que exista una conexión entre uno y otro, si bien, el Juez deberá convalidar esta ampliación, salvo que ya lo hubiera hecho constar en la propia autorización inicial, piénsese por ejemplo, en la información almacenada fuera del dispositivo electrónico, en especial los alojados en servidores externos o en los repositorios telemáticos de datos como la "nube" (*icloud, Dropbox, OneDrive*, etc.). De igual modo, podría darse el supuesto que, durante la práctica de un registro, la Policía Judicial necesite realizar actuaciones en remoto para analizar datos alojados en servidores externos, pues si no se actúa con rapidez, podrían ser borrados (por ejemplo, en delitos de pornografía infantil –art. 189 CP- que las imágenes están alojadas en servidores que podrían ser destruidas si no se actúa con rapidez). De esta manera, se permite para casos de urgencia, a la Policía Judicial y al Ministerio Fiscal, realizar ampliaciones del registro a otros sistemas, informando al Juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, de la forma en que se ha efectuado y su resultado, para lo cual, el Juez también, de forma motivada, podrá revocar o confirmar la actuación en un plazo máximo de setenta y dos horas desde que fue ordenada (art. 588.3 sexies c. *in fine* LECrim.).

De igual modo, para casos de urgencia, en atención a la concurrencia de un interés constitucionalmente legítimo, que haga imprescindible la observancia de las disposiciones mencionadas anteriormente, se permite a la Policía Judicial realizar el examen directo de los datos contenidos en el dispositivo incautado, para lo cual, deberán de comunicar inmediatamente al Juez competente dicha circunstancia, debiendo hacer constar las razones que lo justifican, la actuación realizada, la forma en que se ha efectuado y su resultado (art. 588.3 sexies c. LECrim.). De este modo, se autoriza a iniciativa policial y sin necesidad de autorización judicial previa, el acceso a la información contenida en los sistemas informáticos incautados, para lo cual, se condiciona su actuación a supuestos de urgencia y que exista un interés constitucionalmente legítimo, si bien, deberá ser constatable y objetivo, es decir, la actuación deberá ser debidamente justificada, e imprescindible con el objeto de la investigación[620], como por ejemplo en la prevención e investigación de delitos graves o

[620] Sobre el registro de dispositivos electrónicos sin autorización judicial previa, por razones de urgencia, véase, MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 379-381.

estén en juego bienes jurídicos de especial importancia como la vida o integridad física (piénsese en desapasiones de personas, secuestros, etc.). No obstante, el problema que subyace es el eventual riesgo de que la policía trascienda las garantías constitucionales, sin embargo, se salva esta circunstancia mediante el control judicial *a posteriori*, pues el Juez de instrucción deberá confirmar o revocar la actuación de los agentes de policía, en este último caso, tendrá como efecto la nulidad de la actuación y deberá ser excluida de las actuaciones. De la misma manera, cuando la norma procesal alude al examen directo de los dispositivos, deberá interpretarse que el análisis no puede realizarse de forma exhaustiva, pues la finalidad será averiguar hechos para esclarecer una situación sobrevenida y necesaria.

Finalmente, la norma procesal (art. 588.5 sexies c.) impone a cualquier persona que conozca el funcionamiento del sistema informático o de las medidas aplicadas para proteger los datos informáticos contenidos en el mismo, el deber de colaboración, de tal forma que, habrán de facilitar la información que sea precisa a las autoridades y los agentes encargados de la investigación (piénsese en las personas que posean las claves de desbloqueo del sistema, o bien, la empresa encargada de la programación y comercialización de un determinado sistema operativo), siempre que de ello no derive en una carga desproporcionada para el afectado, todo ello, bajo apercibimiento de incurrir en delito de desobediencia (art. 556 CP). Sin embargo, excepcionalmente se dispensa el deber de colaboración aludido al investigado o encausado, pues en caso contrario, conculcaría con el derecho fundamental del acusado a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE)[621], pero también, a las personas que estén obligadas a declarar por razón de parentesco (art. 416.1 LECrim.)[622], así como la

[621] Acerca de la colaboración del investigado para acceder a los dispositivos electrónicos, y su incidencia con los derechos y deberes fundamentales, véase, MARTÍN RÍOS, M. P. *La colaboración del investigado/encausado en el registro de dispositivos de almacenamiento masivo de información, ¿un supuesto de autoincriminación?...* O.P. Cit… Págs. 161-171.

[622] Art. 416.1 LECrim: *Están dispensados de la obligación de declarar: Los parientes del procesado en líneas directa ascendente y descendente, su cónyuge o persona unida por relación de hecho análoga a la matrimonial, sus hermanos consanguíneos o uterinos y los colaterales consanguíneos hasta el segundo grado civil.*

personas que no puedan declarar en virtud del secreto profesional (art. 416.2 LECrim.)[623].

c) El acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado

Lo normal será que en la ocupación y examen de los dispositivos masivos de información se realice durante la práctica de una diligencia de entrada y registro domiciliario, si bien, en otra ocasiones, también podrá realizarse fuera de la vivienda (art. 588 sexies b. LECrim.), por ejemplo en un vehículo[624] donde se descubre un ordenador, o bien, en un cacheo[625] en la vía pública se encuentra un teléfono móvil o *Smartphone*, de tal forma que, no se habrá acordado una autorización judicial previa, pues el vehículo que se utiliza exclusivamente como medio de transporte no supone *un espacio en cuyo interior se ejerza o desenvuelva la esfera o ámbito privado de un individuo*[626], o bien, el cacheo superficial en la vía pública supone *para el afectado un sometimiento normal a las normas de policía y no implican violación de sus derechos constitucionales a la intimidad (art. 18.1 CE), siempre que la actuación policial esté*

[623] Art. 416.2 LECrim: *Están dispensados de la obligación de declarar: El Abogado del procesado respecto a los hechos que éste le hubiese confiado en su calidad de defensor.*

[624] Examinan el registro de un vehículo, MORENO SANTAMARÍA, A. "El registro de un vehículo en el proceso penal (STS 334/2013, de 15 de abril)". Actualidad Jurídica Aranzadi. Núm. 868. 2013. Pág. 10; SOTO NIETO, F. "Registro de automóviles. Su relación con el registro domiciliario". Diario La Ley Núm. 11943/2001; MISMO AUTOR. "Registro de automóviles. Su consideración procesal". Diario La Ley Núm. 3. 2000. Págs. 1717-1719, llegando a la conclusión que, como norma general, no se precisa de autorización judicial para su ejecución.

[625] Sobre el cacheo, con carácter general, véase, LOMBARDERO EXPÓSITO, L. M. "Conflicto entre derechos fundamentales e investigación policial, el caso del cacheo". Revista de Estudios Jurídicos. Núm. 12. 2012. Págs. 205-242; BAYÓN LÓPEZ, C. "El cacheo policial". Diario La Ley. Núm. 7148. 2009; MAGRO SERVET, V. "La actitud policial en los cacheos y registros como modalidad de las intervenciones corporales en el proceso penal". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 5. 2001. Págs. 1822-1831; GARCÍA VILA, M. "Los cacheos: delimitación y clases". Actualidad Penal. Núm. 13. 2000. Pág. 299.

[626] STS 387/2013, 24 de abril (F.D. 1º) y STS 1365/2003, 17 de octubre (F.D. 1º).

justificada y se mantenga dentro del respeto al principio de proporcionalidad[627]. Sin embargo, aunque en los registros en espacios públicos no sea necesaria autorización judicial, pues no afecta a los derechos fundamentales, los accesos a la información tecnológica, incide en el referido «entorno virtual o digital» del usuario, de tal forma que, cualquier injerencia producida en los dispositivos electrónicos, precisará del oportuno plácet judicial. De esta manera, los agentes de policía pondrán en conocimiento del Juez la incautación fuera del domicilio de los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o repositorios telemáticos de datos, si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización[628].

d) Algunas particularidades observadas en la jurisprudencia y/o doctrina: los hallazgos casuales[629]

Como ya hemos estudiado, de acuerdo con el principio de especialidad, la autorización judicial que habilita el registro de dispositivos de almacenamiento masivo de información debe concretar el delito objeto de la investigación, si bien, puede suceder que en la ejecución de esta clase de medida se descubran otros delitos no previstos en la resolución. De esta manera, como se trata de una medida tecnológica, habrá que aplicar las disposiciones comunes a todas ellas, de tal forma que, el régimen aplicable es el mismo que para la interceptación de las comunicaciones o telemáticas, por lo que, nos remitimos a la parte del presente trabajo dedicada a los hallazgos casuales para esta

[627] STS 156/2013, 7 de marzo (F.D. 1º), STS 941/2012, 29 de noviembre (F.D. 2º) y STS 352/2006, 15 de marzo (F.D. 1º).

[628] Sobre la incautación de dispositivos electrónicos fuera del domicilio, véase, GOMEZ COLOMER, J. L. *Los actos de investigación garantizados (II): Modernos medios tecnológicos de investigación…* O.P. Cit. Pág. 265; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada…* O.P. Cit. Pág. 918; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs. 122-123.

[629] Acerca del hallazgo casual, véase, NADAL GÓMEZ, I. "El Régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la ley de Enjuiciamiento criminal…*"* O.P. Cit.; GARCÍA SAN MARTÍN, J. *El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal…* O.P. Cit. Págs. 309-319; GARCÍA SAN MARTÍN, J. "El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal…" O.P. Cit. Pág. 10.

clase de medida (arts. 588 bis i. por emisión al 579.3 bis. de la LECrim). No obstante, cabe puntualizar que, habrá de distinguir dos supuestos, por un lado, que el delito descubierto sea homogéneo al previsto en la autorización judicial, esto es, constituyan modalidades distintas pero cercanas dentro de la tipicidad penal, de tal suerte que, están contenidos todos los elementos del segundo en el tipo delictivo objeto de la habilitación, o bien, los elementos no comprenden sólo el bien o interés protegido por la norma, sino también, las formas de comportamiento respecto de los que se protegen[630], y por el otro, que el delito descubierto sea heterogéneo respecto al primero, es decir, que los hechos sean diferentes, pues, no existe entre uno y otro una coincidencia con los elementos del tipo objetivo o subjetivo[631]. De esta manera, cuando el delito descubierto sea homogéneo, se deberá proceder de la forma que ha sido examinada para la intervención de las comunicaciones telefónicas y telemáticas, esto es, con arreglo a los arts. 588 bis i. y 579.3 bis LECrim, de tal forma que, se precisa de autorización judicial renovada para continuar con la investigación del nuevo delito. Sin embargo, cuando el delito descubierto sea heterogéneo, se procederá de la misma forma que el anterior, pero además, el Juez debería aplicar el principio de proporcionalidad para decidir sobre la adopción de la nueva autorización judicial, en el sentido de que sea suficientemente grave como para iniciar una investigación respecto de aquel, por ejemplo en el registro de un dispositivo electrónico para la investigación de un delito de organización o grupo terrorista (arts. 571 y 572 CP), se encuentran archivos con información sobre abusos sexuales a menores (art. 188 CP) y/o pornografía infantil (art. 189 CP), de modo que, la gravedad del hecho conlleva que el Estado no puede dejar de investigar los delitos descubiertos por casualidad, en cambio, en un delito de asesinato (arts. 139 y 140 CP), se examina la información de un GPS portátil de un vehículo para averiguar el trayecto que ha realizado, si bien, se aprecia también un delito contra la seguridad vial por exceso de velocidad (art. 379.1 CP), de tal forma que, existe una clara desproporcionalidad entre ambos tipos penales que no justifica su investigación[632].

[630] STS 560/2017, 13 de julio (F.D. 1º).

[631] STS 817/2017, 13 de diciembre (F.D. 13º).

[632] Sobre los delitos hallados por casualidad, hace constar, VELASCO NUÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal...* O.P. Cit. Págs. 123-124, la necesaria proporcionalidad cuando el nuevo delito sea heterogéneo para ampliar la autorización judicial.

8. Registros remotos sobre equipos informáticos

Vamos a examinar la diligencia de registros remotos sobre equipos informáticos (art. 588 septies LECrim.), de tal forma que, esta medida de investigación tecnológica responde a la necesidad del Estado de utilizar las mismas armas para combatir la ciberdelincuencia, si bien, los métodos y tecnología habitualmente empleados por los poderes públicos para perseguir e investigar estos delitos suelen ir un paso por detrás que los utilizados por los cibercriminales. De esta manera, las disposiciones que regulan las medidas tecnológicas dentro de la LECrim, implementadas con arreglo a la L.O. 13/2015, contienen dos clases de registros de dispositivos electrónicos, por un lado los físicos, esto es, se realiza la ocupación y examen directo, de modo que, el investigado presencia la incautación y análisis de los mismos, que ha sido estudiado en el epígrafe anterior (art. 588 sexies LECrim.), y por el otro los virtuales, es decir, los agentes intervienen el equipo informático en remoto, por tanto, sin conocimiento del investigado (art. 588 septies LECrim.).

En efecto, la medida tecnológica de registro en remoto de equipos informáticos que será ahora objeto de análisis, consiste en acceder de forma remota y telemática, a la información contenida en un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos del investigado, de tal forma que, el examen se produce a distancia y sin conocimiento de su titular o usuario. Así, a título de ejemplo, tenemos el delito de autoadiestramiento y autoadoctrinamiento (art. 575.2 CP), pues el hecho se realiza normalmente privadamente en el domicilio, sin contacto con otras personas. Por este motivo, el legislador ha creado presunciones legales a los efectos de inferir la consumación del tipo, de modo que, habrá de suponer la perfección del delito cuando se acceda de manera habitual a los servicios de comunicación en línea, a los contenidos de internet o los servicios de comunicación electrónica cuyos contenidos estén destinados a la incitación, la incorporación o la colaboración en organizaciones o grupos terrorista. En consecuencia, la diligencia de registro remoto sobre equipos informáticos será una medida de investigación idónea para la investigación de esta clase de delitos.

De esta manera, los registros remotos pueden realizarse con la introducción de *datos de identificación y códigos*, para lo cual, se deberá obtener el usuario y contraseñas del dispositivo del investigado, como resultado de una investigación policial, o bien,

mediante el requerimiento judicial de las mismas al proveedor de servicios de telecomunicaciones, obligado pues, a proporcionar los datos almacenados en sus registros por el deber de colaboración que establece la norma procesal (arts. 588 septies b. y 588 ter e LECrim.), de tal forma que, una vez obtenidas las claves, los agentes de policía podrán introducirlas en su ordenador, con el fin de poder observar en tiempo real, en remoto y a distancia los movimientos del investigado, como por ejemplo, con las claves de usuario y contraseñas del *router* o ADSL, podrán abrir los puertos, de modo que, redirigirán las conexiones entrantes del terminal del investigado hacia el equipo informático de la policía. Asimismo, se podrá realizar con la introducción de un *software* o "programa espía" en el ordenador o dispositivo del investigado, de tal forma que, mediante la remisión de algún *malware* o *keylogger*[633] descargable (por ejemplo alojado en un correo electrónico simulado remitido con apariencia de licitud), una vez ejecutado, permite la vigilancia a distancia con duplicados de monitorización, de modo que, hace posible acceder al terminal o dispositivo desde un ordenador en remoto utilizado por el agente de policía encargo de la ejecución de la medida (art. 588.1 septies a. LECrim.)[634]. Sin embargo, la medida de registro remoto sobre equipos informáticos y dispositivos electrónicos presenta grandes dificultades técnicas en su ejecución, puesto que, cuando se accede con *datos de identificación y códigos* el proveedor de servicios puede contar con sistemas de seguridad que alerten al usuario de

[633] Acerca de la introducción de *malware* o troyanos como medida de investigación, afirma, VELASCO NÚÑEZ, E. "ADSL y troyanos, intervención de sus datos y telecomunicaciones en la investigación penal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 82. 2011. Pág. 2, que, "la introducción de un «virus troyano» es una técnica de investigación que mediante la entrada subrepticia de un programa en el ordenador de un sospechoso, pretende adquirir pruebas y vigilar la actividad de éste, consiguiendo sin su conocimiento, pero con autorización judicial, los datos que aquel almacena en su disco duro o en la memoria del PC, así como toda la actividad comunicativa que no sale a la Red —aspectos que no puede conseguir la intervención del ADSL— además del tráfico de entrada y salida de sus telecomunicaciones y de las páginas web que visita, transfiriéndolas a los agentes investigadores facultados, que copiarían los datos seleccionados por el programa para su análisis incriminatorio".

[634] La forma de actuar por las Unidades de Delitos Informáticos de la Policía Judicial ha sido extraída de los portales de internet que se mencionan a continuación: https://www.bloglenovo.es/conectate-a-tu-ordenador-sin-estar-en-casa-descubre-lo-facil-que-es-llevarlo-siempre-contigo/; https://www.softzone.es/manuales-software-2/conexion-remota-con-ip-dinamica/; https://www.eldiario.es/cv/amigoinformatico/acceder-forma-remota-PC-vacaciones_6_674092589.html.

un acceso sospechoso a sus cuentas, para lo cual, habrá que contar con la colaboración de ésta para su ejecución, o bien, la instalación del "programa espía" en el ordenador a través de un archivo descargable dependerá de que el propio usuario quiera abrir el programa, pero además, deberá de no ser reconocido por los posibles programas antivirus que tenga el investigado, pero además, los *software* empleados para su consecución pueden ser costosos económicamente para el erario público (por ejemplo en la contratación de una empresa informática para la programación de esta clase de troyano), pero también, podrá ser necesaria la intervención judicial para autorizar determinadas actuaciones policiales que afecten a otros derechos del investigado, por ejemplo, requerir a la empresa proveedora para que facilite a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema, o bien, deberá acordar una medida entrada en el domicilio para manipular directamente el equipo informático. Por estas razones, la medida objeto de estudio, actualmente es poco utilizada en la práctica, pues los juzgados prefieren acordar otras medidas que su ejecución sea más efectiva, como la ocupación y examen de los dispositivos de almacenamiento masivo de información regulada en el art. 588 sexies LECrim.

En consecuencia, la medida tecnológica que venimos estudiando incide notablemente en los derechos fundamentales del investigado, en particular, a la intimidad (art. 18.1 CE), en su vertiente al "entorno virtual" [635] que abarca la protección de la gran diversidad de datos que pueden guardarse en un dispositivo o sistema informático[636], o bien, a la autodeterminación informativa o protección de datos (art. 18.4 CE). De la misma manera, con frecuencia, el investigado utilizará medios de comunicación interpersonales para contactar con otros usuarios, como puede ser el correo electrónico, mensajería instantánea (*WhatsApp*, *Line*, *Facebook Messenger*, etc.), comunicaciones de texto, voz y vídeo a través de la red, empleando el protocolo IP (VoIP -*Voice over* IP- "voz sobre

[635] C. 5/2019 de FGE, 6 de marzo, *sobre obre registro de dispositivos y equipos informáticos* («BOE» Núm. 70, de 22 de marzo de 2019. Págs. 30159 a 30197) en la conclusión primera dispone que "el registro de dispositivos y equipos informáticos limita el denominado derecho fundamental al entorno virtual del individuo. Para llevarlo a cabo será necesaria siempre autorización judicial, independientemente de que resulte afectado el derecho al secreto de las comunicaciones o simplemente el derecho a la intimidad del investigado".

[636] Sobre el derecho al entorno virtual, véase, la STS Núm. 342/2013, de 17 de abril… O.P. Cit (F.D. 8º).

IP", como *Skype, Viber*, etc.), de tal forma que, como la medida consiste en acceder en remoto a un equipo informático o dispositivo electrónico, sin conocimiento de su titular o usuario, los agentes también podrán observar la conversación mantenida en tiempo real, esto es, en un procedimiento comunicativo en curso, por lo que, inevitablemente se verá afectado también el secreto de las comunicaciones (art. 18.3 CE), de modo que, cualquier injerencia en el contenido de un ordenador o dispositivo electrónico personal por vía de acceso remoto a través de medios técnicos, deberá venir legitimada por el oportuno plácet judicial[637]. De la misma forma, como nos hemos referido anteriormente, cuando fuera necesario acceder a la vivienda para manipular directamente el equipo informático, igualmente entrará en juego la inviolabilidad domiciliaria, por lo que, deberán respetarse las garantías constitucionales contenidas en el art. 18.2 CE.

Una vez realizada las anteriores consideraciones, siguiendo la estructura de la norma procesal, a continuación, se estudiarán los presupuestos de la medida y resolución judicial habilitante (art. 588 septies a. LECrim.), el deber de colaboración de las empresas prestadores de servicios y de las personas que conozcan el funcionamiento del sistema informático (art. 588 septies b. LECrim.) y la duración de la diligencia (art. 588 septies c. LECrim.).

a) Presupuestos y resolución judicial

De esta manera, la diligencia de acceso en remoto al sistema informático o dispositivo electrónico del investigado, franqueando las medidas de seguridad, mediante *la utilización de datos de identificación y códigos o la instalación de software,* se realizará únicamente para la investigación de alguno de los delitos que se detallan a continuación (art. 588.1 septies a. LECrim.): a) los cometidos en el seno de organizaciones criminales (art. 570 bis CP), b) terrorismo (arts. 571-580 CP), c) contra menores o incapaces (prácticamente cualquier delito del Libro II, aunque frecuentemente serán delitos de pornografía infantil del art. 189 CP), d) contra la Constitución (arts. 472 a 543 CP), e) de traición (arts. 581 a 588 CP), f) los relativos a la defensa nacional (arts. 598 a 603 CP), así como, g) cualquier delito cometido a través de instrumentos informáticos o de

[637] STS 795/2016, 25 de octubre (F.D. 12º), STS 426/2016, 19 de mayo (F.D. 7º), STS 97/2015, 24 de febrero (F.D. 4º) y STC 173/2011, 7 de noviembre (F.J. 4º).

cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación[638].

De este modo, a diferencia de lo que ocurría con la medida interceptación de las comunicaciones telefónicas y telemáticas (arts. 588 ter a. en relación con el 579.1 LECrim.), se ha prescindido en su catálogo de delitos, los cometidos en el seno de grupo criminal (art. 570 bis CP), pero tampoco, se ha establecido límite alguno penológico para su persecución, por el contrario, se ha mantenido los delitos informáticos o tecnológicos, pues se pretende que el Estado utilice las mismas armas o instrumentos para combatir la ciberdelincuencia. Así, a título de ejemplo, nos referimos al ciberterrorismo, como el delito de autoadiestramiento y autoadoctrinamiento (art. 575.2 CP) o delito de difusión pública de mensajes o consignas terroristas (art. 579.1 CP).

En cualquier caso, al no establecerse limite penológico alguno para la adopción de esta clase de medida, pero además, como nos hemos referido anteriormente, la afectación en los derechos fundamentales es bastante elevada, el Juez deberá de ponderar suficientemente el sacrificio en los mismos, con los beneficios de la investigación, todo ello, de conformidad con los principios rectores aplicables (art. 588 bis a LECrim.), en especial, deberá indicar los hechos delictivos que pretende investigar (art. 588.3.a. bis c. LECrim.), pues una diligencia tendente a acceder a las informaciones contenidas en

[638] En relación a la medida tecnológica de registro remoto de dispositivos electrónicos, véase, GÓMEZ COLOMER, J. L. *Registros remotos sobre equipos informáticos…* O.P. Cit. Págs. 265-267; NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada…* O.P. Cit. Págs. 925-926; MORENO CATENA, V. *Registro remoto de equipos informáticos (instalación policial de troyanos)…* O.P. Cit. Págs. 293-295; SÁNCHEZ GONZÁLEZ, F. *Registros remotos sobre equipos informáticos. (Actualidad Penal 2017)*. Editorial Tirant lo Blanch. 2017. Págs. 354-355; VILLAR FUENTES, I. M. *El uso de las nuevas tecnologías en las diligencias de investigación. Registro remoto de equipos informáticos…* O.P. Cit. Págs. 591-592; ZARAGOZA TEJADA, J. I. *El registro remoto de equipos informáticos…* O.P. Cit. Págs. 449 – 472; SÁNCHEZ RUBIO, A. *Los registros remotos sobre equipos informáticos, la investigación del "hacker legal"…* O.P. Cit. Págs. 217-228*;* BACHMAIER WINTER, L. "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015". Boletín del Ministerio de Justicia. Año 71. Núm. 2195. 2017. Págs. 1-36; MIRANDA WALLACE, D. "Registro remoto de equipos informáticos. Comentario crítico al artículo 588 Septies LECRIM*"*. Revista General de Derecho Procesal. Núm. 42. 2017.

ordenadores o dispositivos electrónicos de forma subrepticia, puede ser proclive a investigaciones prospectivas, sin embargo, para el hipotético caso de que se descubran delitos no previstos en la autorización judicial inicial, habrá que proceder de la forma aludida *supra* para los hallazgos casuales de las medidas tecnológicas, esto es, será precisa una resolución judicial renovada que habilite continuar con la investigación del hecho delictivo descubierto (arts. 588 bis i en relación con el 579 bis. LECrim.).

De igual modo, la resolución judicial de la medida deberá contener, aparte de los extremos genéricos aplicables a todas las medidas de investigación tecnológica (art. 588.3 bis c. LECrim.), los siguientes específicos, en concreto: *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. 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* (art. 588.2 septies a. LECrim.).

En otro orden de ideas, el Juez competente podrá autorizar la ampliación de los términos del registro, cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en parte del mismo (art. 588.3 septies a. LECrim.). Sin embargo, la ampliación en el registro únicamente podrá realizarse tras la petición de la policía al Juez, y cuando éste la convalide, de tal forma que, no está previsto que, por razones de urgencia se prescinda de la autorización judicial para la investigación de otros sistemas no especificados en la resolución inicial, como sucedía en la medida de registro de dispositivos de almacenamiento masivo de información (art. 588.3 sexies c LECrim.), pues esto se debe a que, el registro del sistema se produce en remoto y sin conocimiento del investigado, por lo que no es necesario tomar una decisión rápida policial por hechos sobrevenidos, como podría ocurrir en un registro de dispositivos en el seno de una injerencia domiciliaria.

b) Deber de colaboración

Como ya nos hemos referido, la ejecución de la medida de registro remoto de dispositivos dependerá de la colaboración prestada por las entidades prestadoras de servicios de telecomunicaciones, así como de los titulares o responsables del sistema informático o base de datos registrados (como por ejemplo los administradores del sistema). Todo ello, de manera similar que en la regulación contenida para la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter e. LECrim.). También éstas entidades o personas, tienen la obligación de colaboración con los agentes investigadores para la práctica de la medida y el acceso al sistema (por ejemplo lo distribuidores de antivirus para su desactivación), así como, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización (art. 588.1 septies b. LECrim.). De este modo, los agentes facultados podrán solicitar al Juez la adopción de una autorización para la cesión de los datos almacenados en las entidades de servicios de telecomunicaciones, como por ejemplo, los datos de identificación y códigos del *router* o ADSL, para poder redirigir la información, monitorizar y visualizar en tiempo real en sus ordenadores las actuaciones realizadas por el investigado, pero también podrán solicitar a éstas, la neutralización de los sistemas de seguridad de alertas al usuario de un acceso sospechoso a sus cuentas. De la misma manera, (art. 588.2 septies b. LECrim.) las autoridades y los 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 para el buen fin de la diligencia (por ejemplo solicitar a técnicos en telecomunicaciones o programadores creadores de algún sistema operativo utilizado por el investigado para que preste la ayuda necesaria a la policía, o bien, a técnicos informáticos expertos en ciberseguridad que procedan a la neutralización de los sistemas de seguridad o antivirus). Además, todos los sujetos mencionados, tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades (art. 588.3 septies b. LECrim.). De igual modo, para el caso de no atender al requerimiento, podrán incurrir en un delito de desobediencia contra la autoridad del art. 556 CP (art. 588.4 septies b. LECrim.). Ahora bien, estás obligaciones no serán aplicables (art. 588.2 septies b. LECrim.) al investigado o encausado, pues en caso contrario se infringiría el derecho fundamental *a no declarar contra sí mismos, a no*

confesarse culpables (art. 24.2 CE)[639]. También se dispensa este deber a las personas que están unidas en razón de parentesco (art. 416.1 LECrim.), y a aquellas otras, en virtud del secreto profesional (art. 416.2 LECrim.). Sin embargo, cabe recordar que, la medida consiste *en el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador o dispositivo electrónico* (art. 588.1 septies a. LECrim.), de forma que, el investigado o encausado desconoce la medida en curso, por lo que difícilmente podrá colaborar con las autoridades. Además, la eficacia de la medida dependerá de que personas cercanas al investigado, como familiares o su abogado, no tengan conocimiento de la práctica de la diligencia. En consecuencia, la única explicación posible para que se haya incluido esta advertencia en la norma, será reforzar los derechos procesales y constitucionales del investigado.

c) Duración

Por último, la norma procesal regula la duración de la medida, de tal forma que, como la medida de registro remoto de equipos informáticos es muy invasiva en los derechos fundamentales del investigado, se ha establecido un plazo de duración relativamente corto, un mes, prorrogable por periodos iguales, hasta un máximo de tres (art. 588 septies c. LECrim.).

9. El agente encubierto

La regulación del agente encubierto[640] se ubica en la Ley de Enjuiciamiento Criminal en el Título III relativo a la Policía Judicial, dentro del Libro II sobre El Sumario, pues viene a regular una función que pueden desempeñar los agentes de policía, sin embargo, deberá considerarse a los efectos del presente trabajo como una medida restrictiva de los derechos fundamentales reconocidos en el art. 18 CE, pues como veremos, durante su

[639] Auto de la AP de León (Sección 3ª) 312/2018, de 7 de marzo (F.D. 2º).

[640] Acerca del agente encubierto, con carácter general, véase, RIZO GÓMEZ, B. "El agente encubierto como herramienta procesal y probatoria contra el crimen organizado*"*. Cuadernos de Política Criminal. Segunda Época. Sección Estudios penales. Núm. 125. 2018; MORENO CATENA, V. *Los agentes encubiertos. Actos de investigación reservados a la instrucción judicial*… O.P. Cit. Págs. 264-270; PLANCHADELL GARGALLO, A. "Investigaciones proactivas: agentes encubiertos*"*. Revista Aranzadi de Derecho y Proceso Penal. Núm. 49. 2018.

práctica pueden producirse injerencias en la intimidad (art. 18.1 CE), el secreto de las comunicaciones (art. 18.3 CE) o la protección de datos (art. 18.4 CE), como así lo establece el propio art. 282.3 bis de la LECrim. De esta manera, vamos a examinar a continuación la medida de infiltración de un agente para investigar actividades de la delincuencia organizada (art. 282 bis LECrim.), si bien, podemos distinguir dos clases de agentes encubiertos, por un lado, al que hemos llamado "tradicional", aunque su habilitación legal es relativamente reciente (L.O. 5/1999)[641], lo cierto es que, la Policía Judicial, venía ejecutando esta diligencia desde mucho tiempo atrás, de tal forma que, consiste en infiltrar a un agente de policía, el cual, se desenvuelve en el mundo físico para investigar actividades ilícitas; y por el otro lado, el "virtual o informático"[642], de

[641] La habilitación legal del agente encubierto fue creada con arreglo a la Ley Orgánica 5/1999, de 13 de enero, *de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves* («BOE» Núm. 12, de 14 de enero de 1999). De esta manera, en lo concerniente al agente encubierto y su habilitación legal, afirma, RODRÍGUEZ FERNÁNDEZ, R. "Comentarios a la LO 5/1999, de 13 de enero, la entrega vigilada y el agente encubierto". Actualidad Jurídica Aranzadi. Núm. 380. 1999. Págs. 1-6, que, "para dar habilitación legal a la figura del «agente encubierto» –que hasta ahora contaba sólo con un desarrollo jurisprudencial–, la LO 5/1999, de 14 de enero, introduce en la LECrim un nuevo artículo, el 282 bis".

[642] Afirma, ZARAGOZA TEJADA, J. I. "El agente encubierto «online»: la última frontera de la investigación penal". Revista Aranzadi Doctrinal. Núm. 1. 2017, que, "son tres los elementos característicos de la figura del agente encubierto que están presentes en todas y cada una de las definiciones plasmadas en el derecho comparado: 1) la infiltración en una red de delincuentes, 2) la ocultación de la verdadera identidad y 3) la condición de agente estatal de quien procede a infiltrarse entre un grupo de delincuentes". Asimismo, expone, SÁNCHEZ GÓMEZ, R. "El agente encubierto informático". La Ley Penal, Núm. 118. Sección Estudios. 2016, que, "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 incorpora dos nuevos apartados al art. 282 bis LEcrim, creando ex novo, la figura del agente encubierto informático. Es una realidad el hecho de que las nuevas tecnologías de la información y de la comunicación han dado lugar al nacimiento de nuevos instrumentos de ataque contra bienes jurídicos, valiéndose de los sistemas informáticos y siendo cada vez más frecuente la producción de actos delictivos cometidos a través de internet". Por su parte, mantiene, LAFONT NICUESA, L. "El agente encubierto en el proyecto de reforma de la Ley de Enjuiciamiento Criminal". Diario La Ley. Núm. 8580. 10 de Julio de 2015, que, "Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, aprobado por el Consejo de Ministros el 13 de marzo de 2015 introduce dos innovaciones en esta técnica investigadora: 1.º) Regula el AE en Internet

modo que, su actuación se desarrolla en el mundo de la red de comunicación. A esto se puede añadir que, cuando sea preciso para la investigación, se puede realizar una combinación de ambos, esto es, iniciar la infiltración en el ámbito informático, y posteriormente concertar una cita con el investigado, de tal forma que, se pasa del mundo virtual al físico. Por estas razones, vamos a dedicar posteriormente a desarrollar brevemente el agente encubierto "tradicional", aunque no se trate de una medida tecnológica, resulta importante examinarlo para relacionarlo con el "virtual o informático", y finalmente, con la combinación de ambos.

a) El agente encubierto tradicional

Los agentes encubiertos únicamente pueden serlo funcionarios de Policía Judicial (Cuerpo Nacional de Policía, Guardia Civil, Agentes de Vigilancia Aduanera[643] y Cuerpos de Comunidades Autónomas -"*Mossos d'Esquadra",* "*Ertzaintza"*; Policía Foral de Navarra o "*Foruzaingoa*"-), pues son los que tienen encomendadas funciones de averiguar los delitos, practicar las diligencias necesarias para su comprobación y descubrir a los delincuentes (art. 126 CE)[644]. La actuación de infiltración queda vetada a

habilitando su intervención en las comunidades cerradas de la red utilizando material ilícito. 2.º) Se establece la posibilidad, previa autorización judicial, de que el AE grabe imágenes y conversaciones del sospechoso o de la actividad criminal". En el mismo sentido, traemos a colación, JORGE PÉREZ, C. "El escondite virtual y el nuevo agente encubierto…" O.P. Cit. Págs. 245-253; CUCARELLA GALIANA, L. A. "El agente encubierto informático*"*. Revista General de Derecho Procesal. Núm. 38. 2016; RIZO GÓMEZ, B. *La infiltración policial en internet. A propósito de la regulación del agente encubierto informático en la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*… O.P. Cit. Págs. Págs. 97-124; VILLAR FUENTES, I. M. y VALIÑO CES, A. *Reflexiones sobre el agente encubierto informático. La actuación del agente encubierto en los delitos informáticos tras la Ley Orgánica 13/2015*… O.P. Cit. Págs. 337-362.

643 Sobre que los Agentes de Vigilancia Aduanera son considerados Policía Judicial, véase, el Acuerdo del Pleno no Jurisdiccional de la Sala Segunda, de 14 de noviembre de 2003, la STS Núm. 297/2006 y la consulta de FGE 2/1999...O.P. Cit.

644 DE LLERA SUÁREZ-BÁRCENA, E. "La atribución de la actividad investigadora a la policía judicial*"*. Revista del Poder Judicial. Núm. Extra 19. 2006. Págs. 101-125; FERNÁNDEZ SEGADO, F. *Las misiones constitucionales de las fuerzas y cuerpos de seguridad. (Estudios de teoría del Estado y*

particulares como colaboradores, testigos o detectives privados[645], si bien, se ha venido permitiendo que el denunciante y testigo protegido, bajo control judicial, pueda colaborar con el agente de policía en la infiltración, aunque no tendrá la consideración propia de agente encubierto, pues no se trata de un miembro policial, sino que será una persona que pone en conocimiento la comisión de unos hechos delictivos, y a partir de ahí, colabora en su investigación y en la identificación de los partícipes[646].

El agente encubierto tiene como función actuar bajo una identidad supuesta. Además, será otorgada por el Ministerio del Interior por un plazo de seis meses prorrogables por períodos iguales, para que se infiltre en el seno de una investigación delictiva en el marco de la delincuencia organizada. Asimismo, el agente encubierto deberá estar habilitado mediante resolución fundada por parte del Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, de hecho, al obtener el apoyo y control judicial, será el momento de estar legitimado para actuar bajo identidad supuesta, adquirir y transportar los objetos, efectos e instrumentos del delito, diferir la incautación de los mismos, participar en el tráfico jurídico y social, pues con la propia autorización, se exonera de la responsabilidad penal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación (art. 282.5 bis LECrim.)[647], de forma que, hasta entones se trataría de un delincuente más.

---

derecho constitucional en honor de Pablo Lucas Verdú. Vol. 3). Editorial de la Universidad Complutense, Facultad de Derecho. Madrid. 2001. Págs. 2087-2114.

[645] Los arts. 10.2 y 37.4 Ley 5/2014, de 4 de abril, *de Seguridad Privada*, dispone la prohibición a los detectives privados para la investigación de delitos perseguibles de oficio. En relación con dicha prohibición, traemos a colación, MARTÍNEZ ATIENZA, G. *Seguridad Pública y Privada*. Edit. Vlex. Madrid. 2016. Pág. 119 y la STS Núm. 908/2016… O.P. Cit. (F.D. 5º).

[646] STS 975/2007, 15 de noviembre (F.D. 2º) y STS 891/2006, 22 de septiembre (F.D. 7º).

[647] Acerca del agente encubierto como medida de investigación policial, afirma, MOLINA MANSILLA, M. C. "El agente encubierto (artículo 282 bis de la LECrim.)*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 62. 2009. Pág. 5, que, "las actividades que está facultado a realizar se describen en el precepto, siendo las de adquirir y transportar los objetos, instrumentos o efectos del delito, limitándose su actuación a realizar tareas de auxilio o colaboración por iniciativa del autor, simulando una disposición a delinquir, que permite una más efectiva intervención policial [STS 13 de junio de 2003]. En este sentido, el párrafo 5.º del precepto exime de responsabilidad penal al agente encubierto por actos que

Por su parte, la resolución debe consignar el nombre verdadero del agente y la identidad supuesta con la que habrá de actuar en la investigación, si bien, por medidas de seguridad y por razones de eficacia de la diligencia, la resolución será secreta (art. 302 LECrim.), así como, deberá conservarse en pieza separada. Acerca del secreto, cabe mencionar que, con el transcurso del tiempo el agente obtiene la confianza de los investigados, en ocasiones también, aunque se haya cesado la operatividad de la investigación, resulta necesario para no levantar sospechas, establecer un periodo de seguridad, es decir, mantener la relación con los investigados para que el agente pueda gradualmente separarse de los mismos, lo cual, jurídicamente supone acordar prórrogas del secreto[648]. Además, mediante resolución judicial motivada, el agente encubierto podrá mantener dicha identidad hasta que testifique en el juicio oral (art. 282.2 bis LECrim.), pudiéndose acoger también al sistema de testigos protegidos (L.O. 19/1994, de 23 de diciembre)[649].

---

sean consecuencia necesaria del desarrollo de la investigación, al estar amparados por una causa de justificación, como es la de obrar en el cumplimiento de su deber de descubrir y detener delincuentes [SSTS 31 de enero de 1998, 3 de febrero de 1999 y 30 de abril de 2002], siempre que siga las pautas recogidas en la Exposición de Motivos de la Ley Orgánica 5/1999, inspirada en el art. 9.3.º. CE, garante de los principios de legalidad y seguridad jurídica, de manera que, en el desarrollo de su actividad, no haya empleado medios de investigación ilícitos o reprochables, que puedan lesionar los principios, derechos y garantías constitucionales de los sujetos investigados". En el mismo sentido, PLANCHADELL GARGALLO, A. "Investigaciones proactivas. Agentes encubiertos*"*. Revista de Derecho y Proceso Penal. Núm. 49. 2018. Págs. 233-240.

[648] Advierte, VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Pág. 174, que, la prórroga del secreto deberá ser un método para que gradualmente el agente encubierto pueda abandonar la organización criminal.

[649] Sobre los testigos protegidos, con carácter general, véase, ESTÉBANEZ IZQUIERDO, J. M. *¿Existe el derecho al anonimato de los testigos protegidos?* Revista de Derecho VLex. Núm. 160. Septiembre 2017; CHOZAS ALONSO, J. M. *El testigo. Garantías procesales. Testimonios especiales. Testigo protegido LO 19/1994, de 23 de noviembre. (El interrogatorio de testigos en los procesos civil y penal. Su práctica ante los Tribunales).* Editorial La Ley. Madrid. 2013. Págs. 721-804; BURGOS LADRÓN DE GUEVARA, J. "La protección del testigo victima en la LO 19/1994 de 23 de diciembre del proceso penal español y la Directiva 2012/29/UE del Parlamento europeo y del Consejo de 25 de octubre de 2012*"*. Revista General de Derecho Procesal. Núm. 31. 2013; MAGRO SERVET, V. "Régimen legal de los testigos protegidos en el proceso penal*"*. La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Núm. 75. 2010. Pág. 2; NAVARRO VILLANUEVA, C. "Protección a testigos y peritos*"*.

Como hemos aludido anteriormente, durante la práctica de esta medida pueden producirse injerencias en los derechos fundamentales, de forma que, aunque el agente puede ser autorizado también por el Ministerio Fiscal, cuando su actuación requiera intervenir las comunicaciones, colocar micrófonos, entrar en un domicilio, registrar un dispositivo masivo de información, etc. se deberá recabar autorización judicial motivada (art. 282.3 bis LECrim.). De la misma manera, el agente encubierto deberá informar a quien autorizó la investigación, esto es, al Juez de Instrucción, o en su caso, al Ministerio Público de lo que vaya descubriendo, pero también, la información deberá aportarse al proceso con las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación, si bien, se valorará en conciencia por el órgano judicial competente (art. 282.1 bis LECrim.). Como hemos advertido anteriormente, la diligencia de agente encubierto únicamente puede ser acordada para la investigación de actividades relacionadas con la delincuencia organizada (art. 282.1 bis LECrim.), la cual, la norma procesal la define como la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno de los delitos contenidos en una lista *numerus clausus* que viene regulada en el art. 282.4 bis LECrim[650]. Por otro lado, como la infiltración en el seno de la

---

Justicia: Revista de Derecho Procesal. Núm. 3-4. 2009. Págs. 89-118; ZAFRA ESPINOSA DE LOS MONTEROS, R. "Algunas cuestiones acerca de la protección de testigos en el proceso penal*"*. Diario La Ley. Núm. 7260. Año XXX. 13 de octubre de 2009.

[650] Art. 282.4 bis LECrim: *A los efectos señalados en el apartado 1 de este artículo, se considerará 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 delitos siguientes: 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*

delincuencia organizada puede ser muy peligroso para un funcionario de Policía Judicial, únicamente podrá ser agente encubierto, el funcionario que libre y voluntariamente decida serlo, esto se desprende cuando la norma procesal establece que (art. 282.2 bis *in fine* LECrim.), *nadie podrá ser obligado a actuar en esta condición*.

Teniendo en cuenta las previsiones legales anteriormente analizadas que, como hemos aludido, legitima al agente encubierto para su actuación, y en consecuencia, queda exonerado de la responsabilidad penal por los hechos que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito (art. 282.5 bis LECrim). Partiendo de lo expuesto acerca del agente encubierto, debemos detenernos en la diferencia entre el agente que descubre la comisión de un delito, de aquel otro que provoca el mismo, de tal forma que, como advierten nuestros tribunales[651] el agente encubierto, tiende exclusivamente a hacer aflorar a la superficie, la actividad delictiva de quien por su propia voluntad y sin instigación ajena, está dedicado a una actividad delictiva, mientras que, para la existencia del delito provocado es exigible que, la provocación (en realidad, una forma de instigación o inducción) parta del agente provocador, de tal modo que, se incite a cometer un delito a quien no tenía previamente tal propósito, surgiendo así en el agente todo el «*iter criminis*», desde la fase de ideación o deliberación a la de ejecución, como consecuencia de la iniciativa y

---

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.

[651] Acerca de la diferencia entre el delito provocado y el delito descubierto, en el seno de una investigación mediante agente encubierto, en la misma línea que de la forma descrita en el cuerpo del presente trabajo, véase, STS 250/2017, 5 de abril (F.D. 9º), STS 277/2016, 6 de abril (F.D. 4º), STS 253/2015, 24 de abril (F.D. 2º), STS 395/2014, 13 de mayo (F.D. 4º), STS 835/2013, 6 de noviembre (F.D. 1º), STS 793/2013, 28 de octubre (F.D. 2º), STS 575/2013, 28 de junio (F.D. 5º), STS 427/2013, 10 de mayo (F.D. 1º), STS 204/2013, 14 de marzo (F.D. 1º), STS 104/2011, 1 de marzo (F.D. 2º), STS 879/2010, 15 de octubre (F.D. 1º), STS 1140/2010, 29 de diciembre (F.D. 6º), STS 1166/2009, 19 de noviembre (F.D. 3º), STS 5/2009, 8 de enero (F.D. 11º), STS 848/2003, 13 de junio (F.D. 2º), STS 262/2003, 19 de febrero (F.D. 1º) y STS 1114/2002, 12 de junio (F.D. 1º).

comportamiento del provocador, que es por ello la verdadera causa de toda la actividad criminal, que nace viciada, pues no podrá llegar nunca a perfeccionarse, por la ya prevista «ab initio» intervención policial. Esta clase de delito provocado, tanto desde el punto de vista de la técnica penal (por el carácter imposible de su producción) como desde el más fundamental principio constitucional de la interdicción de la arbitrariedad de los poderes públicos (art. 9.3 CE) y hasta desde el de la lícita obtención de la prueba (art. 11.1 LOPJ) debe considerarse como penalmente irrelevante, procesalmente inexistente y, por todo ello, impune. De este modo, el agente provocador, incita a cometer un delito a quien no tenía previamente tal propósito, sugiriendo así, en el sujeto todo el «iter criminis», desde la fase de ideación y deliberación a la de ejecución, como consecuencia de la iniciativa y comportamiento del provocador que es por ello la verdadera causa de toda la actividad criminal que nace ya viciada. Así, esta afirmación ha sido mantenida por la jurisprudencia, cuando aparece la voluntad de delinquir en el sujeto, no por su propia y libre decisión, sino como consecuencia de la actividad de otra persona, generalmente un agente o un colaborador de los Cuerpos o Fuerzas de Seguridad, que, guiado por la intención de detener a los sospechosos o de facilitar su detención, provoca a través de su propia y personal actuación engañosa la ejecución de una conducta delictiva que no había sido planeada ni decidida por aquél, y que de otra forma no hubiera realizado, adoptando al propio tiempo las medidas de precaución necesarias para evitar la efectiva lesión o puesta en peligro del bien jurídico protegido. Por el contrario, se niega la existencia del delito provocado cuando la actuación policial haya tenido lugar incidiendo sobre una conducta ya existente que permaneciera oculta, pues simplemente se ha hecho aflorar algo previamente existente e independiente de la referida actuación policial.

Por este motivo, la conducta que, se encamina al descubrimiento de delitos ya cometidos, porque en tales casos los agentes no buscan la comisión del delito sino los medios, las formas o los canales por los que ese tráfico ilícito se desenvuelve, es decir, se pretende la obtención de pruebas en relación a una actividad criminal que ya se está produciendo, pero de la que únicamente se abrigan sospechas. Consecuentemente, a nuestro parecer, sólo cabe hablar de un agente provocador cuando la intervención tiene lugar antes de que los posibles autores hayan comenzado la preparación del hecho punible. En cambio, cuando la preparación para la comisión del delito ya ha comenzado,

y la policía tiene sospechas fundadas de que esto es así, no existe ya una provocación en el sentido de la inducción (art. 28 CP)[652].

Hasta aquí el análisis acerca del "agente encubierto tradicional", es decir, el funcionario de policía judicial que se infiltra y se desenvuelve en el mundo físico, con el fin de descubrir actividades delictivas, de tal forma que, seguidamente se examinará el "agente encubierto virtual o informático".

b) El agente encubierto virtual o informático

Como ya se ha señalado, el "agente encubierto virtual o informático" consiste en un funcionario de Policía Judicial que suplanta o simula una identidad de otro usuario en la

[652] En relación sobre la diferencia entre el agente encubierto que descubre un delito y el agente que provoca un delito, afirma, PÉREZ ARROYO, M. R. "La provocación de la prueba, el agente provocador y el agente encubierto la validez de la provocación de la prueba y del delito en la lucha contra la criminalidad organizada desde el sistema de pruebas prohibidas en el Derecho penal y procesal penal". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 1. 2000. Págs. 1765-1797, que, "concepto básico de agente provocador construido sobre la base de la doctrina: aquel que provoca a otro la comisión de un delito con el fin de que el autor provocado sea castigado precisamente a causa de ese hecho, sin que tenga voluntad de consumación del delito y poniendo para ello las medidas necesarias". Por su parte, mantiene, MONTÓN GARCÍA, M. L. "Agente provocador y agente encubierto, ordenemos conceptos". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 3. 1999. Págs. 2127-2131, que, "delito producido por una persona como consecuencia directa de la incitación de un agente provocador, en referencia expresa al delito provocado -actividad delictual que, por la provocación produce la impunidad del provocado-, por otra, está el delito producido antes de la intervención del agente, que sí es punible, por tratarse del descubrimiento de alguno de los llamados de tracto sucesivo o, en palabras de la jurisprudencia, se trata ahora de la actuación suscitada por un agente provocador. Queriendo indicar, en este segundo caso, que la comisión de un delito incrimina a su autor, siempre y cuando estemos ante una acción u omisión voluntaria producto de una manifestación subjetiva libre tanto en su creación como en su realización; es decir, si su realización es espontánea, no provocada, tal como indicaremos más adelante". De igual modo, expone, GARCÍA LÓPEZ, E. "Agente encubierto y agente provocador, ¿dos figuras incompatibles?" La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 4. 2003. Págs. 1504-1506, que, "el agente provocador mueve al provocado a que realice ciertas conductas reveladoras de la preexistencia de un delito. Quiere decirse, de un delito ya cometido, ya consumado o que se está consumando". En el mismo sentido, traemos a colación, MUÑOZ MARÍN, A. "El agente encubierto y su diferenciación con la provocación para delinquir". CEFLegal: Revista Práctica de Derecho. Comentarios y Casos Prácticos. Núm. 158. 2014. Págs. 189-194.

red, para averiguar los delitos y descubrir a los ciberdelincuentes, de tal forma que, lo mencionado hasta el momento sobre el "agente encubierto tradicional", también será aplicable para esta clase de agente, sin embargo, la norma procesal (art. 282.6 bis LECrim.) establece una serie de particularidades propias que serán seguidamente objeto de análisis[653]. Así, en primer lugar, el agente encubierto virtual únicamente puede ser autorizado por el Juez de Instrucción (art. 282.6 bis LECrim.), pues a diferencia de lo que sucedía con el agente infiltrado del mundo físico, que podía ser acordado también por el Ministerio Fiscal cuando no se veían afectados derechos fundamentales, en este caso, se excluye a éste, la posibilidad de adoptar cualquier autorización, pues *las razones que fundan esa previsión de permiso judicial radican en las posibles injerencias en* dichos *derechos fundamentales amparadas en un engaño o simulación (derecho a no declararse culpable o a no declarar contra sí mismo* del art. 24.2 CE), *a la intimidad* (art. 18.1 CE), *al secreto de las comunicaciones* (art. 18.3 CE), *a la protección de datos* (art. 18.4 CE*),* así como, *a la afectación de derechos de nueva generación como la autodeterminación informativa o el derecho a la identidad virtual[654] o al propio entorno virtual[655]* que indudablemente afectan a la privacidad *y la interdicción de arbitrariedad de los poderes públicos* (art. 9.3 CE).

En segundo lugar, será necesaria solo la autorización judicial cuando el agente encubierto virtual vaya actuar bajo identidad supuesta en comunicaciones mantenidas en

[653] Acerca del agente encubierto informático, con arreglo a la reforma implementada mediante la L.O. 13/2015, véase, ZARAGOZA TEJADA, J. I. "El agente encubierto "online": la última frontera de la investigación penal…" O.P. Cit; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Págs. 171-174; CUCARELLA GALIANA, L. A. "El agente encubierto informático…*"* O.P. Cit; VILLAR FUENTES, I. *Reflexiones sobre el agente encubierto informático…* O.P. Cit. Págs. 363-369; VALIÑO CES, A. "Una lectura crítica en relación al agente encubierto informático tras la Ley Orgánica 13/2015*"*. Diario La Ley. Núm. 8731. 2016, y en concreto, vienen a relacionarlo con las particularidades propias del agente encubierto tradicional.

[654] STC 173/2011, de 1 de noviembre (F.J. 3º), dispone el necesario establecimiento de una serie de garantías frente a los riesgos que existen en 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.

[655] STS 204/2016, de 10 de marzo (F.D. 11º).

canales cerrados de comunicación (art. 282.6 bis LECrim.), lo cual, comprende toda conversación privada telemática, pero también telefónica, pues la Exposición de Motivos de la L.O. 13/2015[656] que vino a regular esta figura, alude que, *los canales abiertos, por su propia naturaleza, no es necesaria*, pero además, como mantienen nuestros tribunales[657] no toda incidencia en estos derechos reclaman inexorablemente habilitación judicial, *pues en el mundo de la red el empleo de una identidad supuesta es la regla: todos se asoman a ese mundo usando un nick. El ciber agente encubierto se diferencia del agente encubierto tradicional en un dato: la asignación de identidad supuesta es una de las vertientes que impulsa a la conveniencia de una autorización, puesto que en la red no se produce engaño por la utilización de pseudónimo, ya que todos lo utilizan, es una regla de ese espacio de comunicación.* Debemos diferenciar, lo que se conoce como *ciber patrulleo,* esto es, *el agente que realiza exploraciones o indagaciones por canales abiertos de comunicación*, de aquel otro, *estricto agente encubierto online que opera en canales cerrados.* Así, *la investigación de la Policía Judicial puede iniciarse mediante un rastreo en internet,* si bien, *esta labor en los* canales abiertos de comunicación (por ejemplo en *redes sociales*, grupos de chats, etc.) *entra dentro de las funciones que corresponden legalmente a las Fuerzas y Cuerpos de Seguridad del Estado (art. 11 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad), puesto que dentro de sus funciones se establece la prevención de la comisión de actos delictivos e investigar los delitos para descubrir y detener a los presuntos culpables,* por lo tanto, *patrullan por la red del mismo modo que sus agentes patrullan por las calles.* En consecuencia, *no se puede confundir esta investigación legítima por los lugares públicos, con una investigación prospectiva prohibida cuando afecte a los derechos fundamentales, ya sea al secreto de las comunicaciones, a la intimidad o a la inviolabilidad del domicilio, reconocidos en la Constitución. Esta labor*

[656] «BOE» Núm. 239, de 6 de octubre de 2015, párrafo IV *in fine* de la Exposición de Motivos de la L.O. 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.*

[657] STS 173/2018, 11 de abril (F.D. 7º); SAN 11/2017, 17 de marzo (F.D. 1º). De igual modo, a título ilustrativo se citan algunas resoluciones judiciales que se vino a adoptar una medida de agente encubierto informático: SAN 12/2018, 26 de abril (F.D. 2º), SAN 5/2018, 7 de marzo (F.D. 1º), SAN 3/2017, 17 de febrero (F.D. 1º), SAP de Barcelona (Sección 6ª) 574/2017, 28 de julio (F.D. 1º) y SAP de Pontevedra (Sección 2ª) 30/2006, 30 de octubre (F.D. 2º).

de vigilancia virtual en la red tiene una importancia fundamental, porque son muchos y muy graves los delitos que se cometen a través de Internet, afectando en muchas ocasiones a las personas más vulnerables.

Por su parte, el agente encubierto informático, con autorización específica acordada por el Juez de Instrucción, ya sea en la propia resolución judicial habilitante de la medida, con motivación separada y suficiente, o bien, en otra distinta acordada *ad hoc*, 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 (art. 282.6 bis *in fine* LECrim.). De esta manera, la autorización judicial específica se desprende de la necesidad de dotar al agente de inmunidad respecto de las actuaciones que objetivamente podrían ser típicas y, por tanto, susceptibles de persecución penal. Debido a lo cual, el agente encubierto informático podría intercambiar o enviar archivos ilícitos para ganarse la confianza del investigado, como por ejemplo videos de pornografía infantil (art. 189 CP)[658] o archivos relativos a la captación, adoctrinamiento o adiestramiento de terroristas *yihadistas* (art. 575 CP)[659]. También, podría analizar los resultados de los algoritmos aplicados para la identificación de aquellos, de modo que, siguiendo la secuencia serial de algoritmo *hash* del contenido del envío telemático se puede descubrir a quién más se ha distribuido el

[658] Sírvase de ejemplo sobre la figura del agente encubierto, como medida de investigación de los delitos contra la pornografía infantil, véase, CAROU-GARCÍA, S. "El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. El guardián al otro lado del espejo". Cuadernos de la Guardia Civil: Revista de seguridad pública. Núm. 56. 2018. Págs. 23-40; VILLAMARÍN LÓPEZ, M. L. *La nueva figura del agente encubierto online en la lucha contra la pornografía infantil. Apuntes desde la experiencia en Derecho Comparado. Nuevas tecnologías y derechos fundamentales en el proceso*. Editorial Thomson Reuters Aranzadi. 2017. Págs. 161-196; VANINETTI, H. A. "El agente encubierto en la investigación de delitos de pornografía infantil, su inclusión en la Ley de Enjuiciamiento Criminal de España. Necesidad de legislarlo en nuestro país*"*. Revista de derecho Penal y Criminología. Núm. 5. 2016. Págs. 191-200; VALIÑO CES, A. *El agente encubierto informático y la ciberdelincuencia, el intercambio de archivos ilícitos para la lucha contra los delitos de pornografía infantil…* O.P. Cit. Págs. 275-285; URIARTE VALIENTE, L. M. "El agente encubierto como medio de investigación de delitos de pornografía infantil en internet*"*. Estudios Jurídicos. Núm. 2012.

[659] Acerca de la figura del agente encubierto como medida de investigación de los delitos relacionados con el terrorismo *yihadista*, véase, VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Pág. 173-174.

material. Asimismo, el Juez podrá autorizar grabaciones de las comunicaciones telemáticas mantenidas a través de ordenadores o dispositivos técnicos utilizados dentro de canales cerrados (art. 282.7 bis LECrim.).

Por su parte, la habilitación judicial del agente informático para que pueda actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados, se podrá acordar únicamente para los delitos referidos *supra* para el "agente encubierto tradicional", esto es, los cometidos en el seno de la delincuencia organizada que tuvieran como fin cometer alguno de los delitos regulados en el art. 282.4 bis LECrim. A estos se añaden también, los delitos que puedan ser objeto de investigación para la interceptación de las comunicaciones telefónicas y telemáticas (arts. 588 ter por remisión al art. 579.1 LECrim.), es decir, los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, cometidos en el seno de un grupo u organización criminal, terrorismo y los cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[660], como por ejemplo el delito de pornografía infantil (art. 189 CP). Esto tiene su explicación en que la mejor manera de averiguar delitos tecnológicos y descubrir a los ciberdelincuentes que, con frecuencia la pena asociada a éstos puede ser escasa, será utilizando sus mismas armas. En cualquier caso, como en toda medida tecnológica restrictiva de derechos fundamentales, para su adopción se deberán respetar los principios rectores (art. 588 bis a LECrim.), en especial la proporcionalidad, pues no existiría justificación alguna para acordar una medida tan gravosa para delitos leves, o bien, algunos menos graves como injurias cometidas a través de la red (art. 208 CP).

c) Combinación de agente encubierto virtual con el agente encubierto tradicional

Como ha sido adelantado anteriormente, en ocasiones será necesario para la operatividad de la investigación que los contactos telemáticos realizados por el agente informático a través de canales cerrados de comunicación (correos electrónicos, mensajería instantánea bidireccional, etc.), pero también, aunque no se requiera autorización judicial inicial, también en canales abiertos (redes sociales, foros, grupos de mensajería instantánea, etc.), dejen paso a encuentros físicos con el investigado, con

[660] STSJ de Cataluña (Barcelona) 20/2018, 5 de marzo (F.D. 3º).

el fin de seguir descubriendo otros aspectos de la actividad delictiva. De este modo, el Juez de Instrucción en la propia resolución inicial habilitante del agente encubierto informático (cuando se trate de canales cerrados), o bien, en otra distinta (cuando se trate de canales abiertos), podrá autorizar el encuentro físico con el investigado, de tal forma que, a partir de entonces se aplicarán las normas reguladoras del agente encubierto tradicional (párrafos 1º a 5º del art. 282 bis LECrim.)[661]. De esta manera, el Juez, o en su caso, el Ministerio Fiscal cuando los encuentros no afecten a los derechos fundamentales (como por ejemplo una cita en la calle o en un local de hostelería abierto al público), podrá autorizar a funcionarios de la Policía Judicial, para que actúen bajo identidad supuesta, a adquirir y transportar los objetos, efectos e instrumentos del delito, diferir la incautación de los mismos, a participar en el tráfico jurídico y social bajo tal identidad. Asimismo, la resolución habrá de consignar los nombres verdaderos de los agentes y las identidades supuestas que, cuando sean distintos se deberán reseñar en pieza separada la nueva filiación, pues con frecuencia, serán funcionarios de Policía Judicial diferentes, pues cada uno estará especializado en su disciplina (art. 282.1 bis LECrim.).

Por su parte, como nos hemos referido anteriormente, el "agente encubierto tradicional" únicamente puede ser acordado para ciertos delitos que, además son más reducidos que para el "agente encubierto informático", por lo cual, surge el problema que, cuando se autorice la investigación para contactos telemáticos para algún delito comprendido para el agente encubierto informático (art. 282.6 bis LECrim.), pero en cambio, no están incluidos para el agente encubierto tradicional (art. 282.4 bis LECrim.), no se podrá salir del entorno virtual al medio físico, pues no se cumplirían los presupuestos legales para su adopción. De igual modo, cuando el funcionario de Policía Judicial en sus labores de patrullaje por la red en canales de comunicación abiertos, esto es, sin previa autorización judicial, descubra la comisión de delitos no comprendidos para el agente encubierto tradicional, no se podrá autorizar esta figura como método de investigación,

[661] En relación a la combinación del agente encubierto tradicional con el informático, advierte, VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Pág. 174; MISMO AUTOR, E. *Entregas vigiladas, infiltración y agente encubierto en internet*… O.P. Cit. Págs. 251-262, que, en cada caso, será de aplicación las disposiciones reguladoras propias de cada uno.

sin embargo, nada impide concertar una cita para proceder a la detención del sospechoso.

Por otro lado, el Juez podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el funcionario de Policía Judicial encubierto y el investigado, aun cuando se desarrollen en el interior de un domicilio (art. 282.7 bis LECrim.), de tal forma que, como nos hemos referido anteriormente, se podrá autorizar para que el "agente encubierto informático" pueda grabar las comunicaciones telemáticas mantenidas a través de ordenadores o dispositivos electrónicos utilizados dentro de canales cerrados, pero también, el "agente encubierto tradicional", en los encuentros que puedan tener lugar con el investigado, podrá obtener imágenes y grabaciones de audio, incluso en espacios físicos pertenecientes a la esfera privada.

10. La problemática de la utilización de otras medidas restrictivas de derechos fundamentales no contempladas en la ley: mención especial de los drones

El Tribunal Constitucional, como nos hemos referido, en su sentencia 145/2014[662], vino a declarar la vulneración del derecho al secreto de las comunicaciones (art. 18.3 CE), en relación con unas grabaciones ambientales directas con dispositivos electrónicos efectuadas a personas sujetas a detención en los calabozos en sede policial, puesto que, consideraba que la regulación que existía en dicho momento no suponía un *defecto por*

[662] Sobre la STC 145/2014, en relación con las medidas tecnológicas no previstas en la ley, véase, OTAMENDI ZOZAYA, F. *Antecedentes y origen de la reforma A) La sentencia del Tribunal Constitucional 145/2014*… O.P. Cit. Pág. 95-148; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Pág. 194-198; LÓPEZ-BARAJAS PEREA, I. y LOZANO EIROA, M. "STC 145/2014, de 22 de septiembre de 2014, Vulneración del derecho al secreto de las comunicaciones: grabación sin garantías de conversaciones verbales mantenidas en dependencias policiales…" O.P. Cit; NISTAL BURÓN, J. "La intervención de las comunicaciones verbales de los detenidos en dependencias policiales (A propósito de la Sentencia 145/2014, de 22 septiembre, de la Sala segunda del Tribunal Constitucional, dictada en el recurso de amparo número 6157-2010)…" O.P. Cit. Págs. 139-153; GONZÁLEZ MONJE, A. *Sentencia del Tribunal Constitucional (Sala Segunda), 145/2014, de 22 de septiembre (BOE núm. 261, de 28-X-2014) Intervención de comunicaciones en dependencias policiales*… O.P. Cit. Págs. 355-357; RODRÍGUEZ LAINZ, J. L. "Sobre la inconstitucionalidad de las vigilancias policiales mediante micrófonos ocultos (A propósito de la STC 145/2014, de 22 de septiembre)…" O.P. Cit.

insuficiencia de la ley, sino que existía una *ausencia total y completa de ley*, toda vez que la norma (antiguo art. 579.2 LECrim.) únicamente regulaba las *intervenciones telefónicas, no a escuchas de otra naturaleza*, de tal forma que, con ello, se ponía en peligro otras medidas de investigación restrictivas de derechos fundamentales que carecían de regulación específica en nuestro ordenamiento. De la misma manera, la mencionada resolución judicial seguía afirmando que *toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, de una habilitación legal*[663]. En la misma línea que lo mencionado anteriormente, el Tribunal Europeo de Derechos Humanos[664] también viene entendiendo que, para que el Juez pueda autorizar una medida tecnológica restrictivas de derechos fundamentales debe estar prevista por una norma que la habilite, pero además, su regulación ha de ser de calidad, con ello se permite que toda persona pueda conocer con antelación las consecuencias de su adopción, pero también, para evitar abusos o arbitrariedades por parte de los Poderes Públicos. Por estas razones, con arreglo a la reforma procesal implementada mediante la L.O. 13/2015 se venían a regular las medidas de investigación tecnológicas, pues como advertía su Exposición de Motivos, *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*

[663] STC Núm. 145/2014… O.P. Cit. (F.D. 7º).

[664] STEDDHH (*Asunto S. y Marper contra Reino Unido*), de 4 diciembre 2008 (párrafo 95); STEDDHH (*Asunto Prado Bugallo contra España*), de 18 febrero 2003 (párrafo 28); STEDDHH (*Asunto Rotaru contra Rumanía*), de 4 mayo 2000 (párrafos 59 y 61); STEDDHH (*Asunto Amman contra Suiza*), de 16 febrero 2000 (párrafo 56); STEDDHH (*Asunto Valenzuela Contreras contra España*), de 30 julio 1998 (párrafos 60 y 61); STEDDHH (*Asunto Kopp contra Suiza*), de 25 marzo 1998 (párrafo 72); STEDDHH (*Asunto Huvig contra Francia*), de 24 abril 1990 (párrafo 29); STEDDHH (*Asunto Kruslin contra Francia*), de 24 abril 1990 (párrafo 33); STEDDHH (*Asunto Malone contra Reino Unido*), de 2 agosto 1984 (párrafo 68).

constitucionales que pueden ser objeto de limitación en el proceso penal[665]. De esta manera, como se ha examinado en los principios rectores dentro de las disposiciones comunes a todas las medidas tecnológicas, cuando el art. 588.1 bis a. LECrim. dice expresamente que "*durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo*", habrá que inferir que, implícitamente se viene a establecer el principio de legalidad[666] para esta clase de diligencias de investigación. Con el referido contexto legal y jurisprudencial, cabe plantear, si el Estado puede utilizar otras medidas de investigación tecnológicas no incluidas en la ley, como por ejemplo el uso de un vehículo aéreo no tripulado o "dron" como artilugio técnico de grabación o aproximación de las imágenes, pues la norma procesal no contiene precepto específico alguno que regule esta clase de instrumento como diligencia de investigación. Por este motivo, hemos decidido examinar a título de ejemplo, la utilización de los "drones como medida de investigación tecnológica, pues a nuestro modo de ver, resulta relevante a los efectos del presente trabajo, determinar hasta donde alcanza el poder del Estado a la hora de investigar la comisión de hechos delictivos, y en especial, los delitos informáticos y tecnológicos.

Así, respecto a los "drones" la única regulación existente es con arreglo al Real Decreto 1036/2017, de 15 de diciembre, *por el que se regula la utilización civil de las aeronaves pilotadas por control remoto*[667], la cual, en su Exposición de Motivos, se establece un régimen específico aplicable para el uso de "drones" en *las operaciones de policía de las Fuerzas y Cuerpos de Seguridad, a las funciones de guardacostas y servicios de aduanas, a las misiones de vigilancia del tránsito viario, y a las operaciones del Centro*

[665] «BOE» Núm. 239, de 6 de octubre de 2015, párrafo IV de la Exposición de Motivos de la L.O. 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*.

[666] Afirma VELASCO NUÑEZ E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal…* O.P. Cit. Pág. 68, que, uno de los principios rectores aplicables a las medidas tecnológicas es la legalidad, de tal forma que, cuando la diligencia no esté expresamente prevista en la ley, no debería ser acordada.

[667] «BOE» Núm. 316, de 29 de diciembre de 2017.

Nacional de Inteligencia[668], de forma que, en suma, consiste en conceder prerrogativas a la policía respecto del resto de ciudadanos (arts. 3.2, 7 y 23.4 ter R.D. 1036/2017), en la utilización de esta clase de instrumentos tecnológicos para la investigación de delitos y descubrir a los presuntos culpables (art. 126 CE, art. 282 LECrim. y art. 11.1.g L.O. 2/1986). Sin embargo, nuestro Tribunal Supremo viene manteniendo que[669], *el alcance de la protección constitucional sólo puede obtenerse adecuadamente a partir de la idea de que el acto de* injerencia domiciliaria (*art. 18.2 CE*) *puede ser de naturaleza física o virtual. En efecto, la tutela constitucional del derecho a la inviolabilidad del domicilio protege, tanto frente la irrupción inconsentida del intruso en el escenario doméstico, como respecto de la observación clandestina de lo que acontece en su interior, si para ello es preciso valerse de un artilugio técnico de grabación o aproximación de las imágenes. El Estado no puede adentrarse sin autorización judicial en el espacio de exclusión que cada ciudadano dibuja frente a terceros. De este modo, se vulnera esa prohibición cuando sin autorización judicial y para sortear los obstáculos propios de la tarea de fiscalización, se recurre a un instrumento técnico que permita ampliar las imágenes y salvar la distancia entre el observante y lo observado. El domicilio como recinto constitucionalmente protegido no deja de ser domicilio cuando las cortinas no*

---

[668] En relación a la normativa sobre el uso de drones, LÓPEZ, J. "Nueva normativa sobre drones*"*. Actualidad Jurídica Aranzadi. Núm. 937. 2018; GONZÁLEZ BOTIJA, F. "La nueva regulación de los drones en el derecho administrativo español*"*. Revista Española de Derecho Administrativo. Núm. 191. 2018. Págs. 193-227; GUERRERO LEBRÓN, M. J. *La regulación civil y militar de las aeronaves civiles pilotadas por control remoto, comentario al RD 1036/2017, de 15 de diciembre*. Editorial Marcial Pons. Madrid. 2018; GARCÍA DEL POYO, R. *Los drones*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 529-549; CASTELLS I MARQUÈS, M. *Drones civiles. (Inteligencia artificial Tecnología Derecho).* Editorial Tirant lo Blanch. Valencia. 2017. Págs. 73-99; FORTES MARTÍN, A. "La disciplina jurídico-administrativa de las operaciones con aeronaves pilotadas por control remoto*"*. Revista General de Derecho Administrativo. Núm. 46. 2017, sostienen que, las operaciones de policía de las Fuerzas y Cuerpos de Seguridad, a las funciones de guardacostas y servicios de aduanas, a las misiones de vigilancia del tránsito viario, y a las operaciones del Centro Nacional de Inteligencia tienen un régimen jurídico especial.

[669] STS 329/2016, 20 de abril, (F.D. 2º y 3º) dispone que, el uso de los drones por las Fuerzas y Cuerpos de Seguridad del Estado para visionar espacios abiertos es perfectamente válida, si bien, la autorización judicial siempre será necesaria cuando se deseé visionar espacios donde se ejerce el derecho a la intimidad.

se hallan debidamente cerradas. La expectativa de intimidad, en fin, no desaparece por el hecho de que el titular o usuario de la vivienda no refuerce los elementos de exclusión asociados a cualquier inmueble. Interpretar que unas persianas no bajadas o unas cortinas no corridas por el morador transmiten una autorización implícita para la observación del interior del inmueble, encierra el riesgo de debilitar de forma irreparable el contenido material del derecho a la inviolabilidad domiciliaria. La protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación funcional del derecho a la inviolabilidad del domicilio (*art. 18.2 CE*). *La existencia de drones, cuya tripulación a distancia permite una ilimitada capacidad de intromisión en recintos domiciliarios abiertos es sólo uno de los múltiples ejemplos imaginables.* Debido a lo cual, *se expresa que en principio la autorización judicial siempre será necesaria cuando sea imprescindible vencer un obstáculo que haya sido predispuesto para salvaguardar la intimidad no siendo en cambio preciso el «Plácet» judicial para ver lo que el titular de la vivienda no quiere ocultar a los demás*[670]. De esta forma, lo cierto es que, la ley procesal no contiene regulación específica sobre la utilización de los "drones" como medida tecnológica[671], sin embargo, se incluyen como

[670] Acerca del uso de los "drones" y su injerencia en la privacidad de los ciudadanos, véase, ANDREA MENDOZA ENRÍQUEZ, O. *La protección de datos personales en la utilización de vehículos aéreos no tripulados (drones)*… O.P. Cit. Págs. 69-76; GÓMEZ-JUÁREZ SIDERA, I. *Drones y privacidad, desafíos de la protección de datos en la utilización civil de aeronaves pilotadas por control remoto*… O.P. Cit. Págs. 39-49; RAMÍREZ LÓPEZ, S. "Del campo de batalla a las calles, el derecho a la intimidad en la era de los drones*"*. Revista Derecho del Estado. Núm. 35. 2015. Págs. 181-199.

[671] Señala BUENO DE MATA, F. "La utilización de drones como diligencia de investigación tecnológica: consecuencias probatorias*"*. Diario La Ley. Núm. 16. 20 de marzo de 2018, que, "la finalidad perseguida con la utilización del dron como diligencia de investigación tecnológica es la de captación de imágenes o vídeos o la medición termográfica de una determinada zona con la finalidad de esclarecer quién y cómo perpetro la acción delictual o ilícita que estamos investigando. De esta manera, la finalidad propia de los drones en estos casos es servir de herramienta para la obtención de pruebas electrónicas que puedan atribuir la autoría del crimen a un determinado autor o a una causa natural concreta". Por su parte, advierten, FERNÁNDEZ GONZÁLEZ, C. M., AYLLÓN SANTIAGO, H. S. y NIETO BALLESTEROS, J. A. *El uso legal de los drones (RPA). Ámbito policial y uso privado*. Edit. Reus. Madrid. 2018, que, los "drones" son utilizados como medida de investigación realizada por los cuerpos policiales.

diligencias de investigación, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos (art. 588 quater a. LECrim.), pero también, la captación de imágenes en lugares o espacios públicos (art. 588 quinquies a. LECrim.). De este modo, como hemos analizado en la parte del presente trabajo dedicada a desarrollar las medidas tecnológicas, el Juez puede autorizar la captación y grabación de las comunicaciones orales directas del investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados (art. 588.1 quater a. LECrim.)[672], pero además, se puede complementar con la obtención de imágenes (art. 588.3 quater a. LECrim.)[673], mientras que, la Policía Judicial, sin la intervención judicial, puede obtener y grabar, por cualquier medio técnico, imágenes del investigado, cuando se encuentre en un lugar o espacio público (art. 588.1 quinquies a. LECrim.). Debido a lo cual, se permite registrar el sonido conjuntamente con la obtención de imágenes en espación públicos y privado (art. aparatado 1 y 2 del 588 quater a. LECrim.), por el contrario, la captación solo de imágenes se permite exclusivamente en lugares públicos (art. 588 quinquies a. LECrim.). Una vez realizadas estas aclaraciones, cabe preguntarse si, la regulación contenida en la norma procesal puede aplicarse a la utilización de los "drones" como medida de investigación, de tal

[672] Sobre la medida de captación y grabación de las comunicaciones orales directas del investigado, con carácter general, véase, GOMEZ COLOMER, J. L. *Los actos de investigación garantizados (II): Modernos medios tecnológicos de investigación*… O.P. Cit. Págs. 239-268; VELASCO NUÑEZ, E. *Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos*… O.P. Cit Págs. 225 – 245; CEDEÑO HERNÁN, M. *Las medidas de investigación tecnológica. Especial consideración de la captación y grabación de conversaciones orales mediante dispositivos electrónicos*… O.P. Cit. Págs. 49-84; GOMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación*… O.P. Cit. Págs. 239-268; VELASCO NÚÑEZ, E. *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Págs. 110-114; MARCHENA GÓMEZ M. Y GONZÁLEZ-CUÉLLAR SERRANO N., *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 336-355.

[673] Acerca de la medida de captación y grabación de las comunicaciones orales, complementada con imágenes, con carácter general, véase, NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*… O.P. Cit. Págs. 909-913; VELASCO NÚÑEZ, E., *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*… O.P. Cit. Págs. 114-116; MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*… O.P. Cit. Págs. 355-360; GÓMEZ COLOMER, J. L. *Diligencia de filmación de lugares públicos*… O.P. Cit. Págs. 204-206.

forma que, cuando el art. 588 quater a. LECrim. sobre la grabación de las comunicaciones orales directas alude a *dispositivos electrónicos*, o bien, el art. 588.1 quinquies a. LECrim. acerca de la captación de imágenes en lugares o espacios públicos refiere a *cualquier medio técnico* puede ser aplicable a las aeronaves pilotadas por control remoto por la Policía Judicial como medida de investigación. De esta manera, cabe concluir que, de acuerdo con la jurisprudencia emanada de nuestro Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos que nos hemos referido *supra*, debemos afirmar que, rige plenamente el principio de legalidad en el sentido de que el Estado no puede acordar otras medidas tecnológicas restrictivas de derechos fundamentales no previstas en la ley, sin embargo, bajo nuestro punto de vista, respecto la utilización de "drones" por la Policía Judicial como diligencia de investigación no consiste en una *ausencia total y completa de ley*, pues tiene cobertura legal al amparo de la normativa reguladora de aeronaves pilotadas por control remoto (R.D. 1036/2017), pero además, para su adopción deberá subsumirse en alguna medidas tecnológica regulada en la LECrim, en concreto, en la grabación de las comunicaciones orales directas del art. 588 quater a. LECrim. y en la captación de imágenes en lugares o espacios públicos del art. 588 quinquies a. LECrim, pues nada impide entender como *dispositivo electrónico* o *medio técnico* esta clase de aeronaves no tripulas por control remoto, cuando fueran utilizadas por las Fuerzas y Cuerpos de Seguridad del Estado como medio para grabar audio y obtener imágenes, pues estarían cumpliendo con su función de averiguar la comisión de delitos y descubrir la posible identidad de sus autores (art. 126 CE, art. 282 LECrim. y art. 11.1.g L.O. 2/1986). Sin embargo, la utilización de "drones", cuando sobrevuelan a cierta altura, que será lo habitual para evitar ser descubiertos, podrán obtener imágenes, pero difícilmente podrá captar el sonido. De este modo, como venimos afirmando que, para registrar imágenes del domicilio u otros lugares cerrados, únicamente puede realizarse, con el oportuno plácet judicial, cuando fuera acompañada de la captación del sonido (art. 588 quater a. LECrim.), es por ello que, la utilización de esta clase de aeronaves no tripuladas como dispositivo electrónico deberá registrar el audio y las imágenes a la vez, pues en caso contrario, no tendría apoyo legal con arreglo a las disposiciones de la LECrim, y por tanto, debería ser descartada como diligencia de investigación, todo ello, pese a que el criterio de la Fiscalía[674] es contraria a esta posición, puesto que vienen manteniendo

[674] Se refiere a dicha cuestión en el punto tercero del ámbito objetivo de aplicación, *in fine*, C. 3/2019, de

que, se permite autorizar la captación y grabación únicamente de imágenes sin sonido. Por su parte, no habría problema alguno en que la Policía Judicial, sin necesidad de recabar autorización judicial, pueda captar las imágenes en lugares o espacios públicos, cuando fuera relevante para el esclarecimiento de los hechos (art. 588.1 quinquies a. LECrim.).

6 de marzo, F.G.E. (BOE Núm. 70 de 22 de marzo de 2019).

B) LA PRUEBA PERICIAL INFORMÁTICA

En las medidas de investigación tecnológicas que han sido examinadas anteriormente, en ocasiones, hemos mencionado a la prueba pericial informática, de tal forma que, ahora abordaremos la manera de acreditar la veracidad del hecho a través de los conocimientos de expertos en materias no jurídicas. De esta manera, cuando se obtienen evidencias electrónicas, esto es, datos digitales que se encuentran almacenados o han sido transmitidos mediante dispositivos electrónicos o equipos informáticos, se precisará, en ocasiones, la realización de una pericial informática, que tendrá como objeto, corroborar su contenido para su adecuada valoración, en especial, cuando existan dudas sobre su autenticidad o integridad. Por este motivo, como nos hemos referido en este trabajo, nuestro Tribunal Supremo[675] viene manteniendo que, la impresión de los archivos en formato papel o "pantallazos" son fuentes de prueba perfectamente válida en Derecho (por ejemplo la impresión de una conversación de mensajería instantánea de *WhatsApp*[676] o mensajes de correo electrónico[677]), si bien, cabe la posibilidad de que sean manipulados los archivos digitales mediante los que se

[675] STS Núm. 300/2015… O.P. Cit. (F.D. 4º).

[676] Con carácter general, en relación a los "pantallazos", véase, SANJURJO RÍOS, E. I. *Las conversaciones de Whatsapp como objeto de investigación y prueba en el proceso penal…* O.P. Cit. Págs. 503-528; ARRABAL PLATERO, P. *El WhatsApp como fuente de prueba…* O.P. Cit. Págs. 325 – 336; BUENO DE MATA, F. *La validez de los «screenshots» o «pantallazo» como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo…* O.P. Cit. Págs. 141 – 152; MISMO AUTOR. "La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 y las últimas reformas procesales en materia tecnológica…" O.P. Cit.; RODRÍGUEZ LAINZ, J. L. "Sobre la naturaleza jurídica de los datos identificadores de aplicaciones de dispositivos de comunicaciones…" O.P. Cit.; MISMO AUTOR. "Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea…" O.P. Cit; DELGADO MARTÍN, J. *La prueba de Whatsapp…* O.P. Cit.; SÁEZ-SANTURTÚN PRIETO, M. "La prueba obtenida a través de mensajes en redes sociales a raíz de la STS 19 de mayo de 2015…" O.P. Cit.

[677] Acerca de los correos electrónicos como prueba en juicio, véase, FUENTES SORIANO, O. *El valor probatorio de los correos electrónicos…* O.P. Cit. Págs. 183-210; RUBIO ALAMILLO, J. "El correo electrónico como prueba en procedimientos judiciales…" O.P. Cit; BERRO, L. "El correo electrónico como prueba documental…" O.P. Cit. Págs. 175-190; GAVILÁN LÓPEZ, J. "Correos electrónicos y sms como prueba…" O.P. Cit. Págs. 30-33.

materializa ese intercambio de ideas, de ahí que, la impugnación de la autenticidad por alguna de las partes, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria, y en tal caso, será indispensable la práctica de una prueba pericial que permita garantizar la identidad, la integridad y la autenticidad de su contenido. Debido a lo cual, seguidamente vamos a analizar la prueba pericial informática, y en concreto, el informe pericial y el perito informático, la técnica forense para la preservación, análisis y exhibición de las evidencias electrónicas en el proceso, así como la pericial informática en el proceso penal.

a) El informe pericial y el perito informático

El informe pericial es un medio de prueba a través del cual se emite un dictamen sobre unos hechos, circunstancias o condiciones para lo que se requiera unos conocimientos científicos, artísticos, técnicos o prácticos. Se trata pues, de auxiliar al Tribunal en ciencias no jurídicas para constatar una realidad no captable directamente por los sentidos[678], y en particular, la pericial informática consiste en asistir al juzgador sobre la identidad, la integridad y la autenticidad de las evidencias electrónicas para su correcta valoración. De este modo, las periciales informáticas[679] que, con mayor frecuencia se

[678] Sobre la definición del concepto de prueba pericial, véase, GÓMEZ COLOMER, J. L. *Informes periciales…* O.P. Cit. Págs. 210-214; ETXEBERRÍA GURIDI, J. F. *Prueba pericial…* O.P. Cit. Págs. 655 – 716; ÁLVAREZ DE NEYRA KAPPLER, S. *La prueba pericial, documental y la inspección ocular…* O.P. Cit. Págs. 163-168; RICHARD GONZÁLEZ, M. *La pericia en el proceso penal. Concepto y características…* O.P. Cit. Págs. 670-777; BEJERANO GUERRA, F. *Informe pericial. (Hacia un catálogo de buenas prácticas para optimizar la investigación judicial).* Centro de Documentación Judicial del Consejo General del Poder Judicial. Madrid. 2009. Págs. 301-316; ABEL LLUCH, X. *La prueba pericial*. JM Bosch. Barcelona. 2009. Págs. 15-248; CAMARENA GRAU, S. "La prueba pericial en el proceso penal". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía: Repertorio General. 2003. Págs. 1339-1354; FONT SERRA, E. "Los informes periciales en el proceso penal". Revista General de Derecho. Núm. 669. 2000.

[679] En relación al concepto de prueba pericial informática como actividad de convicción al tribunal, véase, CALAZA LÓPEZ, M. S. *Prueba pericial electrónica…* O.P. Cit. Págs. 87-105; PINTO PALACIOS, F. y PUJOL CAPILLA, P. "La prueba pericial informática". Diario La Ley, Núm. 5. 3 de abril de 2017; ANGUAS BALSERA, J. *La pericial informática. (Tratado pericial judicial)*. Editorial Wolters Kluwer. Madrid. 2014. Págs. 313-376; CUADRADO SALINAS, C. "Registro informático y prueba digital. Estudio y análisis comparado de la ciberinvestigación criminal en Europa". La Ley Penal, Núm. 107.

pueden realizar son, *la verificación de correos electrónicos o mensajería instantánea* (como *WhatsApp*), de tal forma que, se analiza la autenticidad, para determinar si ha existido manipulación sobre el contenido, la identidad del remitente o el destinatario, la geolocalización, o bien, se examinan los archivos adjuntos o metadatos (en este caso servirá para acreditar cualquier delito que los ciberdelincuentes hayan utilizado estas vías de comunicación); *analizar el contenido de los dispositivos electrónicos u ordenadores*, con el objeto de llegar a la conclusión de si ha existido la eliminación de archivos, y en este caso, de su posible recuperación, si se ha accedido a determinados programas o páginas web, si se ha distribuido determinado material, etc. (por ejemplo para delitos de pornografía infantil del art. 189 CP[680]); *averiguar si ha existido manipulación de archivos digitales*, de modo que, el examen hará posible determinar si los archivos de audio, video o imágenes han sido alterados, o bien, establecer su autenticidad, y su posible procedencia o distribución (por ejemplo para daños informáticos del art. 264 CP); *la certificación de archivos software*, con ello se permite determinar la autenticidad de los programas (por ejemplo para delitos contra la propiedad intelectual del art. 270 CP); *analizar la seguridad informática*, de tal forma que, se emite un informe sobre el dispositivo encriptado, la clave de acceso o los algoritmos matemáticos para determinar el nivel de seguridad, así como la posibilidad

---

marzo-abril 2014; 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. Núm. 7329. 2010; MAGRO SERVET, V. "La prueba pericial informática. La utilización de los medios de prueba informáticos en el proceso penal". La Ley Penal, Núm. 33. diciembre 2006; LÓPEZ-SILVES MARTÍNEZ, A. *Pericial informática*. Estudios de Derecho Judicial. Núm. 71. 2005. Págs. 259-292.

[680] Sobre la pericial para la investigación de delitos de pornografía infantil, ARQUÉS SOLDEVILA, J. M. y GUASCH PETIT, A. "Pericial informática en un caso tipo de pornografía infantil". Revista Aranzadi de Derecho y Proceso Penal. Núm. 30. 2013, señalan que, "caso tipo de pornografía infantil, en el que el ordenador está destinado al uso doméstico1 y que se inicia de forma accidental, a causa de descuidos involuntarios de los poseedores de dicho material. En esta pericial, ello ocurre cuando el técnico encargado de reparar una avería descubre, en dicho ordenador, archivos que contienen fotografías con este tipo de contenido. Tras la denuncia, la policía se incauta del ordenador y se imputa al propietario del mismo por un delito de posesión de pornografía infantil. En este tipo de caso, el análisis forense informático se limitará, generalmente, al disco o discos duros, si hay más de uno. En la pericial que se presenta en este artículo, el alcance de dicho análisis será el contenido local del disco duro incautado".

de acceder por terceros al sistema (por ejemplo para delitos de acceso inconsentido a sistemas informáticos o *hacking* –art. 197 bis CP-).

Por su parte, el perito informático[681] es una persona que, ya sea por su titulación (ingeniería informática, en telecomunicaciones, matemáticas, etc.) o por su experiencia personal o trayectoria profesional, tiene conocimientos en "*informática forense*", esto es, en técnicas científicas y analíticas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro del proceso, tales como, la reconstrucción de datos, examen de datos residuales, explicar las características técnicas de un determinado dispositivo electrónico, etc. De manera que, el perito debe tener conocimientos en el *software* del sistema, en el *hardware*, redes, seguridad, *hacking*, recuperación de información, etc, y tiene por objeto, auxiliar a la Administración de Justicia en los asuntos relacionados con las nuevas tecnologías. De este modo, la prueba pericial de forma genérica, puede ser de parte, esto es, el dictamen será realizado por una persona física o jurídica de carácter privado, de tal forma que, será propuesto y costeado por los propios particulares, o bien, puede realizarse por un perito adscrito al Juzgado. No obstante, para las periciales informáticas, lo habitual será, que sean elaborados dictámenes por agentes de policía[682], en particular, para delitos de especial gravedad, pues la Policía Judicial estatal o autonómicas tienen asignadas diversas unidades para la averiguación de delitos tecnológicos o informáticos y descubrir a los ciberdelincuentes. De esta forma, el Cuerpo Nacional de Policía 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, y en consecuencia le corresponde realizar la elaboración de dictámenes periciales relacionados con la ciberdelincuencia, a la *Unidad de Investigación Tecnológica*

[681] En el mismo sentido que lo mencionado en el cuerpo del presente trabajo, ALDAMA SAÍNZ, C. *Erase una vez un Perito Informático. (La prueba electrónica: validez y eficacia procesal).* Editorial Juristas con Futuro. Madrid. 2016. Pág. 123, describe el concepto de perito informático.

[682] Ponen de manifiesto, GARCÍA SALGUERO, J. M. "El informe pericial". Ciencia Policial: Revista Técnica del Cuerpo Nacional de Policía. Núm. 102. 2010. Págs. 33-86; LLORENTE VEGA, M. J., MARTÍNEZ CORTÉS, J. A. "Informática Forense". Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 135. 2016. Págs. 7-30, la labor policial en la elaboración de dictámenes periciales.

(UIT)[683], dependiente de la *Comisaría General de Policía Judicial*, que a su vez, se subdivide en la *Brigada Central de Investigación Tecnológica*, a la que le 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, y la *Brigada Central de Seguridad Informática*, que se encarga de la investigación de las actividades delictivas que afecten a la seguridad lógica y a los fraudes[684]. Además, la Guardia Civil tiene el *Grupo de Delitos Telemáticos (GDT)*, dentro de la *Unidad Central Operativa de la Guardia Civil*[685], que fue creado para investigar todos aquellos delitos cometidos a través de Internet, pero también, en cada una de las provincias de España existen los *Equipos de Investigación Tecnológica (EDITE)*, los cuales, tienen encomendad asumir la investigación, y en su caso, elaborar informes periciales, sobre la delincuencia relacionada con las redes y sistemas de información[686]. De igual modo, la policía autonómica del País Vasco (*Ertzaintza*), cuenta con un grupo especializado en delincuencia informática, la *Sección Central de Delitos en Tecnologías de la Información (SCDTI)*, viene a asumir la función de

[683] Advierten, JAVIER COSTA, B. "Delitos ciberintrusivos". Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 124. 2014. Págs. 85-106; JAVIER COSTA, B. "Delitos cibereconómicos". Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 111. 2012, Págs. 7-27; COLODRÁS LOZANO, J. M. "La investigación en el campo virtual". Ciencia Policial: Revista del Instituto de Estudios de Policía. Núm. 74. 2004. Págs. 87-100, la labor policial en la averiguación del ciberdelito y descubrimiento del ciberdelincuente.

[684] Sobre las unidades de Policía Nacional encargada de delitos informáticos y tecnológicos, extraído de la siguiente fuente: https://www.policia.es/org_central/judicial/estructura/funciones.html.

[685] Señalan, ORTEGA MALDONADO, A. *Las redes sociales como herramienta de control ético de Internet. Análisis de la actividad en Facebook del Grupo de Delitos Telemáticos de la Guardia Civil relacionada con la persecución de la publicidad ilícita y/o engañosa. (La ética de la comunicación a comienzos del siglo XXI: libro de actas del I Congreso Internacional de Ética de la Comunicación, Facultad de Comunicación 29, 30 y 31 de marzo de 2011)*. Editorial Eduforma. Editorial Mad S.L. Sevilla. 2011. Págs. 1228-1238; SALOM CLOTET, J. "La investigación del delito informático en el Guardia Civil". Estudios de Derecho Judicial. Núm. 71. 2005. Págs. 47-86, las unidades de la Guardia Civil encargadas de la persecución de delitos informáticos.

[686] Las unidades de Guardia Civil encargada de delitos informáticos y tecnológicos, extraído del siguiente portal de internet: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php.

investigar y elaborar informes relacionados con los delitos tecnológicos[687]. De la misma forma, la policía autonómica de Cataluña (*Mossos d'Esquadra*), cuenta con una *Unidad de Delitos en Tecnologías de la Información*, perteneciente a la *Comisaría General de Investigación Criminal*, el cual, le corresponde la función de llevar a cabo la investigación y persecución de las actividades de ciberdelincuencia, y en consecuencia, la elaboración de informes periciales relacionados con esta clase de delitos[688]. De igual manera, la Policía Foral de Navarra cuenta con un *Grupo de Delitos Informáticos* para perseguir la ciberdelincuencia[689], por lo que, será la encargada de realizar los informes periciales informáticos.

b) La técnica forense para la preservación, análisis y exhibición de evidencias electrónicas en el proceso

Una vez examinado el informe pericial, así como, el perito informático, seguidamente vamos a examinar la técnica forense para la preservación, análisis y exhibición de evidencias electrónicas en el proceso[690], si bien, respecto a la preservación de los efectos tecnológicos, inevitablemente nos hemos referido a las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación al tratar las medidas tecnológicas de investigación, puesto que, será una parte esencial para que la diligencia de investigación surta plenos efectos probatorios en el proceso penal.

[687] Las unidades de Ertzaintza encargada de delitos informáticos y tecnológicos, se extrae: https://www.ertzaintza.eus/wps/portal/ertzaintza/

[688] Las unidades de Mossos d´Esquadra encargada de delitos informáticos y tecnológicos, ha sido extraído del siguiente portal de internet: https://mossos.gencat.cat/ca/els_mossos_desquadra/organitzacio/organigrama/

[689] Las unidades de la Policía Foral de Navarra encargada de delitos informáticos y tecnológicos, extraído de la siguiente página web: https://www.navarra.es/home_es/Temas/Seguridad/

[690] Aluden, PINTO PALACIOS, F. y PUJOL CAPILLA, P. "La prueba pericial informática…" O.P. Cit, a la preservación, análisis y exhibición de evidencias electrónicas en el proceso.

a´. Preservación de los efectos electrónicos

Aunque en la ejecución de cualquier medida tecnológica se deben adoptar las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación[691], hemos preferido tomar como referencia la diligencia de registro de dispositivos de almacenamiento masivos de información (art. 588 sexies a. LECrim.), pues será la diligencia más utilizada por los Juzgados para acceder a la información contenida en los dispositivos o equipos informáticos, así como será habitual que se practique una prueba pericial informática para auxiliar al Tribunal en cuestiones técnicas. De este modo, tal y como dijimos en su momento, que conviene recordar y puntualizar, se deberá preservar las evidencias digitales originales, para lo cual, habrá de garantizar que no sufra alteraciones, de tal forma que, primeramente se realizará un "clonado" o "volcado", esto es, hacer una copia exacta (copia *bit* a *bit*) de la información digital contenida en el soporte electrónico original[692], con ello, se consigue tener plena garantías de que el "clon" o copia exacta es igual que la información original. De esta manera, el procedimiento de "clonado" se debe realizar mediante un dispositivo tecnológico especializado de *hardware* o externo, pues la introducción de cualquier *software* o programa informático provocará alteraciones del sistema, pero además, se deberá incluir un sistema que permita bloquear el proceso de escritura en el

[691] Respecto a las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación de otras medidas tecnológicas, en especial, la interceptación de las comunicaciones telefónicas y telemáticas (art. 588 ter LECrim.), nos remitimos a la parte de este trabajo que desarrolla dicha cuestión, si bien, no haremos alusión aquí a ello, debido a que en contadas ocasiones se someterá a prueba pericial la información volcada desde el ordenador central (SITEL), a los soportes digitales, pues como refieren nuestros Tribunales, el contenido de los DVD/Cintas sobre los que se han volcado las grabaciones impresas en el disco duro, gozan de presunción de autenticidad, salvo prueba pericial contradictoria, si bien, prácticamente será ésta inexistente e ineficaz. Todo ello se desprende de la STS 1215/2009, de 30 diciembre (F.D. 1º).

[692] Sobre el clonado o volvado, véase, LÓPEZ-BARAJAS PEREA, I. "Nuevas tecnologías aplicadas a la investigación penal, el registro de equipos informáticos". IDP: Revista de Internet, Derecho y Política… O.P. Cit; AIGE MUT, Mª B. *La nueva diligencia de registro de dispositivos de almacenamiento masivo*… O.P. Cit Págs. 389-397; RODRÍGUEZ ÁLVAREZ, A. *Diligencia de registro de dispositivos y "smartphones"*… O.P. Cit Págs. 255-263; DELGADO MARTÍN, J. "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015…" O.P. Cit.

soporte electrónico original durante el proceso de copia, de modo que, se garantice que la información original no pueda ser manipulada. Una vez finalizado el proceso de "clonado", la imagen forense, que podrá ser almacenada en cualquier formato de disco óptico (CD, DVD, BLU-RAY) o memoria USB, deberá ser firmada digitalmente mediante una función *hash*[693], esto es, técnica que consiste en una relación matemática o algoritmos que, haga posible identificar unívocamente el contenido de la imagen forense con el original, pues cualquier inexactitud en la numeración entre ambos, supone la manipulación de la evidencia tecnológica. Perfectamente posible también, para otorgar garantías de confidencialidad, así como, para conferir mayor protección y seguridad al "clon" o copia exacta, encriptar la imagen en el mismo proceso de obtención, de modo que, además quede restringido a toda persona que no tenga los códigos de acceso. Sin perjuicio de lo mencionado anteriormente, la adquisición de las evidencias tecnológicas deberá realizarse bajo control judicial, para lo cual, éste fijará 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, de tal forma que, podrá determinar en su resolución judicial como garantía la presencia en el "clonado" el Letrado de la Administración de Justicia, mientras que, cuando éste proceso de volcado se realice por peritos particulares, será recomendable la presencia de testigos, o bien, un notario[694] que de fe pública sobre la autenticidad de la evidencia original y el momento en que se obtiene la misma. De igual modo, al menos se deberán obtener dos clones o copias exactas de la evidencia original, de tal forma que, una copia o imagen será puesta a disposición judicial, quedando bajo custodia del Letrado de la Administración de Justicia, o bien, se custodiará en un lugar que garantice la inalterabilidad de su estado (por ejemplo en un lugar seguro en dependencias policiales), mientras que, cuando se trate de una pericial de parte, será conveniente su entrega al notario para su custodia, durante la realización del proceso de análisis. En cambio, la otra copia exacta o imagen, se pondrá a disposición de los peritos encargados

[693] Aborda, PEREIRA I PUIGVERT, S. *Sistema de "hash" y aseguramiento de la prueba informática. Especial referencia a las medidas de aseguramiento adoptadas "inaudita parte"*… O.P. Cit. Págs. 75-83, la técnica *hash*, como garantía de integridad de los efectos.

[694] Alude, SANCHÍS CRESPO, C. *La fe documental y la prueba tecnológica. (El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales)*. Editorial Comares. Granada. 2006. Págs. 205-240, a la presencia del fedatario público en las pruebas electrónicas.

de la elaboración del dictamen, de tal forma que, los técnicos encargados del peritaje cuando reciban la imagen, deberán comprobar que la firma digital o algoritmo *hash* coincide con el original, pues con ello, se hace posible verificar la integridad de la evidencia mediante la comprobación de la firma digital de la misma. Además, se comprobará que la imagen no tenga errores de lectura, u otra clase de daños, pues en caso contrario, habrá que solicitar una nueva copia de la depositada bajo custodia judicial, o en su caso, el notario. Por su parte, todo este proceso habrá de documentarse, por razones de trasparencia a las partes, así como para facilitar la comprobación del resultado por cualquier persona ajena a las partes, o bien, la realización de un contraanálisis, pero además, se deberá levantar un acta con la forma en que se ha obtenido los efectos, recogiendo los detalles técnicos de dicha adquisición. De esta manera, como nos hemos referido en este trabajo, se debe garantizar la cadena de custodia, tanto de los originales, cuando se hayan puesto a disposición judicial o del notario, como de las copias exactas o "clones" realizadas, para ello habrá que documentar la obtención, la entrega y recepción para el análisis y custodia de los efectos tecnológicos, así como habrá de acompañar dicho documento en todo momento del proceso[695]. En efecto, cabe recordar que, la figura jurisprudencial de la cadena de custodia, supone garantizar la identidad, la integridad y la autenticidad (art. 338 y 326 LECrim.) de los efectos intervenidos, de modo que, desde que se procede a la

[695] Desde que se obtiene la evidencia digital hasta la elaboración del informe pericial informático, habrá que documentar en todo momento el proceso, de forma similar que 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,* el cual, viene a regular, la recogida, preparación y envío de muestras toxicológicas, biológicas y criminalísticas para su análisis en el Instituto Nacional de Toxicología y Ciencias Forenses, así como la elaboración de formularios para la remisión y envío de muestras, para asegurar el mantenimiento de la cadena de custodia. En esta línea, nuestros Tribunales se han pronunciado sobre la aplicabilidad de esta norma como formalidad de garantía de la cadena de custodia, si bien, el incumplimiento de dicha disposición legal no supone la ilicitud de la prueba, pues no se produce violación alguna en los derechos fundamentales (art. 11.1 LOPJ), sino que, en todo caso será una cuestión de irregularidad procesal, que tan solo surtirá los efectos valoratorios que correspondan, de tal forma que, se podrá subsanar mediante la introducción en el proceso mediante otras pruebas válidas en Derecho. En este sentido, traemos a colación la STS 682/2017, 18 de octubre (F. D. 8º), STS 849/2013, 12 de noviembre (F.D. 22º), STS 545/2012, 22 de junio (F.D. 2º), STS 773/2013, 22 de octubre (F.D. 3º), STS 920/2013, 11 de diciembre (F.D. 2º), SAP de Madrid (Sección 6ª) 121/2014, 6 de marzo (F.D. 3º) y SAP de Madrid (Sección 1ª) 74/2013, 14 de febrero (F.D. 2º).

ocupación, se examinan o analizan por los peritos, hasta su aportación a fase de plenario, en todo momento es lo mismo, esto es, no han sufrido manipulaciones o alteraciones[696].

b´. Análisis de los efectos tecnológicos

Una vez que se han ocupado los efectos tecnológicos, con las garantías de preservación aludidas, procederá el análisis de la información que ha sido extraída de los ordenadores, dispositivos electrónicos y en los terminales móviles (*Smartphone*), de la forma prevenida anteriormente. Sin embargo, no toda la información puede ser relevante a los efectos de la investigación, así como puede contener datos que afecten a la esfera íntima de las personas (art. 18.1 CE). Por ese motivo, el análisis forense de la información deberá estar dirigido a evitar injerencias innecesarias, para lo cual, el perito informático deberá identificar, de forma selectiva, la información que pueda ser de interés y minimizar o evitar el acceso a otra información que no resulte relevante al objetivo del análisis solicitado. De este modo, se podrá utilizar el método de búsqueda selectiva, esto es, los técnicos no realizan un análisis manual de todos los ficheros, sino que analizan la información realizando búsquedas basados en localizaciones concretas, mediante la selección de una serie de criterios o palabras «clave» a partir de las cuales, se identifican y extraen de las copias exactas o clones aquellos ficheros que contengan alguna de las palabras «clave» objeto de la búsqueda. Asimismo, el proceso de búsqueda podrá realizarse mediante herramientas automatizadas, de tal forma que, se minimice el trabajo y el tiempo del análisis de la documentación, y con ello, se identifica y se selecciona únicamente la información relevante, mientras que se protege la información de carácter privado, cuando resulte innecesaria para la investigación. También será interesante documentar la técnica utilizada para analizar el sistema, pues con ello, se hace posible que el resultado sea verificable y repetible, esto es, cualquier perito informático diferente, partiendo de la copia exacta o "clon", podrá repetir el análisis, o bien, realizar un contraanálisis, de tal forma que, podrá comprobar si obtiene unos idénticos resultados.

[696] RUBIO ALAMILLO, J. "Conservación de la cadena de custodia de una evidencia informática…" O.P. Cit; GARCÍA MATEOS, J. A. *Cadena de custodia vs mismidad…* O.P. Cit. Pág. 130.

c´. Exhibición de pruebas electrónicas en el proceso

Una vez analizados los efectos tecnológicos, de deberá presentar el resultado, de forma que, se transmita la información contenida en los dispositivos de forma objetiva y clara, pues debe proporcionar al Tribunal y a las partes, la información necesaria para poder resolver una cuestión, frecuentemente de alta complejidad técnica, y que puede ser decisiva con el objeto del proceso. De esta manera, el resultado del análisis realizado por técnicos especialistas en informática forense, habrá de presentarse al juzgado en forma de informe o dictamen pericial, el cual, deberá de contener al menos, la filiación del profesional que ha elaborado el informe, una descripción de los objetivos y alcance del trabajo a realizar, una descripción de los procedimientos realizados en el análisis forense y los resultados obtenidos, y por último, las conclusiones. De hecho, las conclusiones será el apartado más importante del informe, pues frecuentemente las partes, y el Juez le bastará su lectura para hacer una valoración del mismo, de modo que, las conclusiones deberán ser breves, objetivas, claras e imparciales, y sin que contenga juicios de valor, pero también, habrá de responder al objeto del encargo del informe.

c) La pericial informática en el proceso penal

De esta manera, vamos a abordar la pericial informática en el proceso penal, para lo cual, desarrollaremos las disposiciones legales contenidas en la LECrim, así como será completada con la jurisprudencia aplicable, si bien, aunque la norma ha sufrido numerosas reformas, ninguna ha venido a incluir una regulación específica para la pericial informática, por lo que, las próximas líneas estarán dedicadas a examinar con carácter general la prueba pericial, pero dirigida al ámbito de las nuevas tecnologías. De este modo, los informes periciales vienen regulados en el procedimiento ordinario para delitos graves dentro de la fase de instrucción en los arts. 456 a 485 LECrim y en la fase de juicio oral en los arts. 723 a 725 LECrim, mientras que, para el procedimiento abreviado, se regula dentro de las diligencias previas en el art. 778 LECrim, así como en la fase de juicio oral en el art. 788.2 LECrim. Una vez realizadas estas aclaraciones, seguidamente, vamos a examinar el número de peritos, la imparcialidad de los mismos, la aportación de los informes periciales, el dictamen pericial, la práctica de la prueba pericial en la fase de juicio oral y su valor probatorio.

a´. El número de peritos

De esta manera, para el procedimiento ordinario para delitos graves, el informe deberá ser emitido por dos peritos (art. 459 LECRim.), mientras que, para el procedimiento abreviado, podrá ser prestado sólo por un perito cuando el Juez lo considere suficiente (art. 778.1 LECRim.). Sin embargo, respeto al número de peritos respecto al primero, cabe mencionar que, nuestro Tribunal Supremo[697] ha matizado la exigencia legal de dos, cuando la elaboración del dictamen sea realizado por un Órgano Oficial, pues como afirma, vienen *dotados de equipos técnicos altamente cualificados integrados por distintos profesionales que intervienen como tales participando cada uno de sus miembros en el trabajo común dentro de la división de tareas o funciones*, de tal forma que, *el mero dato formal de estar suscrito el informe por uno solo de los profesionales del equipo (normalmente el que ejerce facultades representativas del Laboratorio u Órgano informante, como "Responsable" o "Jefe" del Servicio de que se trate) no puede ocultar el hecho real de que el dictamen no es obra de un solo individuo, es decir, de un perito, sino del trabajo de equipo normalmente ejecutado según procedimientos científicos protocolizados en los que intervienen varios expertos, desarrollando cada uno lo que le compete en el común quehacer materializado por todos.* En el caso de los delitos tecnológicos, como nos hemos referido anteriormente, con frecuencia, se encargarán de su elaboración las unidades especializadas de la Policía Judicial, debido a lo cual, como se tratan de funcionarios públicos, bastará con un informe pericial informático.

b´. La imparcialidad de los peritos

Los peritos deberán ser imparciales y objetivos a la hora de emitir un dictamen, de tal forma que, habrán de manifestar, bajo juramento o promesa *de proceder bien y fielmente en sus operaciones y de no proponerse otro fin más que el de descubrir y declarar la verdad* (artículo 474 LECR), pues en caso contrario, podrían incurrir en el delito de falso testimonio (arts. 458, 459 y 460 CP). De la misma manera, cuando las

[697] STS 1365/2003, de 17 de octubre (F.D. 3º) y STS 806/1999, de 10 de junio (F.D. 2º).

partes apreciaran alguna causa de recusación (art. 468 LECrim.)[698], podrían plantearla ante el Juzgado (art. 469 y 470 LECrim.).

c´. La aportación de los informes periciales

El momento procesal para la aportación de los informes periciales es durante la fase de instrucción (sumario y diligencias previas)[699], de tal forma que, durante el transcurso de la misma, la acusación o defensa, podrán solicitar la elaboración de dictámenes, o bien, el Juez acordarlo de oficio. Sin embargo, podrán ser aportados también en la fase preprocesal o policial junto con la denuncia (art. 259 LECrim.) o atestado policial (art. 292 LECrim.), o bien, unidos a la querella (art. 270 LECrim.)[700], como medio para acreditar los hechos. De igual modo, podrán ser aportados en la fase intermedia del proceso penal, esto es, junto con el escrito de calificación provisional en el proceso ordinario para delitos graves (art. 656 LECRim.) o en el escrito de acusación y/o defensa en el proceso abreviado (arts. 781 y 784 LECRim.)[701]. Asimismo, nuestros

[698] Art. 468 LECrim: *Son causa de recusación de los peritos: 1.º El parentesco de consanguinidad o de afinidad dentro del cuarto grado con el querellante o con el reo. 2.º El interés directo o indirecto en la causa o en otra semejante. 3.º La amistad íntima o la enemistad manifiesta*.

[699] Señala, INSA MÉRIDA, F. "La admisibilidad de las pruebas electrónicas en los tribunales: luchando contra los delitos tecnológicos". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía: Repertorio General. 2007. Págs. 1958-1971, que, "durante la investigación, son los agentes de la policía y los fiscales los encargados de custodiar la prueba electrónica en los procedimientos penales. Durante la fase de juicio, es el órgano judicial el encargado de la custodia de estas pruebas (concretamente, la figura del secretario judicial)". Por su parte, advierte, JIMÉNEZ FERNÁNDEZ, C. *El peritaje en los procedimientos penales. (Análisis y valoración de la prueba pericial Social, Educativa, Psicológica y Médica. El Perito Judicial).* Editorial Dykinson. Madrid. 2016. Págs. 57-67, que, como norma general, el momento procesal para la aportación de los informes periciales en el proceso penal será durante la fase de instrucción.

[700] STS 269/2018, 5 de junio, dispone que, la acusación particular ha aportado el informe pericial junto con el escrito de querella.

[701] STS 160/2016, 1 de marzo y STS 701/2014, 30 de octubre (F.D. 3º), disponen que, en un procedimiento penal por delito de daños informáticos del art. 264 CP, se ha solicitado la práctica de una prueba pericial informática en el escrito de defensa, si bien, como se trata de una prueba esencial, procedía su adopción.

Tribunales vienen admitiendo la posibilidad de presentación y solicitud de pruebas, lo cual, habrá de interpretar también, que se incluyen los dictámenes periciales, para momentos procesales posteriores a la calificación o escritos de acusación o defensa (art. 729 LECrim.), si bien, *cuando esté justificada de forma razonada, no suponga un fraude procesal y no constituya un obstáculo a los principios de contradicción e igualdad en garantía de la interdicción de toda indefensión*[702]. Por su parte, en el procedimiento para el juicio sobre delitos leves (Libro VI LECrim.), los informes periciales se podrán aportar en el propio acto de juicio oral (arts. 966 y 969.2 LECRim.), o bien, con anterioridad a la celebración de éste.

En otro orden de ideas, la impugnación del dictamen pericial que obre en la causa tiene como momento procesal idóneo en la fase intermedia, esto es, las partes podrán mostrar sus discrepancias con el informe en los escritos de calificación provisional, o bien, para el procedimiento abreviado en los escritos de acusación y/o defensa[703], si bien, lo normal será que quien pretenda impugnar la pericial sea la defensa. De igual modo, nada impediría que la impugnación del dictamen se realice durante la fase de instrucción, pudiéndose reproducir dicha circunstancia, además, en la fase intermedia. Sin embargo, la mera impugnación formal debe considerarse fraudulenta, pues se *requiere que en estos casos se exprese con la debida claridad la impugnación del dictamen de los especialistas, si bien no se precisa un especial razonamiento de la discrepancia siempre que quede claro lo que no se acepta es dicho dictamen*[704].

Una vez realizada la anterior exposición, debemos puntualizar que, los dictámenes periciales aportados durante la fase de instrucción son diligencias de investigación[705]

[702] STS 307/2014, 1 de abril: (F.D. 3º) y STS 1060/2006, 11 de octubre (F.D. 2º).

[703] STS 574/2011, 3 de junio (F.D. 2º) y STS 115/2015, 5 de marzo (F.D. 8º), disponen que el momento procesal idóneo para la impugnación de prueba será en la fase intermedia del proceso penal, con los escritos de calificación provisionales.

[704] STS 842/2008, 10 de diciembre (F.D. 1º), STS 68/2004, 21 de enero (F.D. 4º), STS 956/2000, 5 de junio (F.D. 5º) y STS 1282/2006, 26 de diciembre (F.D. 2º).

[705] Señalan, GUTIÉRREZ VICÉN, G. "Valoración de las diligencias de investigación en el proceso penal desde la experiencia". Estudios Jurídicos. Núm. 2008 y DE LLERA SUÁREZ-BÁRCENA, E. "Las diligencias previas, contenido; la investigación judicial: su contingencia y su exclusión". Estudios

encaminadas a determinar si existen indicios racionales de criminalidad para acordar la apertura de juicio oral contra determinada persona (en el procedimiento ordinario para delitos graves art. 384 LECrim.; art. 779.1.4º LECrim. en el procedimiento abreviado), o bien, el sobreseimiento de las actuaciones (arts. 634 y siguientes LECrim.), mientras que, tendrá carácter de prueba pericial, únicamente la practicada en el juicio oral (en el procedimiento ordinario para delitos graves el art. 724 LECrim.; art. 788 LECrim. en el procedimiento abreviado) con arreglo a los principios procesales que rigen de inmediación, oralidad, contradicción y publicidad[706], si bien, será objeto de análisis posteriormente.

d´. El dictamen pericial

Para los informes elaborados por peritos adscritos al juzgado, la norma procesal establece que «*el Juez manifestará clara y determinantemente a los peritos el objeto de su informe*» (art. 475 LECrim), pero además, el acto pericial será presidido por el Juez instructor, asistido siempre por el Letrado de la Administración de Justicia que actúe en la causa (artículo 477 LECrim), sin embargo, en la práctica, nunca se realiza de la forma establecida en la ley, puesto que los exámenes se verifican en laboratorios especializados, y en concreto para las periciales informáticas, como venimos afirmando, se realizarán en unidades especializadas de delitos tecnológicos de las Fuerzas y Cuerpos de Seguridad del Estado. De igual modo, como nos hemos referido anteriormente sobre la preservación o aseguramiento de los efectos electrónicos, la pericial informática se realizará siempre sobre la copia exacta o "clon", nunca sobre el original, con ello, se consigue preservar la integridad del soporte original, así como, las partes podrán repetir a su costa, tantas veces como deseen, las operaciones de análisis de los dispositivos electrónicos o equipos informáticos. De la misma manera, *el informe*

Jurídicos. Ministerio Fiscal. Núm. 1. 2000. Págs. 105-138, que, las diligencias de investigación en fase de instrucción, tienen por objeto, poder determinar la apertura de juicio oral respecto al investigado.

[706] Respecto a los principios procesales de inmediación, oralidad, contradicción y publicidad, a modo de ejemplo, véase, STS 778/2017, 30 de noviembre (F.D. 1º), STS 669/2017, 11 de octubre (F.D. 1º), STS 157/2017, 13 de marzo (F.D. 2º), STS 141/2017, 7 de marzo (F.D. 2º), STS 667/2014, 15 de octubre (F.D. 1º), STS 350/2014, 29 de abril (F.D. 5º), STS 1115/2011, 17 de noviembre (F.D. 2º), STS 702/2006, 3 de julio (F.D. 2º), STS 181/2006, 22 de febrero (F.D. 1º) y STS 105/2005, 29 de enero (F.D. 1º).

pericial comprenderá, si fuere posible: 1.º Descripción de la persona o cosa que sea objeto del mismo en el estado o del 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 (art. 478 LECRim.), pudiendo además el Juez, *por su propia iniciativa o por reclamación de las partes, hacer a los peritos, las preguntas que estime pertinentes y pedirles las aclaraciones necesarias* (art. 483 LECRim.).

e´. La práctica de la prueba pericial en la fase de juicio oral

Con carácter previo, advertir que, nuestros Tribunales[707] vienen afirmando que, cuando *los dictámenes e informes sean elaborados por Gabinetes y Laboratorios Oficiales*, en el caso de los delitos informáticos, como venimos afirmando, con frecuencia son elaborados por las unidades especiales de Policía Judicial, por lo que, este criterio jurisprudencia será habitual su aplicación, *no es necesario su ratificación en el Juicio Oral siempre que no hayan sido objeto de impugnación expresa en los escritos de conclusiones. El fundamento de este criterio se encuentra en la innecesariedad de la comparecencia del perito cuando el dictamen ya emitido en fase sumarial es aceptado por el acusado expresa o tácitamente, no siendo conforme a la buena fe procesal la posterior negación de valor probatorio del informe documentado si éste fue previamente aceptado*. De este modo, *cuando la parte acusada no exprese en su escrito de calificación provisional su oposición o discrepancia con el dictamen pericial practicado, ni solicita ampliación o aclaración alguna de éste, debe entenderse que dicho informe oficial adquiere el carácter de prueba preconstituida, aceptada y consentida como tal de forma implícita.* En consecuencia, bastará *con que la defensa impugne el resultado de los dictámenes practicados durante la instrucción, o manifieste de cualquier modo su discrepancia con dichos análisis, para que el documento*

[707] Pleno no jurisdiccional de la Sala Segunda del TS, de 21 de mayo de 1999, ratificado por el posterior de 23 de febrero de 2001, así como, STS 1282/2006, 26 de diciembre (F.D. 2º), STS 749/2005, de 17 de junio (F.D. 2º), STS 1247/2004, 29 de octubre (F.D. 3º), STS 290/2003, de 26 de febrero (F.D. 1º), STS 585/2003, de 16 abril (F.D. 1º), STS 311/2001, de 2 de marzo (F.D. 1º), STS 652/2001, de 16 de abril (F.D. 1º), STS Núm. 574/2011… O.P. Cit. (F.D. 2º), STS Núm. 115/2015… O.P. Cit. (F.D. 9º), STC 127/1990, de 5 de julio (F.D. 4º) y STC 24/1991, de 11 de febrero (F.D. 3º).

sumarial pierda su eficacia probatoria, y la prueba pericial deba realizarse en el juicio oral, conforme a las reglas generales sobre carga y práctica de la prueba en el proceso penal[708]. De esta manera, cuando no fuera necesaria la presencia del perito en fase de juicio oral para ratificar el informe por las razones que se han mencionado *supra*, se tendrá por reproducida, y con ello, se entenderá que las partes pueden someterla en el juicio oral a debate contradictorio, por lo que, el juzgador podrá valorarlas conforme a su sana crítica. Por el contrario, cuando la presencia del perito sea necesaria en fase plenaria para ratificar, aclarar o ampliar el informe[709], la forma de proceder a la práctica

[708] Afirma, DOLZ LAGO, M.-J. "Reflexiones sobre la prueba oficial científica (A propósito del valor probatorio de los informes periciales emitidos por Laboratorios oficiales)". La Ley Penal, Núm. 65. Sección Estudios. Noviembre 2009. Pág. 19, que, "en general, como sistematiza la doctrina, la jurisprudencia ha dado a los informes emitidos por organismos oficiales una especial fuerza probatoria y no ha exigido una estricta sujeción de ellos a las reglas procedimentales para la elaboración de los informes periciales ordinarios… la jurisprudencia ha expresado que la consideración de prueba documental del informe pericial no excluye el derecho de defensa a los medios de prueba pertinentes, de forma que si se produce una impugnación fundada es procedente la presencia de los peritos en el plenario si son propuestos por las partes". Por su parte, alude, PAZ RUBIO, J. M. "Absolución por falta de ratificación de pericial analítica expresamente impugnada". La Ley Penal, Núm. 2. Sección Fundamentos de Casación. Febrero 2004, que, "los Fiscales deben intentar practicar al menos en principio la prueba pericial de la droga de forma contradictoria durante la instrucción en presencia de todas las partes y con comparecencia de los peritos y luego en su escrito de calificación provisional deben pedir ad cautelam la prueba de los peritos al menos para el caso de que la defensa impugnen la prueba en su escrito de defensa, y si así no lo hacen y las defensas impugnan el análisis pericial de la droga en su escrito de calificación provisional, no sirve con dar lectura a esta prueba al amparo del art. 730 de la LECrim, y si no vienen los peritos a juicio se habrá producido indefensión prohibida por el art. 24 de la CE y vulneración del derecho fundamental a la presunción de inocencia de los condenados, por lo que el tema tiene gran importancia práctica". En el mismo sentido, abordan la impugnación del informe pericial, ABEL LLUCH, X., RICHARD GONZÁLEZ, M. y GARCÍA MUÑOZ, P. L. *Introducción y práctica de la prueba pericial en el juicio oral. La impugnación del informe pericial elaborado por laboratorios oficiales…* O.P. Cit. Págs. 711-716; MUÑOZ CUESTA, F. J. "Doctrina del TS sobre la falta de necesidad de que sean ratificados en juicio oral los informes periciales emitidos por organismos oficiales no impugnados por las partes y su relación con la consideración de prueba documental de la pericial sobre droga emitida por organismo oficial en el procedimiento abreviado". Repertorio de Jurisprudencia. Núm. 12. 2003, de tal forma que, vienen a concluir que, precisará de la ratificación en el juicio oral, y en caso, introducir debate contradictorio en juicio, cuando la defensa impugne los informes periciales oficiales.

[709] Afirma, RIFÁ SOLER, J. M. *Actos de investigación, actos de instrucción y actos de prueba. (Estudios sobre prueba penal I)*. Editorial La Ley. Madrid. 2010. Págs. 116 – 250, que, "la doctrina jurisprudencial

del examen será habitualmente de la siguiente manera, el Presidente del Tribunal (para órganos colegiados como Audiencias Provinciales) o el Juez (para órganos unipersonales como el Juzgado de lo Penal) exigirá a los peritos que presten juramento o promesa de imparcialidad y objetividad, seguidamente se procederá a examinar a los peritos, cuando un dictamen haya sido elaborado por varios, o bien, deban informar sobre el mismo objeto, incluso podrán ser examinados juntos (art. 724 LECrim.), para lo cual, se formularán las preguntas que estime pertinente el tribunal, comenzando primero el que la haya propuesto, cuando hayan sido todos, comenzará el Ministerio Fiscal, las acusaciones particulares o populares, y por últimos la defensa, pudiendo el Presidente del Tribunal o Juez interpelar en cualquier momento, del mismo modo, las contestaciones de los peritos no deberán contener juicios de valor, y cuando el informe hubiera sido elaborado por varios, deberán responder a la opinión mayoritaria, haciéndose constar, si hubiera alguna discrepancia entre ellos.

f´. El valor probatorio de la prueba pericial

Por último, vamos a examinar el valor probatorio de la prueba pericial, si bien, como es sabido, en el proceso penal rige el principio de la libre valoración de la prueba[710], lo cual, supone que el Tribunal, dictará sentencia valorando *según su conciencia las*

---

reiterada que sostiene que los dictámenes periciales son pruebas personales que no pierden dicho carácter por el hecho de aparecer documentadas en las actuaciones, no lo es menos que, atendiendo al principio de libre valoración de la prueba que rige en nuestros procedimientos penales, observaremos con facilidad que el precepto trascrito nada añade en materia de valoración probatoria, puesto que la convicción judicial sobre la culpabilidad o inocencia del acusado tanto puede fundarse en prueba pericial como en prueba documental. Por el contrario lo que pretende dicha norma procesal es posibilitar el acceso de la prueba pericial al plenario sin necesidad de que el perito acuda al mismo, siempre que el informe provenga de un laboratorio oficial y haya sido emitido siguiendo determinados protocolos científicos; previsión que, a mi juicio, también resulta extensible a otros procedimientos penales diferentes del abreviado, habida cuenta que no pueden admitirse diferentes formas de valorar la prueba dependiendo del concreto procedimiento penal en el que se aporte".

[710] Sobre el principio de libre valoración de la prueba en el proceso penal, véase, FUENTES SORIANO, O. *Comunicaciones telemáticas: práctica y valoración de la prueba*… O.P. Cit. Págs. 254 – 278; DELGADO MARTÍN, J. "La valoración de la prueba digital". Diario La Ley, Núm. 6. 11 de abril de 2017; BUJOSA VADELL, L. M. *La valoración de la prueba electrónica*… O.P. Cit. Págs. 75-85.

pruebas practicadas en el juicio (art. 741 LECRim. en relación con el art. 117.3 CE)[711]. De este modo, el sistema probatorio en nuestro proceso penal no es de prueba tasada, sino de libre valoración[712], lo cual, conlleva que el Tribunal no está sometido a pauta o regla alguna para valorar las pruebas practicadas en el juicio oral, aunque ésta provenga de Gabinetes y Laboratorios Oficiales, de tal forma que, también la prueba pericial informática será valorada por el Tribunal según las reglas de la sana crítica atendiendo al resto de medios de prueba que se hayan practicado en las sesiones del plenario. Además, para evitar la arbitrariedad de los poderes públicos (art. 9.3 CE), será necesario que la sentencia sea motivada (art. 120.3 CE), esto es, el juzgador habrá de argumentar la valoración de la prueba que se ha practicado bajo los principios de inmediación, contradicción, oralidad y publicidad[713], sin embargo, como mantienen nuestros Tribunales[714], no será necesario contestar a todos y cada uno de los argumentos vertidos por las partes, pues no puede tildarse de deficiente la motivación por no analizar o mencionar cada uno de ellos en la sentencia.

[711] En relación a la libre valoración de la prueba por los tribunales, véase, STC 43/1997, 10 de marzo (F.J. 2º), STC 32/1995, 6 de febrero (F.J. 4º), STC 140/1991, 20 de junio (F.J. 2º), STC 82/1988, 28 de abril (F.J. 2º); STC 47/1986, 21 de abril (F.J. 2º), STC 105/1986, 21 de julio (F.J. 5º), STC 31/1981, 28 de julio (F.J. 3º), STS 914/2016, 2 de diciembre (F.J. 2º), STS 705/2009, 30 de junio (F.D. 2º), STS 695/2002, 17 de abril (F.D. 1º) y STS 1071/2002, 7 de junio (F.D. 1º).

[712] STS 329/2015, 2 de junio (F.D. 2º) y STS 681/2013, 23 de septiembre (F.D. 2º).

[713] Con carácter general, acerca de los principios procesales de inmediación, contradicción y oralidad que rigen en el proceso penal, véase, BARONA VILAR, S. *Principios esenciales y reglas conformadoras de la actividad probatoria*… O.P. Cit. Págs. 103-148; MORENO CATENA V. *La Prueba Penal. Los principios esenciales de la actividad probatoria*… O.P. Cit. Págs. 418 – 420.

[714] STS 733/2016, 5 de octubre (F.D. 4º), STS 413/2015, 30 de junio (F.D. 4º) y STS 290/2014, 21 de marzo (F.D. 12º).

C) JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES EN LA PERSECUCIÓN Y ENJUICIAMIENTO DE LOS DELITOS TECNOLÓGICOS E INFORMÁTICOS

Los delitos tecnológicos, en especial, los cometidos a través de la red, se caracterizan por tener un gran marcado transnacional, esto es, pueden tener lugar en un Estado, pero sus consecuencias pueden afectar a otro[715]. Sin embargo, para la persecución y enjuiciamiento de los delitos rige el principio general del Derecho de territorialidad[716], esto es, como advierte el Sr. Muñoz Conde[717], *el Estado es competente para sancionar, con arreglo a las leyes propias, los hechos cometidos en su territorio (locus regit actum), independientemente de la nacionalidad de quien los haya cometido*, de igual modo, el Sr. Mir Puig[718] mantiene que, *el Derecho español es aplicable a los hechos*

[715] Aborda, VIVÓ CABO, S. "La globalización del delito: ciberdelincuencia". La Ley Penal, Núm. 132. Sección Legislación Aplicada a la Práctica. 2018, la ciberdelincuencia desde la perspectiva de la globalización, y en concreto alude que, "de la misma manera que la red proporciona infinidad de posibilidades a las personas para desenvolverse en sus quehaceres diarios, también suministrará igual cantidad de ocasiones para infringir la ley. La velocidad de los avances tecnológicos, la creciente globalización y el crecimiento exponencial de los mercados mundiales han brindado oportunidades para cometer actividades delictivas a menudo con un bajo riesgo de detección mediante nuevas formas de anonimato. Ahora bien, estas formas de delincuencia no afectan necesariamente a todos los países al mismo ritmo ni con la misma gravedad". En el mismo sentido, advierten, FLORES PRADA, I. "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia". Revista Electrónica de Ciencia Penal y Criminología. Núm. 17. 2015; CORCOY BIDASOLO, M. "Problemática de la persecución penal de los denominados delitos informáticos, particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos". Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Núm. 21. 2007. Págs. 7-32; CLIMENT BARBERÁ, J. "La justicia penal en internet. Territorialidad y competencias penales". Cuadernos de Derecho Judicial. Núm. 10. 2001. Págs. 645-663, sobre la transnacionalidad de los delitos informáticos, así como, exponen la problemática derivada de dicha circunstancia, en especial, en la averiguación del delito y el descubrimiento del ciberdelincuente.

[716] Sobre el principio de territorialidad, véase, ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L. *Límites Espaciales y Principio de Territorialidad*… O.P. Cit. Págs. 91-100; DÍEZ RIPOLLÉS, J. L. *La ley penal en el espacio*… O.P. Cit. Págs. 72 – 99.

[717] MUÑOZ CONDE, F. y GARCÍA ARÁN, M. *Derecho Penal. Parte General*… O.P. Cit. Pág. 153.

[718] MIR PUIG, S. *Derecho Penal. Parte General*… O.P. Cit. Pág. 64.

delictivos cometidos dentro del territorio español. Por su parte, las disposiciones reguladoras españolas vienen a establecer que, la causas por delito cometidos en nuestro territorio corresponderá a la jurisdicción española en el orden penal (art. 23.1 LOPJ), así como, las leyes penales obligan a todos los que se hallen en el territorio nacional (art. 8.1 CC), mientras que, la competencia territorial[719] para la investigación de delitos, recae en el *Juzgado de Instrucción del partido en que el delito se hubiere cometido* ("*forum comissi delicti"*), o en su caso, *el Juez de Violencia sobre la Mujer, o el Juez Central de Instrucción respecto de los delitos que la Ley determine* (art. 14.2 LECrim). De esta manera, con carácter general, para la persecución y enjuiciamientos de los delitos, lo cual, incluye también los tecnológicos, primeramente, habrá que determinar la jurisdicción, esto es, el Estado que le corresponde el conocimiento de la causa, para a continuación, determinar que órganos jurisdiccionales ostentan la competencia territorial. De la misma manera, en el ámbito del Derecho internacional, el Convenio sobre la Ciberdelincuencia hecho en Budapest[720], viene acogiendo el principio de territorialidad como criterio principal, en el sentido de que, los Estados adoptarán las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto a los delitos informáticos (art. 22 C.B.), sin embargo, los Estados han venido flexibilizando dicho criterio, de tal forma que, en el caso español, los apartado 2º, 3º y 4º del art. 23 L.O.P.J, como veremos posteriormente, para determinados supuestos se permite el enjuiciamiento de hechos que hayan sido cometidos fuera de nuestras fronteras. No obstante, el delito tradicional con frecuencia se comete en un lugar concreto del territorio nacional, por lo que, determinar la jurisdicción y competencia suele ser sencillo, mientras que, para los delitos tecnológicos que, pueden tener distintos lugares de conexión o localizaciones de los dispositivos electrónicos o equipos informáticos, incluso en varios Estados diferentes, puede resultar complejo fijar el lugar concreto de su comisión. Por este motivo, la aplicación estricta del principio territorialidad, con arreglo a las disposiciones que venimos exponiendo, puede constituir

[719] En relación con la competencia territorial de los juzgados en el ámbito penal, con arreglo al art. 14.2 LECrim, véase, GÓMEZ COLOMER, J. L. *La competencia penal*… O.P. Cit. Págs. 53 – 70; SANTOS MARTÍNEZ, A. M. *Jurisdicción y competencia*… O.P. Cit. Págs. 33-39; ASENCIO MELLADO, J. M. "Competencias en los órdenes civil y penal". Poder Judicial. Núm. Extra 16. 1990. Págs. 159-165.

[720] «BOE» Núm. 226, de 17 de septiembre de 2010.

un obstáculo para la investigación y enjuiciamiento de delitos cometidos a través de las nuevas tecnologías, pues podrían quedar impunes numerosos hechos realizados en el ciberespacio. Por todo ello, seguidamente vamos a abordar la jurisdicción y competencia de los Tribunales en la persecución de esta clase de delitos, para lo cual, autores y la jurisprudencia de nuestros Tribunales han dado distintas soluciones, y en concreto, la creación de Tribunales internacionales especializados, la aplicación del principio de jurisdicción universal, la aplicación de la teoría de la acción o del resultado, o bien, la ubicuidad.

I. Los Tribunales internacionales

Como venimos exponiendo, los delitos cometidos a través de las nuevas tecnologías pueden tener repercusiones transfronterizas, pues el ciberespacio es un medio donde las comunicaciones superan cualquier límite que pudieran establecer los Estados. Por este motivo, autores como el Sr. Flores Prada[721] vienen proponiendo que, la solución pasaría por la creación de un Tribunal Internacional que tuviera por objeto conocer del enjuiciamiento de delitos tecnológicos. Sin embargo, esta solución surgen problemas prácticos a tener en cuenta, pues cada vez son más frecuentes los hechos delictivos relacionados con el ciberespacio, por lo que, el Tribunal tendría una gran carga de trabajo, pero además, generaría graves dificultades de logística, piénsese en una sede física judicial que se localice en un Estado, mientras que los perjudicados, operadores jurídicos o investigados se encuentren en otro, lo cual, supondría que nunca sería plenamente eficaz la misma.

Otra variante de esta solución, sería que se encargara la Corte Penal Internacional de enjuiciar los delitos más graves relacionados con la informática, como por ejemplo los de propiedad intelectual a gran escala, redes internacionales de pornografía infantil o los fraudes económicos internacionales[722], si bien, aparte de que el Estatuto de Roma de la

[721] Propone, FLORES PRADA I., *Criminalidad Informática. Aspectos sustantivos y procesales…* O.P. Cit Págs. 315-317, como solución para el problema de la transnacionalidad de los delitos informáticos, la creación de un Tribunal Internacional, si bien, advierte también, los problemas que suscita y que han sido aludidos en el cuerpo del texto.

[722] Exponen la competencia de la Corte Internacional Penal, con arreglo al art. 5.1 del Estatuto de Roma de la Corte Penal Internacional, OLÁSOLO ALONSO, H. y CARNERO ROJO, E. *Extensión y límites de*

Corte Penal Internacional[723] no comprende entre sus competencias el conocimiento de delitos tecnológicos, esta solución únicamente podría ser posible con una cooperación eficaz entre los Estados y las organizaciones internacionales, pues habría que definir claramente el reparto de competencias entre ellos, así como establecer la extensión territorial de la conducta con la gravedad delictiva. En definitiva, estas soluciones nos parecen inviable, pues genera más problemas que beneficios en la persecución y enjuiciamientos de los delitos transnacionales como pueden ser los tecnológicos.

II. El principio de jurisdicción universal

La siguiente posible solución para la investigación y enjuiciamiento de los delitos cometidos en el ciberespacio, sería establecer al Juez nacional como Juez universal[724] en materia de delincuencia informática[725], esto es, el Juez nacional de cualquier Estado

---

la jurisdicción personal, territorial y temporal de la Corte Penal Internacional. (El principio de justicia universal, fundamentos y límites). Editorial Tirant lo Blanch. Valencia. 2012. Págs. 105-138; FAKHOURI GÓMEZ, Y. *La competencia de la Corte Penal Internacional, competencia material, personal y temporal y sus condiciones de ejercicio y de control. (Derecho penal y política transnacional).* Editorial Atalier. Barcelona. 2005. Págs. 85-115, de modo que, la competencia se limitará a los crímenes más graves de trascendencia para la comunidad internacional en su conjunto, en concreto, el genocidio, crímenes de lesa humanidad, crímenes de guerra y crimen de agresión, por lo que difícilmente será de aplicación para delitos tecnológicos.

[723] Estatuto de Roma de la Corte Penal Internacional, de 17 de julio de 1998, tras varias enmiendas, entró en vigor el 1 de julio de 2002. «BOE» Núm. 126, de 27 de mayo de 2002.

[724] Con carácter general sobre el principio de justicia universal, véase, CASTAÑÓN ÁLVAREZ, M. J. "Ciberterrorismo: principio de justicia universal". Diario La Ley, Núm. 8.920. Sección Doctrina. 13 de febrero de 2017; VIADA BARDAJÍ, S. "Cuestiones relativas al principio de justicia universal". Estudios Jurídicos. Núm. 2007; OCAÑA RODRÍGUEZ, A. "Cuestiones relativas al principio de justicia universal". Estudios Jurídicos. Núm. 2007; JAÉN VALLEJO, M. *Extraterritorialidad de la jurisdicción española, principio de justicia universal*… O.P. Cit. Págs. 237-250; CONDE-PUMPIDO TOURÓN, C. "La justicia universal en la jurisdicción española". Persona y Derecho: Revista de Fundamentación de las Instituciones Jurídicas y de Derechos Humanos. Núm. 51. 2004. Págs. 49-74; GARCÍA ARÁN, M. *El principio de justicia universal en la L.O. del Poder Judicial español. (Crimen internacional y jurisdicción universal: el caso Pinochet)*. Editorial Tirant lo Blanch. Valencia. 2000. Págs. 63-88.

[725] Mantiene, FLORES PRADA I., *Criminalidad Informática. Aspectos sustantivos y procesales…* O.P. Cit. Págs. 317-318, que, "para determinados delitos, muchos Estados configuran ya a los jueces

podría conocer de los hechos delictivos cometidos mediante las nuevas tecnologías, independientemente del lugar donde se encuentre el autor y de su nacionalidad. Sin embargo, la regulación sobre la jurisdicción universal[726] contenida en la Ley Orgánica del Poder Judicial[727] fue reformada[728] para restringir su ámbito de aplicación[729], en el

---

nacionales como jueces universales, extendiendo su competencia a delitos cometidos en cualquier lugar del mundo y con independencia de la nacionalidad de su autor. Así sudece en España en virtud de lo dispuesto en el art. 23.4 LOPJ… Sin embargo, y por el momento, esta solución no es viable en nuestro país para la delincuencia informática, o al menos para la mayoría de los delitos informáticos". Por su parte, afirman, DE LA CUESTA ARZAMENDI. J.L. y DE LA MATA BARRANCO N.J., *Derecho Penal informático…* O.P. Cit. Págs. 248-249, que, "ni el Convenio sobre Ciberdelincuencia ni la regulación española prevén la aplicación de este principio a los supuestos de cibercriminalidad. En efecto, en el listado de delitos respecto de los cuales rige el principio de justicia universal del art. 23 LOPJ no hay ningún supuesto que refiera específicamente delitos de esta naturaleza". En el mismo sentido, señalan, VELASCO NUÑEZ E., *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 66-69 y FERNÁNDEZ TERUELO, J.G., *Cibercrimen. Los delitos cometidos a través de Internet…* O.P. Cit. Págs. 20-30, que, la justicia universal como medio para la persecución de la investigación o enjuiciamiento de los delitos informáticos, si bien, existen dificultades prácticas para su ejecución.

[726] En relación a la justicia universal para la persecución del ciberterrorismo, CASTAÑÓN ALVAREZ, M. J. "Ciberterrorismo: principio de justicia universal". Diario La Ley. Núm. 8920. 2017, afirma que, "uno de los problemas fundamentales que plantea el ciberterrorismo es el de la determinación de la jurisdicción y de la competencia de los tribunales para conocer este tipo de delincuencia. Es difícil concretar el origen del ataque ciberterrorista porque normalmente no hay seguridad del sitio en que se originó el hecho. Son frecuentes los supuestos en los que un presunto delincuente se encuentra en un país y utiliza para cometer el delito sitios de Internet o servicios de proveedores de servicios de Internet hospedados en otro, o los casos en que personas residentes en un país han creado, administrado y mantenido sitios Web en otro país, para promover la yihad y con otros fines relacionados con el terrorismo. En todos estos supuestos la deslocalización pugna con los tradicionales principios de territorialidad. Por ello, se apuesta por aplicar el principio de jurisdicción universal. Con la última reforma de la justicia universal, operada por Ley Orgánica 1/2014, de 13 de marzo, se desnaturaliza y prácticamente erradica de nuestro ordenamiento jurídico este principio. Pero además, en materia concreta de terrorismo, los límites y condiciones que impone la nueva redacción del art. 23.4 e) de la LOPJ, resultan contrarios al concepto penal de terrorismo e incumplen los mandatos que las Naciones Unidas imponen a los Estados miembros".

[727] En el art. 23 de la L.O.P.J. se regula la jurisdicción de los Tribunales españoles en el orden penal, y en particular: el art. 23.1 de la L.O.P.J. se establece el principio de territorialidad como norma general sobre la jurisdicción en el orden penal, esto es, conocerán los Tribunales españoles de las causas por delitos cometidos en territorio español. Asimismo, en los apartados siguientes se regulan las excepciones al

sentido de, condicionar su aplicación a un tratado internacional que legitime su actuación, o bien, tener una vinculación con España por razón de nacionalidad o de residencia. De esta manera, la solución planteada, difícilmente tendría encaje para la delincuencia informática, pues la norma procesal establece también que, la jurisdicción universal, podrá servir para la persecución de hechos delictivos específicos contenidos en el art. 23.4 LOPJ[730], si bien, están relacionados únicamente con las nuevas

principio de territorialidad, de tal forma que: el art. 23.2 de la L.O.P.J., se regula el criterio de personalidad, esto es, los Tribunales españoles conocerán de los delitos hayan sido cometidos fuera del territorio nacional por ciudadanos españoles; el art. 23.3 de la L.O.P.J. se regula el criterio real de protección, esto es, los Tribunales españoles conocerán de los delitos cometidos fuera del territorio español contra intereses nacionales; el art. 23.4 de la L.O.P.J. se regula la jurisdicción universal de los Tribunales españoles en los términos que venimos estudiando.

[728] Los apartados 2º, 4º y 5º del art. 23 L.O.P.J. sobre la jurisdicción universal, fueron modificados, y se añadiría el apartado 6º mediante la L.O. 1/2014, de 13 de marzo, *de modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, relativa a la justicia universal* («BOE» Núm. 63, de 14 de marzo de 2014) así como, posteriormente se reformaría el apartado 4.e) mediante la Disposición Final Primera de la L.O. 2/2015, de 30 de marzo, *por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo* («BOE» Núm. 77, de 31 de marzo de 2015). De esta manera, refieren a la reforma sobre la justicia universal, y sus repercusiones, OLLÉ SESÉ, M. *La nueva regulación del principio de justicia universal. (La reforma penal de 2013: Libro de Actas. XIV Jornadas de profesores y estudiantes de Derecho Penal de las Universidades de Madrid).* Universidad Complutense de Madrid. 2014. Págs. 57-64; PÉREZ MEDINA, A. "Golpe a la justicia universal". Iuris: Actualidad y Práctica del Derecho. Núm. 209. 2014. Págs. 4-6; MORALES PRATS, F. "La Reforma del Principio de justicia universal". Revista de Derecho y Proceso Penal. Núm. 35. 2014. Págs. 13-20; GUIMERÁ FERRER-SAMA, R. "¿Adiós a la justicia universal?" Práctica Penal: Cuaderno Jurídico. Núm. 75. 2014. Págs. 29-31.

[729] De esta manera, la justicia universal ha sido criticada en la STS 1240/2006, de 11 de diciembre (F.D. 8º), pues dispone que el "Derecho penal internacional parece orientarse más bien hacia los Tribunales internacionales y a la intervención de las Naciones Unidas".

[730] Art. 23.4 LOPJ sobre los delitos perseguibles fuera de nuestras fronteras con arreglo al principio de jurisdicción universal: *a) Genocidio, lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, b) Delitos de tortura y contra la integridad moral c) Delitos de desaparición forzada d) Delitos de piratería, terrorismo, tráfico ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas, trata de seres humanos, contra los derechos de los ciudadanos extranjeros y delitos contra la seguridad de la navegación marítima que se cometan en los espacios marinos, e) Terrorismo f) Los delitos contenidos en el Convenio para la represión del apoderamiento ilícito de aeronaves, g) Los*

tecnologías, el terrorismo (piénsese en el delito de adoctrinamiento de terrorismo a través de internet o de un servicio de comunicaciones electrónicas –art. 575.2 CP-), delitos contra la libertad e indemnidad sexual (por ejemplo delito de pornografía infantil –art. 189 CP-), delito contra la violencia doméstica (por ejemplo amenazas cometidas a través de un servicio de comunicaciones electrónicas contra el cónyuge o persona ligada por una análoga relación de afectividad -art. 171.4 CP-) o delitos sobre falsificación de productos médicos y delitos que supongan una amenaza para la salud pública (piénsese en la distribución por internet de medicamentos falsificados que generen un riesgo para la vida o salud de las personas -arts. 361 y 362 bis CP.-), todo ello, sin perjuicio de que pudiera suscribirse algún Tratado Internacional que pudiera legitimar la persecución de otros delitos informáticos (apartado 4 in fine del art. 23 LOPJ). De la misma manera, la jurisdicción universal como un principio derivado del Derecho internacional que, tiene su apoyo en el interés supranacional de hacer posible que los Tribunales internos puedan ejercer la jurisdicción penal para el enjuiciamiento de determinados crímenes internacionales, que además, deberán ser especialmente gravosos para la comunidad internacional, es por ello que, para delitos tecnológicos ordinarios, difícilmente podrá ser de aplicación esta solución.

En otro orden de ideas, el problema que surge cuando todos los Estados tienen jurisdicción para conocer de los delitos cometidos fuera de su territorio será que puede originar la doble incoación de procedimientos penales, dicho de otro modo, puede darse el supuesto de que se inicie una investigación en un Estado, mientras que en otro se están investigando los mismos hechos, produciéndose por tanto, varias investigaciones paralelas por la misma actuación delictiva, lo cual, podría vulnerar el principio *ne bis in*

---

delitos contenidos en el Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil, h) Los delitos contenidos en el Convenio sobre la protección física de materiales nucleares i) Tráfico ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas, j) Delitos de constitución, financiación o integración en grupo u organización criminal o delitos cometidos en el seno de los mismos, k) Delitos contra la libertad e indemnidad sexual l) Delitos sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, m) Trata de seres humanos, n) Delitos de corrupción entre particulares o en las transacciones económicas internacionales, o) Delitos sobre falsificación de productos médicos y delitos que supongan una amenaza para la salud pública p) Cualquier otro delito cuya persecución se imponga con carácter obligatorio por un Tratado vigente para España o por otros actos normativos de una Organización Internacional de la que España sea miembro.

idem[731]. De esta manera, la prohibición de un doble proceso con un mismo objeto, viene regulado en el Pacto Internacional de Derechos Políticos y Civiles[732] cuando se establece que, *nadie podrá ser juzgado ni sancionado por un delito por el cual haya sido ya condenado o absuelto por una sentencia firme de acuerdo con la ley y el procedimiento penal de cada país* (art. 14.7 P.I.D.P.C.), mientras que, nuestro Tribunal Constitucional mantiene que, *sólo se incurre en esa prohibición cuando el primer proceso ha concluido con una resolución que produzca el efecto de cosa juzgada material*, de tal forma que, según mantiene nuestro Tribunal garante de la Constitución, el principio de *ne bis in idem* afecta únicamente a resoluciones con efecto de cosa juzgada, por lo que, nada impediría iniciar por los mismos hechos dos investigaciones simultáneas, siempre que en alguna de ellas no haya recaído previamente una resolución con efecto de cosa juzgada material negativa o excluyente[733]. Sin embargo, cosa distinta es la litispendencia[734], esto es, la situación y efectos que se producen con la incoación de varios procesos con el mismo objeto, de tal forma que, se ha venido a considerar, como una institución cautelar o tutelar de la cosa juzgada, es decir, lo que hoy está

[731] Acerca del principio de *ne bis in idem*, en especial, en el ámbito de la Unión Europea, véase, GARCÍA RIVAS, N. "Alcance y perspectivas del ne bis in idem en el espacio jurídico europeo". Revista General de Derecho Penal. Núm. 27. 2017; MENDOZA CALDERÓN, S. "Criminalidad organizada económica y aplicación del principio "ne bis in idem" en la Unión Europea". Revista de Derecho y Proceso Penal. Núm. 41. 2016. Págs. 61-88; RAFARACI, T. *"Ne bis in idem" y conflictos de jurisdicción en materia penal en el espacio de libertad, seguridad y justicia de la Unión Europea. (Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal)*. Editorial Lex Nova. Madrid. 2010. Págs. 122-150; BLANCO CORDERO, I. "El principio ne bis in idem en la Unión Europea". La Ley: Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía. Núm. 3. 2005. Págs. 1972-1987.

[732] Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966, ratificado por España el 28 de septiembre de 1976, y publicado en el «BOE» Núm. 103, de 30 de abril de 1977.

[733] STC 222/1997, de 4 de diciembre (F.J. 4º) y STC 159/1987, de 26 de octubre (F.J. 2º) refieren al principio *non bis in idem*.

[734] Sobre la litispendencia, véase, CHOZAS ALONSO, J. M. "La litispendencia efectos y tratamiento procesal". Cuadernos de Derecho Judicial. Núm. 6. 2000. Págs. 71-116; SALAS CARCELLER, A. "La litispendencia y sus relaciones con la cosa juzgada". Revista General de Derecho. Núm. 628-629. 1997. Págs. 81-112.

siendo investigado, probablemente en el futuro será cosa juzgada[735]. De este modo, se podrían iniciar dos investigaciones paralelas, podrían continuar su curso, hasta terminar alguna en resolución con efecto de cosa juzgada material, y entonces, se podría incurrir en una vulneración del principio *ne bis in idem*, el cual, como venimos afirmado, viene prohibido tanto por el derecho interno, como internacional. De esta manera, cuando el órgano judicial que conozca de la instrucción o del enjuiciamiento de un proceso penal en España aprecie indicios suficientes de que, en otro Estado miembro de la Unión Europea, se está tramitando un proceso penal con el mismo objeto, se deberá proceder conforme la Ley 16/2015, de 7 de julio, *por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior*[736], que vino a transponer la Decisión Marco 2009/948/JAI[737], de 30 de noviembre *sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales*, en relación con Decisión 2009/426/JAI del Consejo de 16 de diciembre de 2008[738], que modificaría la Decisión 2002/187/JAI[739], la cual, vino a crear el Eurojust, esto es, el órgano encargado del refuerzo de la cooperación judicial entre los Estados miembros. De este modo, la regulación aludida viene a establecer que, cuando las autoridades competentes tengan conocimiento de que se está tramitando un proceso penal paralelo en otro Estado miembro, deberá requerirle a éste, para intentar llegar a un

[735] En relación a la litispendencia en el proceso civil, DE LA OLIVA SANTOS, A. y DIEZ-PICAZO GIMÉNEZ, I., *Derecho Procesal Civil: El proceso de declaración.* Editorial Universitaria Ramón Areces. Madrid. 2004. Pág. 281, mantiene que es tutelar o cautelar de la cosa juzgada. Sin embargo, a estos efectos, será también, plenamente aplicable para la jurisdicción penal. En el mismo sentido, la STS (Sala de lo Civil) 150/2011, de 11 de marzo (F.D. 3º).

[736] «BOE» Núm. 162, de 8 de julio de 2015.

[737] «DOUE», 15 de diciembre de 2009, L 328/42-47. En este sentido traemos a colación, MARTÍN DIZ, F. "Prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales, comentario a la Decisión Marco 2009/948/JAI del Consejo de 30 de noviembre de 2009*"*. Revista General de Derecho Europeo. Núm. 21. 2010, en el cual, con carácter general, viene a examinar la mencionada Decisión Marco 2009/948/JAI.

[738] «DOUE» Núm. 138, de 4 de junio de 2009. Págs. 14 a 32.

[739] «DOCE» Núm. 63, de 6 de marzo de 2002. Págs. 1 a 13.

acuerdo con el objeto de evitar las consecuencias adversas derivadas de dichos procedimientos simultáneos (arts. 30 L. 16/2015 y 10 D.M. 2009/948/JAI), en caso de no lograrse ningún acuerdo, se podrá trasladar el asunto al Eurojust, siempre que se trate de una materia incluida en su ámbito de competencias (arts. 32.2 L. 16/2015 y 12.2 D.M. 2009/948/JAI), si bien, con arreglo art. 4.1.b) de la Decisión 2002/187/JAI, se incluye la delincuencia informática. Seguidamente, recibido el dictamen del Eurojust, que no será vinculante, el Juez o Tribunal resolverá, por auto motivado, sobre la continuación o no del procedimiento ante la jurisdicción española (arts. 32.4 L. 16/2015). Debido a lo cual, la D.M. 2009/948/JAI deja los conflictos de jurisdicción a la voluntad de los Estados miembros, para lo cual, deberán resolverlo de mutuo acuerdo, y en caso de lograse el mismo, entrará en juego el Eurojust, si bien, en el caso español, su decisión no será vinculante, de tal forma que, el Juez o Tribunal español tendrá la última palabra. Sin embargo, la solución dada por la Unión Europea para resolver los conflictos de jurisdicción, bajo nuestro punto de vista, nos parece insatisfactoria, puesto que no establece criterios claros u obligaciones específicas para que los Estados se abstengan de conocer de un proceso penal que está siendo tramitado en otro Estado miembro. Por esta razón, las teorías que seguidamente vamos a estudiar, nos parecen más adecuadas para resolver los conflictos de jurisdicción, o en su caso, de competencia territorial para la investigación o enjuiciamiento de delitos tecnológicos.

III. La teoría de la acción o del resultado

De esta manera, otra posible solución para determinar la jurisdicción de los Estados para la investigación y enjuiciamiento de los delitos tecnológicos, o bien, lo que será más habitual aquí, fijar la competencia territorial de los Tribunales[740] será aplicar la teoría de

[740] En lo concerniente a la competencia territorial de los Tribunales para la investigación y enjuiciamiento de delitos, véase, VELASCO SAN MARTÍN, C. *Jurisdicción penal aplicable en países europeos con sistema de derecho codificado. España.* (*Jurisdicción y competencia penal en relación al acceso transfronterizo en materia de ciberdelitos)*. Editorial Tirant Lo Blanch. Valencia. 2016. Págs. 191 – 204; ROSENDES, E. E. "Ejercicio de la acción y la competencia en los delitos informáticos". Revista de Derecho Penal y Criminología. Núm. 9. 2012. Págs. 165-175; VELASCO SAN MARTÍN, C. *Jurisdicción y Legislación Aplicable en el Ámbito Internacional.* (*La jurisprudencia y competencia sobre delitos cometidos a través de cómputo e internet)*. Editorial Tirant Lo Blanch. Valencia. 2012. Págs. 199-208; VENTAS SASTRE, R. "Problemas de jurisdicción y competencia en la persecución de los delitos cometidos a través del juego por Internet". Cuadernos de Política Criminal. Núm. 94. 2008. Págs. 239-

la acción o del resultado. De este modo, se ha acuñado los términos *acción* y *resultado*[741] dentro de la teoría general del delito, de tal forma que, se considera *acción* como aquella conducta típica y antijurídica realizada por una persona, mientras que *resultado*, será la modificación del mundo exterior provocada por dicha conducta o la consecuencia de dicha acción. De esta manera, la teoría de la *acción*, supone que la jurisdicción, o en su caso, la competencia territorial del Tribunal, corresponderá en aquel lugar donde el sujeto realiza el inicio de la conducta delictiva, o dicho de otro modo, desde donde se dirige la lesión o puesta en peligro del bien jurídico protegido. Por el contrario, la teoría del *resultado,* conlleva que la atribución de la jurisdicción al Estado, y en su caso, la competencia territorial recaerá en el Tribunal del lugar donde se despliega el perjuicio lesivo[742]. Para una mejor comprensión explicaremos estas teorías con ejemplos, de tal forma que, piénsese en la comisión de un delito de daños informáticos (art. 264.1 CP) que un ciberdelincuente con un ordenador de forma grave borra o daña los datos informáticos de otro sistema ubicado en otro lugar, o bien, en una estafa cometida a través de soportes informáticos (art. 248 CP), en el cual, el ciberdelincuente con un equipo informático, utilizando engaño bastante para producir un error en otro, induce a una persona con un dispositivo electrónico ubicada en otro lugar para realizar un acto de disposición económico, de modo que, conforme la teoría de la *acción*, la jurisdicción recaerá en el Estado del lugar donde se encuentre el equipo informático del sujeto activo del delito, pero también, la competencia territorial del Tribunal vendría atribuida al lugar donde se encuentre el ciberdelincuente con el terminal empleado en la comisión del delito, independientemente de a quién o donde, vaya dirigida la lesión o puesta en peligro del bien jurídico protegido, mientras que, la

254; QUINTERO OLIVARES, G. "Internet y Derecho penal: imputación de los delitos y determinación de la competencia". La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario. Año 4. Núm. 37. 2007. Págs. 5-24.

[741] Sobre los términos de acción y resultado, véase, MIR PUIG S., *Derecho Penal. Parte* General… O.P. Cit. Págs. 155 y 181 a 206); CONDE-PUMPIDO FERREIRO C., *Derecho Penal. Parte General*… O.P. Cit. Págs. 111 a 118; MUÑOZ CONDE F., *Derecho Penal. Parte General*… O.P. Cit. Págs. 211 a 235.

[742] Aborda, VELASCO NUÑEZ E., *Delitos cometidos a través de Internet. Cuestiones Procesales…* O.P. Cit. Págs. 62 – 66, las teorías de la acción y el resultado para determinar la jurisdicción del Estado o la competencia territorial del juzgado en los delitos informáticos.

teoría del *resultado*, la jurisdicción y/o competencia corresponderá al lugar o lugares donde se ubique el sistema objeto del ataque, o bien, el dispositivo de la víctima, independientemente de donde se encuentre el autor del delito.

IV. La teoría de la ubicuidad

Estrechamente relacionada con las teorías enunciadas anteriormente, tenemos la ubicuidad[743], la cual, ha tenido mayor repercusión, y es seguida de manera unánime por nuestros Tribunales[744], si bien, venía siendo utilizada para los delitos continuados (art. 74.1 CP y 18.2 LECrim.), la cual, ahora también puede extenderse para los delitos tecnológicos. De este modo, se trata de una teoría ecléptica que confluyen ambos supuestos mencionados anteriormente, de tal forma que, consiste en reputar cometido el delito tanto en el lugar de ejecución de la acción u omisión o donde se inicia el delito (teoría de la acción), como en el lugar o los lugares en los que se produce o hubiera podido producirse el/los resultado/s, esto es, donde se producen las consecuencias del delito (teoría del resultado), de manera, conforme esta teoría se atribuirá la jurisdicción al Estado, y en su caso, la competencia territorial al Tribunal de cualquiera de ellos, sin embargo, para evitar ocasionar duplicidad de procesos sobre el mismo objeto, conocerá

[743] Abordan la competencia territorial para la investigación y enjuiciamiento de los delitos, en especial los informáticos, GÓMEZ COLOMER, J. L. *Los criterios de atribución. Territorial*… O.P. Cit. Págs. 66-67; ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L. *Lugar de la comisión del delito*… O.P. Cit. Págs. 92-93; MORENO CATENA, V. *Competencia territorial*… O.P. Cit. Págs. 80 – 82; MUERZA ESPARZA, J. "Aspectos procesales del delito continuado". La Ley Penal, Núm. 126, Sección Derecho Procesal Penal, mayo-junio 2017; GRANADOS PÉREZ, C. *Competencia territorial. Principio de ubicuidad. (Acuerdos del Pleno de la Sala Penal del Tribunal Supremo Para Unificación de la Jurisprudencia).* Editorial Tirant Lo Blanch. Valencia. 2017. Págs. 704 – 706; LUZÓN PEÑA, D.-M. *Lugar de comisión del delito*… O.P. Cit. Págs. 119 – 120; CHOZAS ALONSO, J. M. *La competencia territorial en los acuerdos del TS. (Los sujetos protagonistas del proceso penal)*. Editorial Dykinson. Madrid. 2015. Págs. 153-155; QUINTANAR DÍEZ, M., VELASCO NUÑEZ, E. *Competencia. (Delitos cometidos a través de Internet)*… O.P. Cit. Págs. 62 – 75, los cuales, tras analizar los conflictos de competencia, vienen a proponer como solución la teoría de la ubicuidad.

[744] Sírvase de ejemplo de decisiones judiciales que vienen a aplicar el principio de ubicuidad, STS 504/2016, de 9 de junio (F.D. 1º), STS 307/2016, de 13 de abril (F.D. 2º), STS 456/2013, de 9 de junio (F.D. 2º), STS 798/2013, de 5 de noviembre (F.D. 3º), STS 788/2009, de 12 de julio (F.D. 2º), STS 854/2008, de 4 de diciembre (F.D. 3º) y STS 341/2005, de 17 de marzo (F.D. 1º).

el primero que hubiera comenzado la investigación o el enjuiciamiento, siempre que en el mismo se hubiera realizado algún elemento del tipo, debiéndose inhibirse en favor de aquel, los juzgados que incoen procedimientos posteriores. En los ejemplos mencionados anteriormente, en la comisión de un delito de daños informáticos (art. 264.1 CP) o estafa cometida a través de soportes informáticos, tendrá la jurisdicción el Estado, o bien, la competencia territorial recaerá en cualquier juzgado que conozca en primer lugar, siempre que se hubiera realizado algún elemento del tipo en él.

CONCLUSIONES

Seguidamente, vamos a extraer, los aspectos más relevantes del presente trabajo de investigación, en concreto, lo concerniente al ramo procesal de los delitos informáticos y tecnológicos, esto es, las medidas de investigación tecnológicas, la prueba pericial informática, la jurisdicción y competencia de los tribunales en la persecución y enjuiciamiento

I. - Las medidas tecnológicas consisten en el núcleo esencial del presente trabajo, en particular, las restrictivas de los derechos fundamentales (intimidad, inviolabilidad domiciliaria, secreto de las comunicaciones y protección de datos). Además, la reforma procesal implementada en el 2015, supuso otorgar mayores garantías en la adopción de esta clase de diligencias, pues anteriormente existía una grave deficiencia legislativa sobre la materia.

- Se ha examinado la cuestión procesal de los descubrimientos casuales. Así, con arreglo al principio de especialidad, la autorización judicial debe especificar el delito concreto que se pretende investigar con la medida. Ahora bien, el problema surge cuando habiéndose acordado una medida restrictiva de derechos fundamentales para la investigación de un delito se descubre otro distinto no amparado por dicha resolución. Así, no parece que exista justificación alguna para que un funcionario actuante que esté investigando unos hechos con apariencia delictiva cierre los ojos ante los indicios de un delito que se presente a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en la investigación oficial. Por este motivo, cuando se descubra un delito casual en la práctica de una medida tecnológica, como en la interceptación de las comunicaciones telefónicas y telemáticas, se establece que, para continuar la investigación respecto al nuevo hecho delictivo encontrado, se requiere de una autorización judicial renovada. Por tanto, el Juez habrá de comprobar 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. En cambio, en la diligencia de entrada y registro domiciliario, se caracteriza por su realización en unidad de acto, es decir, la medida normalmente se desarrolla en una jornada. Por este motivo, la jurisprudencia viene entendiendo que, cuando en la ejecución de un registro domiciliario, se descubran

delitos inesperados, no es necesario acordar una nueva autorización judicial, pues dicho hallazgo queda amparado por el criterio de la flagrancia. Aunque no faltan ejemplos jurisprudenciales que aplican otros criterios como la proporcionalidad, en el sentido de que el nuevo delito, deba ser tenido como grave.

1) La primera medida tecnológica que hemos analizado es la interceptación de las comunicaciones telefónicas y telemáticas. Así, hay delitos cometidos a través de las nuevas tecnologías que se castigan con penas escasas de prisión, como por ejemplo los delitos de posesión de material pornográfico que se castiga con pena de tres meses a un año de prisión o con multa de seis meses a dos años (art. 189.5 CP). Ahora bien, bajo nuestro criterio, prácticamente la única manera de poder combatir estos delitos tecnológicos, será con la utilización de las mismas armas por parte del Estado. Por este motivo, se ha incluido como presupuesto, la investigación de los delitos tecnológicos, independientemente de la gravedad de los mismos.

- El Juez tiene la obligación de controlar la medida, para ello, la Policía Judicial pondrá a su disposición, con la periodicidad que éste determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. De igual modo, habrá de indicar el origen y destino de las grabaciones. Además, para asegurar la autenticidad e integridad de la información volcada desde el ordenador central (en el caso español, el Sistema Integrado de Interceptación de Telecomunicaciones –SITEL-) a los soportes digitales, se deberán encriptar los contenidos mediante una serie de algoritmos matemáticos (la técnica *hash),* que permita reconocer en todo momento la identidad del contenido, pues cualquier variación en la numeración determina la contaminación del efecto, y en consecuencia, la ruptura de la cadena de custodia.

- Se deberá informar a las personas que hayan participado en las comunicaciones interceptadas pero que sean ajenas a la causa penal, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Esta norma pretende evitar una "corruptela" de la Policía Judicial que consiste en incorporar en el oficio de solicitud de autorización judicial de la adopción de la interceptación de las comunicaciones telefónicas y telemáticas, los números de teléfonos de los investigados junto con otros números de personas que no tienen relación alguna con la investigación. Así, el Juez acuerda su intervención para todos los teléfonos, sin

saber que, algunos no corresponden con la titularidad o uso de los investigados. Sin embargo, en nuestra opinión, esta disposición legal tendrá escasa aplicación, pues será difícil averiguar y comunicar a todos los terceros no investigados que han sido objeto de una medida restrictiva de derechos fundamentales. Además, probablemente los juzgados no dedicarán recursos técnicos y económicos para dicho fin, salvo circunstancias excepcionales, como personas de interés público o cuando el propio interesado expresamente lo solicite.

- La práctica forense demuestra que, el contenido de la conversación cada día resulta menos útil para la investigación, puesto que normalmente los delincuentes para evitar ser descubiertos eluden decir o escribir expresiones que puedan incriminarlos. Por este motivo, el Estado podrá acceder también a los datos electrónicos de tráfico o asociados, esto es, los derivados de una comunicación o a efectos de la facturación de la misma (por ejemplo, número de teléfono, titulares de la línea, fecha, hora y duración de una comunicación, etc.), aunque también, a los datos que se produzcan independientemente del establecimiento de la comunicación (por ejemplo, geolocalización).

- Los prestadores de servicios de telecomunicaciones tienen la obligación de prestar al Juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados la asistencia y colaboración precisa para la ejecución de la medida de intervención de las comunicaciones, pudiendo incluso en caso contrario, incurrir en delito de desobediencia a la autoridad. De este modo, los prestadores de servicios de telecomunicaciones tienen el deber de colaboración con el Estado en todo lo necesario para ejecutar una diligencia de intervención de las comunicaciones, el cual, comprende entre otros aspectos la conservación y cesión de los datos electrónicos de tráfico o asociados. Como ya nos hemos referido, resulta de gran utilidad para la investigación conocer los datos generados en una comunicación. Por esta razón, la norma procesal establece que, los prestadores de servicios únicamente podrán ceder estos datos para su incorporación al proceso con autorización judicial. Sin embargo, la norma procesal no regula el contenido de los datos de tráfico o asociados, para lo cual, deberá ser completada con la legislación administrativa sobre esta materia, en concreto, mediante 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 transpone la Directiva 2006/24/CE, de 15 de marzo, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones* y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.* Ahora bien, el problema ha surgido cuando la Sentencia del T.J.U.E. de 8 de abril de 2014, ha declarado la nulidad de la Directiva 2006/24/CE, debido a que la norma europea venía a establecer la obligación de conservación de los datos asociados por parte de proveedores de servicios sin restricción alguna. Por tanto, sin que se condicione al interés general, la seguridad pública, la prevención de delitos y la lucha contra la delincuencia, en especial, la delincuencia organizada o el terrorismo. En efecto, como dispone la propia sentencia, la obligatoriedad de conservación de datos puede ser admisible para la lucha contra la delincuencia grave, en cambio, no resulta justificada para cualquier otra clase de actuación. En consecuencia, se vino a declarar que, constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad por no respetar el principio de proporcionalidad.

Con la situación jurídica descrita, cabe preguntarse sí, con la declaración de nulidad de la Directiva 2006/24/CE afecta de alguna forma a la norma de derecho interno español que la transpone, esto es, la Ley 25/2007. Así, nuestros tribunales mantienen que, la declaración de nulidad de la Directiva 2006/24/CE, no supone la automática invalidez de la Ley que la traspone al derecho interno, toda vez que, según su criterio, la sentencia hace pronunciamientos que son respetados en la ley (judicialidad de la medida, medidas de seguridad a adoptar, plazo que coincide con el indicado por el Abogado General en sus conclusiones, etc.). Así, se haría una adecuada interpretación de la ley española conforme las normas europeas, y no podría considerarse que la transposición esté subordinada a la Directiva.

Por su parte, el Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo (asuntos acumulados C-203/15 y C-698/15) planteó una cuestión prejudicial ante T.J.U.E. con el objeto de consultar sobre la validez de su norma nacional sobre cesión y conservación de datos asociados, similar a nuestra Ley

25/2007, en relación con la declaración de nulidad de la Directiva 2006/24/CE, la cual, fue resuelta por la Sentencia del T.J.U.E. de la Gran Sala, de 21 de diciembre de 2016. De este modo, se venía a mantener que, los Estados miembros pueden legislar sobre el acceso de las autoridades a los datos conservados, si bien, únicamente puede realizarse para la lucha contra la delincuencia grave, debe existir un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, así como, los datos habrán de conservarse en la UE, todo ello con arreglo a la Directiva 2002/58/CE.

Posteriormente, la Sección Cuarta de la Audiencia Provincial de Tarragona, planteó una cuestión prejudicial ante el T.J.U.E. (asunto C-207/2016), la cual, fue resuelta mediante Sentencia de la Gran Sala de 2 de octubre de 2018. Ahora bien, se solicitaba un pronunciamiento más centrado en el acceso de los datos informáticos almacenados por las empresas operadoras de telecomunicaciones en la prestación de sus servicios, con ocasión, de una investigación penal, que en la propia validez de la normativa nacional sobre el acceso de las autoridades nacionales a los datos conservados por dichas empresas. Aunque esta última sentencia sea poco trascendente sobre la validez de la Ley 25/2007, podemos extraer como conclusión que, la declaración de nulidad de la Directiva 2006/24/CE supone volver a implantar la normativa europea anterior, esto es, la Directiva 2002/58/CE. Asimismo, nuestra legislación sobre la conservación y cesión de los datos electrónicos de tráfico o asociados por parte de las empresas prestadoras de los servicios de telecomunicaciones respeta la Directiva 2002/58/CE. No obstante, pese a que la norma española prevea como garantía para la cesión de los datos, la intervención judicial (arts. 6 y 7 L. 25/2007), lo cierto es que, no contempla restricción alguna en la conservación. En concreto, bajo nuestro punto de vista, debería cumplir con los límites establecidos en el art. 15.1 de la Directiva 2002/58/CE, esto es, la conservación por razones de seguridad nacional, la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos, puesto que se aplica para todos los ciudadanos españoles que tengan dispositivos electrónicos independientemente de si están relacionados con la actividad criminal. En consecuencia, a nuestro modo ver, la regulación excede del espíritu de la Unión Europea, por lo que, se propone como *lege ferenda* que, el Estado español adapte su

legislación interna a los mandatos comunitarios contenidos en la mencionada Directiva 2002/58/CE.

- En todo correo electrónico podemos distinguir tres momentos del proceso comunicativo, de forma que, se inicia mediante el envío del mensaje, continua con la recepción y almacenamiento en el servidor y finaliza cuando el destinatario accede al contenido de la comunicación. De esta manera, cuando el correo electrónico ha sido remitido, pero aún no lo ha abierto, o en su caso, ha sido leído por el destinatario, el proceso comunicativo se encuentra en curso. En cambio, la comunicación ha finalizado cuando el mensaje ha sido descargado desde el servidor, en su caso leído por el receptor y almacenados en alguna de las bandejas del programa de gestión. Bajo nuestro punto de vista, esta distinción tiene relevancia por el diferente régimen constitucional aplicable. Así, cuando el proceso comunicativo se encuentra en curso, como en el primer supuesto aludido, el derecho afectado será el secreto de las comunicaciones (art. 18.3 CE), lo cual, conlleva que cualquier injerencia requiera de autorización judicial. Por el contrario, cuando la comunicación ha visto culminado su ciclo, entonces la protección constitucional viene dada por el derecho a la intimidad (art. 18.1 CE) que, como es sabido, no se exige expresamente de autorización judicial para su intromisión. Además, como en los servidores del correo electrónico se encuentran diversas clases de mensajes, como los enviados, recibidos, los eliminados que permanecen en la papelera de reciclaje, los abiertos, los no leídos, etc, precisar en qué momento se encuentra la comunicación, para determinar qué derecho fundamental ha sido afectado, y así exigir autorización judicial o no, en nuestra opinión, resultaría a efectos prácticos de gran complejidad. Por este motivo, la jurisprudencia venía entendiendo, y tras la reforma implementada con la L.O. 1/2015, también lo dispone expresamente la ley procesal penal que, para las intromisiones en los correos electrónicos se deberá otorgar todas garantías, y en consecuencia, se exige en todo caso de autorización judicial, independientemente de la consideración del mensaje.

  En lo referente a la intervención de las comunicaciones telemáticas correspondientes al correo electrónico, como ya nos hemos referido, las empresas prestadoras de servicios de telecomunicaciones tienen el deber de colaboración con las autoridades españolas (Juez, Ministerio Fiscal y Policía Judicial). Sin embargo, las cuentas de

correo electrónico que son utilizadas normalmente en la actividad delictiva son las gratuitas que, suelen estar erradicadas en países extranjeros, como Estados Unidos (por ejemplo, *Gmail*, *Outlook*, *Hotmail*, Yahoo! Etc.). Por este motivo, para recabar datos de las operadoras erradicadas en EEUU se precisa realizar la solicitud mediante Comisión Rogatoria Internacional. Ahora bien, tras un procedimiento largo y tedioso, en aplicación de la legislación interna norteamericana, suelen denegar la solicitud, puesto que, como regla general, no proporcionan datos de las cuentas de correo electrónico cuando sean para la investigación de delitos cometidos fuera de su territorio nacional. No obstante, podría suceder que estas empresas tengan abierta sede en España (por ejemplo, Microsoft Ibérica, Google España o Yahoo Iberia), de forma que, los juzgados podrían requerir directamente a sus filiales españolas información sobre sus usuarios. Pese a ello, las empresas prestadoras habitualmente tienen los servidores fuera del territorio nacional, por lo que, se limitan a entregar datos del usuario (dirección del correo electrónico, IP, nombre registrado, etc.), pero nunca ceden el contenido de la propia comunicación, alegando que no obra en su poder dicha información. Por este motivo, cuando los tribunales españoles necesiten recabar más datos, deberán acudir a la sede central erradicada en el país de origen, necesariamente mediante Comisión Rogatoria Internacional. En cambio, para obtener información sobre correos electrónicos alojados en servidores de compañías prestadoras de servicios de la Unión Europea (por ejemplo *GMX Mail*, *OpenMailBox*, etc.), la Ley 23/2014, de 20 de noviembre, *de reconocimiento mutuo de resoluciones penales en la Unión Europea*, modificada por la Ley 3/2018, de 11 de junio, que venía a transponer la Directiva 2014/41/CE de 3 de abril de 2014, *relativa a la orden europea de investigación en materia penal* permite emitir una resolución judicial denominada orden europea de investigación (OEI) de un Estado miembro para llevar a cabo medidas de investigación en otro Estado miembro. Así, un Estado miembro puede emitir una orden europea de investigación (OEI) para la intervención de telecomunicaciones en el Estado miembro cuya asistencia técnica se requiera, debiendo reconocer la autoridad de ejecución la OEI sin requerir otra formalidad. Además, deberá asegurar su ejecución de la misma manera y bajo las mismas circunstancias que si la medida de investigación de que se trate hubiera sido ordenada por una autoridad del Estado de ejecución. Por este motivo, en nuestra opinión, obtener información sobre los usuarios de cuentas de correo electrónico de empresas erradicadas en Estados de la Unión Europea, será mucho más accesible que

en el caso norteamericano, pues la autoridad judicial española, de acuerdo con la legislación mencionada, podrá dirigirse directamente a éstas, para recabar la información que sea necesaria en el seno de una investigación penal.

- Respecto la mensajería instantánea como *Whatsapp,* la información transmitida no se conserva en un servidor externo, ni con carácter general, precisa acceder a una sesión para establecer la comunicación, sino que, los datos permanecen en los dispositivos electrónicos utilizados por los usuarios. Por este motivo, la información que podrá únicamente facilitar el proveedor del servicio será la relacionada con los datos de tráfico generados en la conversación. Cuando se pretenda intervenir las comunicaciones, para acceder al contenido del mensaje emitido en tiempo real, habrá que acudir a un *software* específico que permita descifrar o desencriptar los protocolos. Sin embargo, la interceptación de las comunicaciones no podrá referirse a conversaciones que hayan tenido lugar en el pasado, pues como decimos, el contenido del mensaje no se almacena en servidor alguno. Una vez realizada estas aclaraciones, cabe mencionar que, se puede obtener la información contenida en la mensajería instantánea mediante la adopción de alguna medida tecnológica, como la intervención de las comunicaciones telemáticas, el registro de dispositivos de almacenamiento masivo de información o registro remoto sobre equipos informáticos, aunque también, podrán ser aportada por las partes. De esta manera, los mensajes instantáneos utilizados por los usuarios pueden ser incorporados al proceso penal para acreditar determinados hechos, siendo la manera habitual, como un documento en formato papel de los mensajes o "pantallazos", si bien, cuando alguna parte impugne la autenticidad y/o de integridad con argumentos sólidos, se *desplazara la carga de la prueba hacia quien pretenda aprovechar su idoneidad probatoria*, de modo que, *será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido* (STS 300/2015). De igual modo, podrá someterse a prueba personal de declaración de testigos o encartados, para que expongan sobre los mensajes enviados o recibidos.

- Los *chats* pueden ser abiertos, cuando son de libre acceso e intervienen numerosos usuarios, de forma que, cualquier intromisión no plantea problemas en los derechos fundamentales, mientras que, los cerrados, al tratarse de una comunicación

bidireccional privada, las injerencias se deberán realizar con el oportuno plácet judicial. Sin embargo, para obtener los datos de tráfico o asociados a una comunicación de los *chats* abiertos y cerrados, será necesaria autorización judicial. Respecto a lo expuesto sobre los *chats* abiertos, en nuestra opinión, será extensible para los foros y los *blogs*, pues también, se tratan de sitios de la red de libre acceso.

- La primera premisa a los efectos de considerar lícita la grabación entre particulares realizada por uno de los interlocutores es que deberá ser el encuentro voluntario y libre. De esta manera, la jurisprudencia analizada mantiene que, la aportación al proceso penal de grabaciones de conversaciones privadas registradas por uno de los interlocutores, no vulnera el derecho al secreto de las comunicaciones (art. 18.3 CE), si bien, podría verse afectado la intimidad (art. 18.1 CE), cuando la conversación incida en la esfera privada y/o familiar, por lo que, en este caso, entendemos que debería ser descartada del proceso. Por su parte, las grabaciones realizadas en el ámbito particular no vulneran tampoco, el derecho fundamental a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE).

- La relación entre cónyuges o unión de hecho o convivencia *more uxorio*, no existe justificación alguna para realizar entre sí, injerencias en la intimidad o el secreto de las comunicaciones, especialmente cuando se encuentran en plena crisis matrimonial o de pareja. De esta manera, la grabación obtenida para su aportación a un proceso judicial violentando los derechos fundamentales, podrá ser declarada nula por prueba ilícita (art. 11.1 LOPJ), así como, podrán incurrir en el delito contra la intimidad o revelación de secretos del art. 197 CP. Sobre la relación entre padres e hijos, cabe mencionar que, los menores también son titulares de los derechos a la intimidad y al secreto de las comunicaciones. Ahora bien, debemos diferenciar, cuando las intromisiones en el proceso comunicativo se encuentran en curso, por lo que, se vería afectada la inviolabilidad de las comunicaciones. Aunque se trate de los padres respecto de sus hijos, las injerencias no consentidas quedan excluidas. En cambio, cuando el acceso de los progenitores se produce cuando el mensaje ha sido recibido y leído por el menor, dicha situación incide en la intimidad del menor. Así, la jurisprudencia viene entendiendo que, para este último supuesto, será necesario ponderar el conflicto entre el derecho a la intimidad de los menores y la actuación de los progenitores en el ejercicio de la guarda y su deber de protección. De hecho, se

deberá resolver a favor de este último, para casos justificados, como por ejemplo cuando el menor sea víctima de delitos, pueda haber cometido él mismo algún ilícito penal que pueda dar origen a la responsabilidad civil solidaria de los padres (art. 61.3 L.O. 5/2000), o bien, el menor no tenga madurez suficiente como para prestar por sí solo el consentimiento exigido en el código penal en las injerencias en su intimidad.

2) Seguidamente vamos a extraer las ideas principales de la medida de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. Así, se permite la captación del sonido sin imágenes (colocación de micrófonos), pero en cambio, no se admite la grabación de imágenes sin el registro de audio (cámara oculta sin micrófono). No obstante, en nuestra opinión, Fiscalía realiza una interpretación contraria al sentido literal de la ley, pues vienen manteniendo que, se puede autorizar la captación y grabación de imágenes en lugares cerrados sin sonido.

- Lo importante a los efectos del presente trabajo es que no se puede acordar para la investigación de delitos tecnológicos. En nuestra opinión, esto tiene su justificación en que la medida está pensada para la investigación de delitos tradicionales y graves.

- Cuando se lleve a cabo en un lugar cerrado o en el domicilio, se deberá acordar una autorización judicial, lo que la jurisprudencia ha venido a denominar, con "*motivación reforzada*".

3) Acerca de la diligencia que faculta a la Policía Judicial, sin plácet judicial, registrar con videocámara o tomar imágenes fotográficas en espacios públicos, esto es, sin captar audio o sonido. Esta dispensa de la intervención judicial se debe a que las *expectativas razonables de privacidad* en la vía pública son menos intensas que las producidas en la esfera íntima de las personas.

4) Sobre la utilización de dispositivos o medios técnicos de seguimiento y localización o "balizas", cabe mencionar que, no debemos confundirlo con la geolocalización, como dato asociado a una comunicación que permita identificar la localización de un terminal móvil que, como ya hemos aludido, se tratan de datos conservados por las operadoras de telecomunicaciones, y que pueden ser cedidos con el oportuno plácet judicial. En puridad no sería necesaria la autorización judicial para su adopción, ya que la Constitución española no establece expresamente dicha exigencia, para la injerencia de

los mencionados derechos fundamentales. Sin embargo, la legislación procesal ha venido a otorgar las mayores garantías, pues viene a establecer la obligatoriedad de autorización judicial para la colocación de las "*balizas*".

- Por su parte, cuando concurran situaciones de urgencia, que hagan razonablemente temer que, de no colocarse inmediatamente el dispositivo, pueda verse frustrada la investigación, se permite a la Policía Judicial su colocación, dando cuenta a la autoridad judicial. Ahora bien, a nuestro parecer, dejar la intervención judicial para un momento posterior, puede originar "corruptelas" policiales en el sentido de que, puedan ser utilizadas las "balizas" de manera indiscriminada y remitir el oficio, únicamente cuando pretendan judicializar la medida.

5) Acerca del registro de dispositivos de almacenamiento masivo de información la afectación se producirá en el ámbito de la intimidad (art. 18.1 CE), o en su caso, en la autodeterminación informativa o protección de datos (art. 18.4 CE). También, incide en el derecho al «entorno virtual o digital», el cual, está estrechamente relacionado con la privacidad, pues consiste en la información que se genera por el usuario con la utilización de las nuevas tecnologías. El registro de dispositivos masivos de información suele acordarse conjuntamente con la diligencia de entrada y registro domiciliario. Ahora bien, la propia autorización judicial deberá contener una *motivación individualizada*, pues la simple incautación de los dispositivos durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido. No obstante, podrá ser autorizado posteriormente por el Juez. En nuestra opinión, con ello, se pretende evitar una práctica habitual que venían realizando nuestros Tribunales consistente en que la autorización del registro domiciliario comprendía también a todos aquellos soportes tecnológicos de información encontrados en la interior de la vivienda, aunque no se especificara dicho extremo en la resolución judicial habilitante. Con ello, se ha superado la deficiente regulación existente antes de la reforma procesal del 2015, al otorgar mayores garantías en su adopción.

- La norma procesal no regula las cautelas para asegurar la integridad de los datos. Por esta razón, hemos acudido a la jurisprudencia de nuestros Tribunales, para exponer como se debe proceder para respetar la cadena de custodia de los vestigios

tecnológicos intervenidos, si bien, nos remitimos a la parte del presente trabajo dedicada al informe pericial informático.

6) Otra medida tecnológica examinada ha sido los registros remotos sobre equipos informáticos. Así, la medida puede ser detectada por los sistemas de seguridad como antivirus, o bien, el *software* utilizado puede ser muy costoso económicamente para el erario público, por lo que, los juzgados preferirán acordar otras medidas, aunque sean más invasivas en los derechos fundamentales, como la ocupación y examen de los dispositivos de almacenamiento masivo de información. En cualquier caso, la diligencia tecnológica de registro remoto de equipos informáticos consiste en la introducción de *datos de identificación y códigos*, para lo cual, se podrán obtener como resultado de una investigación policial o mediante el requerimiento judicial al proveedor de servicios de telecomunicaciones. Una vez en poder de los agentes de policía de los datos necesarios, podrán introducir el usuario y contraseñas (como por ejemplo del *router* o ADSL), para poder acceder al dispositivo del investigado. También, podrán introducir un *software* o "programa espía" en el ordenador o dispositivo del investigado, como por ejemplo con la remisión de algún *malware* o *keylogger* descargable/ejecutable camuflado en algún correo electrónico con apariencia de fidedigno, de modo que, haga posible la vigilancia a distancia mediante monitorización del sistema del investigado.

7) El agente encubierto se trata de la infiltración de la policía para investigar actividades ilícitas. Ahora bien, para comprender la diligencia, se ha examinado, con carácter previo, el agente encubierto que hemos denominado "tradicional", esto es, el policía que se desenvuelve en el mundo físico para investigar hechos delictivos relacionados con la delincuencia organizada. También, se ha abordado el "agente virtual o informático", de forma que, su actuación se desarrolla en el mundo de la red de comunicación. Finalmente, se ha analizado la combinación de ambos, es decir, la infiltración se inicia en el ámbito informático y tecnológico, y posteriormente se concierta un encuentro con el investigado, pasando del mundo virtual al físico.

- Respecto al agente encubierto informático, para canales abiertos, como *chats*, etc. no será necesaria plácet judicial. En consecuencia, debemos diferenciar, por un lado, el ciber patrulleo, esto es, el agente que realiza exploraciones o indagaciones por canales abiertos de comunicación; de aquel otro, estricto agente encubierto *online* que opera en canales cerrados.

- Por su parte, en la resolución judicial se podrá autorizar intercambiar o enviar archivos ilícitos (como por ejemplo pornografía infantil -art. 189 CP- o archivos relativos a la captación, adoctrinamiento o adiestramiento de terroristas yihadistas -art. 575 CP-), así como, analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos, de manera que, siguiendo la secuencia serial de algoritmo *hash* del contenido del envío telemático se puede descubrir a quién más se ha distribuido el material.

- El agente encubierto "tradicional" únicamente puede acordarse para la investigación de delitos relacionados con la delincuencia organizada, mientras que, el agente encubierto informático se permite, además, para otros delitos, en especial, los cometidos a través de las nuevas tecnologías. Además, para canales abiertos, como hemos mencionado, no será necesaria la autorización judicial. De esta manera, cuando se descubra la comisión de delitos no comprendidos para el agente encubierto tradicional, en nuestra opinión, no se podrá autorizar esta figura como método de investigación. Ahora bien, nada impediría concertar un encuentro con el investigado para proceder a su detención.

8) En relación con las medidas tecnológicas, se ha analizado la problemática de la utilización de otras medidas tecnológicas restrictivas de derechos fundamentales no contempladas en la ley. A raíz de la STC 145/2014, en relación con otras sentencias del TEDDHH que han sido examinadas, mantienen que, toda injerencia estatal en los derechos fundamentales, precisará de una habilitación legal. De este modo, hemos decidido examinar a título de ejemplo, una medida de investigación tecnológica no prevista expresamente en la ley, esto es, la utilización de los "drones". A nuestro modo de ver, resulta relevante a los efectos del presente trabajo, determinar hasta donde puede alcanzar el poder del Estado a la hora de investigar la comisión de hechos delictivos, y en especial, los delitos informáticos y tecnológicos.

- Por este motivo, tras analizar la ley y la jurisprudencia, hemos concluido que, en nuestra opinión, de acuerdo con el principio de legalidad, el Estado no puede acordar otras medidas tecnológicas restrictivas de derechos fundamentales no previstas en la ley.

- Respecto a nuestro ejemplo sobre la utilización de "drones", venimos afirmando que, tiene cobertura legal al amparo de la normativa reguladora de aeronaves pilotadas por control remoto (R.D. 1036/2017). Además, cuando fueran utilizadas como medida de investigación tecnológica, podrá ser subsumible en las disposiciones legales sobre la grabación de las comunicaciones orales directas (art. 588 quater a. LECrim), así como, la captación de imágenes en lugares o espacios públicos (art. 588 quinquies a. LECrim), pues nada impediría entender como *dispositivo electrónico* o *medio técnico* esta clase de aeronaves no tripulas por control remoto. No obstante, para registrar imágenes del domicilio u otros lugares cerrados, como venimos analizando, puede realizarse únicamente con el oportuno plácet judicial, cuando fuera acompañada de la captación del sonido. Así, cuando los "drones" sobrevuelen a cierta altura, que será lo habitual para evitar ser descubiertos, podrán obtener imágenes, pero difícilmente podrán captar el sonido. Cuando se da esta situación, bajo nuestro punto de vista, carecerá de apoyo legal, por lo que debería descartarse como diligencia de investigación. Sin embargo, como hemos advertido, Fiscalía tiene un criterio contrario a esta posición, puesto que, vienen manteniendo que, se puede permitir la autorización de la captación y grabación de imágenes en lugares cerrados sin sonido. En cambio, cuando se pretenda captar imágenes en lugares o espacios públicos, como no se exige autorización judicial, los agentes de policía podrán proceder a su ejecución, cuando fuera relevante para el esclarecimiento de los hechos.

II. – Dentro de la parte procesal se ha analizado también la pericial informática. De esta manera, como mantiene nuestro Tribunal Supremo (STS 300/2015), la impresión de los archivos en formato papel o "pantallazos" son fuentes de prueba perfectamente válida en Derecho (por ejemplo la impresión de una conversación de mensajería instantánea de *WhatsApp* o mensajes de correo electrónico). Ahora bien, cabe la posibilidad de que sean manipulados los archivos digitales, de ahí que, la impugnación de la autenticidad por alguna de las partes, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria, y en tal caso, será indispensable la práctica de una prueba pericial que permita garantizar la identidad, la integridad y la autenticidad de su contenido. Por este motivo, seguidamente vamos a extraer las ideas principales sobre la pericial informática.

- El perito informático será una persona que por su titulación o por su experiencia personal o trayectoria profesional, tenga conocimientos en "*informática forense*". Ahora bien, lo habitual será, que sean elaborados dictámenes por agentes de policía, en especial, para delitos de especial gravedad. Así, la Policía Judicial estatal o autonómica tienen asignadas diversas unidades para la averiguación de delitos tecnológicos o informáticos y descubrir a los ciberdelincuentes, y ostentan, entre sus funciones la elaboración de esta clase de dictámenes.

- La preservación de los efectos tecnológicos, consiste en nuestra opinión, una parte esencial a los efectos probatorios en el proceso penal. Así, en el momento de la ocupación de los dispositivos se puede realizar el "*clonado*" o "*volcado*", esto es, hacer una copia exacta (copia *bit* a *bit*) de la información digital contenida en el soporte electrónico original, mediante un dispositivo tecnológico especializado de *hardware* o externo. Una vez finalizado el proceso de "clonado", la imagen forense, que podrá ser almacenada en cualquier formato, deberá ser firmada digitalmente mediante una función *hash*, esto es, la técnica que consiste en una relación matemática o algoritmos que, haga posible identificar unívocamente el contenido de la imagen forense con el original. Así, cualquier inexactitud en la numeración entre ambos, supone la manipulación de la evidencia tecnológica. De igual modo, cabe la posibilidad de proceder a la incautación de los dispositivos electrónicos o equipos informáticos, para lo cual, se deberá proceder al precintado de los mismos, llevarlos a un lugar seguro en dependencias policiales o sede judicial, en el cual, se desprecintarán y se actuará de la manera mencionada anteriormente. Asimismo, el Juez podrá fijar las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación, para lo cual, será conveniente, aunque no obligatorio, la presencia del Letrado de la Administración de Justicia.

- Posteriormente, se realizará el análisis del "*clon*", permaneciendo el original bajo custodia judicial, encargándose el Letrado de la Administración de Justicia de su depósito. Así, el perito informático deberá identificar, de forma selectiva, la información que pueda ser de interés y minimizar o evitar el acceso a otra información que no resulte relevante al objetivo del análisis solicitado.

- El resultado del análisis realizado por técnicos especialistas en informática forense, lo deberán presentar o exhibir al Juez mediante un informe o dictamen pericial.

- Los peritos deberán comparecer al juicio oral, para ratificar, ampliar o aclarar su informe. Ahora bien, cuando sean elaborados por Gabinetes y Laboratorios Oficiales, no será necesaria su presencia, pues se entiende que adquiere el carácter de prueba preconstituida, aceptada y consentida, todo ello, salvo que las partes expresen en su escrito de calificación provisional su oposición o discrepancia con el dictamen pericial practicado, o solicite ampliación o aclaración del mismo. De esta manera, cuando la elaboración de los informes periciales sea realizada por las unidades especiales de Policía Judicial, como se tratan de organismos oficiales, en nuestra opinión, será de aplicación el criterio jurisprudencial aludido, y por tanto, no será necesaria su presencia, salvo que exista impugnación o precise de aclaraciones.

III. – Por último, dentro de la parte dedicada al proceso penal, hemos analizado la jurisdicción de los Estados y la competencia territorial en la investigación y enjuiciamiento de los delitos tecnológicos e informáticos. De esta manera, los hechos delictivos cometidos a través o contra las nuevas tecnologías o informática se caracterizan por tener un gran marcado transfronterizo. Por tanto, pueden tener lugar en un Estado, pero sus consecuencias pueden afectar a otro. Sin embargo, en el derecho penal rige con carácter general el principio de territorialidad, por lo que, en ocasiones puede ser complicado determinar la jurisdicción del Estado, y en su caso, la competencia territorial, para conocer de un delito que ha podido tener sus consecuencias en varios lugares. Por este motivo, nuestra solución propuesta que, bajo nuestro punto de vista es la más adecuada, aparte de ser la asumida mayoritariamente por los tribunales es la teoría de la *ubicuidad*. Así, consiste en reputar cometido el delito tanto en el lugar de ejecución de la acción u omisión o donde se inicia el delito (teoría de la *acción*), como en el lugar o los lugares en los que se produce o hubiera podido producirse el/los resultado/s, esto es, donde se producen las consecuencias del delito (teoría del *resultado*). De esta manera, conforme la teoría de la *ubicuidad*, se atribuirá la jurisdicción al Estado, y en su caso, la competencia territorial al Tribunal de cualquiera de ellos. Sin embargo, para evitar la duplicidad de procesos sobre el mismo objeto, conocerá el primero que hubiera comenzado la investigación o el enjuiciamiento, siempre que, en el mismo, se hubiera realizado algún elemento del tipo.

BIBLIOGRAFÍA:

ABEL LLUCH X. Y OTROS, Estudios *sobre prueba penal. Volumen I. Actos de investigación y medios de prueba en el proceso penal: competencia, objeto y límites.* Editorial La Ley. Madrid. 2013.

ABEL LLUCH X. Y OTROS, Estudios *sobre prueba penal. Volumen II. Actos de investigación y medios de prueba en el proceso penal: Inspección ocular, declaraciones de inculpados y testigos, intervenciones corporales y prueba pericial.* Editorial La Ley. Madrid. 2013.

ABEL LLUCH X. Y OTROS, Estudios *sobre prueba penal. Volumen III. Actos de investigación y medios de prueba en el proceso penal: Entrada y registro, intervención de comunicaciones, valoración y revisión de la prueba en vía de registro.* Editorial La Ley. Madrid. 2013.

ABEL LLUCH, X, *Prueba y nuevas tecnologías*. *(La prueba judicial: Desafíos en las jurisdicciones civil, penal, laboral y contencioso administrativa)*. Editorial La Ley. 2013. Págs. 428 – 579.

ABEL LLUCH, X. *La Valoración de la Prueba en el Proceso Civil.* Editorial La Ley. Madrid. 2014.

ABEL LLUCH, X. *Prueba electrónica. (Derecho probatorio)*. J.M. Bosch Editor. Barcelona. 2012 Págs. 901-1032.

ABEL LLUCH, X. Y OTROS, La *prueba judicial. Desafíos en las jurisdicciones civil, penal, laboral y contencioso-administrativa.* Editorial La Ley. Madrid. 2011.

AGUADO CORREA, T. Y OTROS. *Comentarios al Código Penal*. Editorial Lex Nova. Madrid. 2011.

AGUIAR DE LUQUE, L. *Constitución, estado de las autonomías y justicia constitucional: (libro homenaje al profesor Gurmesindo Trujillo).* Tirant lo Blanch. Valencia. 2005. Págs. 661-686.

AGUSTÍ MARAGALL, J. *La cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (Derecho Social de la Unión Europea: aplicación por el Tribunal de Justicia)*. Editorial Francis Lefebvre. Madrid. 2018. Págs. 123-156.

AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J, *Aspectos legales de las redes sociales.* Editorial BOSCH. Hospitales de Llobregat (Barcelona). 2016.

ALBA FIGUERO C.; JUANES PECES A. *Reforma del Código Penal: perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio: situación jurídico-penal del empresario*. Editorial El Derecho. Madrid. 2010. Págs. 123-178.

ALBALADEJO GARCÍA, M. *Derecho civil. Tomo I: Introducción y parte general.* Editorial Edisofer, S.L. Madrid. 2013.

ALISTE SANTOS, T. J. *La motivación de las resoluciones judiciales*. Editorial Marcial Pons, Ediciones Jurídicas y Sociales. Madrid. 2011.

ALONSO GARCÍA, J. *Derecho penal y redes sociales*. Derecho penal y redes sociales. Editorial Aranzadi. Navarra. 2015.

ALONSO PALMA, A. L. *Propiedad intelectual y derecho audiovisual.* Editorial CEF. Madrid. 2006.

ALONSO PÉREZ, F. *Intervención de las comunicaciones postales telegráficas y telefónicas legislación, comentarios, jurisprudencia*. Editorial Dykinson. Madrid. 2001.

ALONSO PÉREZ, F. *La policía judicial.* Editorial. Crisol. 1993.

ALONSO RIMO, A, CUERDA ARNAU, M. L. y FERNÁNDEZ HERNÁNDEZ, A. *Terrorismo, sistema penal y derechos fundamentales.* Editorial Tirant lo Blanch. Valencia. 2018.

ALONSO SALGADO, C. *Una cuestión de garantías. La interceptación de las comunicaciones telefónicas de la Ley de Enjuiciamiento Criminal a la propuesta de nuevo Código procesal penal. (Processulus: estudios sobre derecho procesal).* Editores: Editorial Comares. Granada. 2015. Págs. 127-136.

ÁLVAREZ CORA, E. *Esquemas y textos para la historia del derecho español.* Editorial Diego Marín. Murcia. 2009.

ÁLVAREZ DE NEYRA KAPPLER, S. *La prueba pericial, documental y la inspección ocular. (Nociones preliminares de derecho procesal penal)*. Editorial Atelier. Barcelona. 2016. Págs. 163-168.

ÁLVAREZ GARCÍA F. J, GONZÁLEZ CUSSAC J. L. *Comentarios a la Reforma Penal de 2010*. Editorial Tirant lo Blanch. Valencia. 2010. Págs. 249-256.

ÁLVAREZ GARCÍA, F. J, COBOS GÓMEZ DE LINARES MIGUEL ANGEL, GÓMEZ PAVÓN PILAR, MANJÓN-CABEZA OLMEDA ARACELI, MARTÍNEZ GUERRA AMPARO. *Libro homenaje al prof. Luis Rodríguez Ramos*. Editorial Tirant lo Blanch. Valencia. 2013. Págs. 621-655.

ÁLVAREZ GARCÍA, F. J. *Comentarios a la reforma penal de 2010*. Editorial Tirant lo Blanch. Valencia. 2010.

ALVAREZ HERNANDO J. Y CAZURRO BARAHONA. V, *Practicum. Protección de datos. 2016*. Editorial Aranzadi. Pamplona. 2015.

ALVAREZ RODRÍGUEZ, J. R. y RÍUS DIEGO, F. J. *La entrada y registro en lugar cerrado consideraciones procesales, jurisprudenciales y policiales.* Editorial Tecnos. Madrid. 2009.

ÁLVAREZ SUÁREZ, L. *El ministerio fiscal y las diligencias de investigación tecnológica (FODERTICS 6.0: los nuevos retos del derecho ante la era digital*). Editorial Comares. Granada. 2017. Págs. 117-125.

ALVAREZ-CIENFUEGOS SUÁREZ, J. M. *Protección de la intimidad en el tráfico de datos en Internet (2001-2002). (El derecho en la sociedad telemática: estudios en homenaje a Valentín Carrascosa López).* Andavira Editora. La Coruña. 2012. Págs. 183-196.

ALVAREZ-CIENFUEGOS SUÁREZ, J. M. *Protección de la intimidad en el tráfico de datos en internet (Quince años de encuentros sobre informática y derecho: 1987-2002. Vol. 2, Tomo 2).* Editorial Universidad Pontificia Comillas. Madrid. 2002. Págs. 561-570.

ALVAREZ-MANZANEDA, R. R. *La utilización fraudulenta de las tarjetas de pago*. Editorial Aranzadi. Cizur Menor (Navarra). 2011.

ANGEL AGÚNDEZ M. y MARTÍNEZ-SIMANCAS SÁNCHEZ J. *Cuadernos de derecho para ingenieros Vol. 12*. Editorial La Ley, Iberdrola y Colegio de Ingenieros del ICAI. Bilbao. 2011. Págs. 137-156.

ANGUAS BALSERA, J. *La pericial informática. (Tratado pericial judicial)*. Editorial Wolters Kluwer Madrid. 2014. Págs. 313-376.

ANSUÁTEGUI ROIG, F. J. y otros. *Historia de los derechos fundamentales*. Editorial Dykinson. Madrid. 1998. Págs. 1059-1111.

ANSUÁTEGUI ROIG, F. J.. *Historia de los derechos fundamentales*. Dykinson. Madrid. 1998.

ANTÓN MELLÓN, J. *Islamismo yihadista radicalización y contrarradicalización.* Editorial Tirant lo Blanch. Valencia. 2015.

ARAGÜÉS RUIZ, A. *P2P*. Editorial ANAYA MULTIMEDIA. Madrid. 2006.

ARBÓS, A. *Nuevas tecnologías, el correo electrónico. (Integración curricular de las nuevas tecnologías)*. Editorial Ariel. Madrid. 2000. Págs. 125-130.

ARCHER, J. *La falsificación.* Editorial Debolsillo. Barcelona. 2007.

ARIZA COLMENAREJO, M. J. *Especialización y justificación policial ante el Juez de las diligencias de investigación en el ámbito de la ciberdelincuencia. (FODERTICS II: hacia una justicia 2.0).* Editorial Ratio Legis. Salamanca. 2014. Págs. 95-105.

ARMAZA ARMAZA, E. J. y otros. *Temas de Derecho penal. Libro homenaje a Luis Guillermo Cornejo Cuadros*. Editorial Adrus. Lima (Perú). 2008. Págs. 189-202

ARQUILLA, J, RONFELDT, D. *Redes y guerras en red el futuro del terrorismo, el crimen organizado y el activismo político*. Editorial Alianza Editorial. Madrid. 2003.

ARROYO DE LAS HERAS A. *Los delitos de estafa y falsedad documental.* Editorial Bosch. 2005. Barcelona. 2005.

ARROYO DE LAS HERAS A. *Los delitos de estafa y falsedad documental.* Editorial Bosch. Barcelona. 2005.

ARROYO ZAPATERO, L. A. y BERDUGO GÓMEZ DE LA TORRE, I. *Homenaje al Dr. Marino Barbero Santos: "in memorian"*. Ediciones de la Universidad de Castilla-La Mancha. Salamanca. 2001. Págs. 833-852.

ARTOLA GALLEGO, M. *Las declaraciones de derechos y los primeros textos fundamentales galos en los orígenes del constitucionalismo español.* (España y la Revolución Francesa). Editorial Pablo Iglesias. Madrid. 1989. Págs. 73-88.

ASENSIO MELLADO J.M. (y OTROS), *La reforma del proceso penal.* La Ley. Madrid. 2011.

ASUA BATARRITA, A. *Jornadas sobre el nuevo Código penal de 1995, celebradas del 19 al 21 de noviembre de 1996.* Servicio de Publicaciones de la Universidad del País Vasco. 1998. Págs. 43-46.

AVILÉS GÓMEZ M, Y OTROS. *Delitos y delincuentes: cómo son, cómo actúan*. Editorial Club Universitario. San Vicente (Alicante). 2010. Págs. 109-136.

BACIGALUPO ZAPATER, E. *Delitos contra el honor.* Editorial Dykinson. Madrid. 2000.

BAJO FERNÁNDEZ, M. *Criminología y derecho penal al servicio de la persona: libro homenaje al profesor Antonio Beristain.* Editorial Instituto Vasco de Criminología. 1989. Págs. 649-662.

BAJO FERNÁNDEZ, M. *Los delitos de estafa en el Código penal.* Editorial Centro de Estudios Ramón Areces. Madrid. 2004.

BALAGUER CALLEJÓN, M. L. *El recurso de inconstitucionalidad*. Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 2001.

BANACLOCHE PALAO, J. *Responsabilidad penal de las personas jurídicas. Aspectos sustantivos y procesales.* Editorial LA LEY. Madrid. 2011.

BANACLOCHE PALAO, J. y CUBILLO LÓPEZ, I. J, *Aspectos Fundamentales de Derecho Procesal Civil.* Editorial La Ley. Madrid. 2012.

BANACLOCHE PALAO, J. y ZARZALEJOS NIETO, J. *Aspectos Fundamentales de Derecho Procesal Penal*. Editorial La Ley. Madrid. 2011.

BARBER BURUSCO, M. S. *Los actos preparatorios del delito conspiración, proposición y provocación.* Editorial Comares. Granada. 2004.

BARCELONA LLOP, J. *Policía y Constitución.* Editorial Tecnos. Madrid. 1997.

BARRIENTOS PACHO, J. M. *Entrada y registro en domicilio particular*. Manuales de formación continuada del CGPJ. Núm. 12. 2000. Págs. 299-340.

BARRIO ANDRÉS, M. *Ciberdelitos. Amenazas criminales del ciberespacio*. Editorial Reus. Barcelona. 2017.

BARRIUSO RUIZ, C. *Interacción del derecho y la informática.* Editorial Dykinson. Madrid.1996.

BAYLOS GRAU, A. P. *Modelos de derecho del trabajo y cultura de los juristas.* Editorial Bomarzo. Albacete. 2014. Págs. 201-222.

BELTRÁN LÓPEZ, G. *Geolocalización online la importancia del dónde*. Editorial UOC. 2016.

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

BERCOVITZ RODRÍGUEZ-CANO, R. *La copia privada. La reforma en la ley de Propiedad Intelectual.* Editorial Tirant lo Blanch. Valencia. 2015. (Págs. 52-78).

BERDUGO GÓMEZ DE LA TORRE, I. *Honor y libertad de expresión las causas de justificación en los delitos contra el honor.* Editorial Tecnos. Madrid. 1987.

BERDUGO GÓMEZ DE LA TORRE, I. *Lecciones y materiales para el estudio del derecho penal.* Editorial Iustel. Madrid. 2010. Págs. 357-380.

BLANCO LOZANO, C. *Amenazas y coacciones. Lecciones de derecho penal: parte especial.* Editorial Tecnos. Madrid. 2010. Págs. 165-176.

BLANCO LOZANO, C. *Tratado de Derecho Penal Español. Tomo 2. Volumen 1. La Estafa.* Editorial. J.M. Bosch. Barcelona. 2005.

BLANCO VALDÉS, R. L. *La Constitución de 1978.* Alianza Editorial. Madrid. 2003.

BLASCO SOTO, M. C. *La sentencia en la cuestión de inconstitucionalidad.* Editorial J. M. Bosch Editor. 1995.

BLASI CASAGRAN, E. *La protección de datos en las aplicaciones de mensajería instantánea (La protección de datos personales en internet ante la innovación tecnológica riesgos, amenazas y respuestas desde la perspectiva jurídica)*. Editorial Thomson Reuters Aranzadi. Navarra. 2013. Págs. 543-563.

BLÁZQUEZ GONZÁLEZ, F. *La policía judicial.* Editorial Tecnos. Madrid. 1998.

BOCANEGRA MÁRQUEZ, J. *El castigo de la pertenencia a organización criminal en el Código Penal español los delitos de asociación criminal y organización y grupo criminal. (Propuestas penales: nuevos retos y modernas tecnologías: memorias del IV Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, Salamanca, 29 y 30 de junio y 1 de julio de 2015).* Ediciones Universidad de Salamanca. 2016. Págs. 603-615.

BOIX REIG, F. J, JAREÑO LEAL, A. *La protección jurídica de la intimidad. Editorial* Iustel. Madrid. 2010. Págs. 171-196.

BOIX REIG, F. J. *Derecho penal. Parte especial.* Editorial Iustel. Madrid. 2016. Págs. 389-398.

BOIX REIG, F. J. *El delito de usurpación de estado civil*. Editorial de la Universitat de València. 1980.

BONÉ PINA, J. F. y SOTERAS ESCARTÍN, R. *De las falsedades. Comentario de los artículos 386 a 403 del Código penal de 1995.* Editorial Bosch. Barcelona. 1999.

BUENO DE MATA F, *Prueba electrónica y Proceso.* Editorial Tirant Lo Blanch. Valencia. 2014. (Pág. 140-151).

BUENO DE MATA F. *FODERTICS 3.0: (estudios sobre nuevas tecnologías y justicia)*. Editorial Comares S.L. Granada. 2015. Págs. 197-204.

BUENO DE MATA, F. *El agente encubierto en Internet como instrumento para la lucha contra el "child grooming" y el "sexting" (Cambio de paradigma en la prevención y erradicación de la violencia de género)*. Editorial Comares. Granada. 2017. Págs. 3-16.

BUENO DE MATA, F. *El agente encubierto en internet, mentiras virtuales para alcanzar la justicia. (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)*. Editorial Universidad de La Coruña. 2012. Págs. 295-306.

BUENO DE MATA, F. *FODERTICS 3.0 (estudios sobre nuevas tecnologías y justicia).* Editorial Comares. Granada. 2015.

BUENO DE MATA, F. *FODERTICS 4.0 (estudios sobre nuevas tecnologías y justicia): "IV Fórum de expertos y jóvenes investigadores en derecho y nuevas tecnologías, celebrado en la Facultad de Derecho de Salamanca, en 2015".* Editorial Comares. Granada. 2015. Págs. 95-172.

BUENO DE MATA, F. *La validez de los "screenhots" o "pantallazos" como prueba electrónica a tenor de la jurisprudencia del Tribunal Supremo. (Los desafíos de la justicia en la era post crisis).* Editorial Atelier. Barcelona. 2016. Págs. 141-152.

BUENO DE MATA, F. *Prueba Electrónica y Proceso 2.0*. Editorial Tirant Lo Blanch. 2014. Págs. 89 – 182.

CABEZUDO BAJO, M. J. *La inviolabilidad del domicilio y el proceso penal.* Editorial Iustel. Madrid. 2004.

CABEZUDO RODRÍGUEZ, N. *Concepto y alcance del principio de inmediación. (Del principio de inmediación, sus excepciones y los instrumentos tecnológicos).* Editorial Tirant Lo Blanch. Valencia. 2010. Págs. 19-52.

CALVO ÁLVAREZ, S. *De la Web 1.0 a Internet invisible vulnerabilidades, amenazas y delitos. (La seguridad, un concepto amplio y dinámico: V Jornadas de estudios de seguridad, Madrid, 7, 8 y 9 de mayo de 2013)*. Editorial Instituto Universitario General Gutiérrez Mellado. Madrid. 2013. Págs. 491-526.

CALVO SALINERO, R. y PASTORIZA VÁZQUEZ, J. S. *La cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (La revisión de actos en materia tributaria).* Editorial Thomson Reuters-Lex Nova. 2016. Págs. 993-1044.

CAMPO MORENO, J. C. *Los actos preparatorios punibles.* Tirant lo Blanch. Valencia. 2000.

CANCIO MELIÁ, M. *Delitos de organización criminalidad organizada común y delitos de terrorismo (Estudios sobre las reformas del Código Penal: operadas por las LO 5/2010, de 22 de junio, y 3/2011, de 28 de enero)*. Editorial Civitas. Madrid. 2011. Págs. 643-670.

CANCIO MELIÁ, M. *El delito de pertenencia a una organización terrorista en el Código Penal español*. *(Derecho penal del estado social y democrático de derecho: Libro homenaje a Santiago Mir Puig).* Editorial La Ley. Madrid. 2010. Págs. 987-1010.

CANCIO MELIÁ, M. *Los delitos de terrorismo en derecho penal español. (Terrorismo e justiça penal: Reflexôes sobre a eficiência e o garantismo)*. Editorial Belo Horizonte: Fórum. 2014. Págs. 183-226.

CANCIO MELIÁ, M. *Los delitos de terrorismo estructura típica e injusto.* Editorial Reus. Barcelona. 2010.

CANCIO MELIÁ, M. *Sentido y límites de los delitos de terrorismo*. *(Estudios penales en homenaje a Enrique Gimbernat).* Editorial Edisofer. Madrid. 2008. Págs. 1879-1906.

CARBAJO CASCÓN, F. *Publicaciones electrónicas y propiedad intelectual.* Editorial Colex. Madrid. 2002.

CARBONELL MATEU, J. C. *Constitución, derechos fundamentales y sistema penal (semblanzas y estudios con motivo del setenta aniversario del profesor Tomás Salvador Vives Antón)*. Editorial Tirant lo Blanch. 2009. Págs. 945-974.

CARMONA SALGADO, C. *Calumnias, injurias y otros atentados al honor. Perspectiva doctrinal y jurisprudencial.* Editorial Tirant lo Blanch. Valencia. 2012.

CARMONA SALGADO, C. *La nueva Ley de propiedad intelectual especial consideración al delito introducido en el Código penal tras la reforma de 1987*. Editorial RDU. Madrid. 1988.

CARNELUTTI, F, *«La Cenicienta», en Cuestiones sobre el Proceso Penal* (trad. Sentís Melendo), Librería el Foro, Buenos Aires, 1994, (págs. 13 y ss).

CARNELUTTI, F, *Instituciones del Proceso Civil: Tomo I*. Ediciones Jurídicas Europa-América. Buenos Aires. 1959.

CARRASCO ANDRINO, M. M. *La protección penal del secreto de empresa*. Cedecs. Madrid. 1998.

CARRASCOSA ALVAREZ, V. *El documento electrónico como medio de prueba. (Dogmática penal, política criminal y criminología en evolución).* Editorial Centro de Estudios Criminológicos de la Universidad de Tenerife. Canarias. 1997. Págs. 187-202.

CARRASCOSA GONZALEZ, J. *Internet y derechos de la personalidad: los retos para el Derecho internacional privado europeo y español. (España y la Unión Europea en el orden internacional: XXVI jornadas ordinarias de la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales. Universidad de Sevilla, 15 y 16 de octubre de 20159.* Editorial Tirant Lo Blanch. Valencia. 2017. Págs. 807 – 830.

CARRASCOSA GONZÁLEZ, J. *Internet y derechos de la personalidad: los retos para el derecho internacional privado europeo y español. (España y la Unión Europea en el orden internacional).* Editorial Tirant Lo Blanch. Valencia. 2017. Págs. 807 – 830.

CARRETERO GONZÁLEZ, C, DE MONTALVO JÄÄSKELÄINEN, F, GISBERT POMATA, M. y SERRANO MOLINA, A. *Retos de la abogacía ante la sociedad global.* Editorial Civitas/Universidad Pontificia Comillas. Madrid. 2012. Págs. 1475-1490.

CARRIZO GONZÁLEZ-CASTELL, A. *El agente encubierto como instrumento de lucha contra la corrupción, análisis comparado de las regulaciones española y colombiana (El estado de derecho colombiano frente a la corrupción: retos y oportunidades a partir del Estatuto Anticorrupción de 2011)*. Editorial Universidad del Rosario. 2013. Págs. 105-126.

CASANOVA MARTÍ, R. *Nueva regulación de la intervención de las comunicaciones orales directas en la LO 13/2015, de 5 de octubre.* (Los desafíos de la justicia en la era post crisis). Editorial Atelier. Madrid. 2016. Págs. 165-177.

CASANUEVA SANZ I, PUEYO RODERO J. A. Y OTROS. *Cuadernos penales José María Lidón. El anteproyecto de modificación del Código Penal de 2008: algunos aspectos*. Publicaciones Universidad de Deusto. Bilbao. 2009. Págs. 183-201.

CASAS VALLÈS, R. *Derecho y nuevas tecnologías.* Editorial UOC. 2005. Págs. 287-338.

CASTÁN TOBEÑAS J, *Derecho Civil Español, Común y Foral. Tomo Segundo. Derecho de Cosas. Volumen Primero. Los derechos reales en general. El dominio. La posesión.* Editorial Reus SA. Madrid. 1987.

CASTÁN TOBEÑAS J, *Derecho Civil Español, Común y Foral. Tomo Segundo. Derecho de Cosas. Volumen Segundo. Los derechos reales restringidos.* Editorial Reus SA. Madrid. 1986.

CASTÁN TOBEÑAS. J. *Derecho Civil Español Común y Foral. Tomo I: Introducción y parte general. Vol. 2: Teoría de la relación jurídica. La persona y los derechos de la personalidad. Las cosas*. Editorial Reus. Madrid. 2005.

CASTAÑEDA GONZÁLEZ A. Y OTROS. *Derecho tecnológico: respuesta jurídica a nuevos retos: guía práctica*. Ediciones Experiencia S.L. Barcelona. 2004. Págs. 223-276.

CASTELLS I MARQUÈS, M. *Drones civiles. (Inteligencia artificial Tecnología Derecho).* Editorial Tirant lo Blanch. Valencia. 2017. Págs. 73-99.

CASTILLEJO MANZANARES, R. y otros.*Temas actuales en la persecución de los hechos delictivos.* Editorial La Ley. 2012. Págs. 373-396.

CASTILLO BLANCO, F. A. *Situación actual y tendencias de la función pública española.* Editorial Comares. Granada. 1998. Págs. 477-496.

CASTIÑEIRA PALOU, M. T. y otros. *Lecciones de derecho penal: parte especial.* Editorial Atelier. Barcelona. 2006. Págs. 181- 253.

CEREZO MIR J, *Curso de derecho penal español. Parte General. Introducción.* Editorial Tecnos. Madrid. 2004.

CEREZO MIR, J. Y OTROS. *El nuevo Código Penal: presupuestos y fundamentos: (libro homenaje al profesor Doctor Don Angel Torío López).* Editorial Comares. Granada. 1999.

CERVELLÓ DONDERIS, V. *El delito de coacciones en el Código penal de 1995. Anexo con índice jurisdiccional.* Editorial Tirant lo Blanch. 1999.

CERVELLÓ DONDERIS, V. *Régimen y organización interna. Seguridad y vigilancia. (Derecho Penitenciario)*. Editorial Tirant Lo Blanch. Valencia. 2016. Págs. 183-186.

CHAMOCHO CANTUDO M. A. *Sobre un hito jurídico, La Constitución de 1812 reflexiones actuales, estados de la cuestión, debates historiográficos.* Universidad de Jaén. 2012. Págs. 195-221.

CHIOVENDA, G, *Principios de Derecho Procesal Civil. Tomo II.* Editorial Reus. Madrid. 1925.

CHOCLÁN MONTALVO, J. A. *El delito de estafa*. Editorial Bosch. Barcelona. 2000.

CHOZAS ALONSO, J. M. *El testigo. Garantías procesales. Testimonios especiales. Testigo protegido LO 19/1994, de 23 de noviembre. (El interrogatorio de testigos en los procesos civil y penal. Su práctica ante los Tribunales).* Editorial La Ley. Madrid. 2013. Págs. 721-804.

CHOZAS ALONSO, J. M. *La competencia territorial en los acuerdos del TS. (Los sujetos protagonistas del proceso penal)*. Editorial Dykinson. Madrid. Págs. 153-155.

CIE 10: Clasificación internacional de enfermedades. (Tomo I y II). Editorial del Boletín Oficial del Estado. Madrid. 2015.

CLEMENTE MEORO, M. E, CAVANILLAS MÚGICA, S. *Responsabilidad civil y contratos en Internet su regulación en la ley de servicios de la sociedad de la información y de comercio electrónico.* Editorial Comares. Granada. 2003.

COBO DEL ROSAL M. *Comentarios al Código Penal.* Editorial Edersa. Granada. 1999. Págs. 769-780.

COBO DEL ROSAL, M. *Constitución y Derecho Penal. El principio de legalidad en materia criminal. (Estudios jurídicos: libro conmemorativo del bicentenario de la Universidad de la Laguna).* Vol. 1. Tenerife. 1993. Págs. 157-168.

COBO DEL ROSAL, M. *Derecho penal español: parte especial.* Editorial Dykinson. Madrid. 2005. Págs. 1117-1128.

COBO DEL ROSAL, M. *Sobre la apología criminal y los delitos de terrorismo. (Dogmática y ley penal: libro homenaje a Enrique Bacigalupo).* Editorial Marcial Pons. Madrid. 2004. Págs. 103-114.

Código Penal de España. Imprenta Nacional. Madrid. 1850.

COLMENERO GUERRA, J. A. *Acotaciones al sistema de medios de impugnación tras la reforma de la Ley de Enjuiciamiento Criminal en 2015. Nuevos horizontes del derecho procesal. Libro-homenaje al Prof. Ernesto Pedraz Penalva*. Editorial Bosch. Barcelona. 2016. Págs. 559-585.

COLOMER BEA, D. *La incriminación del terrorismo individual en la reforma penal de 2015 ¿violencia política organizada? (Terrorismo, sistema penal y derechos fundamentales).* Editorial Tirant lo Blanch. Valencia. 2018. Págs. 135-158.

COLOMER HERNÁNDEZ, I. *La motivación de las sentencias sus exigencias constitucionales y legales.* Editorial Tirant lo Blanch. Valencia. 2003.

COLOMER HERNÁNDEZ, I. *Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016.* Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute. Sepin Editorial Jurídica. Madrid. 2018. Págs. 767-781.

COLOMER HERNÁNDEZ, I. *Uso y cesión de datos de las comunicaciones electrónicas para investigar delitos tras la STJUE de 21 de diciembre de 2016 (Estudios sobre Jurisprudencia Europea: materiales del I y II Encuentro anual del Centro español del European Law Institute).* Sepin Editorial Jurídica. 2018. Págs. 767-781.

COMAS DE ARGEMIR CENDRA, M. *La aplicación judicial del principio de Justicia Universal en España. (El principio de justicia universal)*. Editorial Constitución y Leyes, COLEX. Madrid. 2001. Págs. 173-179.

CONDE-PUMPIDO FERREIRO C, *Derecho Penal. Parte General.* Editorial Colex. Madrid. 1990.

CONDE-PUMPIDO FERREIRO, C. *Estafas*. Editorial Tirant lo Blanch. Valencia. 1997

CORCOY BIDASOLO M. Y OTROS. *Nuevas tendencias en política criminal: una auditoría al Código Penal español de 1995.* Editorial Reus. Madrid. 2006.

CORCOY BIDASOLO, M. *Comentarios al Código penal: reforma LO 5/2010*. Editorial Tirant lo Blanch. Valencia. 2011.

CORCOY BIDASOLO, M. GÓMEZ MARTÍN V, VALIENTE IVAÑEZ, V. *Fraude a consumidores y Derecho penal fundamentos y talleres de leading cases*. Editorial Edisofer. Madrid. 2016.

CORONAS GONZALEZ S.M, *Manual de Historia del Derecho español.* Tirant lo Blanch. Valencia. 1999.

CORRALES ELIZONDO, A. *El principio de jurisdicción penal universal y su incidencia en el Estatuto del Tribunal Penal Internacional. (Hacia una justicia internacional: XXI Jornadas de Estudio: 9 a 11 de junio de 1999).* Editorial del Ministerio de Justicia. Madrid. 2000. Págs. 527-536

CORTÉS BECHIARELLI, E. *Responsabilidad penal y procesal de las personas jurídicas.* Editorial Francis Lefebvre. Madrid. 2015.

CORZO SOSA, E. *La cuestión de inconstitucionalidad*. Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 1998.

COWEN, D. *Superutilidades Hacker*. Editorial Anaya Multimedia. Madrid. 2006.

CRESPO BARQUERO, P. *Intervenciones judiciales en materia de comunicaciones telefónicas e internet. (Problemas actuales del proceso penal y derechos fundamentales)*. Editorial Universidad de Deusto. Bilbao. 2010. Págs. 55-104.

CRUZ DE PABLO, J. A. *Derecho penal y nuevas tecnologías, aspectos sustantivos: adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 de noviembre, especial referencia al nuevo artículo 286 CP*. Editorial Marcial Pons (Difusión Jurídica y Temas de actualidad). Madrid. 2006.

CUELLO CALÓN, E. *Código Penal. Texto revisado 1963 y leyes penales especiales*. Editorial Bosch. Barcelona. 1963.

CUELLO CONTRERAS, J. *La conspiración para cometer el delito interpretación del art. 4. I CP: los actos preparatorios de la participación.* Editorial Bosch. Barcelona. 1978.

CUERDA ARNAU M. R. y FERNÁNDEZ HERNÁNDEZ A, *Menores y Redes Sociales ciberbullying, ciberstalking, cibergrooming, pornografía, sexting, radicalización y otras formas de violencia en la red.* Ediciones Tirant Lo Blanch. Valencia. 2016.

CUERDA ARNAU, M. L. Y GARCÍA AMADO, J. A. *Protección jurídica del orden público, la paz pública y la seguridad ciudadana.* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 83-118.

DARÍO CERINA, G. *La lucha contra la delincuencia organizada, notas desde el derecho penal sustantivo y referencias al agente encubierto como medio de investigación extraordinario en una interna y supranacional (Dos décadas de reformas penales).* Editorial Comares. Granada. 2008. Págs. 145-176.

DAVARA RODRÍGUEZ M. A. *JIS'2000: III Jornadas sobre informática y sociedad*. Editorial Universidad Pontificia Comillas. 2001. Págs. 159-186.

DAVARA RODRÍGUEZ M. A. *X años de encuentros sobre informática y derecho.* Editorial Aranzadi. 1997. Págs. 371-380.

DAVARA RODRÍGUEZ M. A. *XVII Encuentros sobre Informática y Derecho. 2002-2003*. Editorial Universidad Pontificia Comillas. 2003. Págs. 423-434.

DAVARA RODRÍGUEZ M.A, *Manual de derecho informático.* Editorial Thomson-Aranzadi. Navarra. 2008. (Págs. 355-396).

DAVARA RODRÍGUEZ, M. A. *Código de Internet*. Editorial Aranzadi. 2004. Cizur Menor (Navarra).

DAVARA RODRÍGUEZ, M. A. *Delitos informáticos*. Editorial Thomson Reuters Aranzadi. Navarra. 2017.

DAVARA RODRÍGUEZ, M. A. *X años de encuentros sobre informática y derecho, 1996-1997.* Editorial Aranzadi. 1997. Cizur Menor (Navarra).

DAVARA RODRÍGUEZ, M. A. *XIV Encuentros sobre Informática y Derecho: 2000-2001*. Editorial Aranzadi. Cizur Menor (Navarra). 2001. Págs. 45-50.

DAVARA RODRÍGUEZ, M. A. *XVII Encuentros sobre Informática y Derecho, 2002-2003.* Editorial de la Universidad Pontificia Comillas. Madrid. 2003. Págs. 423-434.

DE ARÍSTEGUI, G. *El islamismo contra el islam las claves para entender el terrorismo yihadista*. Ediciones B. Barcelona. 2004.

DE ASÍS ROIG, R. F. *El Juez y la motivación en el derecho*. Editorial Dykinson. Madrid. 2005.

DE COSSÍO Y MARTÍNEZ, M. *Derecho al honor, técnicas de protección y límites.* Editorial Tirant lo Blanch. Valencia. 1993.

DE ESTEBAN J. *Tratado de Derecho Constitucional I.* Servicio de Publicaciones. Facultad de Derecho. Universidad Complutense de Madrid. Madrid. 2001. Págs. 297-304.

DE ESTEBAN J. Y GONZALEZ-TREVIJANO P.J. *Tratado de Derecho Constitucional II.* Servicio de Publicaciones. Facultad de Derecho. Universidad Complutense de Madrid. Madrid. 2004.

DE LA CUESTA ARZAMENDI, J. L, DE LA MATA BARRANCO. N. J. *Responsabilidad penal de las personas jurídicas.* Aranzadi. Cizur Menor (Navarra) 2013.

DE LA CUESTA ARZAMENDI. J.L. y DE LA MATA BARRANCO N.J, *Derecho Penal informático.* Editorial Thomson-Reuters. Navarra. 2010.

DE LA IGLESIA CHAMARRO, A. *Videovigilancia, espacio público y derechos fundamentales. (Conflictos de derechos fundamentales en el espacio público)*. Editorial Marcial Pons. Madrid. 2017. Págs. 37-70.

DE LA MATA, N. J. *Delitos contra los sistemas de información. (Derecho penal económico y de la empresa).* Editorial Dykinson. Madrid. 2018. Págs. 727-759.

DE LA OLIVA SANTOS, A. (y OTROS), *Curso de Derecho Procesal Civil I. Parte General.* Editorial Universitaria Ramón Areces. Madrid. 2012.

DE LA OLIVA SANTOS, A. (y OTROS), *Curso de Derecho Procesal Civil II. Parte Especial.* Editorial Universitaria Ramón Areces. Madrid. 2012.

DE LA OLIVA SANTOS, A. (y OTROS), Derecho *Procesal Civil: Ejecución forzosa. Procesos especiales.* Editorial Universitaria Ramón Areces. Madrid. 2005.

DE LA OLIVA SANTOS, A. (y OTROS), *Derecho Procesal Penal*. Editorial Universitaria Ramón Areces. Madrid. 2007.

DE LA OLIVA SANTOS, A. (y OTROS), *Derecho Procesal: Introducción.* Editorial Universitaria Ramón Areces. Madrid. 2004.

DE LA OLIVA SANTOS, A. *Objeto del proceso y cosa juzgada en el proceso civil*. Editorial Civitas. Madrid. 2005.

DE LA OLIVA SANTOS, A. y DIEZ-PICAZO GIMÉNEZ, I, *Derecho Procesal Civil: El proceso de declaración.* Editorial Universitaria Ramón Areces. Madrid. 2004.

DE LA QUADRA-SALCEDO Y FERNÁNDEZ DEL CASTILLO, T, VIDA FERNÁNDEZ J. *Derecho de las telecomunicaciones adaptado a la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*. Editorial Thomson Reuters-Civitas. Pamplona. 2015.

DE LA QUADRA-SALCEDO Y FERNÁNDEZ DEL CASTILLO, T. y VIDA FERNÁNDEZ, J. *Derecho de las telecomunicaciones adaptado a la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*. Editorial Thomson Reuters-Civitas. Madrid. 2015.

DE LA ROSA CORTINA, J. M, *Los delitos de pornografía infantil. Aspectos penales, procesales y criminológico*. Editorial Tirant lo Blanch. Valencia. 2011.

DE MARCELO RODAO, J. *Guía de campo de los virus informáticos*. Editorial RA-MA. Madrid. 1995.

DE MARCELO RODAO, J. *Virus de sistemas informáticos e Internet*. Editorial RA-MA. Madrid. 1999.

DE MEER LECHA-MARZO, F. *La constitución de la II República autonomías, propiedad, iglesia, enseñanza.* Editorial Universidad de Navarra, Ediciones Universidad de Navarra. EUNSA. Pamplona. 1978.

DE MONTALVO JÄÄSKELÄINEN, F. *Los derechos y libertades públicas (Lecciones de Derecho Constitucional)*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 395-397

DE NOVA LABIÁN. *Delitos contra la propiedad intelectual en el ámbito de internet.* Editorial Dykinson S.L. 2010.

DE PERAY BAIGES, A. *La entrada y registro domiciliario. (La prueba en el proceso penal).* Revista general de derecho. Madrid. 2000. Págs. 309-436.

DE PORRES ORTIZ DE URBINA E. *Hacia un catálogo de buenas prácticas para optimizar la investigación judicial.* Consejo General del Poder Judicial. Madrid. 2009. Págs. 413-452.

DE ROS CEREZO, R. M. *Derecho de internet: la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.* Editorial Aranzadi. Cizur Menor (Navarra). 2003. Págs. 65-196.

DE URBANO CASTRILLO E. Y OTROS. *Delincuencia informática. Tiempos de cautela y amparo.* Editorial Thomson Reuters. Pamplona. 2012.

DE URBANO CASTRILLO, E. *La valoración de la prueba electrónica*. Editorial Tirant Lo Blanch. Valencia. 2009.

DE URBANO CASTRILLO, E. *El derecho al secreto de las comunicaciones.* Editorial La Ley. Madrid. 2011.

DE URBINA GIMENO, I. O. *Memento práctico Francis Lefebvre. Penal económico y de la empresa.* Ediciones Francis Lefebvre. Madrid. 2011. Pág. 4200.

DE VERDA Y BEAMONTE, J. R. *Veinticinco años de aplicación de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.* Editorial Aranzadi. 2007. Cizur Menor (Pamplona). Págs. 93-118.

DEL CAMINO VIDAL FUEYO, M. *La constitucionalidad de determinadas diligencias de investigación policial que afectan a la intimidad. (La constitución política de España. Estudios en homenaje a Manuel Aragón Reyes).* Centro de Estudios Políticos y Constitucionales. 2016. Págs. 947-966.

DEL MORAL GARCÍA, A, RODRÍGUEZ MOURULLO, G. *Delitos de injuria y calumnia régimen procesal.* Editorial Constitución y Leyes, COLEX. 1990.

DEL MORAL GARCÍA, A. y SANTOS VIJANDE, J. M. *Publicidad y secreto en el proceso penal.* Editorial Comares. Granada. 1996.

DEL POZO PÉREZ, M. *El agente encubierto como medio de investigación procesal en el ámbito de la cooperación jurídica internacional. (Constitución Europea: aspectos históricos, administrativos y procesales).* Editorial Santiago de Compostela: Tórculo. 2006. Págs. 271-328.

DEL RÍO FERNÁNDEZ, L. *El delito de amenazas (en el nuevo Código Penal) análisis doctrinal y jurisprudencial, requisitos y modalidades.* Editorial General de Derecho. Sedavi (Valencia). 1997.

DEL ROSAL, J. Y OTROS. *Política criminal y reforma penal: homenaje a la memoria del prof. Dr. D. Juan del Rosal.* Editoriales de Derecho Reunidas. EDERSA. 1993. Madrid. Págs. 761-791 y 833-841.

DELGADO GARCÍA, M. D. *El Agente encubierto técnicas de investigación: problemática y legislación comparada. (La criminalidad organizada ante la justicia)*. Editorial de la Universidad de Sevilla. 1996. Págs. 69-84.

DELGADO MARTÍN, J. *El proceso penal ante la criminalidad organizada. El agente encubierto. (Problemas actuales de la justicia penal: los juicios paralelos, la protección de los testigos, la imparcialidad de los jueces, la criminalidad organizada, los juicios rápidos, la pena de multas)*. Editorial J. M. Bosch Editor. Barcelona. 2001. Págs. 91-132.

DELGADO MARTÍN, J. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Editorial La Ley Wolters Kluver. Madrid. 2016.

DELGADO PORRAS, A. *Propiedad Intelectual.* Editorial Aranzadi. 2005.

DÍAZ LÓPEZ, J. A. *El delito de usurpación del estado civil*. Editorial Dykinson. Madrid. 2010.

DÍEZ RIPOLLÉS J.L. *La ciencia del derecho penal ante el nuevo siglo: libro homenaje al profesor doctor Don José Cerezo Mir*. Editorial Tecnos. Madrid. 2002. Págs. 1281-1298.

DÍEZ RIPOLLÉS, J. L. *La ley penal en el espacio. (Derecho Penal Español Parte General).* Editorial Tirant lo Blanch. 2016. Valencia. Págs. 72 - 99

DIEZ-PICAZO L. Y GULLÓN A, *Sistema de Derecho Civil. Volumen Primero. Introducción. Derecho de personas. Autonomía Privada. Persona Jurídica.* Editorial Tecnos. Madrid. 2005.

DUEÑAS SANTOFIMIA, J. P. *La intervención de las comunicaciones.* Editorial Estudios jurídicos. Cuerpo de Secretarios Judiciales. Núm. 1. 2000. Págs. 83-112.

DURÁN SILVA, C. M. *La Videovigilancia en el Proceso Penal. Tratamiento Procesal y Eficacia Probatoria*. Editorial Tirant Lo Blanch. Valencia. 2018. Págs. 55-59.

DURÁN SILVA, C. *La diligencia de entrada y registro: su necesaria adaptación a la realidad actual (La reforma del proceso penal)*. Editorial La Ley. 2013. Madrid. Págs. 351-421.

ECHANO BASALDUA, J. I. *Estudios jurídicos en memoria de José María Lidón.* Universidad de Deusto. 2002. Págs. 537-566.

ELVIRA PERALES, A. *¿Qué hay de nuevo en torno al derecho al secreto de las comunicaciones? (La constitución política de España estudios en homenaje a Manuel Aragón Reyes).* Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 2016. Págs. 601-616.

ELVIRA PERALES, A. *El derecho al secreto de las comunicaciones telefónicas a golpe de jurisprudencia. (Estudios sobre la Constitucion Española: homenaje al profesor Jordi Solé Tura, Vol. 2).* 2008. Editorial del Congreso de los Diputados. Madrid. Págs. 1.143-1.154.

ENCABO VERA, M. A. *Estudios sobre derechos de propiedad intelectual.* Editorial Fundación AISGE. Madrid. 2015.

ENRIQUE PÉREZ LUÑO, A. *Manual de informática y derecho.* Editorial Ariel. Barcelona. 1996.

ESCUDERO J.A, *Curso de Historia del Derecho. Fuentes e Instituciones Político-administrativas.* Autor-Editor. Madrid. 2003.

ESPADAS BURGOS, M. *La época de la restauración: (1875-1902).* Editorial Espasa Calpe. Madrid. 2000. Págs. 29-70.

ESTANISLAO ESCALANTE BARRETO, C. *La indagación y la investigación en el proceso penal, límites constitucionales: el agente encubierto y la interceptación telefónica*. Editorial Ibáñez. Bogotá (Colombia). 2015.

ESTHER MORÓN LERMA *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías.* Editorial Aranzadi. Cizur Menor (Navarra). 2002.

ESTRELLA RUIZ, M. *Entrada y registro, interceptación de comunicaciones postales, telefónicas, etc...* Cuadernos de derecho judicial. Núm. 12. 1996. Págs. 351-392.

ETXEBERRÍA GURIDI, J. F. *Prueba pericial. (La Prueba Tomo II la Prueba en el Proceso Penal).* Editorial Tirant Lo Blanch. 2017. Págs. 655 – 716.

FAKHOURI GÓMEZ, Y. *Algunas cuestiones relativas a la competencia "ratione materiae" de la Corte Penal Internacional. (Derecho y justicia penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuéllar García)*. Editorial Constitución y Leyes, COLEX. Madrid. 2006. Págs. 521-544.

FARALDO-CABANA, P, PUENTE ABA, L. M, RAMOS VÁZQUEZ, J. A. *Política criminal y reformas penales.* Editorial Tirant lo Blanch. Valencia. 2007. Págs. 259-281.

FARALDO-CABANA, P. *Nuevos retos del derecho penal en la era de la globalización.* Editorial Tirant lo Blanch. Valencia. 2004. Págs. 381-410.

FAYOS GARDÓ A, ANDRÉS SEGOVIA, B. *La propiedad intelectual en la era digital.* Editorial Dykinson. Madrid. 2016.

FAYOS GARDÓ, A, CONDE COLMENERO, P. *Los derechos a la intimidad y a la privacidad en el siglo XXI.* Editorial Dykinson. Madrid. 2014. Págs. 113-130.

FAYOS GARDÓ, A. y CONDE COLMENERO, P. *Los derechos a la intimidad y a la privacidad en el siglo XXI.* Editorial Dykinson. Págs. 113-130.

FERNÁNDEZ DE FRUTOS, M. *El procedimiento de la cuestión de inconstitucionalidad*. Editorial Cedecs. Barcelona. 2003.

FERNÁNDEZ DE GATTA SÁNCHEZ, D. *La evolución de la ciencia y su relación con la libertad (o su falta). (Creación Científica e Innovación Tecnológica: una Aproximación Desde el Derecho Público)*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 162-163.

FERNÁNDEZ GONZÁLEZ, C. M, AYLLÓN SANTIAGO, H. S. y NIETO BALLESTEROS, J. A. *El uso legal de los drones (RPA). Ámbito policial y uso privado*. Editorial Reus. Madrid. 2018.

FERNÁNDEZ ORDÓÑEZ, M. CREMADES GARCÍA J. y ILLESCAS ORTIZ R. *Régimen jurídico de internet.* Editorial Wolters Kluwer. Madrid. 2001. Págs. 257-310.

FERNÁNDEZ RODRÍGUEZ, J. J, SANSÓ-RUBERT PASCUAL, D. *Internet, un nuevo horizonte para la seguridad y la defensa.* Editorial Universidade de Santiago de Compostela, Servizo de Publicacións e Intercambio Científico. 2010.

FERNÁNDEZ RODRÍGUEZ, J. J. *La intervención de las comunicaciones digitales a propósito del sistema SITEL. (Cuestiones de inteligencia en la sociedad contemporánea)*. Editorial del Ministerio de Defensa. Madrid. 2011. Págs. 61-76.

FERNÁNDEZ RODRÍGUEZ, J. J. *Secreto e Intervención de las Comunicaciones en Internet.* Editorial Aranzadi. Aranzadi. 2004.

FERNÁNDEZ RODRÍGUEZ, J. J. *Secreto e Intervención de las Comunicaciones en Internet*. Editorial Aranzadi. Pamplona. 2004.

FERNÁNDEZ SÁNCHEZ, M. T. *Protección penal del secreto de empresa.* Editorial Constitución y Leyes. COLEX. Madrid. 2000.

FERNÁNDEZ SEGADO F, *El Sistema Constitucional Español.* Editorial Dykinson. Madrid. 1992.

FERNÁNDEZ SEGADO, F. *Las misiones constitucionales de las fuerzas y cuerpos de seguridad. (Estudios de teoría del Estado y derecho constitucional en honor de Pablo Lucas Verdú. Vol. 3)*. Editorial de la Universidad Complutense, Facultad de Derecho. Madrid. 2001. Págs. 2087-2114.

FERNÁNDEZ TERUELO J.G, *Cibercrimen. Los delitos cometidos a través de Internet.* Editorial Constitutio Criminalis Carolina. Oviedo. 2007.

FERNÁNDEZ TERUELO J.G, *Derecho Penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes.* Editorial Lex Nova. Valladolid. 2011.

FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J. A. *Diligencias de investigación. Registro de ordenadores. (Cuestiones actuales del Proceso Penal).* Ediciones Experiencia. Barcelona. 2015. Págs. 138-140.

FERRÉ OLIVÉ, J. C. *El derecho penal de la posguerra.* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 467-485.

FIESTAS LOZA A. *Homenaje al profesor Alfonso García-Gallo. Vol. 3.* Publicaciones Universidad Complutense. Madrid. 1996. Págs. 257-284.

FIGUEROA NAVARRO, M. C. *La cadena de custodia en el proceso penal.* Editorial EDISOFER. Madrid. 2015.

FLORES PRADA I, *Criminalidad Informática. Aspectos sustantivos y procesales.* Tirant lo Blanch. Valencia. 2012.

FONT SERRA, E. *Homenaje a don Eduardo Font Serra. Tomo II*. Ministerio de Justicia, Centro de Estudios Jurídicos de la Administración de Justicia. Madrid. 2004. Págs. 1849-1880.

FRIGOLA J. y otros. *Delitos contra el orden público, terrorismo, contra el Estado o la comunidad internacional*. Editorial Bosch, S.A. Barcelona. 1998.

FRIGOLS 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.* (*La protección jurídica de la intimidad)*. Editorial Iustel. Madrid. 2010. Págs. 37-90.

FUENTES SORIANO, O. *Justicia penal y nuevas formas de delincuencia.* Editorial Tirant Lo Blanch. Valencia. 2017.

FUENTES SORIANO, O. *Medio de investigación tecnológica y Problemas probatorios. (El proceso penal. Cuestiones fundamentales)*. Editorial Tirant Lo Blanch. Valencia. 2007. Págs. 253-385.

GALÁN JUÁREZ, M. *Intimidad nuevas dimensiones de un viejo derecho.* Editorial Centro de Estudios Ramón Areces. Madrid. 2005.

GALÁN MUÑOZ, A. *El fraude y la estafa mediante sistemas informáticos análisis del artículo 248.2 C.P.* Editorial Tirant lo Blanch. Valencia. 2005.

GALINDO, F. *Derecho e informática*. Editorial La Ley. Grupo Wolters Kluwer. Madrid. 1998.

GÁLLEGO HIGUERAS, G. F. *Código de Derecho Informático y de Las Nuevas Tecnologías.* Editorial Aranzadi. Cizur Menor (Navarra). 2003.

GARCÍA ARÁN, M. *El principio de justicia universal en la L.O. del Poder Judicial español. (Crimen internacional y jurisdicción universal: el caso Pinochet)*. Editorial Tirant lo Blanch. Valencia. 2000. Págs. 63-88.

GARCÍA CUADRADO, A. M. *Principios de derecho constitucional*. Editorial Eolas. León. 2013.

GARCÍA DE ENTERRÍA MARTÍNEZ-CARANDE, E. *Comentarios a la Ley General de Telecomunicaciones, Ley 32/2003, de 3 de noviembre.* Editorial Thomson Reuters-Civitas. Cizur Menor (Navarra). 2004. Págs. 985-999.

GARCÍA GONZÁLEZ J, *Ciberacoso. La tutela penal de la intimidad, la integridad y la libertad sexual en Internet.* Editorial Tirant lo Blanch. Valencia. 2010.

GARCÍA GONZÁLEZ, J. *La violencia de género en la adolescencia.* Editorial Thomson Aranzadi. Cizur Menor (Navarra). 2012. Págs. 291-324.

GARCÍA MATEOS, J. A. *Cadena de custodia vs mismidad*. *(La prueba electrónica, validez y eficacia procesal).* Editorial Juristas con Futuro. Desafíos Legales. Madrid. 2016. Pág. 130.

GARCÍA MESCUA, D. *Aportación de mensajes de whatsapp a los procesos judiciales. Tratamiento procesal*. Editorial Comares. Granada. 2018.

GARCÍA RIVAS, N. *Globalización y justicia penal universal, paralelismos. (El Derecho penal frente a la inseguridad global)*. Editorial Bomarzo. Albacete. 2007. Págs. 9-26

GARCÍA RIVAS, N. y otros. *Delitos de organización: Arts. 515 y 516, 570 bis y ss, 571 y ss. (Asociaciones ilícitas, organizaciones criminales y delitos de terrorismo) (Consideraciones a propósito del proyecto de ley de 2009 de modificación del Código Penal: Conclusiones del Seminario interuniversitario sobre la reforma del Código Penal celebrado en la Universidad Carlos III de Madrid).* Editorial Tirant lo Blanch. Valencia. 2010. Págs. 409-424.

GARCÍA SAN MARTÍN, J. *Diligencias y medios de prueba. Diligencias Sumariales. Registro de dispositivos de almacenamiento masivo de información. (Doctrina penal actualizada)*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 265-266.

GARCÍA SAN MARTÍN, J. *El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal (Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas: memorias del Proyecto I.F.O. Illegal Flow Observation JUST/2011/ISEC/DRUGS/AG/3671).* Editorial Thomson Reuters-Aranzadi. Pamplona. 2015. Págs. 309-319.

GARCÍA VITORIA, A. *Consideraciones de parte general. Características comunes de las diversas figuras criminales referentes a los peritos. (Actividad pericial y proceso penal)*. Editorial Tirant Lo Blanch. Valencia. 2009. Págs. 25-88.

GARCÍA-ESCUDERO MÁRQUEZ, P. y PENDÁS GARCÍA, B. Propiedad intelectual. Editorial Praxis. Barcelona. 1989.

GARCÍA-PABLOS DE MOLINA A, *Tratado de Criminología.* Editorial Tirant lo Blanch. Valencia. 2003.

GARCIMARTIN MONTERO, R. *Los medios de investigación tecnológicos en el proceso penal.* Editorial Thomson-Aranzadi. Pamplona. 2018.

GARCIMARTIN MONTERO, R. *Los medios de investigación tecnológicos en el proceso penal*. Editorial Thomson Reuters Aranzadi. Navarra. 2018.

GARRIGA DOMÍNGUEZ, A. *Datos masivos, dispositivos de geolocalización, etiquetas y dispositivos RFID e internet de las cosas. (Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua)*. Editorial Dykinson. Madrid. 2016. Págs. 25-36

GASCÓN INCHAUSTI, F. *Infiltración policial y "agente encubierto"*. Editorial Comares. Granada. 2001.

GAZAPO LAPAYESE, M. J. *Daesh o el secuestro y deformación de una religión. Islam y terrorismo. Conceptos (des)vinculados. (Los estudios militares y de seguridad en los albores del siglo XXI*). Editorial Universidad de Granada. 2017. Págs. 133-148.

GIL GIL, A. y MACULAN, E. (DIR.) *Derecho penal internacional.* Editorial Dykinson. Madrid. 2016. Págs. 285-302.

GIMENO SENDRA, J. V. y REGUEIRO GARCÍA, M. T. *Nuevas tendencias en la interpretación de los derechos fundamentales*. Universitas Editorial. Madrid. 2015.

GIMENO SENDRA, V. *Manual de derecho procesal penal (Cuarta parte. La Instrucción. Los actos de investigación)*. Editorial Castillo de Luna. Madrid. 2018.

GÓMEZ COLOMER, J. L. *Diligencia de entrada y registro en lugar cerrado. (Derecho Jurisdiccional III. Proceso Penal).* Editorial Tirant Lo Blanch. Valencia. 2018. Págs. 223-228.

GÓMEZ COLOMER, J. L. *Diligencia de filmación de lugares públicos (Derecho Jurisdiccional III Proceso Penal)*. Editorial Tirant Lo Blanch. Valencia. 2015. Págs. 204-206.

GÓMEZ COLOMER, J. L. *El Tribunal Penal Internacional, investigación y acusación*. Editorial Tirant lo Blanch. Valencia. 2003.

GOMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Los poderes del Estado. La organización territorial del estado. Volumen II)*. Editorial Tirant lo Blanch. Valencia. 2016. Págs. 239-268.

GÓMEZ COLOMER, J. L. *Los actos de investigación garantizados. Modernos medios tecnológicos de investigación. (Derecho Jurisdiccional III, Proceso Penal)*. Editorial Tirant Lo Blanch. Valencia. 2015. Págs. 224-225.

GÓMEZ COLOMER, J. L. y GONZÁLEZ CUSSAC, J. L. *La reforma de la justicia penal: (estudios en homenaje al Prof. Klaus Tiedmann)* Editorial de la Universitat Jaume I. Castellón. 1997. Págs. 409-426.

GÓMEZ DE LA TORRE, I. B. *Lecciones y materiales para el estudio del derecho penal. Vol. 3, Tomo 1: Derecho penal. Parte especial.* Editorial Iustel. Madrid. 2010. Págs. 325-355.

GÓMEZ DE LIAÑO FONSECA HERRERO, M. *El agente encubierto como medida de investigación del terrorismo en el contexto internacional (Terrorismo y estado de derecho).* Editorial Iustel. Madrid. 2010. Págs. 417-434.

GÓMEZ NAVAJAS, J. *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. (Lecciones de Derecho Penal. Parte Especial)*. Editorial Tirant lo Blanch. Valencia. 2018. Págs. 161-162.

GÓMEZ ORBANEJA, E, *«Derecho Procesal Penal»*, Madrid, 1951.

GÓMEZ RIVERO, M. C. *Los delitos contra la propiedad intelectual e industrial. La tutela penal de los derechos sobre bienes inmateriales.* Editorial Tirant lo Blanch. Valencia. 2012.

GONZALEZ CUSSAC, J. L. *Comentarios a la reforma del código penal de 2015*. Editorial Tirant lo Blanch. Valencia. 2015.

GONZÁLEZ CUSSAC, J. L. *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. (Derecho Penal. Parte Especial)*. Editorial Tirant lo Blanch. Valencia. 2016. Págs. 255-256.

GONZÁLEZ DE LA GARZA, L. M. *Redes sociales, instrumentos de participación democrática*. *Análisis de las tecnologías implicadas y nuevas tendencias*. Editorial Dykinson. Madrid. 2015.

GONZÁLEZ GOZALO, A. *La propiedad intelectual sobre la obra audiovisual.* Editorial Comares. Granada. 2001.

GONZÁLEZ LAGE, J. *La prueba pericial en la práctica judicial penal las redes sociales en el proceso penal. (Peritaje y prueba pericial).* Editorial Bosch. Barcelona. 2017. Págs. 563-569.

GONZÁLEZ MONJE, A. *Nuevas tecnologías e investigación penal*. *La superación de los métodos tradicionales. (FODERTICS 3.0: estudios sobre nuevas tecnologías y justicia)*. Editorial Comares. Granada. 2015. Págs. 149-158.

GONZÁLEZ RUS, J. J. *Delito e Informática: algunos aspectos*. Universidad de Deusto. Bilbao. 2007

GONZÁLEZ-CUÉLLAR SERRANO, N. *Garantías constitucionales de la persecución penal en el "entorno digital". (Derecho y justicia penal en el siglo XXI: liber amicorum en homenaje al profesor Antonio González-Cuéllar García)*. Editorial Constitución y Leyes, COLEX. Madrid. 2006. Págs. 887-916.

GOODY, J. *El islam en Europa.* Editorial Gedisa D.L. Barcelona. 2015.

GORDILLO ÁLVAREZ-VALDÉS, I. *IV jornadas de derecho penal el empresario y el consumidor en el código penal.* Universidad Cardenal Herrera-CEU. Elche. 2003. Págs. 49-102.

GORJÓN BARRANCO, M. C. *Ciberespacio y delito: la transposición de los instrumentos internacionales en la realidad penal española. (Política Criminal Ante el Reto de la Delincuencia Transnacional).* Editorial Tirant lo Blanch ARS IVRIS. Valencia. 2016. Págs. 650 – 691.

GRANADOS PÉREZ, C. *Competencia territorial. Principio de ubicuidad. (Acuerdos del Pleno de la Sala Penal del Tribunal Supremo Para Unificación de la Jurisprudencia).* Editorial Tirant Lo Blanch. Valencia. 2017. Págs. 704 – 706.

GUERRERO LEBRÓN, M. J. *La regulación civil y militar de las aeronaves civiles pilotadas por control remoto, comentario al RD 1036/2017, de 15 de diciembre*. Editorial Marcial Pons. Madrid.

GUERRERO PICÓ, M. C. *Registro de vehículos y otros espacios no domiciliarios*. Grupo Editorial Universitario. Granada. 2001.

GUERRICAECHEVARRIA, C. y ECHEBURUA-ODRIOZOLA, E. *Abuso sexual en la infancia: victimas y agresores: un enfoque clínico*. Editorial Ariel. Barcelona. 2005.

GUTIÉRREZ ZARZA, A. *Garantías La protección de la intimidad y los datos personales del sospechoso o acusado al que se refiere la OEI. (Procesales de Investigados y Acusados. Situación Actual en el Ámbito de la Unión Europea).* Editorial Tirant lo Blanch. Valencia. 2018. Págs. 436-440.

GUTIÉRREZ, J D. y LÓPEZ GUISADO, A. *Seguridad digital y Hackers*. Editorial Anaya Multimedia. Madrid. 2004.

HAVA GARCÍA, E. *Delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad. (Tratado de derecho penal español: Pate especial. IV. Delitos contra la Constitución)*. Editorial Tirant lo Blanch. Valencia. 2016. Págs. 623-666.

HEREDERO CAMPO, M. T. *Derechos fundamentales y videovigilancia*. (*Compartiendo visiones de Seguridad: IV Congreso ADESyD)*. Editorial Asociación de Diplomados en Seguridad y Defensa. Madrid. 2018. Págs. 366-381.

HERNÁNDEZ DÍAZ, L. *Delitos relacionados con la criminalidad organizada y el terrorismo. (Adaptación del derecho penal español a la política criminal de la Unión Europea)*. Editorial Aranzadi. Navarra. 2017. Págs. 401-428.

HERNÁNDEZ MARÍN, R. L. *Relaciones entre la aplicación de los enunciados jurídicos y la motivación de las decisiones judiciales. (Interpretación y argumentación, problemas y perspectivas actuales).* Editores Marcial Pons. 2011. Págs. 239-252.

HERRERA CAMPOS, R. *Homenaje al profesor Bernardo Moreno Quesada*. Servicio de Publicaciones de la Universidad de Almería. 2000. Págs. 1019-1029.

HERRERO-TEJEDOR ALGAR, F. *La intimidad como derecho fundamental.* Madrid. Diputación de Castellón. 1998.

HIGUERA GUIMERÁ, J. F, CEREZO MIR, J. *El delito de coacciones.* Editorial Editorial Bosch. Madrid. 1978.

HIMANEN, P. *La ética del hacker y el espíritu de la era de la información.* Editorial Destino. Barcelona. 2002.

HINOJOSA SEGOVIA, R. *La diligencia de entrada y registro en lugar cerrado en el proceso penal.* Editoriales de Derecho Reunidas. EDERSA. Madrid. 1996.

HORMAZÁBAL MALARÉE, H. *Estudios de derecho penal en memoria del prof. Juan José Bustos Ramírez.* Editorial Ubijus. Ciudad de México. 2011. Págs. 631-658.

IGARTUA SALAVERRÍA, J. *La motivación de las sentencias, imperativo constitucional*. Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 2003.

IGNACIO ANITUA, G. Y OTROS. *Derecho penal internacional y memoria histórica desafíos del pasado y retos del futuro*. Editorial Fabian di Placido. Buenos Aires. 2012. Págs. 351-381.

INSA, F y BENCOMO MÁRQUEZ, M. *Revisión jurídico-técnica del proceso de computer forensics y la prueba electrónica como herramienta fundamental en el s- XXI. (El derecho en la sociedad telemática: estudios en homenaje a Valentín Carrascosa López).* Editorial Andavira Editora. Santiago de Compostela, La Coruña. 2012. Págs. 441-455.

IÑESTA PASTOR E. *El código penal español de 1848.* Editorial Tirant lo Blanch. Valencia. 2010

ITURRALDE SESMA, V. *Aplicación del derecho y justificación de la decisión judicial.* Editorial Tirant lo Blanch. Valencia. 2004.

IZQUIERDO SANS, C. *La cuestión prejudicial ante el TJUE. (Lecciones de jurisdicción social).* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 865-886.

JAÉN VALLEJO, M. *Libertad de expresión y delitos contra el honor.* Editorial Constitución y Leyes, COLEX. Madrid. 1992.

JAÉN VALLEJO, M. y PERRINO PÉREZ, Á. L. *La reforma penal de 2015: análisis de las principales reformas introducidas en el Código Penal por las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*. Editorial Dykinson. Madrid. 2015.

JAREÑO ALGOBIA P. *Internet. Edición 2005.* EDITORIAL ANAYA MULTIMEDIA. Madrid. 2005.

JAVIER ÁLVAREZ GARCÍA F. y otros. *La adecuación del derecho penal español al ordenamiento de la Unión Europea la política criminal europea.* Editorial Tirant lo Blanch. Valencia. 2009. Págs. 411-426.

JAVIER QUEL LÓPEZ, F. *Hacia una jurisdicción internacional penal permanente, el proyecto del Estatuto de un Tribunal Penal Internacional de la Comisión de Derecho Internacional. (Las Naciones Unidas y el Derecho Internacional)*. Editorial Ariel. Madrid. 1997. Págs. 152-172.

JIMENO BULNES, M. *La cuestión prejudicial. (El sistema jurisdiccional de la Unión Europea).* Editorial Thomson Reuters Aranzadi. Navarra. 2013. Págs. 173-210.

JIMENO GARCÍA, M. T, y otros. *Hacker*. Editorial Anaya Multimedia. Madrid. 2008.

JORDÀ CAPITÁN, E, DE PRIEGO FERNÁNDEZ, V, SÁDABA CHALEZQUER, C. *La protección y seguridad de la persona en internet aspectos sociales y jurídicos.* Editorial Reus. Barcelona. 2014. Págs. 123-157.

JORGE BARREIRO, A. *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo.* Editorial Civitas. Madrid. 2005. Págs. 949-968.

JOVER PADRÓ, J. *La videovigilancia, a los ojos de la Ley Orgánica 15/1999. (XVIII Encuentros sobre Informática y Derecho, 2003-2004).* Editorial Universidad Pontificia de Comillas. Madrid. 2004. Págs. 93-98.

JUAN JOSÉ GONZÁLEZ RUS. *El Código Penal de 1995, cinco años después. Jornadas de Derecho Penal.* Editorial Servicio de Publicaciones de la Universidad de Córdoba. 2002.

JUANATEY DORADO, C, FERNÁNDEZ-PACHECO ESTRADA, C. *El nuevo panorama del terrorismo en España perspectiva penal, penitenciaria y social.* Servicio de Publicaciones de la Universidad de Alicante. 2013.

JUANES PECES A. *Reforma del Código Penal perspectiva económica tras la entrada en vigor de la Ley Orgánica 5/2010 de 22 de junio: situación jurídico-penal del empresario.* Editorial El Derecho. Madrid. 2010.

LAGARES GARCÍA, D. *Internet y el Derecho, tecnología y jurisprudencia: dos conceptos obligados a entenderse*. Editores Carena. Barcelona. 2000.

LAMEIRAS FERNÁNDEZ, M. y ORTS BERENGUER, E. *Delitos sexuales contra menores abordaje psicológico, jurídico y policial.* Editorial Tirant lo Blanch. Valencia. 2014.

LASARTE C, *Propiedad y derechos reales de goce. Principios de Derecho Civil IV.* Editorial Marcial Pons. Madrid. 2009.

LASARTE, C. *Tomo Primero. Parte general y derecho de la persona principios de derecho civil.* Editorial Marcial Pons. Madrid. 2017. Págs. 263-266.

LAURENZO COPELLO, P. *Los delitos contra el honor.* Editorial Tirant lo Blanch. Valencia. 2002.

LEVIN, R. B. *Virus informáticos: tipos, protección, diagnosis, soluciones.* Editorial McGraw-Hill Interamericana de España. Nueva York (E.E.U.U.) 1991.

LEWIS, B. *La crisis del islam guerra santa y terrorismo.* Ediciones B. Barcelona. 2003.

LLEDÓ GONZÁLEZ, C. *Entradas y registros. (Hacia un catálogo de buenas prácticas para optimizar la investigación judicial)* Editorial del Consejo General del Poder Judicial. Madrid. 2009. Págs. 413-452

LLORENTE SANCHEZ-ARJONA, M, *Las garantías procesales en el espacio europeo de justicia penal.* Editorial Tirant lo Blanch. Valencia. 2014.

LLORIA GARCÍA, P. *Intimidad y redes sociales ¿cómo alcanzar la tutela penal? (Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías).* Editorial Universidad de Valencia. 2011. Págs. 467-475.

LOPEZ BARJA DE QUIROGA J. (Y OTROS), *Códigos penales españoles. 1822, 1848, 1850, 1870, 1928, 1931, 1844. Recopilación y concordancias.* Ediciones Akal. Madrid. 1987.

LÓPEZ BARJA DE QUIROGA, J. *Diligencias de investigación relacionadas con teléfonos móviles y ordenadores. (Tratado de Derecho Procesal Penal)*. Editorial Aranzadi. Navarra. 2014.

LÓPEZ BARJA DE QUIROGA, J. *Tratado de Derecho Procesal Penal. Tomo I*. Editorial Aranzadi. Pamplona. 2014.

LÓPEZ BARJA DE QUIROGA, J. *Tratado de Derecho Procesal Penal. Tomo II*. Editorial Aranzadi. Pamplona. 2014.

LOPEZ GUERRA, L, Y OTROS. *Derecho Constitucional*. *Volumen I. El ordenamiento constitucional. Derechos y deberes de los ciudadanos.* Ediciones Tirant Lo Blanch. Valencia. 2007.

LOPEZ GUERRA L, Y OTROS. *Derecho Constitucional*. *Volumen II.* Los poderes del Estado. La organización territorial del Estado. Editorial Tirant Lo Blanch. Valencia. 2007.

LÓPEZ GUISADO, A. *Seguridad de redes locales.* Editorial ANAYA MULTIMEDIA. Madrid. 2008.

LÓPEZ JIMÉNEZ. R. *Régimen jurídico de los datos personales obtenidos en los descubrimientos casuales durante la investigación de los delitos. (Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios).* Editorial Thomson Reuters-Aranzadi. Pamplona. 2017. Págs. 315-343.

LÓPEZ MARTÍN, A. G, CHINCHÓN ALVAREZ, J. *Nuevos retos y amenazas a la protección de los Derechos humanos en la era de la globalización.* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 65-94.

LÓPEZ ULLA, J. M. *La cuestión de inconstitucionalidad en el derecho español*. Editorial Marcial Pons. Madrid. 2000.

LÓPEZ YAGÜES, V. *La inviolabilidad de las comunicaciones con el abogado defensor*. Editorial Tirant lo Blanch. 2002.

LÓPEZ-BARAJAS PEREA I, *La Intervención de las comunicaciones Electrónicas.* Editorial La Ley. Madrid. 2011.

LÓPEZ-BARAJAS PEREA, I. *El secreto de las comunicaciones con el abogado defensor en la nueva sociedad de la información. (Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal -I Internacional-, La Coruña, 2 y 3 de junio de 2011).* Editorial Editorial Universidad de La Coruña. 2012. Págs. 517-530.

LÓPEZ-BARAJAS PEREA, I. *La intervención de las comunicaciones electrónicas*. Editorial Wolters Kluwer. 2011.

LÓPEZ-BARAJAS PEREA, I. *La protección del derecho al secreto de las comunicaciones en la investigación penal. (Constitución y democracia: ayer y hoy: libro homenaje a Antonio Torres del Moral, Vol. 2).* Editorial Universitas. Madrid. 2012. Págs. 1651-1667.

LÓPEZ-FRAGOSO ÁLVAREZ, T. V. *Las intervenciones telefónicas en el proceso penal*. Editorial Constitución y Leyes. Madrid. 1991.

LÓPEZ-MUÑIZ GOÑI, M. *La prueba pericial: guía práctica y jurisprudencia*. Editorial Colex. Madrid. 2008.

LORENTE JESÚS VALLEJO, M. *Orígenes del Constitucionalismo en el Mundo Hispano. De la Constitución al Estado (1814-1914). (Manual de Historia del Derecho).* Editorial Tirant Lo Blanch. Valencia. 2012. Págs. 328-402.

LORENTE, M. y VALLEJO, J, *Manual de historia del derecho.* Editorial Tirant lo Blanch. Valencia. 2012.

LORENZO SALGADO, J. M. y MAPELLI CAFFARENA, B. *El delito de amenazas consideraciones sobre el bien jurídico protegido. Estudios penales en memoria del profesor Agustín Fernández-Albor.* Editorial Servicio de Publicaciones de la Universidade de Santiago de Compostela. 1989. Págs. 439-480.

Los derechos fundamentales y libertades públicas: XII Jornadas de Estudio Centro de Publicaciones del Ministerio de Justicia. Madrid. 1992. Págs. 543-625 y 691-707.

LUZÓN CUESTA, J. M. *La prueba en el proceso penal derivada de la entrada y registro domiciliario.* Editorial Constitución y Leyes, COLEX. Madrid. 2000.

MAGRO SERVET, V. *Guía práctica profesional de investigación policial y medios de prueba en el proceso penal.* Editorial La Ley. Madrid. 2011.

MAGRO SERVET, V. *Manual práctico de actuación policial-judicial en medidas de limitación de derechos fundamentales (análisis práctico y manual de buenas prácticas a la hora de llevar a efecto las diligencias de investigación penales de intervenciones teleónicas, entradas y registros en lugar cerrado, intervenciones corporales, circulación vigilada de drogas.* Editorial La Ley. Madrid. 2006.

MAGRO SERVET, V. *Manual práctico de actuación policial-judicial en medidas de limitación de derechos fundamentales*. Editorial La Ley. Madrid. 2006.

Manual diagnóstico y estadístico de los trastornos mentales. *Quinta edición. DSM-V*. Editorial Médica Panamericana. Madrid. 2014.

MANUEL MATA Y MARTÍN, R. JAVATO MARTÍN, A. M. *La propiedad intelectual en la era digital límites e infracciones a los derechos de autor en internet*. Editorial Wolters Kluwer. 2011.

MANZANARES SAMANIEGO J.L, *Código Penal (Comentarios y jurisprudencia). I Parte General (Artículos 1 a 137).* Editorial Comares. Granada. 2010.

MANZANARES SAMANIEGO J.L, *Código Penal (Comentarios y jurisprudencia). II Parte Especial (Artículos 138 a 639).* Comares. Granada. 2010.

MANZANARES SAMANIEGO, J. L. *La reforma del código penal de 2015: conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo.* Editorial La Ley. Madrid. 2015.

MARCHENA GÓMEZ, M. *Perseguibilidad de los delitos en Internet. (JIS'2000: III Jornadas sobre informática y sociedad).* Editorial Universidad Pontificia Comillas. Madrid. 2001. Págs. 159-186.

MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N. *La Reforma de la Ley de Enjuiciamiento Criminal en 2015*. Ediciones Jurídicas. Castillo de Luna. Madrid. 2015.

MARCO MOLINA, J. *La propiedad intelectual en la legislación española.* Editorial Marcial Pons. Barcelona. 1995.

MARICA, V-A. *INTERPOL y EUROPOL, actores principales en la escena de la seguridad internacional. (Luces y sombras de la seguridad internacional en los albores del siglo XXI)*. Editorial Instituto Universitario General Gutiérrez Mellado. Vol. 3. Madrid. 2010. Págs. 237-254.

MARÍN ALONSO, I. *El poder de control empresarial sobre el uso del correo electrónico en la empresa su limitación en base al secreto de las comunicaciones*. Tirant lo Blanch. Valencia. 2005.

MARIOLA DÍAZ CORTÉS L. *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales: memorias II Congreso Internacional de Jóvenes investigadores en Ciencias Penales 27, 28 y 29 de junio de 2011*. Editorial Universidad de Salamanca. Salamanca. 2012. Págs. 29-50.

MARQUÉS ARPA, T. y SERRA RUIZ, J. *Cadena de custodia en el análisis forense. Implementación de un marco de gestión de la evidencia digital. (RECSI XIII. Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. Alicante, 2-5 de septiembre de 2014)*. Editorial Universidad de Alicante, Servicio de Publicaciones. 2014. Págs. 167-172.

MÁRQUEZ LOBILLO, P. *Consideraciones críticas sobre el régimen jurídico aplicable a las aeronaves civiles pilotadas por control remoto en el ordenamiento español. (Nuevos enfoques del derecho aeronáutico y espacial)*. Editorial Marcial Pons. Madrid. 2015. Págs. 539-558.

MARTÍN GARCÍA, P. *La prueba en el proceso penal*. Revista general de derecho. Madrid. 2000. Págs. 309-436.

MARTÍN MORALES, R. *El régimen constitucional del secreto de las comunicaciones.* Madrid: Civitas. 1995.

MARTÍN RÍOS, M. P. *Diligencia de entrada y registro en lugar cerrado. (Nociones preliminares de derecho procesal penal para criminólogos).* Editorial Atelier. Barcelona. 2017. Págs. 89-94.

MARTÍN, A. Mª. *Respuestas del estado de derecho ante la ciberdelincuencia.* (Cátedra "Jorge Juan": ciclo de conferencias: curso 2015-2016) Editorial Universidad de La Coruña. 2017. Págs. 137-145.

MARTÍNEZ ATIENZA, G. *Seguridad y delitos tecnológicos. (Seguridad Pública y Privada)*. Editorial Vlex. Madrid. 2016. Págs.195-212

MARTÍNEZ DE AGUIRRE Y ALDAZ, C. *La propiedad intelectual. Curso de derecho civil. Vol. 3, Derechos reales.* Editorial Edisofer. Madrid. 2016. Págs. 237-260.

MARTÍNEZ GARCÍA, M. P. *Competencia penal de la audiencia nacional en matería de terrorismo ¿tribunal de excepción? (Cuestiones actuales de la jurisdicción en España).* Editorial de la Real Academia de Jurisprudencia y Legislación. Madrid. 2010. Págs. 883-897

MARTÍNEZ VAL, J. M. *Galería de grandes juristas.* Editorial Bosch. Barcelona. 1993.

MARTÍNEZ, R. *Policía judicial y Constitución.* Editorial Thomson Reuters-Aranzadi. Pamplona. 2001

MARTÍNEZ-BUJÁN PÉREZ, C. *Delitos relativos al secreto de empresa*. Editorial Tirant lo Blanch. Valencia. 2010.

MARTÍNEZ-SIMANCAS SÁNCHEZ, J, ARAGÓN REYES, M. *La Constitución y la práctica del derecho.* Editorial Sopec. Madrid. 1998. Págs. 1015-1026.

MARTOS NÚÑEZ, J. A. *El perjuicio patrimonial en el delito de estafa.* Editorial Civitas. Madrid. 1990.

MASFERRER A. *Estado de derecho y derechos fundamentales en la lucha contra el terrorismo una aproximación multidisciplinar (histórica, jurídico-comparada, filosófica y económica)*. Editorial Thomson Aranzadi. Pamplona 2011. Págs. 327-358.

MASFERRER A. *La codificación española una aproximación doctrinal e historiográfica a sus influencias extranjeras, y a la francesa en particular.* Editorial Thomson Reuters-Aranzadi. Pamplona. 2014. Págs. 193-270.

MATAS GARCÍA, A. M. y otros. *Hacker. Edición 2006.* Editorial Anaya Multimedia. Madrid. 2005.

MATEU DE ROS CEREZO, R. y CENDOYA MÉNDEZ DE VIGO, J. M. *Derecho de Internet: la contratación electrónica y firma digital.* Editorial Aranzadi. Cizur Menor (Navarra). 2000.

MEINI MÉNDEZ, I. *Lecciones y materiales para el estudio del derecho penal. Delitos contra el honor*. Editorial Iustel. Madrid. 2010. Págs. 267-295.

MENDOZA CALDERON S, *El derecho penal frente a las formas de acoso a menores: bullying, ciberbullying, grooming y sexting.* Editorial Tirant lo Blanch. Valencia. 2014.

MICELI, J. E, ORSI, O. G. y RODRÍGUEZ GARCÍA, N. *Análisis de redes sociales y sistema penal.* Tirant lo Blanch. Valencia. 2017.

MIR PUIG S, *Derecho Penal. Parte General.* Editorial Reppertor. Buenos Aires. 2007.

MIR PUIG S. *Delincuencia informática*. Editorial Promociones y Publicaciones Universitarias, PPU (Marcial Pons). Madrid. 1992. Págs. 67-82. (El fenómeno del delito informático). Págs. 145-176.

MIR PUIG, S, CORCOY BIDASOLO, M, GÓMEZ MARTÍN, V. *Garantías constitucionales y Derecho penal europeo.* Editorial Marcial Pons, Ediciones Jurídicas y Sociales. Madrid. 2012.

MIR PUIG, S. *Delincuencia informática*. Editorial Promociones y Publicaciones Universitarias, PPU. Barcelona. 1992. Págs. 145-176.

MIRÓ LLINARES, F. *Cometer delitos en 140 caracteres, el derecho penal ante el odio y la radicalización en Internet*. Editorial Marcial Pons. Madrid. 2017.

MOLINA MANSILLA, M. C. *Mecanismos de investigación policial, entrega vigilada y agente encubierto*. Editorial Bosch. Barcelona. 2009.

MONTAÑÉS PARDO, M. A. *La Intervención de las Comunicaciones.* Editorial Aranzadi. Cizur Menor (Navarra). 1999.

MONTERO AROCA, J. *La intervención de las comunicaciones telefónicas en el proceso penal (un estudio jurisprudencial).* Editorial Tirant lo Blanch. Madrid. 1999.

MONTERO RÍOS, E. *Ley Provisional de Enjuiciamiento Criminal*. Edición Oficial. Imprenta del Ministerio de Gracia y Justicia. Madrid. 1872.

MONTOYA MELGAR, A. *Cuestiones actuales de la jurisdicción en España.* Editorial Real Academia de Jurisprudencia y Legislación. Madrid. 2010. Págs. 871-882.

MORÁN MARTIN R, *Materiales para un curso de Historia del Derecho español. Tomo II*. Universidad Nacional de educación a Distancia. Madrid. 2000.

MORÁN MARTÍN, R. *Historia del derecho privado, penal y procesal.* Editorial Universitas. Madrid. 2002.

MORENO CATENA, V. *Actos de investigación que afectan a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones. (Derecho Procesal Penal).* Editorial Tirant Lo Blanch. Valencia. 2017. Págs. 271-275.

MORETÓN TOQUERO, M. A. *Delitos contra el honor: la calumnia.* Editorial Bosch. Madrid. 2001.

MORETÓN TOQUERO, M. A. *Delitos contra el honor: la injuria.* Editorial Bosch. Madrid. 2001.

MORETÓN TOQUERO, M. A. *Delitos contra la propiedad intelectual.* Editorial Bosch. Barcelona. 2002.

MORILLAS CUEVA, L, SUÁREZ LÓPEZ, J. M. *Derecho y consumo aspectos penales, civiles y administrativos*. Editorial Dykinson. Madrid. 2013. Págs. 187-212.

MORILLAS CUEVA, L. *Sistema de derecho penal: parte especial. 2ª edición, revisada y puesta al día conforme a las leyes Orgánicas 1/2015 y 2/2015.* Editorial Dykinson. Madrid. 2015. Págs. 1357-1374.

MORODO LEONCIO R, y DE VEGA GARCÍA P. *Estudios de teoría del Estado y derecho constitucional en honor de Pablo Lucas Verdú.* Ediciones de la Facultad de Derecho de la Universidad Complutense. Madrid. 2001. Págs. 1929-1948.

MUÑOZ CONDE F, *Derecho Penal. Parte General.* Editorial Tirant Lo Blanch. Valencia. 2004.

MUÑOZ CONDE F. J, Y OTROS. *Un derecho penal comprometido: libro homenaje al prof. Dr. Gerardo Landrove Díaz.* Editorial Tirant lo Blanch. Valencia. 2011. Págs. 819-827.

MUÑOZ CONDE, F. *Derecho Penal. Parte Especial.* Editorial Tirant Lo Blanch. Valencia. 2017.

MUÑOZ CONDE, F. J. *Problemas actuales del derecho penal y de la criminología. Estudios penales en memoria de la Profesora Dra. María del Mar Díaz Pita*. Tirant lo Blanch. Valencia. 2008. Págs. 881-904.

MUÑOZ CONDE. F. J. Y OTROS. *Un derecho penal comprometido libro homenaje al prof. Dr. Gerardo Landrove Díaz.* Tirant lo Blanch. Valencia. 2011. Págs. 363-383.

MUÑOZ CUESTA. J. *Cuestiones prácticas sobre la reforma penal de 2015* Editorial Thomson-Aranzadi. Pamplona. 2015.

MUÑOZ MACHADO, S. *Libertad de prensa y procesos por difamación.* Editorial Ariel. Barcelona. 1988.

MUR, A y otros. *Virus informáticos.* Editorial América Ibérica, D.L. Madrid. 1994.

MUR, A. *Protección contra virus informáticos*. Anaya Multimedia-Anaya Interactiva. Madrid. 1994.

MURILLO DE LA CUEVA, P. L. *Notas sobre el derecho fundamental al secreto de las comunicaciones*. *(Constitución, estado de las autonomías y justicia constitucional: libro homenaje al profesor Gurmesindo Trujillo).* Editorial Tirant lo Blanch. Valencia. 2005. Págs. 661-686.

NEVADO HOLGADO, A. B. *Ley de Enjuiciamiento Criminal, con jurisprudencia sistematizada*. Editorial Tirant lo Blanch. Valencia. 2017. Págs. 902-909.

NIEVA FENOLL, J. y BUJOSA VADELL, L. M. *Nociones preliminares de derecho procesal penal*. Editorial Atelier. Barcelona. 2016. Págs. 95-100.

NOYA FERREIRO, M. L. *La intervención de comunicaciones orales directas en el proceso penal*. Editorial Tirant lo Blanch. Valencia. 2000.

OBACH MARTÍNEZ, J. *Los reconocimientos de identidad, los seguimientos y la intervención de comunicaciones. (Nociones preliminares de derecho procesal penal para criminólogos).* Editorial Atelier. Madrid. 2017. Págs. 75-82.

OLÁSOLO ALONSO, H, CARNERO ROJO, E. *Extensión y límites de la jurisdicción personal, territorial y temporal de la Corte Penal Internacional. (El principio de justicia universal, fundamentos y límites)*. Editorial Tirant lo Blanch. Valencia. 2012. Págs. 105-138.

OLIVERIO FERRARIS, A, GRAZIOSI B. *¿Qué es la pedofilia?* Editores Paidós Ibérica. Barcelona. 2004

OLMO FERNÁNDEZ-DELGADO, L. *El descubrimiento y revelación de secretos documentales y de las telecomunicaciones estudio del artículo 197.1º del Código Penal.* Madrid. Editorial Dykinson. 2009.

ONTIVEROS ALONSO. M. *La responsabilidad penal de las personas jurídicas fortalezas, debilidades y perspectivas de cara al futuro.* Editorial Tirant lo Blanch. Valencia. 2014.

OREJUELA ARENAS, M. D. *Propiedad intelectual, Web de enlaces y la responsabilidad derivada por actos de reproducción, comunicación pública y puesta a disposición. Reflexiones sobre derecho privado patrimonial. Vol. 5.* Págs. 261-283. 2015.

ORTEGA MALDONADO, A. *Las redes sociales como herramienta de control ético de Internet. Análisis de la actividad en Facebook del Grupo de Delitos Telemáticos de la Guardia Civil relacionada con la persecución de la publicidad ilícita y/o engañosa. (La ética de la comunicación a comienzos del siglo XXI: libro de actas del I Congreso Internacional de Ética de la Comunicación, Facultad de Comunicación 29, 30 y 31 de marzo de 2011)*. Editorial Eduforma. Editorial Mad S.L. Sevilla. 2011. Págs. 1228-1238.

ORTIZ DE URBINA GIMENO, I. *Memento práctico Francis Lefebvre. Penal económico y de la empresa.* Ediciones Francis Lefebvre. Madrid. 2011. Pág. 6600-6900.

ORTIZ PRADILLO, J. C. *Cooperación penal europea e internacional en la obtención de prueba electrónica. (Presente y futuro de la e-Justicia en España y la Unión Europea).* Thomson Reuters Aranzadi. Navarra. 2010. Págs. 559-574.

ORTIZ PRADILLO, J. C. *Desafíos legales de las diligencias de investigación tecnológica. (El proceso penal: cuestiones fundamentales).* Editorial Tirant lo Blanch. Valencia. 2016. Págs. 303-315.

ORTIZ PRADILLO, J. C. *El Ministerio Fiscal y la Policía Judicial. (Nociones preliminares de derecho procesal penal).* Editorial Atelier. Madrid. 2016. Págs. 41-47.

ORTIZ URCULO, J. C. *Derecho al secreto de las comunicaciones.* Estudios jurídicos. Núm. 2006.

ORTS BERENGUER E. y ROIG TORRES M. *Delitos informáticos y delitos comunes cometidos a través de la informática.* Editorial Tirant lo Blanch. Valencia. 2001.

ORTS BERENGUER, E, BORJA JIMÉNEZ, E, CARBONELL MATEU, J. C, GONZÁLEZ CUSSAC, J. L, VIVES ANTÓN, T. S, MARTÍNEZ BUJÁN PÉREZ, C, CUERDA ARNAU, M. L, *Derecho Penal Parte Especial*. Editorial Tirant lo Blanch. Valencia. 2016.

ORTS BERENGUER, E. y GONZÁLEZ CUSSAC, J. L. *Límites Espaciales y Principio de Territorialidad. (Compendio de Derecho Penal Parte General)*. Editorial Tirant lo Blanch. 2017. Valencia. Págs. 91-100.

ORTUÑO NAVALÓN, M. C. *Aspectos procesales de la prueba electrónica. Procesos penales. Garantías de conservación y custodia. (La prueba electrónica ante los tribunales)*. Editorial Tirant Lo Blanch. Valencia. 2014. Págs. 101-103.

OSORIO ITURMENDI, L, MARTÍNEZ, S. *La prueba electrónica, avances y retos. (La prueba en el procedimiento arbitral).* Editorial Aranzadi. Navarra. 2017. Págs. 147-184.

OUBIÑA BARBOLLA, S. *Datos personales y nuevas diligencias de investigación tecnológica, oportunidades, retos y límites. (Cesión de datos personales y evidencias entre procesos penales y*

procedimientos administrativos sancionadores o tributarios). Editorial Thomson-Reuters-Aranzadi. Pamplona. 2017. Págs. 221-277.

PABLO RIVES SEVA, A. *La intervención de las comunicaciones en la jurisprudencia penal.* Thomson Reuters Aranzadi. Navarra. 2000.

PACHECO, J. F. *El Código Penal concordado y comentado. Tomo III.* Imprenta de D. Santiago Saunaque. Madrid. 1848. Págs. 347-378.

PADULLÉS JOAN BALCELLS, CERRILLO I MARTÍNEZ A, PEGUERA POCH M, PEÑA-LÓPEZ, I, PIFARRÉ DE MONER, M. J, VILASAU SOLANA, M. (*Internet, derecho y política una década de transformaciones: Actas del X Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 3-4 de julio de 2014.* Editorial Huygens. Barcelona. 2014. Págs. 467-479.

PALOMINO MARTÍN, J. M. *Derecho penal y nuevas tecnologías: hacia un sistema informático para la aplicación del derecho penal*. Editorial Tirant Lo Blanch. Valencia. 2013. Págs. 33-41.

PALOMO HERRERO, Y. *La diligencia de entrada y registro en domicilio. (Homenaje a don Eduardo Font Serra. Tomo II)*. Centro de Estudios Jurídicos de la Administración de Justicia, Ministerio de Justicia. Madrid. 2004. Págs. 1849-1880.

PARDO GARCÍA, J. B. *La Policía Judicial en Euskadi.* (*Primeras jornadas de reflexión sobre la administración de justicia en la Comunidad Autónoma de Euskadi)*. Editorial Gobierno Vasco, Servicio Central de Publicaciones. 1982. Págs. 191-238.

PEDRAZ PENALVA E, *Protección de Datos y Proceso Penal*. Editorial La Ley. Madrid. 2010.

PERALES SANZ, J. L. *La seguridad jurídica en las transacciones electrónicas seminario organizado por el Consejo General del Notariado en el UIMP*. Editorial Civitas. Madrid. 2002.

PÉREZ ÁLVAREZ F. Y MARIOLA DÍAZ CORTÉS L. *Moderno discurso penal y nuevas tecnologías: memorias del III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013.* 2014. Págs. 107-124.

PÉREZ ÁLVAREZ, F. *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales memorias II Congreso Internacional de Jóvenes investigadores en Ciencias Penales 27, 28 y 29 de junio de 2011.* Ediciones Universidad de Salamanca. Salamanca. 2012.

PÉREZ ÁLVAREZ, F. *Universitas vitae homenaje a Ruperto Núñez Barbero*. Ediciones Universidad de Salamanca. Salamanca. 2007. Págs. 649-670.

PÉREZ ÁLVAREZ, F. y otros. *Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas memorias del Proyecto I.F.O. Illegal Flow Observation*

JUST/2011/ISEC/DRUGS/AG/3671. Editorial Thomson Reuters-Aranzadi. Cizur Menor (Navarra). 2015. Págs. 91-138.

PÉREZ CEBADERA, M. A. *La organización y competencia de la Corte Penal Internacional. (La Corte Penal Internacional: un estudio interdisciplinar)*. Editorial Tirant lo Blanch. Valencia. 2002. Págs. 139-161.

PÉREZ CEPEDA, A. I. *El principio de justicia universal, fundamentos y límites*. Editorial Tirant lo Blanch. Valencia. 2012.

PÉREZ CEPEDA, A. I. y BENITO SÁNCHEZ, C. D. *El principio de justicia universal, una propuesta de "lege ferenda"*. Editorial Ratio Legis. Valladolid. 2013.

PÉREZ FERRER, F. *Repercusiones de la reforma de la LO 1/2004, de 28 de diciembre, en los delitos de lesiones, amenazas y coacciones. La ley integral un estudio multidisciplinar.* Editorial Dykinson. Madrid. 2009. Págs. 375-394.

PÉREZ GIL J, DE ROMÁN PÉREZ, R. *Estudios jurídicos sobre la empresa y los negocios una perspectiva multidisciplina: libro conmemorativo del XXV aniversario de la Facultad de Derecho de Burgos.* Editorial de Universidad de Burgos. 2011. Págs. 355-382.

PÉREZ GIL, J. *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar probar el delito.* Editorial La Ley. Madrid. 2012.

PÉREZ GIL, J. *Hacia una futura superación de la equivalencia funcional entre prueba por archivos electrónicos y prueba documental en el proceso civil. (Problemas actuales del proceso iberoamericano).* Editorial Centro de Ediciones de la Diputación de Málaga (CEDMA) Diputación de Málaga. 2006. Págs. 527-542.

PEREZ GIL, J. *Los datos sobre localización geográfica en la investigación penal. (Protección de datos y proceso penal)*. Editorial La Ley. 2013. Págs. 491-571.

PEREZ GIL, J. *Nuevas técnicas de obtención de información: intervención de comunicaciones, datos de localización, obtención de pruebas electrónicas, videovigilancia. El nuevo papel de la telefonía móvil en el proceso penal: ubicación y perfiles de desplazamiento. (El proceso penal en la sociedad de la información: las nuevas tecnologías para investigar y probar el delito)*. Editorial La Ley. Madrid. 2013. Págs. 255-328.

PÉREZ GONZÁLEZ M. *Hacia un nuevo orden internacional y europeo: estudios en homenaje al profesor don Manuel Díez de Velasco.* Editorial Tecnos. Madrid. 1993. Págs. 807-826.

PÉREZ MARÍN M.A, *La lucha contra la criminalidad en la Unión Europea. El camino hacia una jurisdicción penal común*. Editorial Atelier. Barcelona. 2013.

PÉREZ ROYO, F. J. *Cuestión de inconstitucionalidad. (Temas básicos de Derecho Constitucional. Tomo II. Organización general y territorial del Estado)*. Editorial Civitas. Madrid. 2011. Págs. 319-322.

PÉREZ ROYO, F. J. y CARRASCO DURÁN, M. *Curso de derecho constitucional.* Marcial Pons. Madrid. 2016.

PEREZ-CRUZ MARTÍN A.J. Y OTROS, *Derecho Procesal Penal*. Editorial Civitas. Pamplona. 2014.

PÉREZ-PEDRERO, E. B. *El derecho al secreto de las comunicaciones.* Anuario. Parlamento y Constitución. Núm. 2. 1998. Págs. 169-194.

PERIS RIERA J. M. *El pensamiento criminológico en la obra de Mariano Ruiz-Funes García, el cientifismo prudente de un penalista demócrata.* Editorial Fundación Séneca. Murcia. 2006.

PICÓ I JUNOY, J, GINÉS CASTELLET, N. y ABEL LLUCH, X. *La prueba electrónica*. J.M. Bosch Editor. Barcelona. 2011.

PLAZA PENADÉS J. *Cuestiones actuales de derecho y tecnologías de la información y la comunicación (TICs).* Editorial Thomson Aranzadi. Pamplona. 2006. Págs. 188-204.

POLAINO NAVARRETE, M. *La reforma penal española de 2003: una valoración crítica.* Editorial Tecnos. Madrid. 2004.

POLAINO NAVARRETE, M. *Lecciones de derecho penal. Parte especial. T.I: adaptadas a las leyes orgánicas 2/2010 y 5/2010 de Reforma del código penal.* Editorial Tecnos. Madrid. 2010.

POLAINO NAVARRETE, M. *Lecciones de derecho penal. Parte especial.* Editorial Tecnos. Madrid. 2010. Págs. 529-548.

PORTILLA CONTRERAS, G. (DIR.), PÉREZ CEPEDA, A. I. *Terrorismo y contraterrorismo en el siglo XXIun análisis penal y político criminal.* Editorial Ratio Legis. Salamanca. 2016.

PRADA FERNÁNDEZ DE SANMAMED, J. L. *Historia constitucional española de los derechos fundamentales y su presencia en la Constitución española de 1978* (*La enseñanza de las ideas constitucionales en España e Iberoamérica: actas del congreso internacional sobre la enseñanza de las ideas constitucionales celebrado en la Universitat de Valencia de 16 al 21 de octubre de 2001).* Editorial Ene. 2001. Págs. 255-290.

PRAT, E. *Mujer y justicia: estudio de la jurisprudencia desde la perspectiva de género. Delitos de amenazas.* Editorial Cedecs. Barcelona. Págs. 125-138.

PRIETO RODRÍGUEZ J. I. *Aproximación al Código Penal de 1995*. Editorial Ilustre Colegio de Abogados de Tarragona. 1999.

PUJOLS PÉREZ, S. *El derecho penal frente a las conductas de stalking reconducción al delito de quebrantamiento de condena antes y después de la LO 1/2015. Derecho, filosofía y sociedad: una perspectiva multidisciplinar*. Editorial Andavira Editora. Santiago de Compostela (A Coruña). 2016. Págs. 185-201.

QUESADA ALCALÁ, C. *La Corte Penal Internacional y la soberanía estatal*. Editorial Tirant lo Blanch. Valencia. 2005.

QUINTANAR DÍEZ, M, ORTIZ NAVARRO, J. F. *La ley penal en el espacio. (Elementos de Derecho. Penal Parte General)*. Editorial Tirant lo Blanch. 2014. Valencia. Págs. 31-38.

QUINTANAR DÍEZ, M. F, COBO DEL ROSAL, M. *Delitos contra el orden público (V). Delitos de terrorismo (Derecho penal español: parte especial).* Editorial Dykinson. Madrid. 2005. Págs. 1141-1156.

QUINTANO RIPOLLES, A. *Curso de Derecho Penal.* Editorial Revista de Derecho Privado. Tomo I. Madrid. 1963.

QUINTERO OLIVARES G, *Comentario a la reforma del Código Penal de 2015*. Editorial Aranzadi. Pamplona. 2015.

QUINTERO OLIVARES, G. *La reforma penal de 2010: análisis y comentarios.* Editorial Thomson-Aranzadi. Pamplona. 2010.

RAFARACI, T. *"Ne bis in idem" y conflictos de jurisdicción en materia penal en el espacio de libertad, seguridad y justicia de la Unión Europea. (Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal)*. Editorial Lex Nova. Madrid. 2010. Págs. 122-150.

RAMÍREZ JIMÉNEZ, M. *Constitución y democracia ayer y hoy: libro homenaje a Antonio Torres del Moral. Editorial Universitas*. 2012. Págs. 1651-1667.

RANSTORP, M. *Al Qaeda en el ciberespacio desafíos del terrorismo en la era de la información. El nuevo terrorismo islamista: del 11-S al 11-M.* 2004. Editorial Temas de hoy. Madrid. Págs. 201-222.

Real Decreto-Ley de 8 de septiembre de 1928 publicando el Código penal. Editorial Reus. Madrid. 1928.

REIG REIG J. V. *Estudio sobre la Ley orgánica 15/2003, de 25 de noviembre. Su incidencia en el libro I del Código penal.* Editorial Dijusa. Madrid. 2004.

RIBAS MAURA, A. *La cuestión de inconstitucionalidad.* Editorial Cívitas. Madrid. 1991.

RIBERA BLANES, B. *El derecho de reproducción en la propiedad intelectual.* Editorial Dykinson. Madrid. 2002.

RICO PÉREZ, F. *Centenario del Código Civil.* Editorial Universidad Popular Enrique Tierno Galván. Vol. 2. Madrid. 1986. Págs. 477-492.

RIDAURA MARTÍNEZ, M. J. *Seguridad Privada y Derechos Fundamentales*. Editorial Tirant Lo Blanch. Valencia. 2015. Págs. 49-51.

RIFÁ SOLER, J. M. *El testigo protegido y el agente infiltrado. (Estudios sobre prueba penal. Volumen II actos de investigación y medios de prueba: inspección ocular, declaraciones de inculpados y testigos, intervenciones corporales y prueba pericial)*. Editorial La Ley. Madrid. Págs. 473-508.

RIVAS ALEJANDRO, J. *Aspectos Jurídicos del Comercio Electrónico en Internet.* Editorial Aranzadi. Cizur Menor (Navarra). 2003.

RIVERO SÁNCHEZ-COVISA, F. J. *Secreto de las comunicaciones en el ámbito de las nuevas tecnologías. (Revisión del concepto constitucional del secreto de las comunicaciones).* Editorial Dykinson. Madrid. 2017. Págs. 63-114.

RIVES SEVA A.P, *La Prueba en el Proceso Penal. Doctrina de la Sala Segunda del Tribunal Supremo.* Editorial Aranzadi. Navarra. 1996.

RIVES SEVA A.P. (Y OTROS), *La Prueba en el Proceso Penal. Doctrina de la Sala Segunda del Tribunal Supremo.* Editorial Aranzadi. Navarra. 2011.

RIVES SEVA, A. P. *La intervención de las comunicaciones en la jurisprudencia penal.* Editorial Aranzadi. Cizur Menor (Navarra). 2000.

RIVES SEVA, A.P. *La diligencia de entrada y registro domiciliario.* Editorial Bosch, S.A. Barcelona. 2004.

ROBLEDO VILLAR, A. *Delitos contra el patrimonio y el orden socioeconómico. Comentarios a los artículos 234 a 289 del nuevo Código Penal*. Editorial Bosch. Barcelona. 1997.

ROBLES GARZÓN, J. A. y ÁLVAREZ ALARCÓN, A. *Lecciones breves de derecho procesal penal.* Editorial Comares. Granada. 2017.

RODRÍGUEZ ÁLVAREZ, A. *Intervención de las comunicaciones telefónicas y telemáticas y smartphones. Un primer estudio a propósito de la ley orgánica 13/2015, de 5 de octubre, de modificación de la ley de enjuiciamiento criminal (Justicia penal y nuevas formas de delincuencia).* Editorial Tirant lo Blanch. Valencia. 2017. Págs. 149-180.

RODRIGUEZ DEVESA J.M, *Derecho Penal español. Parte especial.* Artes gráficas Carasa. Madrid. 1980.

RODRIGUEZ DEVESA J.M, *Derecho Penal español. Parte general.* Artes gráficas Carasa. Madrid. 1979.

RODRÍGUEZ FERNÁNDEZ, R. *El "agente encubierto" y la "entrega vigilada". (Criminalidad organizada: reunión de la sección nacional española preparatoria del XVI Congreso de la AIDP en Budapest)*. Editorial Universidad de Castilla-La Mancha. 1999. Págs. 91-124.

RODRÍGUEZ FERNÁNDEZ, R. *La diligencia de entrada y registro como excepción al derecho fundamental de inviolabilidad domiciliaria. Presupuestos y requisitos (Homenaje al Dr. Marino Barbero Santos: "in memorian" Vol. 2)*. Ediciones de la Universidad de Castilla-La Mancha. 2001. Págs. 833-852.

RODRÍGUEZ LAINZ J. L. *Intervención judicial en los datos de tráfico de las comunicaciones la injerencia judicial en los listados de llamadas y otros elementos externos de la telecomunicaciones electrónicas.* Editorial Bosch. Barcelona. 2003.

RODRÍGUEZ LAINZ J. L. *La intervención de las comunicaciones telefónicas su evolución en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo.* Editorial Bosch. Barcelona. 2002.

RODRÍGUEZ LAINZ, J. L. *Sobre la influencia de la jurisprudencia del Tribunal Europeo de Derechos Humanos en la actual regulación legal del llamado "derecho al entorno virtual" (Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios)*. Editorial Thomson Reuters Aranzadi. Navarra. 2017. Págs. 279-312.

RODRÍGUEZ MESA, M. J. *Conducta típica. (Los delitos de daños)*. Editorial Tirant lo Blanch. Valencia. 2017. Págs. 73 – 77.

RODRÍGUEZ RAMOS L, *Código Penal (Comentado y con Jurisprudencia).* La Ley. Madrid. 2009.

RODRÍGUEZ RUIZ, B. *El secreto de las comunicaciones tecnología e intimidad.* Editorial McGraw-Hill Interamericana de España. Madrid. 1998

RODRIGUEZ-MEDEL NIETO C. Y OTROS, *Manual Práctico de Reconocimiento Mutuo Penal en la Unión Europea.* Editorial Tirant Lo Blanch. Valencia. 2015.

ROGEL VIDE C. *Estudios sobre propiedad intelectual*. Editorial J. M. Bosch Editor. Barcelona. 1995.

ROGEL VIDE, C. *Estudios completos de propiedad intelectual.* Editorial Reus. Madrid. 2003.

ROGEL VIDE, C. *Nuevos estudios sobre propiedad intelectual.* Editorial J. M. Bosch Editor. Barcelona. 1998.

ROMEO CASABONA, C. M. *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Editorial Comares. Granada. 2006. Págs. 191-205.

ROMEO CASABONA, C. M. *Genética y derecho penal: previsiones en el Código Penal Español de 1995*. Editorial Comares. Granada. 2001. Págs. 201-238.

ROVIRA DEL CANTO, E, *Delincuencia informática y fraudes informáticos.* Editorial Comares. Granada. 2002.

ROVIRA FLÓREZ DE QUIÑONES, M. C. *Los derechos humanos en la Constitución de 1869. (Los derechos en el constitucionalismo histórico español).* Servicio de Publicaciones de la Universidad de Santiago de Compostela. La Coruña. 2002. Págs. 111-134.

ROXIN, C, *Derecho Penal Parte General. Tomo I. Fundamentos. La estructura de la Teoría del Delito.* Thomson Civitas. Madrid. 2006.

ROXIN, C, *Derecho Penal Parte General. Tomo II. Especiales forma de aparición del delito.* Thomson Civitas. Pamplona. 2014.

RUBIO LLORENTE, F. *Las reformas administrativas en la II República.* Editorial Instituto Nacional de Administración Pública (INAP). Madrid. 2009. Págs. 27-38.

RUEDA MARTÍN, M. A. *Protección penal de la intimidad personal e informática. (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 de Código Penal)* Editorial Atelier. Barcelona. 2004.

RUIZ COLOMÉ, M. A, CUERDA RIEZU, A. R. *Observaciones sobre el estatuto del tribunal penal internacional. (El nuevo Código Penal: presupuestos y fundamentos: libro homenaje al profesor Doctor Don Angel Torío López)*. Editorial Comares. Granada. 1999. Págs. 212-134.

RUIZ LANDÁBURU, M. J. *Provocación y apología delitos de terrorismo.* Editorial Constitución y Leyes, COLEX. Madrid. 2002.

RUIZ MARCO F. *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática.* Editorial Constitución y Leyes, COLEX. Madrid. 2001.

RUIZ RODRÍGUEZ, L. R. *Sistema penal de protección del mercado y de los consumidores: actas del II Seminario Internacional de Derecho Penal Económico, Jerez, diciembre 2000.* Tirant lo Blanch. Valencia. 2002. Págs. 71-90.

RUIZ RUIZ, R. *Discrecionalidad judicial, justicia constitucional y objeción contramayoritaria*. Editorial Aranzadi. Pamplona. 2016.

RUIZ Y RODRIGUEZ, H. M. *Compilación general de las disposiciones vigentes sobre el Enjuiciamiento Criminal, concordada, anotada y seguida de observaciones*. Imprenta de la revista de legislación. Madrid. 1880.

SAIZ GARITAONANDIA, A. *Algunas notas sobre telefonía móvil y derecho al secreto de las comunicaciones en supuestos de detención. (El derecho procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños)*. Editorial Tirant lo Blanch. Valencia. 2012. Págs. 1173-1186.

SAIZ GARITAONANDIA, A. *Guía crítica sobre la nueva regulación de la intervención de las comunicaciones telefónicas y telemáticas.* (Tiempo de reformas: perspectiva académica y realidad judicial). Editorial Universidad País Vasco. 2017. Págs. 103-114.

SALA DONADO, C. *La policía judicial.* McGraw-Hill Interamericana de España. Madrid. 1999.

SALOM CLOTET, J. *Inseguridad en la red y delincuencia informática. Actuación de la Guardia Civil. (La actualidad de la intervención social, 18, 19, 20 de junio de 2008*). Editorial Gobierno de La Rioja, Consejería de Salud. 2008. Págs. 145-156.

SAN JOSÉ VIECO, J. I, BLANCO RODRÍGUEZ DE GUZMÁN, J, DE DIOS DE DIOS, J. J. *La identificación por radiofrecuencia (RFID) y sus aplicaciones (Investigación y transferencia en la Escuela Politécnica de Cuenca).* Ediciones de la Universidad de Castilla-La Mancha. 2015. Pág. 24.

SÁNCHEZ BLANCO, A. Y OTROS. *La nueva regulación de la Oficina Judicial.* Editorial Aranzadi. Cizur Menor (Navarra) 2006. Págs. 43-62 y 119-158.

SÁNCHEZ GONZÁLEZ, D. *La codificación penal en España los códigos de 1848 y 1850.* Editorial Centro de Estudios Políticos y Constitucionales. Madrid. 2004.

SÁNCHEZ GONZÁLEZ, F. *Registros remotos sobre equipos informáticos. (Actualidad Penal 2017)*. Editorial Tirant lo Blanch. 2017. Págs. 354-355.

SÁNCHEZ TOMÁS, J. M. *La violencia en el derecho penal su análisis jurisprudencial y dogmático en el CP 1995.* Editorial Bosch. Madrid. 1999.

SÁNCHEZ YLLERA, I. *Valenzuela Contreras C. España (STEDH de 30 de julio de 1998)la deficiente calidad de las normas que habilitan la intervención de las comunicaciones telefónicas (Conflicto y diálogo con Europa: las condenas a España del Tribunal Europeo de Derechos Humanos).* Editorial Civitas. Madrid. 2013. Págs. 443-470.

SANCHEZ-ARCILLA BERNAL, J. *Manual de Historia del Derecho*. Editorial Dykinson. Madrid. Págs. 525-539.

SANCHEZ-TEJERINA, I. *Código penal anotado*. Instituto Editorial Reus. Madrid. 1948.

SANCHÍS CRESPO, C. *La prueba en soporte electrónico. Las tecnologías de la información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Editorial Thomson-Aranzadi. Pamplona. 2012. (Pág. 713).

SANTOS MARTÍNEZ, A.M. *Medidas de investigación tecnológica en la instrucción penal*. Editorial Bosch Wolters Kluwer. Barcelona. 2017.

SANZ HERMIDA, Á. M. *Las cuestiones prejudiciales. El Tribunal de Justicia de la Unión Europea. Instituciones y Derecho de la Unión Europea Instituciones de la Unión Europea. Volumen I.* Editorial Tirant lo Blanch. Valencia. 2015. Pags. 520-524.

SEGURA ORTEGA, M. *Los derechos en el constitucionalismo histórico español.* Editorial Servicio de Publicaciones de la Universidad de Santiago de Compostela. 2002. Págs. 135-176.

SENDÍN GARCÍA, M. A, GÓMEZ DÍAZ R. *Régimen jurídico de los documentos aspectos administrativos, civiles, penales y procesales*. Editorial Comares. Granada. 2009. Págs. 357-410.

SERRANO GÓMEZ, E. y DURÁN RIVACOBA, R. *La propiedad intelectual y las nuevas tecnologías.* Editorial Civitas. Madrid. 2000.

SERRANO MASIP, M. *La conservación sistemática y preventiva de datos de tráfico y localización generados por las comunicaciones electrónicas reacciones contrarias y posible cambio de rumbo en la Unión Europea.* (Temas actuales en la persecución de los hechos delictivos). Editorial La Ley. Madrid. 2012. Págs. 437-500.

SERRANO PÉREZ, M. M. y REBOLLO DELGADO, L. *El derecho fundamental a la intimidad*. Editorial Dykinson, S.L. Madrid. 2005.

SERRANO-PIEDECASAS FERNÁNDEZ, J. R, CRESPO EDUARDO, D. *Cuestiones actuales de derecho penal empresarial. La imagen de portada del libro no está disponible.* Editorial COLEX. Madrid. 2010. Págs. 301-314.

SERRANO-PIEDECASAS FERNÁNDEZ, J. R, DEMETRIO CRESPO, E. *Terrorismo y estado de derecho*. Editorial Iustel. Madrid. 2010.

SIDRO Y SURGA, J. *Código penal reformado planteado provisionalmente por Ley de 3 de junio de 1870*. Librería de L. P. Villaverde. Madrid. 1872.

SILVA SÁNCHEZ J.M, PASTOR MUÑOZ N. *El nuevo Código Penal comentarios a la reforma.* Editorial La Ley. Madrid. 2012. Págs. 367-376.

SUÁREZ-MIRA RODRÍGUEZ, C, JUDEL PRIETO, A. y PIÑOL RODRÍGUEZ J. R. *Delincuencia informática tiempos de cautela y amparo.* Editorial Thomson Reuters. Madrid. 2012. Págs. 221-232.

TAPIA BALLESTEROS, P. *El nuevo delito de acoso o "stalking"*. Editorial Wolters Kluwer. Madrid. 2016.

TATO PLAZA. A. Y FERNÁNDEZ ALBOR BALTAR. A. *Comercio electrónico en Internet.* Editorial Marcial Pons. Madrid. 2001.

TERRADILLOS BASOCO J. M. *Política criminal de "La Pepa" el Derecho penal de la cotidianeidad.* Editorial Universidad de Cádiz, Servicio de Publicaciones. 2012. Págs. 103-130. (La libertad de imprenta, verdadero vehículo de las luces. Análisis de la libertad de imprenta en la Constitución de 1812 y el Código Penal de 1822).

TERRADILLOS BASOCO, J. M. *Terrorismo y derecho. Comentario a las leyes orgánicas 3 y 4/1988, de reforma del código penal y de la ley de enjuiciamiento criminal.* Editorial Tecnos. Madrid. 1988.

TORRALBA MENDIOLA, E. C, ROCA I JUNYENT, M. *Derecho a la intimidad: el secreto de las comunicaciones e Internet (Régimen jurídico de internet).* Editorial Wolters Kluwer. Madrid. 2001. Págs. 181-200.

TORRES AGUILAR M. *Génesis parlamentaria del Código penal de 1822.* Ediciones SICANIA University Press. Università degli Studi di Messina. Italia. 2008.

TORRES BOURSAULT, L. *Protección del derecho a la correspondencia privada de los internos en la Jurisprudencia del Tribunal Europeo de los Derechos del Hombre. (Ministerio fiscal y sistema penitenciario: III Jornadas de Fiscales de Vigilancia Penitenciaria)*. Centro de Publicaciones del Ministerio de Justicia. 1992. Págs. 373-379.

TORRES DEL MORAL, A. *Constitucionalismo histórico español*. Editorial Universitas. Madrid. 2015.

TORRES FERNÁNDEZ, M. E. *Los delitos de desórdenes públicos en el Código penal español.* Editorial Marcial Pons. Madrid. 2001.

URBINA GIMENO, I. *Reforma penal: Ley orgánica 5/2010*. Editorial Ediciones Francis Lefebvre. Madrid. 2010.

URIZARBARRENA, M. *Virus en Internet*. Editorial Anaya Multimedia-Anaya Interactiva. Madrid.1999.

VALCUENDE DEL RÍO, J. M, VASQUEZ, A. P. y MARCO MACARRO, M. J. *Sexualidades. Represión, resistencia y cotidianidades.* Editorial Aconcagua Libros. 2016.

VALENCIA SÁIZ A. *Investigaciones en ciencias jurídicas: desafíos actuales del derecho*. Málaga. 2014. *Págs. 455- 461.*

VALLE MUÑIZ, J. M. *El Delito de estafa delimitación jurídico-penal con el fraude civil.* Editorial Bosch. Madrid. 1987.

VALLÉS CAUSADA, L. *La policía judicial, un referente en la defensa de los derechos fundamentales en la era de las TIC. (Nuevas tendencias en la interpretación de los derechos fundamentales)*. Universitas Editorial. Madrid. 2015. Págs. 697-716.

VARELA SUANZES-CARPEGNA, J. *La Constitución de 1876.* Editorial Iustel. Madrid. 2009.

VÁZQUEZ IRUZUBIETA, C. *De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución. (Comentario a la Ley de Enjuiciamiento Criminal, actualizada por las Leyes 13/2015, y 41/2015, de 5 de octubre)*. Editorial Vlex. Madrid. 2015. Pág. 455-480.

VÁZQUEZ RUANO, T. *La inserción de enlaces en una "web" cuestiones de propiedad industrial y competencia desleal.* Editorial Marcial Pons. Ediciones Jurídicas y Sociales. Madrid. 2013.

VEGA VEGA, J. A. *Protección de la propiedad intelectual.* Editorial Reus. Madrid. 2002.

VEGAS TORRES, J. *Las medidas de investigación tecnológica (Nuevas tecnologías y derechos fundamentales en el proceso)*. Editorial Thomson Reuters Aranzadi. Navarra. 2017. Págs. 21-47.

VELASCO NUÑEZ E, *Delitos tecnológicos: definición, investigación y prueba en el proceso penal. Actualizado a las reformas del Código Penal y la Ley de Enjuiciamiento Criminal de 2015.* Editorial SEPIN. Madrid. 2016.

VELASCO NUÑEZ, E. *Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. (Investigación Tecnológica y Derechos Fundamentales. Comentarios a las modificaciones introducidas por la Ley 13/2015)*. Editorial Aranzadi. Navarra. 2017. Págs. 225 – 245.

VELASCO NUÑEZ, E. *Delitos cometidos a través de Internet. Cuestiones Procesales.* Editorial La Ley. Madrid. 2010.

VELASCO SAN MARTÍN C, *La Jurisdicción y Competencia sobe delitos cometidos a través de sistemas de cómputo e internet.* Editorial Tirant Lo Blanch. Valencia. 2012. (Pág. 79-98).

VELASCO SAN MARTÍN, C. *La jurisprudencia y competencia sobre delitos cometidos a través de cómputo e internet*. Editorial Tirant Lo Blanch. Valencia. 2012.

VELÁZQUEZ BARÓN, A. *Las coacciones. Biblioteca Básica de Práctica Procesal nº 217.* Editorial Bosch. Madrid. 2004.

VELÁZQUEZ BARÓN, A. *Las coacciones.* Editorial Bosch. Madrid. 2002.

VERA SÁNCHEZ, J. S. *Organización y grupo criminal. Asociación ilícita (arts. 515-521; 570 bis, ter y quáter) (Manual de derecho penal. Parte Especial. Doctrina y jurisprudencia con casos solucionados. Tomo 1).* Editorial Tirant lo Blanch. Valencia. 2015. Págs. 784-794.

VERVAELE, J. A. E. *Derechos fundamentales en el espacio de libertad, seguridad y justiciael "ne bis idem" praetoriano del Tribunal de Justicia. (El proceso penal en la Unión Europea: Garantías esenciales)*. Editorial Lex Nova. Madrid. 2008. Págs. 80-105.

VICENTE GIMÉNEZ, T. *Sobre los nuevos paradigmas de la justicia penal, la justicia universal, la justicia restaurativa y la justicia transicional. (Crímenes internacionales y justicia penal. Principales desafíos).* Editorial Aranzadi. Navarra. 2016. Págs. 23-50.

VICENTE ROJO, J. *Los Peritos y la Prueba Pericial en el Procedimiento Civil.* Editorial Tirant Lo Blanch. Valencia. 2014.

VILALTA NICUESA, A. E, MÉNDEZ TOMÁS, R. M. *Acciones relacionadas con la propiedad intelectual*. Editorial Bosch. Madrid. 1999.

VILLACAMPA ESTIARTE, C. *El Delito de Online Child Grooming o Propuesta Sexual Telemática a Menores.* Editorial Tirant lo Blanch. Valencia. 2015.

VILLACAMPA ESTIARTE, C. *La delincuencia organizada un reto a la política-criminal actual.* Editorial Thomson Reuters Aranzadi. Navarra. 2013.

VILLACAMPA ESTIARTE, C. *Stalking y derecho penal relevancia jurídico-penal de una nueva forma de acoso.* Editorial Iustel. Madrid. 2009.

VILLACAMPA ESTIARTE, C. y AGUADO CORREA, T. *Delitos contra la libertad e indemnidad sexual de los menores adecuación del Derecho español a las demandas normativas supranacionales de protección.* Editorial Aranzadi. Cizur Menor (Navarra). 2015.

VILLANUEVA TURNES, A. *El recurso de inconstitucionalidad. (El Tribunal Constitucional español: una visión actualizada del supremo intérprete de la Constitución).* Editorial Tébar Flores. Madrid. 2018. Págs. 61-84.

VILLAR FUENTES, I (Coord. RODRÍGUEZ TIRADO, A. M.). *El uso de las nuevas tecnologías en las diligencias de investigación. Especial referencia a supuestos de terrorismo. (Cuestiones actuales de derecho procesal reformas procesales). Meditación y arbitraje.* Editorial Tirant lo Blanch. Valencia. 2017. Págs. 573-596.

VILLAR FUENTES, I, *Diligencias de investigación tecnológica, terrorismo y situaciones de excepción. (FODERTICS 5.0. Estudios sobre nuevas tecnologías y justicia).* Editorial Comares. Granada. 2016. Págs. 297-307.

Virus informáticos. Editorial McGraw-Hill Interamericana de España. Nueva York (E.E.U.U.) 2002.

VIVES ANTÓN T. S. *Libertad de prensa y responsabilidad criminal (la regulación de la autoría en los delitos cometidos por medio de la imprenta).* Editorial de la Universidad Complutense. Madrid. 1977.

VOGEL, J. *Principio de legalidad, territorialidad y competencia judicial (Eurodelitos: el derecho penal económico en la Unión Europea)*. Ediciones de la Universidad de Castilla-La Mancha. Toledo. 2005. Págs. 31-34.

WALKER, A. *Seguridad, spam, spyware y virus*. Editorial Anaya Multimedia. Madrid. 2006.

YÁÑEZ BARNUEVO, J. A. *Hacia un tribunal de la Humanidad, la Corte Penal Internacional. (Cursos euromediterráneos Bancaja de Derecho Internacional).* Editorial Tirant lo Blanch. Valencia. 2002. Págs. 805-830

ZAFRA ESPINOSA DE LOS MONTEROS, R. *El policía infiltrado*. Editorial Tirant Lo Blanch. 2010.

ZAFRA ESPINOSA DE LOS MONTEROS, R. *La lucha contra el crimen organizado en el borrador del Código Procesal Penal, el agente encubierto. (Reflexiones sobre el nuevo proceso penal: Jornadas sobre el borrador del nuevo Código Procesal Penal)*. Editorial Tirant lo Blanch. Valencia. 2015. Págs. 557-577.

ZAMORA BONILLA, J y RUS RUFINO, S *Una polémica y una generación: razón histórica de 1898: actas del Congreso "1898: Pensamiento Político, Jurídico y Filosófico. Balance de un Centenario": León, 10-13 de moviembre de 1998.* Editorial Universidad de León. 1999. Págs. 227-242.

ZAMORA, T. *Justicia Universal y Tribunal Penal Internacional. (Homenaje a D. Iñigo Cavero Lataillade).* Editorial Tirant lo Blanch. Valencia. 2005. Págs. 1199-1206.

ZARAGOZA AGUADO, J. A. *De los delitos de terrorismo (artículos 573 a 580). (Comentarios prácticos al Código penal. Vol. 6. 2015).* Editorial Thomson Reuters Aranzadi. Navarra. Págs.605-684.

ZARAGOZA TEJADA, J. I. y otros. *Investigación tecnológica y derechos fundamentales.* Editorial Aranzadi. Navarra. 2017.

ZOCO ZABALA, C. *Igualdad en la aplicación de las normas y motivación de sentencias (artículos 14 y 24.1 CE). Jurisprudencia del Tribunal Constitucional (1981-2002).* Editorial J. M. Bosch Editor. Barcelona. 2003.

ZOCO ZABALA, C. *Intervención de las comunicaciones e intervención de las conversaciones, una misma protección iusfundamental. (Del verbo al bit)*. Editorial Sociedad Latina de Comunicación Social. 2017. Págs. 344-363

ZOCO ZABALA, C. *La intervención judicial de las comunicaciones ¿privadas? regulación legal y nuevos escenarios tecnológicos.* Editorial Thomson Reuters Aranzadi. Navarra. 2014.

ZOCO ZABALA, C. *Medidas de investigación tecnológica en la reforma de la Ley de Enjuiciamiento Criminal. Secreto de las comunicaciones, intimidad, protección de datos personales, e inviolabilidad del domicilio (La pantalla insomne).* Editorial Sociedad Latina de Comunicación Social. 2016. Págs. 648-677.

ZUGALDÍA ESPINAR, J. M. Y BLANCA MARÍN DE ESPINOSA CEBALLOS, E. *Aspectos prácticos de la responsabilidad criminal de las personas jurídicas.* Editorial Aranzadi-Thomson Reuters. Cizur Menor (Navarra). 2013. Págs. 217-228.

ZUGALDÍA ESPINAR, J. M. y LÓPEZ BARJA DE QUIROGA, J. *Dogmática y ley penal: libro homenaje a Enrique Bacigalupo.* Editorial Marcial Pons. Madrid. 2004. Págs. 1433-1460.

ZÚÑIGA RODRÍGUEZ, L, MÉNDEZ RODRÍGUEZ, C, DIEGO DÍAZ-SANTOS, M. R. *Derecho penal, sociedad y nuevas tecnologías.* Editorial COLEX. 2001. Págs. 111-133.

ZÚÑIGA RODRÍGUEZ, L. *Problemas de interpretación de los tipos de organización criminal y grupo criminal estudio a la luz de la realidad criminológica y de la jurisprudencia (Instrumentos jurídicos y operativos en la lucha contra el tráfico internacional de drogas: memorias del Proyecto I.F.O. Illegal Flow Observation JUST/2011/ISEC/DRUGS/AG/3671).* Editorial Thomson Reuters Aranzadi. Navarra. 2015. Págs. 91-138.

Universidad
Rey Juan Carlos

Aspectos procesales

de los delitos informáticos y tecnológicos

Don Álvaro Gómez Rodríguez