Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Derecho

GRADO EN DERECHO

TRABAJO FIN DE GRADO

INVESTIGACIÓN PENAL Y NUEVAS TECNOLOGÍAS: LA INTERCEPTACIÓN DE COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

Criminal investigation and new technologies: interception of telephone and telematic communications

Alumno: Pablo Roca Heres

Convocatoria: Extraordinaria segundo semestre

RESUMEN

En la investigación penal es preciso con frecuencia llevar a cabo actuaciones que afectan a la privacidad del sujeto investigado, al ámbito más íntimo de su vida; es necesario acceder a espacios privados, registrar domicilios, escuchar conversaciones, revisar correo postal o telemático, tomar fotografías o grabar vídeos, establecer dispositivos de vigilancia o de seguimiento, acceder a dispositivos de almacenamiento. La evolución tecnológica no solo ha permitido nuevas formas de delincuencia, sino que también ha puesto a disposición de policías, fiscales y jueces nuevos medios de investigación. En el presente trabajo se analiza la interceptación de las comunicaciones telefónicas y telemáticas, una de estas diligencias de investigación que ha tenido que adaptar su regulación a la evolución tecnológica.

ABSTRACT

In criminal investigation, it is often necessary to conduct criminal proceedings that might affect privacy of individuals under investigation, their most intimate realms; at times it is necessary to access private spaces, to search and seizure, to listen to private conversations, to check postal or telematic mail, to take photos or record videos, to establish surveillance and tracking devices, or to access storage devices. Technological evolution has not only allowed emerging forms of crime, it has also made new investigation tools available to police, prosecutors and judges. This paper analyzes interception of telephone and telematic communications, one of these investigative proceedings that has been forced to adapt its regulation to technological evolution.

ABREVIATURAS Y ACRÓNIMOS

AJI..... Auto Juzgado de Instrucción
CE.....Constitución Española de 1978
CGPJ ..... Consejo General del Poder Judicial
CNI.....Centro Nacional de Inteligencia
CP..... Código Penal
FFCCSS..... Fuerzas y Cuerpos de Seguridad del Estado
FGE..... Fiscalía General del Estado
LCDCE.....Ley 25/2007, de 18 de octubre (conservación datos relativos a comunicaciones)
LECrim (*) ..... Ley de Enjuiciamiento Criminal
LOPJ.....Ley Orgánica del Poder Judicial
MF..... Ministerio Fiscal
PJ..... Policía Judicial
SAN..... Sentencia de la Audiencia Nacional
STJUE/SSTJUE ..... Sentencia/Sentencias del Tribunal de Justicia de la Unión Europea
STC/SSTC .....Sentencia/Sentencias del Tribunal Constitucional
STEDH/SSTEDH.....Sentencia/Sentencias del Tribunal Europeo de Derechos Humanos
STS/SSTS.....Sentencia/Sentencias del Tribunal Supremo

(*) Todos los artículos que no van seguidos de abreviatura son de la LECrim

GLOSARIO DE TÉRMINOS

ADSL. Asymmetric Digital Subscriber Line (línea de abonado digital asimétrica). Modalidad de acceso a internet a través de "banda ancha", con diferente velocidad para enviar y recibir información.

BTS. Base Transceiver Station (estación base de transmisión/recepción). Son las antenas o "repetidores" de telefonía móvil que dan acceso a la red; en la investigación penal permiten la ubicación aproximada de los dispositivos que se conectan a la red a través de ellas.

DSL. Digital Subscriber Line (línea de abonado digital). Modalidad de acceso a internet a través de "banda ancha".

EMS. Enhanced Message Service (servicio de mensajes mejorado). Servicio de mensajería que, además de texto, permite enviar "emoticonos".

IMEI. International Mobile Equipment Identity (Identificación internacional de móviles). Se trata de un código que identifica cada terminal móvil; permite a la compañía prestadora del servicio identificar el terminal desde el que se establece la conexión.

IMSI. International Mobile Subscriber Identity (Identidad Internacional del Abonado Móvil). Es el identificados de la línea o servicio, pero no indentifica al abonado.

IP. Internet protocol (protocolo de internet). La dirección IP es el número que identifica a cada equipo que se conecta a una red.

MMS. Multimedia Message Service (servicio de mensajes multimedia). Servicio de mensajería que permite el envío de archivos multimedia.

P2P. Red entre iguales o entre pares; proviene de "peer to peer". Permite el intercambio de archivos directamente (sin servidores) entre los equipos conectados a la red. Utilizan este sistema programas como edonkey, eMule o Ares.

RAMSONWARE. Ramson (rescate) y ware (software). Se denomina así a determinados programas dañinos que bloquean o encriptan archivos para luego solicitar el pago de una cantidad por liberarlos.

REDES DE ANONIMATO. La falta de seguridad de internet ha hecho surgir proyectos de redes que favorecen el anonimato. **TOR**: The Onion Router (rúter cebolla); **DEEP WEB** (red o web profunda).

SIM. Subscriber identity module (módulo de identificación de abonado). Es la tarjeta que se inserta en el terminal móvil y permite establecer la comunicación; va asociada a un número

de teléfono y a un operador de servicio de telefonía e incluye el código IMSI que permite la identificación del número utilizado para establecer la conexión y, si se trata de una tarjeta de contrato, la identificación del titular del mismo.

SITEL. Sistema Integrado de Interceptación Legal de Telecomunicaciones. Es una herramienta titularidad del Ministerio del Interior que utilizan las Fuerzas y Cuerpos de Seguridad del Estado, así como el CNI. Se encuentra regulado en el RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

SMS. Short Message Service (servicio de mensajes cortos). Servicio de mensajería de texto.

SPAM. Correo o mensaje basura.

WIFI. Proviene de *Wireless Fidelity* (fidelidad inalámbrica); en la actualidad, identifica la tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

ÍNDICE

1.- INTRODUCCIÓN

La LECrim, con casi 140 años, es una de las leyes más vetustas de nuestro ordenamiento; que el proceso penal español necesita una nueva ley de enjuiciamiento es algo que nadie cuestiona: se podrá debatir acerca del modelo, si debe o no instruir el MF o si se ha de dar entrada o no al principio de oportunidad, pero sobre lo que no hay debate es acerca de la necesidad de un nuevo Código Procesal Penal. Las inevitables consecuencias del paso del tiempo son especialmente significativas en relación a las nuevas tecnologías y su influencia en el proceso penal es doble: nuevas formas de delincuencia y nuevos instrumentos de investigación. El Sistema Procesal Penal asume la función de garantizar un adecuado equilibrio entre la investigación de los delitos y el respeto a los derechos fundamentales[1]; ese trascendente papel que debería corresponder a la LECrim ha tenido que ser desempeñado por los tribunales con un meritorio esfuerzo de interpretación que, sin embargo, no es suficiente. En efecto, como explica con claridad y precisión la Circular 2/2019 FGE sobre interceptación de comunicaciones telefónicas y telemáticas, con anterioridad a la reforma de 2015 el TEDH venía advirtiendo acerca de las carencias de la regulación del secreto de las comunicaciones en la LECrim (STEDH de 30 de julio de 1988, caso Valenzuela Contreras contra España); su reforma por la LO 4/1988, de 25 de mayo, introduciendo tres apartados en el artículo 579, no fue suficiente y las advertencias continuaron (STEDH de 18 de febrero de 2003, caso Prado Bugallo contra España)[2]; fueron entonces nuestros tribunales, los que construyeron un cuerpo jurisprudencial con los estándares y exigencias mínimas para la legalidad de las intervenciones telefónicas, que sí fue respaldado por el TEDH (Decisión de inadmisión de 25 de septiembre de 2006, caso Abdulkadir Coban contra España).

Tras dos frustrados intentos de reforma integral del proceso penal, la LO 13/2015 ha venido a llenar ese vacío legal, actualizando disposiciones existentes, dando cobertura legal a criterios consolidados en la práctica, corrigiendo algunas notorias deficiencias e introduciendo diligencias de investigación nuevas derivadas de los avances tecnológicos[3].

---

[1] GÓMEZ COLOMER, J. L. en Derecho Jurisdiccional III. El Proceso Penal. MONTERO AROCA, J. y otros. Tirant lo Blanch. 27ª ed. Valencia, 2019, pp. 242-243.

[2] Se trató de una reforma, en palabras de GÓMEZ COLOMER, "*muy defectuosa, ya que el supuesto normativo resultó poco preciso y con evidentes lagunas*" (MONTERO AROCA, J. y otros, Derecho Jurisdiccional III… ob. cit. p. 249).

[3] El TS ha considerado que "l*as insuficiencias de nuestro marco legal han sido puestas de manifiesto tanto por esta misma Sala, como por el TC (SSTC 26/2006, de 30 de enero, 184/2003, de 23 de octubre, 49/1999, de 5 de abril) y el TEDH (SSTEDH de 18 de febrero de 2003, Prado Bugallo contra España, y de 30 de julio de 1998, Valenzuela Contreras contra España). La LECrim dedica a esta materia el art. 579, en el Título VIII del Libro II, y las nuevas normas legales sectoriales no complementan adecuadamente sus insuficiencias, que requieren imperativamente y sin más demoras una regulación completamente renovada, en una nueva Ley procesal penal*

Entre estas nuevas diligencias de investigación tecnológica se incluye la interceptación de las comunicaciones telefónicas y telemáticas, cuyo estudio es el objetivo de este trabajo. Se trata de una de las diligencias de investigación más comunes en la práctica judicial, presente de manera habitual en muchas de las noticias de contenido jurídico que conocemos a través de los medios de comunicación. Han sido algunas de estas noticias las que me hicieron recordar aspectos estudiados en Derecho Procesal I y decidir elegirlo como tema del Trabajo Fin de Grado.

Para su elaboración he partido de la regulación legal y he tomado en consideración los comentarios y estudios doctrinales, con apoyo en las resoluciones más destacadas del TC, del TS y del TEDH.

En cuanto a la estructura del trabajo, tras una referencia inicial a la LO 13/2015, en la que se trata de delimitar el contexto en que fue aprobada, se da paso al estudio de las disposiciones generales, comunes a todas las diligencias de investigación tecnológicas; a continuación se aborda el estudio de la interceptación de las comunicaciones telefónicas y telemáticas, que constituye el núcleo central del trabajo y se divide en tres subapartados, conforme a las secciones que prevé la propia LECrim. El apartado final incluye las conclusiones a las que he llegado, fruto del estudio realizado.

2.- LA LO 13/2015

Viene siendo común a los Ministros de Justicia de todo signo político, realizar grandes anuncios de reforma del proceso penal; todos han defendido la necesidad de una reforma integral a través de una nueva Ley de Enjuiciamiento[4]. Tales anuncios han ido unidos, en ocasiones, a la creación de comisiones o grupos de trabajo que, incluso, elaboraron sendos anteproyectos que no llegaron a presentarse como proyectos de ley. Dejando aparte las buenas intenciones, lo cierto es que la reforma integral del enjuiciamiento penal sigue siendo, pese a todo, una asignatura pendiente.

que supere la obsolescencia de nuestra legislación decimonónica. Lo que por fin se ha producido por la reforma operada por LO 13/2015, artículo único, apartados trece y catorce, introduciendo los nuevos artículos 588 bis apartados a) a k) y 588 ter apartados a) a i)" (STS 2ª, sec. 1ª, 86/2018 de 19 febrero [RJ 2018\1029]).

[4] Francisco Caamaño, en su toma de posesión como Ministro de Justicia del gobierno de Rodríguez Zapatero (febrero de 2009), se comprometió a llevar a cabo la reforma del proceso penal; en nota de prensa posterior al Consejo de Ministros de 22 de julio de 2011, el Ministerio de Justicia de cuenta de la aprobación del Anteproyecto de Ley de Enjuiciamiento Criminal.

Ruiz Gallardón, Ministro de Justicia del gobierno de Rajoy Brey, constituyó una Comisión Institucional para la elaboración de una propuesta de texto articulado de Ley de Enjuiciamiento Criminal (BOE nº 62, de 13 de marzo de 2012) y presentó en el Congreso de los Diputados el 8 de mayo de 2013 las líneas maestras de las propuestas de la nueva Ley de Enjuiciamiento Criminal y de la Ley Orgánica del Poder Judicial elaboradas por dicha Comisión.

Con las diversas leyes aprobadas durante 2015, sin abandonar la aspiración de reforma integral, se vuelve a lo habitual, a las reformas parciales[5]. En lo que se refiere al objeto de este trabajo, el Anteproyecto de Ley Orgánica de diciembre de 2014 se articuló finalmente a través de sendos proyectos que dieron lugar a la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales y a la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Con la reforma se trata de "*dar cobertura legal a distintas diligencias de investigación que sirvan para investigar ciberdelitos de una manera garantista … que abren la puerta al uso de figuras tan polémicas como los drones, el agente encubierto en Internet o los virus de control remoto*"[6]

En este ámbito de las diligencias de investigación mediante la utilización de nuevas tecnologías, el núcleo fundamental de la reforma es la introducción de los capítulos IV a X en el Título VIII del Libro II de la LECrim: disposiciones comunes (588 *bis* a-k), interceptación de comunicaciones telefónicas y telemáticas (588 *ter* a-m), captación y grabación de comunicaciones orales (588 *quater* a-e), utilización de dispositivos técnicos de captación de imágenes, seguimiento y localización (588 *quinquies* a-c), registro de dispositivos de almacenamiento masivo (588 *sexies* a-c), registro remoto de equipos informáticos (588 *septies* a-c). También se introduce la regulación del agente encubierto informático (282 *bis* 6-7) y de los hallazgos casuales (579 *bis*).

De manera mayoritaria, la doctrina coincide en valorar de manera muy positiva la significativa actualización que supone la reforma. Se ha calificado como transgresora[7] y al

[5] Las reformas parciales han sido el denominador común, hasta el punto de que la LECrim, hasta la fecha, ha sido reformada por 76 leyes (53 con posterioridad a la CE). En 2015, el entonces Ministro de Justicia, Catalá Polo (sustituto de Ruiz Gallardón), mientras mantenía sometido a exposición pública el texto articulado de Ley de Enjuiciamiento Criminal impulsado por su predecesor, promovió una importante reforma procesal que justificó por razones de urgencia ("*resulta preciso afrontar de inmediato ciertas cuestiones que no pueden aguardar a ser resueltas con la promulgación del nuevo texto normativo que sustituya a la más que centenaria Ley de Enjuiciamiento Criminal*" –Preámbulos LO 13/2015 y LO 41/2015–).

El actual Ministro de Justicia Campo Moreno, el 17 de febrero de 2020 durante su comparecencia ante la Comisión de Justicia, anunció un anteproyecto de reforma de la Ley de Enjuiciamiento Criminal para antes de final de año; a tal efecto, en nota de prensa de 8 de mayo de 2020, el Ministerio da cuenta de la constitución del grupo de expertos al que se encargó su elaboración.

[6] BUENO DE MATA, F. *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. Diario LA LEY, nº 8627, de 19 de octubre de 2015, Nº 8627, p. 3.

[7] Idem. p. 11.

legislador de audaz[8], aunque no se eviten "*preocupantes disfunciones necesitadas de una profunda reflexión*"[9]; aspira de manera loable a dar cobertura a los avances tecnológicos "*al permitir la utilización futura de otras formas de comunicación que vayan surgiendo*"[10].

3.- DISPOSICIONES GENERALES COMUNES A LAS MEDIDAS

Un aspecto positivo a destacar en la regulación de las diligencias de investigación tecnológicas es que se incorpora unas disposiciones generales comunes a las distintas diligencias de investigación (588 *bis* a-k); con ello, se dota a la nueva regulación de cierta uniformidad.

Tal uniformidad descansa en la circunstancia de que las distintas diligencias de investigación reguladas tienen en común que su contenido encierra en actos de injerencia en la esfera privada del sujeto investigado y, con frecuencia, de terceros; incidencia que afecta a los derechos fundamentales previsto en el artículo 18 CE (intimidad, propia imagen, secreto de las comunicaciones y protección de datos personales).

Las disposiciones generales establecen el conjunto de garantías cuyo respeto resulta imprescindible para poder ser adoptadas. La previsión general del artículo 588 *bis* a, para la adopción de cualquiera de las medidas de investigación previstas en el capítulo IV exige **autorización judicial** dictada con plena sujeción a los principios de **especialidad**, **idoneidad**, **excepcionalidad**, **necesidad** y **proporcionalidad** de la medida.

Se trata de una regulación novedosa en la legislación procesal penal española, sin embargo, no así para el proceso penal. Me refiero a que si bien la regulación de la LECrim se limitaba a lo dispuesto en el artículo 579, tanto el TC como el TS, en gran medida a remolque del TEDH, habían ido configurado un cuerpo bastante sólido de jurisprudencia (auténtico "*corpus iuris* de creación jurisprudencial"[11]); con la LO 13/2015 se incorpora a la LECrim[12]. La

[8] RODRÍGUEZ LAINZ, J. L. *Aspectos polémicos de la intervención de comunicaciones como medida de vigilancia secreta*. La Ley Penal nº 125, marzo-abril 2017. p. 2.

[9] Idem. p. 2.

[10] SANCHÍS CRESPO, C. *Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas (1)*, La Ley Penal nº 125, marzo-abril 2017, p. 11.

[11] LÓPEZ YAGÜES, V. en Derecho Procesal Penal, ASENCIO MELLADO, J. Mª (Dir.), Tirant lo Blanch, Valencia, 2019, p. 232.

[12] La STC Primera 77/2019 de 12 febrero hace un interesante resumen de su doctrina y cita numerosas sentencias del propio TC (114/1984, 5/1994, 86/1995, 181/1985, 49/1996, 54/1996, 81/1998, 121/1998, 151/1998, 49/1999) del TEDH (de 6 de septiembre de 1978, caso Klass y otros contra Alemania [TEDH 1978\1]; de 2 de agosto de 1984, caso Malone contra el Reino Unido [TEDH 1984\1]; de 30 de julio de 1988, caso Valenzuela Contreras contra España [TEDH 1998\31]; de 24 de abril de 1990, caso Kruslin contra Francia [TEDH 1990\1]; de

Circular FGE 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, realiza un minucioso estudio del estado de la cuestión. El propio legislador confirma lo dicho, introduciendo numerosas referencias en su preámbulo a la jurisprudencia, hasta el punto de que la Circular FGE 1/2019 las interpretó como "*voluntad legislativa deliberada de integrarla en el texto legal mediante su incorporación expresa o, en cualquier caso, como guía interpretativa de las nuevas disposiciones*"[13].

3.1.- JURISDICCIONALIDAD

Nuestra Carta Magna "*garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*"; con esta salvedad está reservando a los Jueces y Magistrados (conforme a las correspondientes normas de distribución de competencias) la posibilidad de autorizar una actividad investigadora que suponga una injerencia en el derecho fundamental al secreto de las comunicaciones; esta exclusividad jurisdiccional de la autorización es, en palabras del TS, "*la principal garantía para la validez constitucional de una intervención telefónica*"[14]. Como explica GÓMEZ COLOMER, "*no se trata de autorizar a la PJ para que sea ésta la que limite el derecho, sino que lo dispuesto en la norma es que la limitación queda comprendida en el ámbito estricto de la actuación de los jueces y tribunales*"[15]

Sentada la jurisdiccionalidad, la LECrim se encarga de establecer los requisitos que debe reunir la autorización judicial; y lo hace exigiendo la necesidad de una investigación judicial en curso y fijando la iniciativa, la forma, el contenido, el plazo de la autorización. Para la interceptación de comunicaciones se disponen particularidades que se analizan más adelante (4.2).

3.1.1.- Necesidad de investigación judicial en curso

Las disposiciones generales comunes a todas las diligencias de investigación relacionadas con las nuevas tecnologías comienzan estableciendo la necesidad de que se autoricen durante la instrucción de las causas. Teniendo en cuenta que en el proceso penal

25 de junio de 1997, caso Halford contra el Reino Unido [TEDH 1997\37]; de 25 de marzo de 1998, caso Kopp contra Suiza [TEDH 1998\9]).

Por su parte, el TS ha destacado de manera reiterada su labor complementando la insuficiente regulación legal (STS 2ª, sec, 1ª, 634/2019 de 19 de diciembre [RJ 2019\5494]).

[13] Circular FGE 1/2019, p. 4.

[14] STS 2ª, sec. 1ª, 413/2015 de 30 junio [RJ 2015\4592].

[15] En MONTERO AROCA, J. Derecho Jurisdiccional III … ob. cit. p. 252.

español la instrucción se atribuye al Juez de Instrucción, parece fácil concluir que la resolución judicial que autorice una de tales diligencias de investigación tienen que adoptarse en el curso de una investigación judicial. Como ha manifestado el TC, "*la garantía jurisdiccional del secreto de las comunicaciones no se colma con la concurrencia formal de una autorización procedente de un órgano jurisdiccional, sino que ésta ha de ser dictada en un proceso, único cauce que permite hacer controlable, y con ello jurídicamente eficaz, la propia actuación judicial*"[16].

La fase de instrucción se denomina sumario en el proceso ordinario y diligencias previas en el abreviado; sin embargo, en la práctica es frecuente que se abran diligencias indeterminadas a partir de las cuales, en función de su resultado, se incoarán diligencias previas o sumario, según corresponda. El TC y el TS han considerado que estas diligencias indeterminadas no tienen la consideración de auténtico proceso, por lo que su práctica debe ser excepcional, no siendo un ámbito procesal adecuado para autorizar la interceptación de comunicaciones[17]. No obstante, ambos han ido matizando su doctrina en el sentido de concretar que lo reprochable no son las diligencias indeterminadas en sí, sino el secretismo en el que pueden desembocar, practicándose sin conocimiento del MF; cuando se unen, sin solución de continuidad, al proceso incoado en averiguación del delito, satisfaciendo así las exigencias de control a través, obviamente, de la notificación al Ministerio Fiscal, que es preceptiva en la incoación de las diligencias previas, pero que no se realiza en las indeterminadas, no suponen quiebra alguna de garantías constitucionales[18].

3.1.2.- Autorización judicial

La adopción de cualquier diligencia de investigación que afecte a derechos fundamentales requiere autorización judicial. Así se prevé con carácter general en el artículo 588 *bis* a y de manera específica, para la intervención de las comunicaciones, en el artículo 588 *ter* d. Con ello se está destacando la jurisdiccionalidad de la autorización, dando cumplimiento a lo previsto en la CE (18.3).

La autorización judicial se puede acordar de oficio, a instancia del MF o de la PJ. En el caso de solicitud, ésta habrá contener: la delimitación del ámbito objetivo, que viene referido

[16] STC Pleno 49/1999, de 5 de abril.

[17] Para el TC las diligencias indeterminadas "*no constituyen en rigor un proceso legalmente existente*" (STC Pleno 49/1999, de 5 de abril. Por su parte, el TS ha considerado que al no estar previstas específicamente en la LECrim no constituyen un proceso legal hábil para adoptar una medida de esta naturaleza, razón por la que ha recordado insistentemente a los instructores la necesidad de autorizarlas en el seno de diligencias previas o sumario (STS 2ª 467/1998, de 3 de abril [RJ 1998\3282]).

[18] STS 2ª, sec. 1ª, 301/2013 de 18 abril [RJ 2013\5014].

a la descripción del hecho investigado; la delimitación del ámbito subjetivo, que se refiere a la identidad del sujeto investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos; la justificación de la medida, para lo cual habrán de exponerse de manera detallada las razones por las que se solicita de acuerdo a los principios rectores establecidos en el artículo 588 *bis* a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa; las circunstancias específicas de la medida, como su contenido, extensión, forma de ejecución, duración y, en su caso, medios de comunicación empleados que permitan la ejecución de la medida; la Unidad investigadora de la PJ que se hará cargo y sujeto obligado que llevará a cabo la medida. La solicitud adquiere una especial significación en un doble sentido: es el documento sobre el que el juez ha de valorar si procede o no autorizar la medida solicitada; es utilizada, de manera habitual, para cumplir la exigencia de motivación judicial para acordar la medida, mediante lo que se conoce como motivación por remisión, admitida tanto por el TC[19], como por el TS[20].

El juez debe resolver en el plazo de 24 horas, aunque puede requerir la ampliación o la aclaración de la solicitud, con suspensión, entonces del plazo; la autorización habrá de adoptar la forma de auto motivado y su contenido es prácticamente una reiteración de lo exigido a la solicitud: ámbito objetivo (hecho punible investigado y calificación jurídica), ámbito subjetivo (identidad de los investigados y demás afectados por la medida, de ser conocidos), motivación y circunstancias de la medida (indicios racionales en que se funda, finalidad perseguida, extensión, motivación en relación a los principios rectores, duración), unidad investigadora que se hará cargo y sujeto obligado a llevarla a cabo, con expresa mención del deber de colaboración y de guardar secreto, cuando proceda, bajo apercibimiento de incurrir en delito de desobediencia y, por último, forma y periodicidad con que el solicitante informará al juez de los resultados de la medida.

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.

---

[19] "*Aunque lo deseable es que la expresión de los indicios objetivos que justifiquen la intervención quede exteriorizada directamente en la resolución judicial, ésta puede considerarse suficientemente motivada si, integrada incluso con la solicitud policial, a la que puede remitirse, contiene los elementos necesarios para considerar satisfechas las exigencias para poder llevar a cabo con posterioridad la ponderación de la restricción de los derechos fundamentales que la proporcionalidad de la medida conlleva*" (STC Pleno 167/2002, de 18 de septiembre).

[20] "*Y aunque es deseable que la resolución judicial contenga en sí misma todos los datos anteriores, la jurisprudencia constitucional admite, como ya hemos expresado anteriormente, la motivación por remisión, de modo que la resolución judicial puede considerarse suficientemente motivada si, integrada con la solicitud policial, a la que puede remitirse, contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad*" (STS 2ª, sec. 1ª 216/2018 de 8 mayo [RJ 2018\3193]).

Las medidas pueden adoptarse aun cuando afecten a **terceras personas** en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas.

3.2.- PRINCIPIOS

La autorización judicial de cualquiera de las medidas reguladas en el Capítulo IV (del título VIII, del Libro II) debe sujetarse a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

La **especialidad** supone que la medida ha de estar relacionada con la investigación de un delito concreto; es habitual en el enjuiciamiento penal la prohibición de las investigaciones prospectivas y de las causas generales[21]. En este sentido, la LECrim traslada a su contenido y da cobertura legal a la reiterada doctrina emanada del TS[22].

Con la **idoneidad** se hace referencia a la necesidad de que de la medida quepa esperar resultados útiles para la investigación (STS 2ª, sec. 1ª, 634/2019 de 19 diciembre [RJ 2019\5494], 641/2014 de 1 octubre [RJ 2014, 5575]) y que se presente como adecuada para los fines de la instrucción (STS 2ª, sec. 1ª, 85/2017 de 15 febrero [RJ 2017\1909]); se refiere, en definitiva, a la utilidad o aptitud de la medida para lograr la finalidad que con ella se persigue. Sirve para definir su ámbito objetivo (qué y cómo se investiga) y subjetivo (a quién se investiga), así como su duración (por cuánto tiempo).

La **excepcionalidad** y la **necesidad** guardan relación con la intención del legislador de que la medida sea lo menos gravosa posible para el investigado, dentro de la utilidad que debe reportar a la investigación. Así, la excepcionalidad se refiere a la inexistencia de otras medidas menos gravosas, pero igualmente útiles y la necesidad a la grave dificultad que se ocasionaría a la investigación si no se autorizase la medida. A partir de la excepcionalidad se debe descartar la autorización de una medida cuando exista otra u otras de las que se espera una similar utilidad (igualmente idóneas), pero cuya injerencia en la intimidad del investigado sea menor. A partir de la necesidad debe descartarse la medida si, a pesar de no autorizarla, la investigación no se vería gravemente dificultada.

---

[21] AGUILERA MORALES, M. *Tratamiento procesal de las causas generales*, en Proceso Penal y causa general, Monografías Cívitas (BIB 2008\2834), 2008, Aranzadi Instituciones BIB 2012\8069.

[22] "*La intervención debe estar relacionada con la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas a una prospección sobre la conducta de una persona en general. En este aspecto debe delimitarse objetivamente la medida a través de la precisión del hecho que se trata de investigar y subjetivamente mediante la suficiente identificación del sospechoso, vinculando con él las líneas telefónicas que se pretende intervenir*" (STS 2ª 1419/2004, de 1 diciembre, [RJ 2004\8022]).

La **proporcionalidad** indica que el sacrificio de los derechos e intereses afectados no debe ser superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho. Realmente, tanto la doctrina[23] como la jurisprudencia[24] se refieren a la proporcionalidad en sentido amplio y en sentido estricto. En sentido amplio la proporcionalidad engloba los principios de idoneidad, de necesidad y de proporcionalidad (en sentido estricto), de manera que exige la superación de un triple control, uniendo al de idoneidad y al de necesidad, ya vistos, el de proporcionalidad (en sentido estricto); éste supone una ponderación de la restricción de los derechos fundamentales[25], de manera que el sacrificio de los derechos e intereses afectados (coste) no debe ser superior al beneficio que de su adopción resulte para el interés público y de terceros (beneficio).

Para realizar el juicio de ponderación la valoración del interés público se basará en la gravedad del hecho[26], su trascendencia social o el ámbito tecnológico de producción[27], la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

4.- INTERCEPTACIÓN DE COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

Los artículos 588 *ter* a – m (Capítulo V), bajo el rótulo la interceptación de las comunicaciones telefónicas y telemáticas regulan, en realidad, tres actividades distintas a las que, respectivamente, se refieren las tres secciones que constituyen este capítulo: la propia interceptación de comunicaciones telefónicas y telemáticas, que a su vez incluye las

[23] La distinción tiene su origen en Alemania (vid. GONZÁLEZ-CUELLAR SERRANO, N. Proporcionalidad y derechos fundamentales en el proceso penal, Constitución y Leyes, Colex, 1990, págs. 24 y ss.).

[24] Tanto el TC (STC Segunda 173/2011 de 7 noviembre) como el TS (STS 2ª, sec. 1ª, 469/2016 de 31 mayo [RJ 2016\3114]).

[25] STC 1ª 197/2009, de 28 de septiembre, STC Primera 5/2010, de 7 de abril, STC Segunda 26/2010, de 27 de abril.

[26] Debe tenerse en cuenta que la referencia a la gravedad no debe relacionarse de manera directa con la pena que la conducta investigada pueda llevar aparejada. Como ya expuso el TC, la gravedad no solo se ha de valorar en atención a la pena, sino que también debe hacerse en "*atención al bien jurídico protegido y a la relevancia social del mismo*" (STC Primera 166/1999, de 27 de septiembre). La gravedad, por tanto, no se determina en función de lo dispuesto en los artículos 13 (delitos) y 33 (penas) del CP.

[27] Se refiere a la potencialidad lesiva que puede derivarse del uso de instrumentos informáticos para la comisión del delito (STC Primera 104/2006 de 3 abril).

disposiciones generales (sec. 1ª), la incorporación al proceso de datos incluidos en archivos automatizados de los prestadores de servicios (sec. 2ª) y la identificación de usuarios, terminales y dispositivos (sec. 3ª). En el primer supuesto se autoriza la interceptación previa de futuras comunicaciones, ya sean telefónicas, ya sean telemáticas a través de correo electrónico, redes sociales, chats, etc.[28]; en el segundo se autoriza la incorporación al proceso de datos ya existentes, como puede ser el registro de llamadas o la localización de las mismas, el registro de accesos a una determinada web, los datos descargados, el historial de correos electrónicos, las conversaciones de whatsapp, etc.; en el tercero, se prevén actuaciones accesorias para recabar la información necesaria para solicitar la intervención de las comunicaciones (IP, número de abonado, terminal, SIM, IMSI, IMEI, titular, etc.).

Durante los últimos años del siglo pasado, la interceptación de las comunicaciones se limitaba a los conocidos como *pinchazos* telefónicos, que su nombre obedece a la necesidad de que los operarios de telefonía accedieran físicamente a la instalación, *pinchando* el cable. En la actualidad, con las comunicaciones digitales, todas estas actuaciones se realizan mediante sofisticados dispositivos, como es SITEL, a lo que debe unirse la obligación de los prestadores de servicios de conservar determinados datos, así como su deber de colaboración (588 *ter* e –vid. 4.5–).

A falta de definición legal, siguiendo a GIMENO SENDRA, se puede entender por intervención telefónica o telemática "*todo acto de investigación, limitativo del derecho fundamental al secreto de las comunicaciones, por el que el Juez de Instrucción, en relación con un hecho punible de especial gravedad y en el curso de un procedimiento penal, decide, mediante auto especialmente motivado que, por la policía judicial, se proceda al registro de llamadas, correos electrónicos o datos de tráfico y/o a efectuar la grabación magnetofónica o electrónica de las conversaciones telefónicas o correos electrónicos del imputado durante el tiempo imprescindible para poder preconstituir la prueba del hecho punible y la participación de su autor*"[29].

4.1.- PRESUPUESTOS (ÁMBITO OBJETIVO)

Comienza la regulación con la referencia a los presupuestos de la intervención de las comunicaciones, aunque, en realidad, lo que se recoge es la delimitación del ámbito objetivo,

[28] Se incluyen todo tipo de comunicaciones e intervenciones a través de las múltiples aplicaciones disponibles: Skype, FaceTime, Viber, Twitter, Facebook, SMS, MMS, WhatsApp, Messenger, Telegram, Hangouts, etc.

[29] GIMENO SENDRA, V. Derecho Procesal Penal, 2ª ed. Civitas-Thomson Reuters. Proview, 22.I.2.A.

que se circunscribe a la investigación de los siguientes delitos: a) los previstos en el artículo 579.1 , es decir, los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal, delitos de terrorismo: b) los cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. Se trata de una delimitación que conjuga distintos criterios: por un lado, la intencionalidad delictiva (dolosos) y la extensión de la pena (tres años de prisión); por otro, el especial reproche social (cometidos en el seno de un grupo y organización criminal o terrorismo), con independencia de la pena; por último, la utilización de determinados instrumentos en su comisión (tecnología de la información o de la comunicación), también con independencia de la pena.

El hecho de que para este último tipo de delitos no se establezca un mínimo penológico ha sido valorado positivamente por cuanto facilita su investigación, dificultada hasta la reforma de 2015 por la exigencia de que se tratase de delitos castigados con pena superior a cinco años[30]. Criterio por otro lado coincidente con el que viene aplicando el TC respecto a la gravedad del delito como elemento integrante pero no determinante del juicio de proporcionalidad (vid. nota 17). El TJUE, por su parte, al resolver la cuestión prejudicial planteada por la AP de Tarragona, también sostuvo que la normativa europea (Directiva 2002/58, art. 15.1) se refiere a delitos, en general, sin exigir su consideración como graves[31].

Debe tenerse en cuenta, como ha destacado la FGE, que aunque se delimiten los tipos delictivos que permiten autorizar la intervención de las comunicaciones, ello no releva al Juez de la necesidad de realizar el juicio de proporcionalidad en los términos que ya se ha expuesto (vid. 3.2)[32].

---

[30] ZARAGOZA TEJADA, J. I. *La investigación de la dirección IP tras la Reforma operada por Ley 13/2015.* Revista Aranzadi Doctrinal núm. 2/2017, Aranzadi Instituciones [BIB 2017\10618].

[31] STJUE (Gran Sala) C-207/16, de 2 de octubre de 2018. En esta sentencia, el TJUE no tiene en consideración la gravedad del delito, sino la gravedad (intensidad) de la injerencia, concluyendo: "*El artículo 15, apartado 1, de 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 (Directiva sobre la privacidad y las comunicaciones electrónicas), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, consagrados en los citados artículos de la Carta de los Derechos Fundamentales, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave*".

[32] Circular FGE 1/2019, p. 11.

4.2.- EXTENSIÓN E INSTRUMENTOS DE LA INTERVENCIÓN

En pocos años, la manera de comunicarse ha ido evolucionado con tal rapidez que sin darnos cuenta hemos pasando de la simple conversación telefónica a la video llamada múltiple y del correo postal al envío de complejos archivos multimedia. Por otro lado, la tecnología lleva asociada una cantidad de información impensable hace años; la utilización de SITEL "*no sólo permite la interceptación de las comunicaciones telefónicas, sino la localización geográfica de los interlocutores y los datos asociados a la comunicación, como son la fecha, hora y duración de las llamadas, la identificación del IMEI y número de móvil afectado en la intervención, la distribución de llamadas por día, la información contenida en SMS, carpeta de audio, etc., números de teléfonos de los interlocutores*" (DOLZ LAGO)[33]. Todo ello dota a esta diligencia de investigación de una especial complejidad que se traslada al contenido de la autorización.

Dispone la LECrim (588 *ter* b 2) que la autorización puede extenderse al acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación. La LECrim hace esta distinción, resolviendo el problema que se venía planteando en la práctica, con ocasión de autorizaciones excesivamente genéricas[34]. El Juez debe detallar la extensión de la autorización y justificar cada una de las actuaciones autorizadas, ya sea el acceso al contenido de las comunicaciones (conversaciones, mensajes de voz, de texto o multimedia), a los datos electrónicos de tráfico o asociados a la comunicación (ficheros y archivos adjuntos de datos, de imágenes o multimedia) y a los que se produzcan con independencia del establecimiento o no de una comunicación (situación y utilización del dispositivo[35]). El momento de inflexión que cuestionó

---

[33] DOLZ LAGO, M. J. *¿Hacia una jurisprudencia electrónica? (Breves reflexiones sobre SITEL)*, La Ley Penal nº 74, septiembre 2010, p. 3. Sobre SITEL: BACH I FABREGÓ, R., E*l sistema integrat d'intercepció legal de les telecomunicacions (SITEL)* Revista Catalana de Seguretat Pública, nº 22, 2010, pp. 157-165. https://www.raco.cat/index.php/RCSP/article/view/193737/259660. VIDAL MARÍN, T. y RUIZ DORADO, M. *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 num.9/2016, Aranzadi Instituciones, BIB 2016\4915. Sobre la doctrina del TS en relación a SITEL: CASANOVA MARTÍ, R. *SITEL: una nueva realidad para intervenir las comunicaciones*, Revista Aranzadi de Derecho y Proceso Penal num. 29/2012, Aranzadi Instituciones BIB 2012\3239.

[34] "*Se termina, de esta manera, con una práctica que se había venido generalizando con anterioridad a la reforma LECrim consistente en la inclusión sistemática, en las resoluciones que acordaban la intervención de comunicaciones, de todos los datos de tráfico o asociados que pudieran ser aportados por el operador telefónico y, todo ello, sin fundamentación alguna que lo justificara*" (Circular FGE 2/2019, pp. 11 y 12).

[35] Las estaciones base de telefonía móvil (BTS) permiten determinar la localización de los terminales móviles que se conectan a la red a través de ellas (SAN Penal, sec. 3ª, 16/2019 de 29 marzo [ARP 2019\1307]; SAN Penal, de 16 octubre 2013 [ARP 2013\984]).

la adecuación constitucional de las autorizaciones genéricas fue el voto particular que formuló el actual presidente de la sala 2ª del TS, Marchena Gómez, a la STS 2ª, sec. 1ª 316/2011 de 6 abril (RJ 2011\3339).

> La Sala "validó" el AJI 3 Guecho, Vizcaya, que autorizó una intervención y escucha por el sistema SITEL, de dos teléfonos para la captación del tránsito de llamadas recibidas y realizadas, el contenido de los mensajes de texto o SMS, identificación y localización de los repetidores, identificación de los números que interaccionan con el intervenido (llamante o llamado), los IMEIs correspondientes a los teléfonos intervinientes, la identidad del titular de los teléfonos que interactúan, los listados de llamadas efectuadas y entrantes, con identificación de los titulares de las mismas. Sin embargo, el voto particular puso de manifiesto su discrepancia con lo que consideraba que constituía "*un entendimiento excesivamente convencional del derecho al secreto de las comunicaciones proclamado por el artículo 18.3 de la CE*" porque el auto "*no se limita a autorizar la intervención de las conversaciones telefónicas, sino que va mucho más allá … de la escucha y grabación de los flujos de comunicación verbal entre el ciudadano observado y sus interlocutores* ", permitiendo a la Policía "*el acceso sin límites, no ya a la completa identidad de los terceros que contactaban con los sospechosos -tuvieran o no relación con el delito investigado-, sino a todos los mensajes de texto, voz o imagen emitidos desde los terminales intervenidos y, por si fuera poco, a los datos de ubicación geográfica de quienes mantenían una conversación telefónica*". En razón a ello, no cuestiona que tales injerencias no puedan tener interés para la investigación, lo que no comparte y lo que centra la discrepancia con la decisión de la mayoría, es "*que la resolución que autoriza el menoscabo del derecho al secreto de las comunicaciones no dedique una sola línea a explicar el porqué de su necesidad y, además, silencie el ineludible juicio de proporcionalidad*"[36].

La propia LECrim se encarga de explicar que se consideran datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga (588 *ter* b *in fine*). Se trata de una extensa delimitación que permite un amplio acceso a toda la información que pueda obtenerse de la comunicación interceptada, ya sea el contenido de la misma, los datos relativos a su origen, destino, ruta, hora, fecha, tamaño y duración[37], los datos relativos a los abonados[38] o

---

[36] Sobre este voto particular, vid. RODRÍGUEZ LAINZ, J. L. *SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas*, Diario La Ley, Nº 7689, 7 de Septiembre de 2011, Ref. D-329; CASANOVA MARTÍ, R. *SITEL: una nueva realidad …* p. 16 y 17.

[37] Artículo 1.d del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, BOE» núm. 226, de 17 de septiembre de 2010 [BOE-A-2010-14221].

[38] Por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios (Artículo 18.3 del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, BOE» núm. 226, de 17 de septiembre de 2010 [BOE-A-2010-14221]).

cualesquiera otros, conforme a lo dispuesto en la LCDCE[39]; además, la expresa mención a "*los que se produzcan con independencia del establecimiento o no de una concreta comunicación*", extiende la necesidad de autorización también a ellos. Se trata de los supuestos en que se lleva a cabo el acceso a la red sin establecer una comunicación, entendiendo que está existe cuando se ponen en contacto, al menos, dos sujetos. Así, por ejemplo, cuando un individuo sube a la red archivos de contenido pedófilo, no establece realmente una comunicación, puesto que no hay interlocutor; aunque se ha planteado que en tales supuestos no se ve afectado el secreto a las comunicaciones (18.3 CE), sino la intimidad personal (18.4 CE), con un nivel de protección menor[40], la LECrim no establece distinciones y también exige autorización judicial[41]

La condición de investigado delimita el ámbito subjetivo de la interceptación, pero no es determinante del mismo; primero, porque puede tener como finalidad la identificación del propio investigado; segundo, porque lo relevante es la utilización de un terminal o medio de comunicación por el investigado, pero no su titularidad.

Se prevé la posibilidad de intervenir terminales y medios de comunicación utilizados por el investigado, ya sea de manera habitual u ocasionalmente; no es necesario que sea el titular, ya que la relación del investigado con el terminal o medio de comunicación objeto de intervención se establece por la utilización que hace del mismo. Con ello se permite la intervención de terminales y medios de comunicación de empresa o incluidos en un mismo contrato (p. ej. contratos familiares).

La LECrim va más allá y permite la intervención de los terminales o medios de comunicación, aunque no sean utilizados por el investigado. Lo permite respecto a la víctima cuando sea previsible un grave riesgo para su vida o integridad; lo permite respecto a terceros cuando el investigado se sirva de ese tercero para transmitir o recibir información, cuando ese tercero colabore con el investigado en sus fines ilícitos o se beneficie de su actividad y cuando el dispositivo sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular[42].

---

[39] La LCDCE establece la obligación de los prestadores de servicios de conservar los datos necesarios para rastrear e identificar en una comunicación su origen y destino, la fecha, hora y duración, el tipo, el equipo y su localización (con detalle en el artículo 3 LCDCE).

[40] ZARAGOZA TEJADA, J. I. "*La investigación de la dirección IP …*" op. cit., pp. 8 y 9.

[41] Circular FGE 2/2019, pp. 13 y 14.

[42] Tal situación se daría si la posible actividad delictiva investigada se lleva a cabo utilizando un dispositivo, por ejemplo un ordenador, sin conocimiento de su titular.

4.3.- SOLICITUD Y AUTORIZACIÓN JUDICIAL

Se trata de medidas de investigación y prevención del delito de naturaleza compleja por cuanto no incluyen una sola actividad, sino que habitualmente requieren la realización de varias conjuntamente, algunas de las cuales, tienen carácter accesorio para tomar conocimiento de los datos que deben incorporarse a la solicitud de autorización.

Puede conocerse la identidad del sujeto investigado, pero ser necesaria la identificación de los medios o instrumentos (terminal, operador, equipo informático, IP, etc.), aunque lo más habitual es que como consecuencia de la investigación policial, se haya localizado una IP desde la que, supuestamente, se haya cometido un hecho delictivo, pero se desconozca quién es su usuario[43]. Tales circunstancias, cuando la medida de investigación sea solicitada por el MF o la PJ, deben incluirse en la solicitud, de manera que, aparte de lo previsto en las disposiciones generales (588 *bis* b LECrim) [44], deberá contener la identificación del número de abonado, del terminal o de la etiqueta técnica, la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate (588 *ter* d). En la medida en que tales datos pueden ser desconocidos, los artículos 588 *ter* k, l y m regulan las actuaciones que pueden llevarse a cabo para conocer la identificación de usuarios, terminales y dispositivos de conectividad (vid. 6).

La autorización judicial determinará la extensión de la medida, que podrá consistir en: el registro y la grabación del contenido de la comunicación, indicando su forma o tipo; el conocimiento del origen o destino de la comunicación y su localización geográfica; el conocimiento de otros datos de tráfico asociados o no asociados, pero de valor añadido a la comunicación, con indicación de los datos concretos que han de ser obtenidos (588 *ter* d).

---

[43] ZARAGOZA TEJADA, J. I. "*La investigación de la dirección IP …*" op. cit., pp. 1-2.

[44] 1.º *La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.* 2.º *La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.* 3.º *Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.* 4.º *La extensión de la medida con especificación de su contenido.* 5.º *La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.* 6.º *La forma de ejecución de la medida.* 7.º *La duración de la medida que se solicita.* 8.º *El sujeto obligado que llevará a cabo la medida, en caso de conocerse.*

Debe adoptar la forma de auto[45] e incluir los requisitos generales exigidos por el artículo 588 *bis* c , así como aquellos establecidos para la solicitud[46]. No estamos ante una mera formalidad, sino de la necesidad tanto de justificar constitucionalmente la medida, como el respeto a los principios a los que debe ajustarse. Es en este punto donde adquiere especial relevancia la necesidad de motivación, que ha de extenderse de manera individualizada a cada una de las actuaciones autorizadas; no caben, pues autorizaciones genéricas o carentes de definición acerca de lo que buscan.

4.4.- AUTORIZACIÓN GUBERNATIVA Y CONVALIDACIÓN JUDICIAL

Un aspecto polémico de la regulación de la intervención de las comunicaciones lo constituye la posibilidad de que pueda ser autorizada por el Ministro del Interior o por el Secretario de Estado de Seguridad (588 *ter* d 3). La regulación de esta posibilidad está rodeada de excepcionalidad con la clara intención de evitar contrariar lo dispuesto en el artículo 18.3 CE respecto a la necesidad de resolución judicial.

Se establece una limitación objetiva en razón a los delitos investigados, que solo pueden ser aquellos relacionados con la actuación de bandas armadas o elementos terroristas. Respecto a la previsión general hay, por tanto, dos exclusiones: no cabe autorización gubernativa cuando se trate de delitos del artículo 579.1.1º (delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión) o de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

Para justificar esta excepcionalidad se utilizan dos razones: la urgencia y el carácter imprescindible de la medida. En mi opinión, lo relevante es la urgencia y no el carácter imprescindible; éste ya vendría exigido por los principios de excepcionalidad y de necesidad. La redacción es confusa y todo indica que lo que debe apreciarse con razones fundadas como imprescindible no es la medida en sí, sino la adopción inmediata de la misma, sin esperar a obtener la autorización judicial. Así parece desprenderse de la Circular FGE 2/2019, que ni siquiera hace mención a tal carácter imprescindible y considera que la LECrim remite a una

[45] No solo por la exigencia de motivación (588.bis.c), sino también porque afecta al derecho fundamental al secreto de las comunicaciones del artículo 18.3 CE (245.1.b LOPJ, 141 LECrim).

[46] Respecto a la interceptación de comunicaciones se establecen particularidades para la solicitud (588 *bis* b), pero no para la autorización; no cabe duda que ésta deberá incluir las circunstancias exigidas para aquella.

"*situación de necesidad justificada por la imposibilidad de recabar autorización judicial ante la urgencia del caso*"[47].

GÓMEZ COLOMER (y no es el único crítico[48]) advierte de los riesgos de esta autorización gubernamental que podría cuestionar el equilibrio entre "*la exigencia de tutelas específicas por la sociedad en peligro y los derechos del ciudadano investigado o sospechoso de haber cometido un crimen de esa naturaleza, siempre inocente hasta la sentencia de condena*" [49]. Desde un punto de vista de política criminal, el especial rechazo social a los delitos que pueden dar lugar a esta autorización (relacionados con la actuación de bandas armadas o elementos terroristas), unido a la situación de riesgo real de atentados, es justificación más que suficiente para favorecer la investigación y excluir de manera excepcional, la autorización judicial. Desde el punto de vista jurídico, sin embargo, no deben ser suficientes tales motivaciones; en este sentido, no debe olvidarse que la CE solo admite injerencias en el secreto de las comunicaciones a través de resolución judicial y lo que se admite en este caso, es una convalidación en lugar de una autorización.

En definitiva, el legislador ha sacrificado la autorización judicial previa de la interceptación por razones de urgencia, limitando su ámbito objetivo a los delitos relacionados con bandas armadas y terrorismo, exigiendo la inmediata comunicación el Juez competente, en todo caso, dentro del plazo máximo de 24 horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. Si tenemos presente que cualquier medida restrictiva de derechos fundamentales debe ser autorizada dentro de una investigación judicial (vid. 3.1.1), la justificación de la urgencia a través de las razones fundadas exigidas puede no resultar sencilla; no será fácil explicar que ha podido obtenerse la autorización del Ministro del Interior o del Secretario de Estado de Seguridad y no la del Juez de Instrucción[50].

Por otro lado, la LECrim no establece los requisitos que debe reunir la autorización gubernativa, limitándose a exigir la existencia de razones fundadas que hagan imprescindible

---

[47] Circular FGE 2/2019, p. 22.

[48] En la doctrina, SANCHÍS CRESPO, C. *Puesta al día de la instrucción penal …* p. 6. Por su parte, el CGPJ en su Informe al anteproyecto de ley orgánica de modificación de la ley de enjuiciamiento criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de integración tecnológica (Acuerdo del Pleno de 12 de enero de 2015) también se mostró muy crítico, dudando de su encaje constitucional (vid. p. 86). El informe está disponible en la web del CGPJ, en las sucesivas pestañas "actividad" e "informes".

[49] GÓMEZ COLOMER, J. L. Derecho Jurisdiccional… op. cit. p. 243.

[50] Distinta es la posibilidad que prevé el artículo 588 *sexies* c 4 que permite a la PJ y al fiscal, por razones de urgencia, ampliar el registro de dispositivos de almacenamiento masivo de información a los no incluidos inicialmente en la autorización.

la medida. La Circular FGE 2/2019 ha interpretado que la misma no está sujeta a las exigencias formales que la LECrim prevé para la autorización judicial habilitante[51]. No considero que deba admitirse tal interpretación porque siempre y en todo caso cualquier diligencia de investigación que afecte a los derechos reconocidos en el artículo 18.3 CE deben autorizarse y ordenarse con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Su control judicial posterior solo es posible si la autorización gubernativa exterioriza el cumplimiento de tales principios.

El juez competente, de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida, ha de considerarse aplicable lo dispuesto en el artículo 588 *bis* c.1, siendo necesario oír al MF.

4.5.- DEBER DE COLABORACIÓN

La LECrim establece un deber general de asistencia y colaboración con el Juez, el MF y la PJ, que obliga a prestar la asistencia para la práctica de la medida y a facilitar el cumplimiento de los autos de intervención de las telecomunicaciones. La particularidad de dicho deber es que, además de afectar a los prestadores de servicios tecnológicos (ya sea de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información), se extiende a toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. Entre los profesionales, el deber de colaboración afecta a los operadores de telefonía, proveedores de internet, gestores o creadores de aplicaciones para *tablets* y móviles, portales y motores de búsqueda, etc.); entre los particulares, se verán afectados de manera especial quienes gestionen o sean responsables de redes privadas.

Este deber de colaboración reviste especial importancia para la obtención de los datos necesarios que permitan llevar a cabo el contenido específico de la medida (registro y grabación del contenido de la comunicación, origen o destino, otros datos de tráfico asociados o no asociados); por esa razón, aparte de la previsión general, se recogen expresamente obligaciones para permitir el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad (vid. apdo. 6).

Quienes sean requeridos para prestar colaboración, están a su vez obligados a guardar secreto, pudiendo incurrir en la responsabilidad penal derivada del delito de desobediencia.

[51] Circular FGE 2/2019, p. 23.

4.6.- DURACIÓN, CONTROL E INCORPORACIÓN

Con carácter general toda medida de investigación tecnológica está sujeta a una duración determinada que no puede exceder del tiempo imprescindible para el esclarecimiento de los hechos; la resolución que la autorice debe fijar expresamente dicha duración. La intervención de las comunicaciones está sujeta a una duración máxima inicial de tres meses a contar desde fecha de su autorización; esta duración podrá extenderse acordando prórrogas por períodos sucesivos de igual duración, sin que pueda superarse en total el plazo máximo de dieciocho meses. La prórroga debe autorizarla el Juez competente mediante auto motivado, ya sea de oficio o a petición razonada del solicitante, debiendo subsistir las causas que motivaron la medida. La solicitud debe incluir un informe detallado del resultado de la medida, así como las razones que justifican su continuación; específicamente debe aportarse la transcripción de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.

En el plazo de dos días siguientes a la presentación de la solicitud, el Juez ha de resolver, pudiendo solicitar aclaraciones o mayor información. La prórroga se computa a partir de la fecha de expiración del plazo de la medida acordada.

La medida cesa en todos sus efectos una vez transcurrido el plazo por el que resultó concedida (sea el inicial o el de la prórroga), así como cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos (588 *bis* j).

La actividad llevada a cabo como consecuencia de la medida acordada está sujeta a control judicial, debiendo la PJ informar del desarrollo y los resultados en la forma y con la periodicidad que se hubiera especificado en el auto que la hubiera acordado (588 *bis* c 3 f). Esta exigencia es de especial aplicación en los supuestos en que la medida, para su ejecución, precisa de una duración temporal; supone una especial garantía con la que se pretende que el Juez disponga de los elementos de juicio suficientes para apreciar de manera continuada la concurrencia de los requisitos y el respeto a los principios exigidos. A la vista de la información periódica que reciba, el Juez puede ordenar el cese en cualquier momento, con independencia de la duración que se hubiera acordado inicialmente.

Por lo que se refiere a la incorporación al proceso, se distingue entre las grabaciones y la transcripción de las mismas. La utilización del sistema SITEL para llevar a cabo la interceptación de las comunicaciones telefónicas, permite el almacenamiento y la gestión de un archivo centralizado en el Ministerio del Interior; la PJ aportará al proceso las grabaciones

íntegras en soporte DVD, acompañando la transcripción de los pasajes que considere de interés. La cuestión más delicada es garantizar la autenticidad e integridad de la información; la LECrim exige su aseguramiento mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable.

4.7.- ACCESO DE LAS PARTES A LAS GRABACIONES

Resulta de aplicación a la interceptación de las comunicaciones telefónicas y telemáticas la previsión general del artículo 588 *bis* d que dispone su sustanciación *en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa*, algo que se ha considerado obvio, "*porque si el interceptado sabe que le están grabando no dirá nunca nada que tenga relevancia penal en su contra*"[52]; evitar que el investigado tenga conocimiento de la autorización judicial para llevar a cabo una intervención de comunicaciones (o cualesquiera de las medidas previstas en este mismo capítulo V) es absolutamente imprescindible para el buen fin de la investigación; ésta "*solo puede resultar eficaz para la investigación de hechos delictivos si efectivamente se da un total desconocimiento de la medida por parte de los dos comunicantes o, al menos, de uno de ellos*"[53]. El legislador ha optado por considerar que el secreto es una característica innata de las diligencias de investigación tecnológica, evitando que el Juez de Instrucción tenga que acordar y motivar el secreto en cada caso concreto[54].

Ello no impide que, una vez realizada, las partes puedan tomar conocimiento de lo realizado. El TEDH ya se manifestó en este sentido, reconociendo ese derecho del investigado a conocer qué es lo que se conoce de él, relacionándolo con el ejercicio del derecho de defensa[55].

El nuevo artículo 588 *ter* i regula el acceso de las partes a las grabaciones y transcripciones realizadas y también el derecho de los terceros, ajenos al proceso, cuyas comunicaciones hayan resultado intervenidas, a conocer la intervención y, eventualmente, obtener copias de las mismas.

---

[52] GÓMEZ COLOMER, J.L. en MONTERO AROCA, J. y otros, Derecho Jurisdiccional III. Proceso Penal. 27ª ed., Tirant lo Blanch, Valencia, 2019, p. 247.

[53] MORENO CATENA, V. Derecho Procesal Penal, 9ª ed. Tirant lo Blanch, Valencia, 2019, p. 294.

[54] RODRÍGUEZ LAINZ, J. L. *Aspectos polémicos de la intervención …* pp. 5 y 6.

[55] STEDH Pleno de 6 de septiembre de 1978, caso Klass y otros contra Alemania.

En relación a las partes, no se establecen diferencias entre el investigado y las demás personadas; a todas se reconoce su derecho a acceder a una copia de las grabaciones y transcripciones realizadas una vez que se alce el secreto y que expire la vigencia de la medida; se exceptúan los supuestos en que hubiera datos que afecten a la intimidad, evitando el Juez que se entreguen, dejando constancia de que no se incluye la totalidad de la grabación. Corresponde, por tanto, al Juez filtrar la información a facilitar, evitando entregar los datos referidos a aspectos de la vida íntima de las personas que no sean relevantes para la investigación en curso[56]; como igualmente le corresponde resolver sobre la solicitud de inclusión o exclusión que formule cualquiera de las partes[57].

Respecto a los terceros (no investigados) que intervengan en las comunicaciones interceptadas, el Juez debe notificarles la actuación realizada e informarles de las concretas comunicaciones en las que hayan participado. La persona notificada puede solicitar copia de la grabación o transcripción que le será entregada en la medida en que ello no afecte al derecho a la intimidad de otras personas ni resulte contrario a los fines del proceso en que se hubiera adoptado.

4.8.- DESTRUCCIÓN DE REGISTROS

Se prevé como disposición común a toda diligencia de investigación tecnológica el borrado y eliminación de los registros originales y la destrucción de las copias, una vez que se ponga término al procedimiento mediante resolución firme (588 bis k). Se trata de una medida de prevención que pretende evitar que se conserven grabaciones que pudieran afectar a la intimidad personal, más allá del tiempo imprescindible para el enjuiciamiento penal. Se recoge así el criterio sostenido por el TS que, en relación a la utilización del sistema SITEL, ha declarado: "*que los Tribunales, de oficio, en las causas en las que se haya procedido a la realización de intervenciones telefónicas, deberán acordar en sus sentencias la destrucción de las grabaciones originales que existan en la unidad central del sistema SITEL y de todas las copias, conservando solamente de forma segura las copias entregadas a la autoridad judicial, y verificando en ejecución de sentencia, una vez firme, que tal destrucción se ha producido* (STS 2ª, sec. 1ª, 293/2011 de 14 abril [RJ 2011\3349]).

[56] Circular FGE 2/2019, p. 37.

[57] Aunque la LECrim solo hace mención a la posibilidad de solicitar la inclusión de los datos que hubieran sido excluidos, debe entenderse que también podrá, cualquiera de las partes, solicitar la exclusión de aquellos datos que considera afectan a su intimidad (Circular FGE 2/2019, p. 38).

La redacción no es excesivamente afortunada y adolece de cierta indefinición. Así, nada establece respecto a quién corresponde ordenar la destrucción; entiendo que corresponde al tribunal que hubiera dictado la resolución que adquiere firmeza. Se prevé la conservación de una copia bajo custodia del Letrado de la Administración de Justicia, excepto en los supuestos en que se trate de una resolución firme decretando el sobreseimiento libre o una sentencia absolutoria respecto al investigado, siempre que a juicio del tribunal no fuera precisa su conservación. Las copias conservadas deben destruirse cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito. A falta de indicación en la Ley, corresponderá acordar la destrucción al tribunal bajo cuya custodia se conservaban las copias. En todo caso, la destrucción corresponde a la Policía Judicial que actuará bajo las órdenes de los tribunales.

5.- INCORPORACIÓN AL PROCESO DE DATOS ELECTRÓNICOS DE TRÁFICO O ASOCIADOS

Con autonomía respecto a la interceptación de las comunicaciones que se ha analizado, contempla la LECrim la posibilidad de incorporar al proceso los datos electrónicos en poder de los prestadores de servicios que consten en sus archivos automatizados. En este caso, la medida guarda relación con actuaciones ya realizadas y se refiere, por tanto, a datos que ya obran en poder de los prestadores de servicios; no se refiere, por tanto, a comunicaciones actuales ni futuras, sino a las ya realizadas[58]. Los prestadores de servicios pueden disponer de los datos por exigir su conservación la LCDCE o por propia iniciativa (por motivos comerciales, de seguridad o de cualquier otro tipo); a ello ha de sumarse la posibilidad que prevé el artículo 588 *octies* que, como medida de aseguramiento, permite al MF y la PJ requerir su conservación en tanto obtienen la autorización judicial para su cesión, durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.

La obligación de los prestadores de servicios es doble, porque a la conservación de los datos ha de unirse la necesidad de preservar el secreto de las comunicaciones y la intimidad de las personas; es por ello que el artículo 588 *ter* j prohíbe su cesión, salvo que medie autorización judicial para ello. Este control judicial sobre la cesión de datos por los prestadores

[58] La LCDCE cumple la finalidad de transponer la normativa comunitaria 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 (Directiva 2006/24/CE de 15 de marzo que modifica la Directiva 2002/58/CE). La nulidad de esta Directiva declarada por la STJUE Gran Sala, de 8 de abril de 2014, caso Comisión contra Hungría (TJCE 2014\104) plantea el problema acerca de si ello afecta a la LCDCE.

de servicios confirma lo que ya venía establecido en el artículo 6 LCDCE[59] y había sido sostenido por el TJUE[60].

Cuando el conocimiento de esos datos resulte indispensable para la investigación, el Juez puede recabar la información, incluida la búsqueda entrecruzada o inteligente de datos. Aunque la LECrim solo hace referencia a la posibilidad de solicitar del juez competente, de ello no debe concluirse que no pueda éste requerir la información de oficio. En cualquier caso, es necesario que en la autorización se precise la naturaleza de los datos que hayan de ser conocidos y las razones que justifican su cesión e incorporación al proceso.

No se trata de intervenir futuras comunicaciones, sino de aportar al proceso los datos de los que dispone el correspondiente prestador de servicios. Se suele distinguir entre datos dinámicos y datos estáticos, refiriéndose los primeros a los que se generan durante un proceso de comunicación (conversación, mensaje de texto, correo electrónico), mientras que los segundos aparecen almacenados en las bases de datos de los prestadores de servicios de comunicación para posibilitar esas comunicaciones, pero no se generan como consecuencia de una comunicación concreta (identificación o geolocalización del terminal, titularidad de la tarjeta)[61] Con la actual tecnología y a partir de la obligación de conservación que tienen los prestadores de servicios, es posible acceder al registro de llamadas o de cualquier otro tipo de comunicación (redes sociales, mensajería instantánea, correo electrónico, etc.), determinar el establecimiento y finalización de las mismas, la geolocalización de los terminales, ya sea en el momento de las llamadas o con independencia de éstas. El artículo 3 LCDCE determina los datos que deben conservarse y da idea de la información relevante que puede obtenerse, agrupándolos en datos necesarios para rastrear e identificar el origen y el destino de una comunicación[62], para determinar la fecha, hora y

[59] Artículo 6.1 LCDCE: "*Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial*".

[60] STJUE Gran Sala, de 8 de abril de 2014, caso Comisión Europea contra Hungría, [TJCE 2014\139].

[61] Circular FGE 2/2019, p. 42.

[62] Respecto a telefonía: número de teléfono de llamada y nombre y dirección del abonado o usuario registrado; respecto a Internet (acceso, correo y telefonía): identificación de usuario, del número de teléfono con que se acceda a la red pública de telefonía y nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

duración de una comunicación[63], para identificar el tipo de comunicación[64], para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación[65] y para identificar la localización del equipo de comunicación móvil[66].

Lo relevante, tanto de la solicitud como de la autorización judicial, es que deben precisar cuáles son los datos que el prestador de servicios debe proporcionar; no es suficiente una autorización genérica, sino que debe especificar lo solicitado.

Una cuestión polémica respecto a la cesión de datos es si su ámbito objetivo de aplicación se circunscribe a los delitos previstos en el artículo 588 *ter* a. La interpretación sistemática conduce a su aplicación; el Capítulo V (Titiulo VIII, Libro II) contiene unas disposiciones generales que deben ser de aplicación a todo él, incluida su sección 2ª. La Circular FGE 2/2019, sin embargo, a partir de la evolución prelegislativa, llega a la conclusión contraria y entiende que "*esa delimitación objetiva solo es predicable de la interceptación de la comunicación en sentido estricto, pero no de la incorporación al proceso de los datos*"[67]. Con todo el respeto a la Circular, parece una interpretación un tanto forzada, que trata de mantener el criterio sostenido por el Consejo Fiscal en su informe, en contra de la sistemática de la LECrim[68].

---

[63] Respecto a la telefonía: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia; respecto a Internet (acceso, correo y telefonía): fecha y hora de la conexión y desconexión, IP e identificación del usuario o abonado.

[64] Respecto a la telefonía: el servicio telefónico utilizado, tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia); respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

[65] Respecto a la telefonía de red fija: los números de teléfono de origen y de destino; respecto a la telefonía móvil: los números de teléfono de origen y destino, la identidad internacional del abonado (IMSI) y del terminal (IMEI), tanto del llamante como del receptor; en el caso de servicios anónimos de pago adelantado (tarjetas prepago), fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio. Respecto a Internet (acceso, correo y telefonía): número de teléfono de origen en caso de acceso mediante marcado de números, línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

[66] La etiqueta de localización (identificador de celda) al inicio de la comunicación y los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

[67] "*El análisis de los precedentes legislativos y del proceso de gestación de la LO 13/2015 conduce a inclinarse por la segunda postura. Efectivamente, el Anteproyecto de la Ley de reforma limitaba expresamente la posibilidad de incorporación de los datos al proceso a los delitos para los que se autorizaba la medida de intervención telefónica. Esta previsión fue objeto de críticas en el informe del Consejo Fiscal, que ponía de relieve que la incorporación de los datos al proceso supone una medida mucho menos invasiva que la interceptación de las comunicaciones. La consecuencia final ha sido la eliminación del art. 588 ter j de toda referencia expresa al catálogo de delitos para los que se permite la interceptación de comunicaciones, por lo que parece que la previsión podría interpretarse en un sentido más amplio*" (Circular FGE 2/2019, pp. 44 y 45).

[68] Me refiero al Informe del Consejo Fiscal al anteproyecto de ley orgánica de modificación de la ley de enjuiciamiento criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la

6.- ACCESO A LOS DATOS NECESARIOS PARA LA IDENTIFICACIÓN DE USUARIOS, TERMINALES Y DISPOSITIVOS DE CONECTIVIDAD

Suele ser habitual que la información obtenida a partir de una investigación policial permita apreciar la existencia de indicios delictivos, pero que sea necesario completar la investigación con otras actuaciones para las que haya que recabar la autorización judicial. Ya se han expuesto las exigencias que debe reunir la solicitud (apdo. 4.3) y entre ellas, han de incluirse determinados datos que pueden desconocerse. Para acceder a tales datos, imprescindibles para poder justificar la solicitud, se prevén las diligencias accesorias de identificación de usuarios, de terminales y de dispositivos.

Tienen en común su carácter accesorio o instrumental respecto a la eventual interceptación que pudiera acordarse con posterioridad; su finalidad es acceder a una información que, por sí sola, tiene escasa relevancia, pero que resulta imprescindible para formalizar debidamente la solicitud de la interceptación.

6.1.- IDENTIFICACIÓN MEDIANTE NÚMERO IP

Destaca ZARAGOZA TEJADA la importancia que la determinación de la dirección IP tiene en la investigación de los delitos cometidos a través de internet[69], pero advierte, al mismo tiempo, de las dificultades con que se encuentran los investigadores de la PJ, habida cuenta de la infinidad de *trucos* utilizados por los delincuentes para evitar ser localizados, ya sea aprovechando los propios avances tecnológicos, la utilización de *redes de anonimato* (TOR, DEEP WEB) o buscando el anonimato de equipos y locutorios públicos[70].

Es frecuente que, en las funciones de prevención y averiguación de delitos, la PJ lleve a cabo muestreos y utilice programas informáticos que rastrean la red, facilitando información

regulación de las medidas de investigación tecnológicas, que se encuentra disponible en la web: https://www.fiscal.es/documents/20142/fee385a4-e606-4d8c-677a-20605cb1185f

[69] "*Una vez obtenida dicha dirección IP, la identificación del número de abonado asignado a la misma en el momento exacto en el cual se produjo la conexión permitiría la concreción de las personas presuntamente responsables del hecho ilícito cometido a través de la red*" (ZARAGOZA TEJADA, J. I. *La investigación de la dirección IP*… op. cit. p. 1).

[70] Explica ZARAGOZA TEJADA que "*la proliferación en la actividad de troyanización de equipos informáticos ajenos, la utilización de malware malicioso para infectar a los mismos, o la posible sustracción e ilícito acceso a redes wifi ajenas provoca que, en la mayoría de los casos, la investigación se encamine a equipos informáticos o números de abonado que poco, o nada, tienen que ver con los verdaderamente utilizados para perpetrar el ilícito. En otros casos, aun consiguiendo determinar satisfactoriamente el equipo informático desde el que se ha ejecutado la conducta delictiva, las dificultades para identificar al autor pueden subsistir cuando dicho ordenador está ubicado en lugares de acceso público (organismos o instituciones públicas, universidades, cibercafés etc.) en el que resulta una pluralidad de personas las que tienen acceso al mismo o cuando el autor de dichas ilícitas conductas utiliza conexiones wifi ajenas abiertas*" (ZARAGOZA TEJADA, J. I. *La investigación de la dirección IP*… op. cit. p. 1).

acerca de direcciones IP desde las que podrían estar realizándose actividades sospechosas (descargas e intercambios de archivos de manera masiva o de contenido ilícito). Conocida la IP, para identificar y localizar el terminal o el dispositivo de conectividad e identificar al sospechoso, se puede solicitar al Juez de Instrucción que requiera la cesión de tales datos a los prestadores de servicios y demás agentes sujetos al deber de colaboración (588 ter k). La LECrim exige, por tanto, autorización judicial para comprobar quién está detrás de la IP[71], pero la localización de ésta pueda ser realizada por la PJ sin necesidad de autorización. Con ello se da cobertura legal a la reiterada doctrina del TS que ha venido considerando que el acceso por parte de la PJ a redes y foros abiertos, así como a redes P2P no supone injerencia en la intimidad ni vulnera derechos fundamentales[72]. Como explica la Circular FGE 2/2019, la dirección IP "*no identifica, pero permite identificar*"; por eso el acceso de la PJ a una IP no afecta ni al secreto de las comunicaciones ni a la intimidad, porque por sí sola no identifica a persona alguna[73]

Esta diligencia se refiere a las comunicaciones a través de internet y está prevista para identificar quién se encuentra detrás de una IP; requiere, por tanto, el previo conocimiento de ésta; de no ser así, sería de aplicación lo dispuesto en el artículo 588 *ter* j, analizado en el apartado anterior (vid. 5).

Sobre la utilidad real de esta diligencia, IBÁÑEZ LÓPEZ-POZAS se ha mostrado muy pesimista, habida cuenta de la variedad de formas que adoptan los ataques informáticos que, casi nunca, se realizan de manera directa por el delincuente desde su propio ordenador[74].

La actual regulación del artículo 588 *ter* k es plenamente coincidente con la doctrina establecida por el TEDH en su Sentencia de 1 de abril de 2018, caso Benedik v. Eslovenia [TEDH 2018\73]. En el supuesto en cuestión, las autoridades policiales suizas, tras acceder a

---

[71] Tal y como había adelantado el Acuerdo no jurisdiccional del pleno de la Sala 2ª del TS, de 23 febrero 2010 [JUR 2010\59653]: "*Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre*".

[72] SSTS 2ª, sec. 1ª, 739/2008, de 12 de noviembre [RJ 2009\167], 292/2008, de 28 de mayo [RJ 2008\3241] y 236/2008, de 9 de mayo [RJ 2008\4648].

[73] Circular FGE 2/2019, p. 47.

[74] Lo habitual es la utilización "*de mensajes de spam o de phishing para que se ejecute determinado fichero adjunto o bien sino acceda a una determinada URL, mensajes de correo que contienen directamente como adjunto el fichero dañino, Web Exploit Kits que se aprovechan de vulnerabilidades en el navegador o en los plugins instalados (drive-by downloads). Si el usuario navega a un sitio web «capturado» un iframe redirecciona el navegador a un segundo sitio dañino que a través de alguna vulnerabilidad del navegador o de alguno de sus plugins introducirá el ramsonware*" (LÓPEZ IBÁÑEZ-POZAS, F. L. en La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas, DÍAZ MARTÍNEZ, M. Y LÓPEZ-BARAJAS PEREA, I. (DIR.) Y OTROS, Tirant lo Blanch, Valencia, 2018, pp. 321 y 322.

una red en la que los usuarios compartían archivos con pornografía infantil, se ponen en contacto con las autoridades policiales de los Estados correspondientes a las IPs de los usuarios; la policía de Eslovenia se dirigió directamente al prestador de servicios de internet (amparándose en un artículo de la ley procesal eslovena), accediendo a la identificación del titular; tras solicitar un registro domiciliario, se localiza un ordenador con el programa eMule y diversos archivos con pornografía infantil, utilizado habitualmente por el hijo del titular de la línea de acceso a internet. El Tribunal consideró que la injerencia no había sido conforme a derecho, tal y como exige el artículo 8 del CEDH, debiendo someterse el acceso a los datos asociados a una IP a supervisión judicial o supervisión de otra autoridad independiente[75].

6.2.- IDENTIFICACIÓN DE LOS TERMINALES MEDIANTE CAPTACIÓN DE CÓDIGOS DE IDENTIFICACIÓN DEL APARATO O DE SUS COMPONENTES

De manera similar a lo dispuesto respeto a la identificación a través de IP, para las comunicaciones telefónicas se admite que la PJ se sirva de artificios técnicos (actuales o futuros, de acuerdo con el estado de la tecnología)[76] para acceder a códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI. La habilitación a la PJ se justifica, como en el apartado anterior, en que la identificación no afecta a los sujetos, sino a los aparatos o sus componentes, no existiendo, por tanto, intromisión; lo único que se exige es que la tecnología utilizada se ponga en conocimiento del Juez, posibilitando así el control judicial.

Con la obtención de los códigos, la PJ dispone de los datos necesarios para solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 *ter* d (apartado a).

[75] Un comentario a esta sentencia: 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. 9241, de 18 de julio de 2018.

[76] En la actualidad, la PJ acude habitualmente a la utilización de escáneres para acceder a los códigos de identificación.

6.3.- IDENTIFICACIÓN DE TITULARES O TERMINALES O DISPOSITIVOS DE CONECTIVIDAD

La LECrim dedica el último artículo de éste Capítulo V a regular la posibilidad de que tanto el MF como la PJ puedan dirigirse a los prestadores de servicios y recabar directamente de ellos, sin necesidad de autorización judicial, los datos identificativos del titular de un número de teléfono o de cualquier medio de comunicación o, en sentido inverso, la identificación del teléfono o del medio de comunicación que utilice una persona determinada. La peculiaridad, es este caso, es que la investigación no aparece vinculada a un proceso de comunicación, por lo que supone una injerencia menor que no requiere autorización judicial.

CONCLUSIONES

PRIMERA. La reforma llevada a cabo por la Ley 13/2015 supone una importante actualización de la regulación de la investigación penal incorporando a la LECrim los criterios jurisprudenciales hasta entonces elaborados por el TC y por el TS, siguiendo las pautas marcadas por el TEDH. No introduce novedades significativas, pero da cobertura legal a dicha jurisprudencia.

La incorporación de disposiciones generales (588 *bis* a-k) es un aspecto positivo de la reforma, en tanto que proporcionan uniformidad y establecen los requisitos comunes, con independencia de las particularidades propias de cada una de las diligencias de investigación reguladas.

SEGUNDA. La regulación de la intervención de las comunicaciones telefónicas o telemáticas va mucho más allá de la visión tradicional de la medida, limitada a los *pinchazos* telefónicos; los medios tecnológicos actuales permiten acceder a toda la información que se genera con las comunicaciones, que no se limita al contenido de éstas, sino que incluye datos de vital importancia para la investigación, como es la ubicación de los terminales móviles, la identificación de los titulares de líneas o conexiones a internet, así como de los equipos a través de los que se accede a la red.

La delimitación del ámbito objetivo ampliando los supuestos generales a los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, con independencia de la pena que lleven aparejada, merece una valoración positiva ya que, habitualmente, se trata de infracciones que de otra forma no permitirían la práctica de estas diligencias.

No sucede lo mismo respecto a la autorización gubernativa que, aunque se sujete a la inmediata convalidación judicial, no parece que pueda justificarse una situación de urgencia tal que no permita recabar la autorización judicial.

TERCERA. El deber de colaboración se extiende, de manera acertada, no solo a los prestadores de servicios tecnológicos, sino a toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, incluidos los sujetos particulares. De esta manera, los sujetos administradores de redes privadas, de páginas web o portales de acceso a contenidos, de sistemas informáticos, etc. quedan incluidos dentro del ámbito del deber de

colaboración, sujeto a responsabilidad, tanto por el incumplimiento de tal deber, como por el incumplimiento del también previsto de guardar secreto.

CUARTA. La autorización judicial debe incluir *la forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida*. Tal exigencia, prevista especialmente para aquellas medidas que su ejecución precisa de una duración temporal, supone una especial garantía con la que se pretende que el Juez disponga de los elementos de juicio suficientes para apreciar de manera continuada la concurrencia de los requisitos y el respeto a los principios exigidos.

QUINTA. La investigación exige que cualquier interceptación de comunicaciones se realice sin que el investigado tenga conocimiento de ello; de ahí que se autorice legalmente que se lleven a cabo en secreto, sin necesidad de declarar éste para el resto de actuaciones. En todo caso, el derecho de defensa determina, sin ninguna duda, la necesidad de que una vez practicada la medida, el investigado tenga acceso a su contenido; esta posibilidad se extiende, en los mismos términos, a las demás partes personadas. Dado que en las comunicaciones pueden participar terceros, también a éstos se les reconoce el derecho a acceder a su contenido, solicitando copia de las mismas. En todo caso, al Juez corresponde preservar la intimidad de todos los afectados, debiendo impedir que en las copias se incluyan aspectos de la vida íntima de las personas que intervengan.

SEXTA. Es establecimiento de comunicaciones telefónicas o telemáticas genera un volumen significativo de información, más allá del contenido de las mismas. Aparte de poder acceder a tal información como consecuencia de la interceptación de futuras comunicaciones, también es posible acceder a la ya generada. En este sentido, mediante autorización judicial se puede solicitar a los prestadores de servicios la cesión de los datos relativos a las comunicaciones, tanto los que están obligados a conservar como cualesquiera otros, para su incorporación al proceso.

SÉPTIMA. La regulación de la interceptación de comunicaciones se completa con la posibilidad de llevar a cabo determinadas actuaciones de carácter accesorio con la finalidad de recabar los datos necesarios para poder formular la solicitud de interceptación.

BIBLIOGRAFÍA

AGUILERA MORALES, M. *Tratamiento procesal de las causas generales*, en Proceso Penal y causa general, Monografías Cívitas (BIB 2008\2834), 2008, Aranzadi Instituciones BIB 2012\8069.

ASENCIO MELLADO, J. Mª (DIR.) Y OTROS. Derecho Procesal Penal, Tirant lo Blanch, Valencia, 2019.

BACH I FABREGÓ, R., E*l sistema integrat d'intercepció legal de les telecomunicacions (SITEL)* Revista Catalana de Seguretat Pública, nº 22, 2010, pp. 157-165. https://www.raco.cat/index.php/RCSP/article/view/193737/259660

BUENO DE MATA, F. *Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. Diario LA LEY, nº 8627, de 19 de octubre de 2015, Nº 8627.

CARRETERO SÁNCHEZ, A. *Las intervenciones telefónicas*, Diario La Ley, Nº 7117, 18 de febrero de 2009, Ref. D-51, LA LEY 166/2009.

CASANOVA MARTÍ, R. *SITEL: una nueva realidad para intervenir las comunicaciones*, Revista Aranzadi de Derecho y Proceso Penal núm. 29/2012, Aranzadi Instituciones BIB 2012\3239.

DÍAZ MARTÍNEZ, M. Y LÓPEZ-BARAJAS PEREA, I. (DIR.) Y OTROS. La nueva reforma procesal penal. Derechos fundamentales e innovaciones tecnológicas. Tirant lo Blanch, Valencia, 2018.

DOLZ LAGO, M. J. *¿Hacia una jurisprudencia electrónica? (Breves reflexiones sobre SITEL)*, La Ley Penal nº 74, septiembre 2010 (pp. 1-22)

GIMENO SENDRA, V. Derecho Procesal Penal, 2ª ed. Civitas-Thomson Reuters. Proview.

GONZÁLEZ-CUELLAR SERRANO, N. Proporcionalidad y derechos fundamentales en el proceso penal, Constitución y Leyes, Colex, 1990.

MAGRO SERVET, V. *Las intervenciones electrónicas e informáticas por los agentes de la autoridad. Medidas restrictivas de derechos fundamentales en estos supuestos*. La Ley Penal, nº 84 (julio 2011), La Ley 542/2011.

MONTERO AROCA, J. Y OTROS. Derecho Jurisdiccional III. Proceso Penal. 27ª ed., Tirant lo Blanc, Valencia, 2019.

MORENO CATENA, V. Y CORTÉS DOMÍNGUEZ, V. Derecho Procesal Penal, 9ª ed. Tirant lo Blanch, Valencia, 2019.

RODRÍGUEZ LAINZ, J. L. *SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas*, Diario La Ley, Nº 7689, 7 de septiembre de 2011, Ref. D-329

- *Aspectos polémicos de la intervención de comunicaciones como medida de vigilancia secreta*. La Ley Penal nº 125, marzo-abril 2017 (pp. 1-14)

- Acceso policial a información sobre atribución de IP dinámicas (Comentario a la STEDH del caso Benedik v. Eslovenia). Diario La Ley núm. 9241, de 18 de julio de 2018 (pp. 1-15)

SANCHÍS CRESPO, C. *Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas (1)*, La Ley Penal nº 125, marzo-abril 2017 (p. 1-13).

VIDAL MARÍN, T. y **Ruiz Dorado, M**. *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 num.9/2016, Aranzadi Instituciones BIB 2016\4915.

ZARAGOZA TEJADA, J. I. *La investigación de la dirección IP tras la Reforma operada por Ley 13/2015.* Revista Aranzadi Doctrinal núm. 2/2017, Aranzadi Instituciones BIB 2017\10618.

OTRAS FUENTES

Circular FGE 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

Circular FGE 1/2019, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal.

Circular FGE 2/2019, sobre interceptación de comunicaciones telefónicas y telemáticas.

Informe del Consejo Fiscal, de 23 de enero de 2015, al anteproyecto de ley orgánica de modificación de la ley de enjuiciamiento criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.

Informe del CGPJ, de 12 de enero de 2015, al anteproyecto de ley orgánica de modificación de la ley de enjuiciamiento criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de integración tecnológica.

RESOLUCIONES JUDICIALES

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

STEDH de 6 de septiembre de 1978, caso Klass y otros contra Alemania [TEDH 1978\1]

STEDH de 2 de agosto de 1984, caso Malone contra el Reino Unido [TEDH 1984\1]

STEDH de 30 de julio de 1988, caso Valenzuela Contreras contra España [TEDH 1998\31]

STEDH de 24 de abril de 1990, caso Kruslin contra Francia [TEDH 1990\1]

STEDH de 25 de junio de 1997, caso Halford contra el Reino Unido [TEDH 1997\37]

STEDH de 25 de marzo de 1998, caso Kopp contra Suiza [TEDH 1998\9]

STEDH de 18 de febrero de 2003, caso Prado Bugallo contra España [TEDH 2003\6]

STEDH de 1 de abril de 2018, caso Benedik contra Eslovenia [TEDH 2018\73]

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

STJUE Gran Sala, de 8 de abril de 2014, C-288/12, caso Comisión contra Hungría [TJCE 2014\139]

STJUE Gran Sala, de 2 de octubre de 2018, C 207/16 [TJCE 2018\231]

TRIBUNAL CONSTITUCIONAL

STC Segunda 114/1984, de 29 de noviembre

STC Primera 181/1985, de 20 de diciembre

STC Primera 5/1994, de 17 de enero

STC Primera 86/1995, de 6 de junio

STC Primera 49/1996, de 26 de marzo

STC Primera 54/1996, de 26 de marzo

STC Pleno 81/1998, de 2 de abril

STC Segunda 121/1998, de 15 de junio

STC Segunda 151/1998, de 13 de julio

STC Pleno 49/1999, de 5 de abril

STC Pleno 167/2002, de 18 de septiembre

STC Pleno 184/2003, de 23 de octubre

STC Segunda 26/2006, de 30 de enero

STC Primera 104/2006 de 3 abril

STC Primera 197/2009, de 28 de septiembre

STC Segunda 26/2010, de 27 de abril

STC Primera 5/2010, de 7 de abril

STC Segunda 173/2011 de 7 noviembre

STC Primera 77/2019 de 12 febrero

TRIBUNAL SUPREMO

STS 2ª 467/1998, de 3 de abril [RJ 1998\3282]

STS 2ª 1419/2004, de 1 diciembre, [RJ 2004\8022]

STS 2ª, sec. 1ª, 236/2008, de 9 de mayo [RJ 2008\4648]

STS 2ª, sec. 1ª, 292/2008, de 28 de mayo [RJ 2008\3241]

STS 2ª, sec. 1ª, 739/2008, de 12 de noviembre [RJ 2009\167]

STS 2ª, 300/2010, de 23 febrero 2010 [JUR 2010\59653]

STS 2ª, sec. 1ª, 173/2011 de 7 noviembre [RJ 2011\2778]

STS 2ª, sec. 1ª 316/2011 de 6 abril (RJ 2011\3339)

STS 2ª, sec. 1ª, 293/2011 de 14 abril [RJ 2011\3349]

STS 2ª, sec. 1ª, 301/2013 de 18 abril [RJ 2013\5014]

STS 2ª, sec. 1ª 641/2014 de 1 octubre [RJ 2014, 5575]

STS 2ª, sec. 1ª, 413/2015 de 30 junio [RJ 2015\4592]

STS 2ª, sec. 1ª, 469/2016 de 31 mayo [RJ 2016\3114]

STS 2ª, sec. 1ª, 85/2017 de 15 febrero [RJ 2017\1909]

STS 2ª, sec. 1ª, 86/2018 de 19 febrero [RJ 2018\1029]

STS 2ª, sec. 1ª 216/2018 de 8 mayo [RJ 2018\3193]

STS 2ª, sec. 1ª, 634/2019 de 19 de diciembre [RJ 2019\5494]

AUDIENCIA NACIONAL

SAN Penal, sec. 3ª, de 16 octubre 2013, caso Faisán [ARP 2013\984]

SAN Penal, sec. 3ª, 16/2019 de 29 marzo [ARP 2019\1307];