TRABAJO DE FIN DE GRADO

Grado en Derecho

Curso académico: 2021/2022

AUTORA: DEJANIRA RAMÍREZ ANTEQUERA

TUTORA: MARÍA DEL CARMEN SENÉS MOTILLA

LA INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS EN EL PROCESO PENAL

THE INTERCEPTION OF TELEPHONE AND TELEMATIC COMMUNICATIONS IN THE CRIMINAL PROCESS

El proyecto realizado a continuación aborda la interceptación de las comunicaciones telefónicas y telemáticas conforme a lo establecido en nuestro régimen jurídico tras la reforma de la LECrim debido al avance tecnológico sufrido los últimos años.

The following project deals with the interception of telephone and telematic communications in accordance with the provisions of our legal system following the reform of the LECrim due to technological advances in recent years.

ÍNDICE

SIGLAS Y ABREVIATURAS

- Art(s): Artículo(s).

- CE: Constitución Española.

- CEDH: Convenio Europeo de Derechos Humanos.

- CD: Disco Compacto.

- DVD: Disco Versátil Digital.

- FGE: Fiscalía General del Estado.

- IMEI: Internacional Mobile Equipment Identify o Identidad Internacional de Equipo Móvil.

- IMSI: Internacional Mobile Subscriber Identity o Identidad Internacional del Abonado Móvil.

- IP: Internet Protocol o Protocolo de Internet.

- LECrim: Ley de Enjuiciamiento Criminal aprobada por el Real Decreto de 14 de septiembre de 1882.

- LSSICE: Ley 34/2002, de 11 de julio de Servicios de la Sociedad de Información y Comercio Electrónico.

- Núm.: Número.

- Pág(s).: Página(s).

- SIM: Subscriber Identity Module o Módulo de Identificación de Abonado.

- ss.: Siguientes.

- TFG: Trabajo Fin de Grado.

- TJUE: Tribunal de Justicia de la Unión Europea.

1. INTRODUCCIÓN

El Trabajo de Fin de Grado expuesto a continuación se titula *"La intervención de las comunicaciones telefónicas y telemáticas en el proceso penal"*, llevado a cabo en la asignatura final del Grado en Derecho (curso académico 2021/2022).

Haber elegido este tema se debe, además de mi gran interés y aprendizaje en la materia del Derecho Procesal Penal, al consejo dado por mi tutora María del Carmen Senés Motilla, cuando en mi indecisión por la elección de este, me lo propuso. El desarrollo de este trabajo, además, ha hecho que me introduzca aún más en el ámbito del Cuerpo de Policía Nacional, pues es mi vocación profesional. Además, es un tema muy interesante y de continuo cambio en la actualidad debido a los números avances tecnológicos existentes en la sociedad.

Como acabo de decir, el continuo avance en la tecnología ha provocado que la regulación existente en nuestra Ley de Enjuiciamiento Criminal quedase desfasada y haya sido necesaria una modificación en el ámbito de la interceptación de las comunicaciones telefónicas y telemáticas. Esta reforma ha sido operada por la Ley Orgánica 13/2015, del 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica

Con ella se ha conseguido una limitación más exhaustiva y garantizada en algunos de nuestros derechos fundamentales, más concretamente en el secreto de las comunicaciones y, por supuesto, una mejora en la regulación de las medidas de investigación tecnológica para llevar a cabo correctamente la intervención. Introduce además, los Capítulo IV y V del Título VIII del Libro II, referidos a las disposiciones comunes y a la interceptación de las comunicaciones telefónicas y telemáticas, que serán los puntos más complejos y en los que se basa nuestro trabajo.

El siguiente trabajo se encuentra estructurado en ocho apartados principales, donde seguidamente nos adentraremos más a fondo en lo establecido en cada uno de ellos. El primer punto es la mera introducción, mientras que, el segundo apartado, versa sobre el derecho fundamental al secreto de las comunicaciones. En él podemos encontrar toda su regulación legal tanto a nivel nacional e internacional, el ámbito protegido, quiénes pueden gozar de este derecho fundamental y las garantías que proporciona.

El apartado tercero trata el concepto de la interceptación de las comunicaciones y su relación con el artículo 18 CE, referente al derecho fundamental al secreto de las comunicaciones nombrado anteriormente. La interceptación de las comunicaciones telefónicas y telemáticas se encuentran reguladas en el Capítulo V del Título VIII del Libro II, desde el art. 588 ter a) hasta el art. 588 ter m), constando de tres secciones de la Ley de Enjuiciamiento Criminal tras la reforma de esta operada por la Ley Orgánica 13/2015, de 5 de octubre.

Seguidamente, los epígrafes cuarto y quinto se adentran en la regulación legal de las intervenciones. El apartado cuarto, referido a las disposiciones comunes a los medios de investigación tecnológica, se encuentra divido a su vez en siete subapartados que comprenden desde el artículo 588 bis a) hasta el 588 bis k), recogidos en el Capítulo IV, Título VIII del Libro II de la LECrim. El quinto epígrafe, consta de once subapartados bajo la rúbrica de *"regulación legal de la interceptación de las comunicaciones telefónicas y telemáticas"*, el cual lo localizamos en el Capítulo V, Título VIII del Libro II, dividido en tres secciones. La primera comprende desde el art. 588 ter a) hasta el art. 588 ter i). La Sección 2ª solo incluye el apartado j) del art. 588 ter. Y por último, la tercera sección regula los apartados k), l) y m) del mismo precepto, todos ellos establecidos en la Ley de Enjuiciamiento Criminal.

El sexto epígrafe versa sobre el Sistema Integrado de Interceptación Legal de las Comunicaciones o más conocido como SITEL. En él trataremos de fijar un concepto, el procedimiento llevado a cabo por la labor de la Policía Judicial bajo la regulación legal establecida, la cual es muy variada ya que no mantiene una propia ni específica sino que, la podemos buscar en diferentes normas jurídicas o bien, en la jurisprudencia del Tribunal Supremo.

Para finalizar, se concluye el trabajo con los apartados siete y ocho, donde se localizan las conclusiones y la bibliografía. En ellas encontraremos la materia expuesta a continuación de manera más concentrada y la correlación de temas con otras exposiciones de interés que nos han servido para la realización del trabajo.

2. EL DERECHO FUNDAMENTAL AL SECRETO DE LAS COMUNICACIONES

Para dar comienzo al apartado del derecho fundamental al secreto de las comunicaciones, indicaremos que encuentra reconocimiento en el art. 18.3 de la Sección Primera, Capítulo II, del Título I de la Constitución Española, la cual proporciona el máximo nivel de protección haciéndole contar con las siguientes garantías:

1. El art. 53.1 y 81.1 CE establecen la obligación de ser desarrollado por una ley orgánica, respetando su "contenido esencial".

2. Debe estar protegido ante los tribunales ordinarios y su amparo ante el TC (art. 53.2 CE).

3. Su reforma se llevará a cabo a través del procedimiento agravado del artículo 168 CE.

Estas garantías se encuentran recogidas por la Constitución. Pero es cierto que, no solo nuestra Carta Magna se encarga de establecerlas sino que, otras leyes como es el Código Penal, también lo hacen.

En palabras de DÍAZ REVOIRO *"existe una garantía que protege las comunicaciones entre las personas, de manera que cualquier supuesto admisible de interceptación de las mismas se presenta como excepcional, y rodeado de límites, requisitos y garantías, dado que esa práctica afecta a un derecho fundamental, y solo el cumplimiento de esos requisitos y garantías permitirá que esa afectación no se convierta en vulneración".*[1]

Es un derecho de carácter formal, donde se plasma la dignidad de la persona y el libre desarrollo de su personalidad que se garantiza a través del artículo 18.3 CE: *"Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial"*[2]. La garantía que proporciona se encarga de dar la seguridad necesaria a nuestras comunicaciones, de manera que, para poder realizar una interceptación,

[1] DÍAZ REVORIO F. J., "El derecho fundamental al secreto de las comunicaciones", en Revista de la Facultad de Derecho, Pontificia Universidad Católica del Perú, 2007, núm. 59, pág. 159-173

[2] Constitución Española, Boletín Oficial del Estado, 29 de diciembre de 1978.

sin que llegue a ser una vulneración del derecho fundamental, se han establecido unos requisitos y unos límites que se han de cumplir.

Una vez contemplado su reconocimiento en nuestro ordenamiento jurídico, también podemos encontrarlo en la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948, en el Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales, de 4 de noviembre de 1950 o bien, en el Pacto Internacional de Derechos Civiles y Políticos, de 19 de diciembre de 1966. Aunque, recientemente se ha incluido en el art. 7 de la Carta de Derechos Fundamentales de la Unión Europea, bajo la rúbrica *"Respeto de la vida privada y familiar que toda persona tiene el derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".*

Como hemos señalado, este derecho se encuentra en el art. 18 CE junto a otros derechos fundamentales con los que mantiene una relación en común pues, también intentan garantizar la protección de la privacidad del sujeto en su esfera más íntima. Asimismo, el art. 12 de la Declaración Universal de Derechos Humanos menciona:

> *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".*[3]

El acelerado avance en las nuevas tecnologías nos obliga a realizar una nueva interpretación del concepto de comunicación y, por ende, una nueva visión del objeto de protección del derecho fundamental al secreto de las comunicaciones. Nos encontramos ante una era digital que, en su visión positiva, nos proporciona un fácil acercamiento con nuestros allegados pero que, en un aspecto negativo, trae consigo nuevos hechos ilícitos.

Para que entre en acción el ejercicio del secreto a las comunicaciones es necesario el empleo de un medio de comunicación, como puede ser un teléfono o una postal telegráfica, pues la simple conversación directa entre dos personas no se encuentra protegida por este derecho.

[3] Declaración Universal de Derechos Humanos, 10 de diciembre de 1948.

Los nuevos medios de comunicación otorgan tanto a los poderes públicos como a los particulares el acceso a unas herramientas que pueden llegar a poner en peligro el secreto de las comunicaciones.

Dejando a un lado su fundamentación legal, cuando llevamos a cabo el análisis de un derecho fundamental, en este caso, el secreto a las comunicaciones, perteneciente al ámbito privado, la titularidad del derecho recaerá en toda persona física o jurídica, nacional o extranjera y, además, también lo serán los menores de edad, como así se recoge en el artículo 4 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor. Como es lógico, los padres o tutores deberán respetarlo y protegerlo frente a los ataques que pudieran surgir.

ELVIRA PERALES establece que son titulares del derecho: *"Cualquier persona física o jurídica, nacional o extranjera. En efecto, este derecho protege a cualquier tipo de persona de las injerencias que puedan sufrir por parte de poder público. En el caso de las personas jurídicas, al considerar nuestro sistema el art. 18.3 CE como un derecho de contenido formal y no material, vinculado a la intimidad, hace que resulte aún más fácil atribuirles la titularidad del derecho".*[4]

En cuanto al ámbito o bien constitucionalmente protegido, y así poner fin a este apartado, debemos señalar que como garantía del derecho al secreto de las comunicaciones nos referimos a toda comunicación que se mantenga o se haya mantenido en el tiempo, independientemente de su contenido.

Además de protegerse el contenido de una conversación, también lo es el medio que se utiliza para llevarla a cabo y, por supuesto, sus circunstancias, es decir, se protege todo aquel proceso y libertad de comunicación sin tener en cuenta la técnica utilizada.

El Tribunal Constitucional, en relación con los terceros ajenos a la comunicación, afirma de forma clara:

> "*No hay «secreto» para aquel a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el artículo 18.3 de la Constitución la retención, por cualquier medio, del contenido del mensaje […]. Quien entrega a otro la carta recibida o quien emplea*

[4] ELVIRA PERALES, A., "Titularidad y eficacia del derecho" en El derecho al secreto de las comunicaciones, Breviarios jurídicos, Madrid, 2007, págs.19-23

durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera «íntima» del interlocutor, pudiesen constituir atentados al derecho garantizado en el artículo 18.1 de la Constitución".[5]

3. CONCEPTO DE INTERCEPTACIÓN DE LAS COMUNICACIONES

El concepto de interceptación de las comunicaciones manifiesta la intromisión en una conversación entre varios sujetos a través de algún medio de comunicación. Este tipo de comunicaciones se encuentran dentro de la esfera íntima y privada de la persona, la cual se protege y garantiza por medio del derecho fundamental al secreto de las comunicaciones del artículo 18 CE.

El Tribunal Supremo desarrolla el concepto de la interceptación de las comunicaciones telefónicas y telemáticas, como:

"*Una diligencia de investigación, acordada por la autoridad judicial en fase de instrucción, ejecutada bajo el control y supervisión del órgano jurisdiccional competente y acordada con el objeto de captar el contenido de las comunicaciones del sospechoso o de otros aspectos del 'iter' comunicador, con el fin inmediato de investigar un delito, sus circunstancias y autores y con el fin último de aportar al juicio oral materiales probatorios "bien frente al imputado, bien frente a otros con los cuales éste se comunique".*[6]

Las comunicaciones mantenidas entre dos o más personas a través de los dispositivos electrónicos pueden llegar a considerarse, desde el punto de vista de una investigación, como una medida de interceptación de las comunicaciones, tanto telefónicas como telemáticas. Esta diligencia de investigación se lleva a cabo en la fase de instrucción que se encuentre en curso en una investigación penal.

[5] STC 114/1984, de 29 de noviembre (fundamento jurídico 7).

[6] STS nº 246/1995, de 20 de febrero (fundamento jurídico 3).

Para poder poner en marcha esta medida debemos dirigirnos hasta su regulación que, tras la reforma de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, podemos localizarla en el Capítulo V del Título VIII del Libro II, desde el art. 588 ter a) hasta el art. 588 ter m), constando de tres secciones.

En consecuencia del avance tecnológico y de los medios de comunicación empleados, la medida de investigación nombrada anteriormente, ya se encontraba regulada en nuestra LECrim, concretamente en su artículo 579.1.

Esta regulación comenzó a ser deficiente y desfasada en el momento en el que las nuevas tecnologías entran, de forma potencial, en nuestra vida diaria.

El Capítulo V, es un capítulo redactado por el legislador, donde se ha plasmado las exigencias requeridas por el Tribunal Europeo de Derechos Humanos, por el Tribunal Constitucional y por el Tribunal Supremo. A partir de esta nueva redacción, se ha establecido una garantía y una regulación legal de la interceptación de las comunicaciones telefónicas y telemáticas.

Sin embargo, el art. 588 ter a) establece cuál debe ser el objeto de la investigación para así poder autorizar la medida llevada a cabo por el Juez para investigar los delitos estipulados en el art. 579 LECrim:

1. Delitos dolosos castigados con pena con un límite máximo de, al menos, tres años de prisión.

2. Delitos cometidos en el seno de un grupo u organización criminal.

3. Delitos de terrorismo.

4. O bien, aquellos delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación.

Finalmente, podemos realizar una distinción entre una comunicación telefónica que, como bien su nombre indica, se realiza a través de un teléfono y, por otro lado, entre una comunicación telemática, donde el medio de comunicación empleado puede ser tanto un ordenador o tablet como una comunicación postal o telegráfica entre otros.

RICHARD GONZÁLEZ aclara esta distinción:

«Se podría distinguir, según un criterio de familiaridad conceptual, como telefónica la comunicación oral a distancia mediante dispositivos electrónicos que identificamos con un terminal telefónico y la telemática aquella que incluye comunicación oral, de imágenes o datos, que puede tener lugar por los mismos dispositivos u otros como son computadoras, «tablets» u otros variopintos dispositivos, como pueden ser las cámaras fotográficas, que pueden incluir sistemas de wifi y que pueden por tanto transmitir datos susceptibles de intervención judicial». [7]

4. DISPOSICIONES COMUNES A LOS MEDIOS DE INVESTIGACIÓN TECNOLÓGICA

La LO 13/2015, de 5 de octubre, introduce por el apartado trece del artículo único de esta, la reforma de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Esta modificación llegó con la intención de poner fin a las graves deficiencias que, desde hacía años, arrastraba nuestra legislación procesal en el ámbito de la limitación del derecho fundamental al secreto de las comunicaciones en la investigación de comportamientos delictivos.

Las medidas de investigación tecnológica se hallan recogidas en el Capítulo IV, Título VIII del Libro II bajo la rúbrica de *"Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos",* comprendidas entre los artículos 588 bis a) al 588 bis k).

Las medidas deben estar fundadas en una base real de que se haya cometido un delito, es decir, deberán estar fundadas por indicios o sospechas de carácter racional. En palabras de la jurisprudencia del Tribunal Supremo se exige la existencia de datos *"objetivos, serios*

[7] RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», Diario La Ley, nº. 8808, 2016, págs. 3-4.

y contrastados…" en la solicitud de la intervención, o que "…se cuente con la noticia racional del hecho delictivo que se quiere comprobar y de la probabilidad de su existencia". [8]

Estas disposiciones comunes tratan de localizar al autor o a los autores del delito cometido pero, para que se puedan llevar a cabo es necesario una autorización judicial que cumpla, primeramente, los requisitos establecidos en los principios rectores recogidos en el art. 588 bis a) 2º al 5º.

Claro está que estas disposiciones no solo se encuentran basadas en unos principios rectores sino que, es necesario que se cumplan otros requisitos, también regulados en este capítulo, como lo son la solicitud de la autorización y su resolución judicial, el secreto y la afectación de terceras personas, su duración y su posible solicitud de prórroga, su control judicial, el cese de la medida, la destrucción de registros o bien, la utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales. De todas ellas nos encargaremos más adelante.

4.1. Principios rectores

En nuestro ordenamiento jurídico aparecen unos principios que ayudan a dar certeza y seguridad a todos los ciudadanos para que en ningún momento se encuentren en una situación de arbitrariedad frente a las posibles injerencias que se puedan llevar a cabo en nuestros Tribunales.

Por ende también, a estos principios se les conoce como "inspiradores" ya que, tratan de inspirar cuando infunden en las diligencias previas de investigación penal limitativas de los Derechos Fundamentales, y dentro de estas, las intervenciones telefónicas y telemáticas. Dichos principios vienen contenidos en el artículo 588 bis a) de la LECrim.

Las medidas de investigación o bien, la concurrencia de unos requisitos que establece la reforma de la LECrim de 2015 se podrá acordar durante la instrucción siempre y cuando medie una autorización o resolución judicial, donde el juez determinará la naturaleza y extensión de la medida en relación con la investigación concreta y con los resultados esperados.

[8] STS 232/1998, de 20 de febrero.

Dicha autorización será dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

a) Principio de especialidad.

El principio de especialidad encuentra su regulación en el apartado 2º del art. 588 bis a) LECrim. En él se refleja la exigente relación que debe existir entre la medida y la investigación de un delito concreto. Aquellas medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva, no podrán autorizarse.

En palabras de LÓPEZ-BARAJAS PEREA *"el principio de especialidad exige que la actuación de que se trate tenga por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose las medidas de investigación tecnológica de naturaleza prospectiva que supondrían una autorización en blanco. No bastan meras conjeturas, hipótesis subjetivas o sospechas genéricas o difusas, sino que deben existir indicios objetivamente fundados. Nos encontramos ante una medida post delictum, dictada una vez que ha llegado al Juez la notitia criminis."*[9]

Por tanto, es mera necesidad que la medida se dirija a la investigación de la actividad criminal o delictiva, es decir, es necesario estar basado en hechos realmente punibles en el momento en el que se pretende interceptar las comunicaciones pues, no está permitido el uso de estas medidas para ver qué se descubre. La medida no podrá acordarse para la investigación de otros tipos de delitos que no estén establecidos en el art. 579.1 LECrim.

b) Principio de idoneidad.

Este principio viene contenido en el apartado tercero del artículo 588 bis a), el cual servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad.

[9] LÓPEZ-BARAJAS PEREA, I., *"Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley",* ed. UNED, Revista de Derecho Político, Nº 98, enero de 2017, págs. 91-119.

Por ámbito objetivo, entendemos que son los delitos por los que procede la medida. En cuanto al subjetivo, se entiende que se podrá acordar la medida aunque esta afecte a terceras personas como recoge el art. 588 bis h). Y, la duración de la medida podrá prorrogarse siempre y cuando se consiga lo estrictamente necesario para la investigación.

Esta medida deberá asegurar la obtención de pruebas y de que la duración no se exceda o sobrease del plazo establecido pues estaríamos vulnerando los derechos del investigado. Solo así la medida será idónea y útil.

c) Principios de excepcionalidad y necesidad.

En aplicación de estos principios, dice el artículo 588 bis a) en su apartado tercero que, solo podrá acordarse la medida: a) cuando en atención a las características, no estén a disposición de la investigación otras medidas menos gravosas para los derechos fundamentales del investigado o encausado; o b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito, se vea gravemente dificultada sin el recurso a esta medida.

LÓPEZ-BARAJAS PEREA, hace hincapié en que *"la excepcionalidad exige que no estén a disposición de la investigación otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles para el esclarecimiento de los hechos (art. 588 bis a 4 LECrim)".*[10]

Por tanto, el juez no deberá autorizar medidas de investigación condicionantes cuando existan otras vías menos invasivas para los derechos fundamentales del investigado.

d) Principio de proporcionalidad

Establece el artículo 588 bis a) en su apartado quinto de la LECrim que las medidas de investigación solo serán consideradas proporcionadas cuando el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés

[10] LÓPEZ-BARAJAS PEREA, I., *"Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley",* ed. UNED, Revista de Derecho Político, Nº 98, Enero de 2017, págs. 91-119.

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.

Este precepto trata de encontrar no solo las concretas circunstancias del caso sino que, las medidas de investigación deben ser proporcionadas pues, cuando el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros.

La doctrina del Tribunal Constitucional lo ha venido exponiendo, constatando tres requisitos, el primero sería la idoneidad de la medida, el segundo sería la necesidad de esa medida y el tercero si esa medida es equilibrada. [11]

Además, LÓPEZ-BARAJAS PEREA considera *"en el juicio de proporcionalidad acerca de la interceptación de las comunicaciones, junto a la gravedad de la pena y a la entidad del bien jurídico protegido, también puede ponderarse la incidencia del uso de las tecnologías de la información y de la comunicación. Podrán acordarse estas medidas respecto de aquellas modalidades delictivas que se sirven de las posibilidades de anonimato que brinda Internet para su comisión y difusión, siempre que se produzca una mínima gravedad o relevancia social".*[12]

4.2. Solicitud de la autorización y resolución judicial

En el presente apartado analizaremos la solicitud judicial y su posterior reflejo en la resolución judicial que habilita la medida de investigación tecnológica.

La reforma llevada a cabo por la LO 13/2015, en su Preámbulo, mantiene los aspectos formales tanto de la solicitud como el contenido de la resolución. Además, el legislador considera muy importante que el derecho fundamental al secreto de las comunicaciones se encuentre protegido y, es por ello por lo que, presta demasiada atención a todos los extremos en el momento de la adopción de la medida.

---

[11] STC 204/1996, de 16 de diciembre de 1996.

[12] LÓPEZ-BARAJAS PEREA, I., *"Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley",* ed. UNED, Revista de Derecho Político, Nº 98, Enero de 2017, págs. 91-119.

Dicha solicitud de autorización judicial debe instarse a un órgano jurisdiccional, generalmente el que ha iniciado la instrucción. Además, la solicitud regulada en el artículo 588 bis b) LECrim, deberá incluir una previa valoración de los principios rectores nombrados anteriormente. Esta es una habilitación legal para que el proceso penal pueda obtener información de carácter relevante derivada de las comunicaciones telefónicas y telemáticas.

En cuanto a la legitimación, se encuentra establecido en el art. 588 bis b) en su apartado primero de la LECrim, por el cual entendemos que será el juez instructor aquel que pueda acordar las medidas reguladas en este capítulo de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. El Legislador establece cuáles son los sujetos legitimados para instar la medida. Además del Ministerio Fiscal y la Policía Judicial, el propio Juez de Instrucción podrá adoptarla de oficio.

En cuanto al concepto de Policía Judicial debemos incluir, según lo previsto en las leyes y su desarrollo por la Jurisprudencia del Tribunal Supremo a las policías autonómicas y al Servicio de Vigilancia Aduanera. Aunque el artículo exponga solo estos sujetos, no se impide que tanto la acusación particular como la popular, planteen al Juez la adopción de la medida.

Por otro lado, el contenido que debe presentar la solicitud de la medida viene establecido en el artículo 588 bis b) apartado 2. Cuando el Ministerios Fiscal o la Policía Judicial soliciten del juez de instrucción una medida de investigación tecnológica, la petición habrá de contener:

1º) La descripción del hecho objeto de investigación y de la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2º) La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo con 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.

3º) 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.

4º) La extensión de la medida con especificación de su contenido.

5º) La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6º) La forma de ejecución de la medida.

7º) La duración de la medida que se solicita.

8º) El sujeto obligado que llevará a cabo la medida, en caso de conocerse.

Todo lo expuesto en el párrafo anterior presenta una bilateralidad con los extremos regulados en el art. 588 bis c) apartado tercero de la LECrim.

Con respecto al contenido de la resolución judicial, ARMENTA DEU dice que *"la resolución será mediante auto motivado, habiendo antes oído al Ministerio Fiscal, y en un plazo no superior a veinticuatro horas desde que se presente la solicitud. Dicho plazo podrá interrumpirse para ampliar o aclarar los términos de la solicitud siempre que resulte necesario resolver sobre la solicitud de autoridad judicial".*[13]

El artículo 141 de la LECrim impone la necesidad de que aquellas resoluciones adoptadas por los Juzgados y Tribunales que afecten a derechos fundamentales serán autos. Seguidamente, la resolución judicial requerirá la previa audiencia del MF. La jurisprudencia del TS añade también la importancia de un informe previo del Ministerio Fiscal como requisito de legalidad de la medida pues, la falta de la presentación de este supone un déficit de control en la adopción pero, este informe no siempre es necesario si es el MF el que insta la diligencia.

Al mismo tiempo, el artículo 588 bis c), apartado número 3, manifiesta que, la resolución judicial que autorice la medida concretará al menos los siguientes extremos:

a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida.

b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido.

c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a).

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

---

[13] ARMENTA DEU, T., Lecciones de derecho procesal penal, ed. Marcial Pons, Madrid, 2019, págs. 198-199.

e) La duración de la medida.

f) La forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida.

g) La finalidad perseguida con la medida.

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

Una vez descrito lo regulado en el anterior artículo, debemos hacer referencia al alcance objetivo y subjetivo de la resolución.

Dentro del alcance objetivo, se produce el análisis de los extremos recogidos en los apartados a) y c) del art. 588 bis c) 3. En el apartado a), se hace referencia a los principios de especialidad y proporcionalidad pues, la presencia de estos es exigida para la autorización de la medida, pues el incumplimiento de las previsiones del apartado a) puede llegar a poner en riesgo la aplicación de los principios rectores.

Con respecto a los indicios que recoja la resolución judicial, no bastarán intuiciones policiales ni sospechas "vagas", sino que, deberán ser fundadas en datos objetivos.

Conforme al ámbito subjetivo, el apartado b) del art. 588 bis c, apartado tercero, exige la identidad de los investigados como la de cualquier afectado por la medida, es decir que, la resolución deberá determinar la identidad de estos, siempre y cuando sean conocidos, de no ser así, se reemplazará la identificación por los datos de los que se disponga.

Así mismo y en definitiva, los apartados d) y h) exigen que la adopción de la medida precise la unidad investigadora de Policía Judicial que llevará a cabo la interceptación y, además, al sujeto que se encargará de su realización debiendo colaborar y guardar secreto cuando proceda.

4.3. Secreto y afectación de terceras personas

El siguiente apartado referido al secreto regulado en el artículo 588 bis d) de la Ley de Enjuiciamiento Criminal, perteneciente a las disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, establece que la solicitud y las actuaciones

posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa.

Con este último artículo, la doctrina muestra su disconformidad, pues para que las medidas resulten efectivas, es necesario acordar el secreto de estas y es por ello, por lo que no se entiende que el secreto no se extienda también a la causa.

Hacemos referencia además, a la afectación de terceros del artículo 588 bis h) de la LECrim pues, cabe acordar las medidas de investigación reguladas en los siguientes capítulos 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.

Estos dos preceptos se encuentran relacionados entre sí ya que, es necesario el secreto aun también cuando afecten a terceras personas y además, sea preciso el secreto de su identidad.

4.4.Duración de las intervenciones y solicitud de prórroga

En cuanto al elemento temporal que encontramos en las medidas reguladas en este Capítulo IV, más concretamente, en los preceptos 588 bis e) y f) de la LECrim, la duración de la medida y a la solicitud de prórroga, se encuentra íntimamente relacionada esta última con el apartado 2 del mismo 588 bis e).

El artículo 588 bis e), en su apartado 1, establece que la duración de las medidas se debe especificar para cada una de ellas y que, no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos. Así, ÁGUILA SÁNCHEZ considera que, *"en la ejecución, tanto de las medidas que cuentan con un plazo máximo como de las que no, debe tenerse presente esta aspiración genérica a evitar cualquier exceso en la limitación del derecho fundamental. Para conseguir tal fin, la sujeción a los principios de idoneidad y de proporcionalidad se revela como una guía adecuada".* [14]

Pero una medida que supone la intromisión, como señala el Tribunal Europeo de Derechos Humanos,

[14] ÁGUILA SÁNCHEZ, C., "La interceptación de las comunicaciones telefónicas y telemáticas en el proceso penal", Diario La Ley, Nº 9303, 2018.

"Será legítima cuando media la autorización de un juez de acuerdo con la ley en la esfera propia del derecho fundamental al secreto de las comunicaciones no puede durar indefinidamente, y mucho menos sin que el afectado sepa que se está produciendo una limitación del mismo, vigilándole secretamente; eso nos llevaría a un Estado-policía, intolerable en un sistema democrático incluso para salvaguardar las instituciones". [15]

En los siguientes apartados del artículo, se menciona que la medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron y que, una vez, transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga o, en su caso, finalizada esta, cesará a todos los efectos.

A este precepto debemos añadirle lo establecido y regulado por el artículo 588 ter g) de la LECrim, que hace referencia a la duración máxima de la medida de la intervención, la cual se computará desde la fecha de la autorización judicial que será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses.

Como ya hemos mencionado, la medida podrá ser prorrogada. Dicha solicitud se encuentra regulada en el artículo 588 bis f) de la LECrim. En su apartado primero, la solicitud se dirigirá por el Ministerio Fiscal o la Policía Judicial al juez competente con la antelación suficiente a la expiración del plazo concedido, la cual deberá incluir lo siguiente:

a) Un informe detallado del resultado de la medida.

b) Las razones que justifiquen la continuación de la misma.

En el plazo de los dos días siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante auto motivado. Además, antes de dictar la resolución podrá solicitar aclaraciones o mayor información. Ya concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada.

Por último añadiremos las palabras de ARMENTA DEU sobre un *"aspecto discutido y conexo, como es el de la notificación a los interesados de la medida adoptada, en cuanto supone un conflicto entre la evidente necesidad de que el intervenido desconozca la situación para garantizar una eficacia mínima y el hecho de que constituyéndose el intervenido*

[15] STEDH de 6 de septiembre de 1978 (caso Klass y otros).

en la condición de investigado, como parte procesal, se le deberá dar conocimiento de las actuaciones (arts. 118.I y II y 302.1 LECrim)".[16]

4.5. Control judicial y cese de la medida

Debemos tener en cuenta que, para que la medida sea efectiva, hay que exigir un control judicial a la hora de la ordenación y desarrollo de esta.

Es necesario recalcar pues, que la interceptación telefónica y telemática limita un derecho fundamental. Es por ello por lo que, se exige un efectivo control que se encuentra regulado en el artículo 588 bis g), por el cual entendemos que la Policía Judicial informará al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que este determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma.

Por consiguiente, como nos encontramos ante unas situaciones limitadas por ciertos derechos fundamentales que acogen, en este caso, al investigado, sería de lo más normal el cese de la medida al desaparecer las causas que dieron lugar a su petición y desarrollo.

El artículo 588 bis j, establece que el juez acordará el cese de la medida cuando:

1) Desaparezcan las circunstancias que justificaron su adopción.

2) Cuando resulte evidente que a través de la misma no se están obteniendo los resultados pretendidos.

3) Cuando no haya transcurrido el plazo para el que hubiera sido autorizada.

Con el fin de la medida, a todas aquellas personas afectadas se les proporcionará el derecho de recibir una copia de las grabaciones.

[16] ARMENTA DEU, T., Lecciones de derecho procesal penal, ed. Marcial Pons, Madrid, 2019, págs. 198-199.

4.6.Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales

Como se encuentra establecido en el artículo 588 bis i), la utilización de la información obtenida en un procedimiento distinto y además, aquellos descubrimientos casuales se regularán con arreglo a lo dispuesto en el artículo 579 bis de la LECrim.

Encontramos el precepto mencionado en el apartado anterior, en el Capítulo III, el cual tiene por nombre: *"De la detención y apertura de la correspondencia escrita y telegráfica".* Esta rúbrica se encuentra introducida por el artículo único. 10 de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Acto seguido pasamos a desarrollar el artículo 579 bis introducido en la misma Ley:

- → El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal.
- → A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas la peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen.
- → La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, este comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el dicho secreto se alce.

Como podemos observar, el apartado segundo del precepto citado encontramos una íntima relación con algunos de los artículos anteriormente mencionados, así como la solicitud

de la autorización judicial y de prórroga y aquellas resoluciones judiciales, todas estas mencionadas y regulados en las disposiciones comunes del Capítulo IV de esta Ley, en relación con la interceptación de las comunicaciones telefónicas y telemáticas.

4.7.Destrucción de registros

El objetivo principal de este apartado es que, para garantizar la intimidad del afectado por la medida y así, evitar posibles difusiones posteriores o daños irreparables a este, se regula en el artículo 588 bis k) la destrucción de registros.

Una vez que se ponga término al procedimiento mediante resolución firme, se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Se conservará una copia bajo la custodia del Letrado de la Administración de Justicia.

Además, se acordará la destrucción de las copias conservadas cuando:

- Hayan transcurrido cinco años desde que la pena se haya ejecutado.
- Se haya decretado el sobreseimiento libre.
- Haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del tribunal (art. 588 bis k).

Finalmente, los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados.

5. REGULACIÓN LEGAL DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS

En este apartado, trataremos de ahondar detalladamente en las interceptaciones telefónicas y telemáticas como medida de investigación y, además, cómo el avance de las nuevas tecnologías ha provocado la ansiada reforma de la Ley de Enjuiciamiento Criminal pues, el marco procesal con el que contábamos antes de esta quedó obsoleto por las grandes lagunas legales. A raíz de la necesitada modificación de la ley por las exigencias del Tribunal Constitucional, el Tribunal Supremo y el Tribunal Europeo de Derechos Humanos, el legislador

ha llevado a cabo la elaboración de una ley que ha permitido una reglamentación adecuada de la intervención de las comunicaciones telefónicas y telemáticas.

Para ello, nos ayudaremos de los artículos en los cuales se hace referencia a su regulación en la LECrim y por supuesto, de jurisprudencia y doctrina.

5.1.Fundamento legal

El fundamento legal de esta medida de investigación, lo encontramos en el Capítulo V del Título VIII del Libro II de la LECrim, introducido por el apartado catorce del art. único de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Este capítulo cuenta con tres secciones: la sección 1ª trata las disposiciones generales, la sección 2ª versa sobre la incorporación al proceso de datos electrónicos de tráfico o asociados y la sección 3ª sobre el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

La Sección 1ª comprende desde el art. 588 ter a) hasta el art. 588 ter i), la cual se estructura de la siguiente manera: a) Presupuestos; b) Ámbito; c) Afectación a tercero; d) Solicitud de autorización judicial; e) Deber de colaboración; f) Control de la medida; g) Duración; h) Solicitud de prórroga; i) Acceso de las partes a las grabaciones.

Con respecto a la Sección 2ª, solo se incluye el apartado j) del art. 588 ter de la LECrim, relativo a los datos obrantes en archivos automatizados de los prestadores de servicios.

En el caso de la Sección 3ª, se regulan los apartados k), l) y m), del artículo. El apartado k) hace referencia a la identificación mediante número IP. El l), a la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes y, finalmente, el apartado m), pone de manifiesto la regulación para la identificación de titulares o terminales o dispositivos de conectividad.

A diferencia del punto desarrollado anteriormente, referente a las disposiciones comunes a las intervenciones de las comunicaciones, el Capítulo V se ocupa de un análisis mucho más profundo. Las disposiciones comunes nos ayudan a entender el procedimiento a

seguir en la adopción de la medida, como un esquema o referencia que debemos seguir para ello.

5.2.Delitos habilitantes y prohibición de las intervenciones prospectivas

En cuanto a los delitos habilitantes de la diligencia de investigación, dispone el art. 588 ter a) LECrim que, para que se produzca la autorización judicial, será necesario que la investigación tenga por objeto los delitos del artículo 579.1 de esta ley:

1. Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.

2. Delitos cometidos en el seno de un grupo u organización criminal.

3. Delitos de terrorismo.

4. Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

5.3.Ámbito de aplicación material

En el siguiente apartado hacemos referencia al ámbito de aplicación material u objetivo de la medida, el cual encontramos regulado en el artículo 588 ter b) de la LECrim. En este precepto, encontramos un doble punto de vista pues, no solo es analizado desde un ámbito objetivo sino también desde el ámbito subjetivo establecido en el art. 588 ter b.1), el cual lo desarrollaremos en el apartado siguiente.

Una vez examinado y diferenciado el artículo nombrado en el párrafo anterior, comenzamos con el desarrollo del ámbito objetivo establecido en el apartado segundo del art. 588 ter b).2 el cual menciona que:

"La intervención judicialmente acordada podrá autorizar el 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, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario".[17]

El ámbito de aplicación de este acto de investigación no es nada exacto a la hora de determinar los terminales utilizados por el investigado. La LECrim no establece un límite para concretar ni el titular ni el medio utilizado.

Además, es un requisito indispensable la participación del sujeto, indistintamente de si participa como emisor o receptor de la comunicación. Incluye el legislador, una posible interceptación para casos especiales en los que la víctima corra un grave peligro para su vida o integridad.

Por último y como mera definición de datos electrónicos nombrados en este artículo, se establece que serán aquellos que provoquen como consecuencia, conducir una comunicación al investigado a través de alguna red de comunicación telefónica o telemática de naturaleza análoga.

"Se incluyen por tanto, todos los datos a los que hace referencia el art. 3 de la Ley 25/2007, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, donde se encuadran: la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet; los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación; la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada; la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada; o la línea digital de abonado (DSI) u otro punto terminal identificador del autor de la comunicación, entre otros".[18]

---

[17] L.O. 13/2015, de 5 de octubre, *"de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*", Boletín Oficial Español, Nº 239, de 6 de octubre de 2015, págs. 90192 a 90219.

[18] SANTANA LÓPEZ, S., "La interceptación de las comunicaciones telefónicas y telemáticas", Martell Abogados, de 16 de marzo de 2021.

5.4. Ámbito de aplicación subjetivo y afectación de terceros

Para el desarrollo del siguiente apartado del trabajo, el cual abarca el ámbito subjetivo y la afectación a terceros, debemos hacer referencia a la regulación legal de estos. La subjetividad de la medida a adoptar y la afectación de terceras personas, se encuentran establecidas en los arts. 588 ter b.1) y 588 ter c) de la Ley de Enjuiciamiento Criminal.

Es necesario la distinción entre ambos pues, en el primero de ellos se intenta restringir el derecho fundamental del propio sujeto que está siendo investigado pero, sin embargo, en el segundo lo que se intenta limitar es el derecho de un tercero a través del cual se transmite o se recibe información relevante para la investigación y los hechos delictivos del investigado.

En cuanto al artículo 588 ter b.1) LECrim, el cual establece que: *"Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado".*[19]

El ámbito subjetivo desarrollado por el legislador deja por determinar qué terminales son susceptibles de investigación pues, desde mi punto de vista y desde un punto de vista práctico, podrían ser intervenidos todos aquellos medios de comunicación que el sujeto empleara en cualquier momento. Entiendo que se amplía el ámbito de interceptación cuando el legislador menciona los términos "habitual u ocasionalmente" quedando en suspenso las garantías procesales y el derecho fundamental al secreto de las comunicaciones del art. 18.3 CE, ya que serán objeto de la medida todos los medios de comunicación que pasen por las manos del sujeto.

Referente a la afectación de terceras personas, el art. 588 ter c) LECrim se encarga de limitar el derecho fundamental al secreto de las comunicaciones de terceras personas no investigadas. Podemos encontrarnos ante tres supuestos:

[19] L.O. 13/2015, de 5 de octubre, *"de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*", Boletín Oficial Español, Nº 239, de 6 de octubre de 2015, págs. 90192 a 90219.

- Exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información. Aquellas comunicaciones posibles por intervenir serían tanto las emitidas como las recibidas, en los supuestos en los que la colaboración del tercero no resulte suficiente para dirigir también contra él la investigación como cómplice o cooperador.

- Se incluye la conciencia o voluntariedad de la colaboración del tercero, cuando se trate de familiares.

- Vulneración de las medidas de seguridad de redes informáticas para su uso sin consentimiento o empleo de cualquier tipo de programa maligno que controle dispositivos ajenos con el fin de utilizarlos para entablar conversaciones, como las técnicas de desvío de llamadas o uso fraudulento de la conectividad, pudiéndose ampliar la medida, siempre y cuando se encuentre acreditada su relación con el investigado.

En relación con el segundo supuesto del artículo, podrá acordarse la medida, siempre y cuando se encuentre probado que el titular del terminal y el investigado, colabore o se beneficie de los fines ilícitos de este.

Por otro lado, la doctrina del Magistrado RODRÍGUEZ LAINZ, menciona que: *"Al igual que el art. 588 ter c de la LECrim., permite la interceptación de determinados terminales de uso por terceras personas, sin que los mismos participen necesariamente en su condición de codelincuentes o de alguna concreta infracción criminal relacionada con un objeto de investigación, el mencionado § 106 abre las puertas a la expansión de tal círculo a datos sobre comunicaciones de terceras personas; siempre que por otros motivos tal conservación pudiera contribuir a la lucha contra la delincuencia que justifica su adopción. El § 119 vuelve a insistir en esta línea de apertura cuando habla por una parte de la posibilidad de incidir no solo en quienes se sospeche que planean, van a cometer o han cometido un delito grave, sino también en aquellas personas que puedan estar implicadas de un modo u otro en un delito grave. Apertura a terceros que, al menos en los supuestos de actividades terroristas que pudieran amenazar a la seguridad nacional, la defensa o la seguridad pública, procedería sin duda «…cuando existan elementos objetivos que permitan considerar*

que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra dichas actividades»".[20]

Finalmente, debemos dar importancia al primer párrafo de este artículo pues, aquí el sujeto investigado utiliza el terminal de un tercero totalmente ajeno e inconsciente de los fines llevados a cabo. Se impone la necesidad de una mayor motivación de la resolución judicial habilitante, pues se está limitando el derecho fundamental de un tercero ajeno no responsable de la actividad delictiva, por el principio de proporcionalidad, necesidad y excepcionalidad, los cuales exigen una mayor justificación, debiendo reflejarse además de indicios suficientes, la relación del investigado con el medio o la persona que transmite o recibe la información, y la importancia de esa interceptación para los fines de la investigación.

5.5. Deber de colaboración con las autoridades y de guardar secreto

Para poder llevarse a cabo la interceptación de las comunicaciones es necesario tener en cuenta el art. 588 ter e) de la Ley de Enjuiciamiento Criminal, por el cual se impone tanto el deber de colaboración y asistencia como el de guardar secreto.

Este precepto se encuentra relacionado con los arts. 588 bis b.2.8º y 588 bis c.3.h), es decir, a la solicitud y resolución judicial para el acuerdo de la medida. Además, si es posible, deberá darse a conocer la identidad del sujeto obligado.

Por otro lado, se hará referencia al art. 39.1 LGT, en cual se aclara cuáles son los sujetos obligados a colaborar:

- Prestadores y operadores de servicios y acceso a redes de telecomunicaciones.

- Aquellos prestadores que mantengan un lugar de Internet por el cual se establezcan contrataciones de bienes y servicios.

- Cualquier sujeto que ayude al traspaso de las comunicaciones a través de algún medio electrónico.

En esta obligación legal es posible que surja algún tipo de problema de jurisdicción como suelen ser los prestadores de servicios que se encuentren fuera de España. El criterio

[20] RODRÍGUEZ LAINZ, J.L., "La definitiva defenestración de la Ley Española sobre conservación de datos relativos a las comunicaciones", Diario La Ley, Nº 8901, 2017.

por el cual se rige el Juez se determina en el art. 2.4 LSSICE y es que, precisa cuando un servicio está establecido en territorio español:

- Cuando su residencia o domicilio social o bien, donde se realice la gestión o dirección del servicio, se encuentre en España.

- Cuando el servicio prestado se realice en un establecimiento situado en territorio español.

- Cuando se encuentre inscrito en el Registro Mercantil o en cualquier registro público.

Por último, se consideran acreedores del deber de colaboración, el Juez, el Ministerio Fiscal y el cuerpo de la Policía Judicial.

Finalmente, la necesidad de guardar secreto se debe a que puede llegar a ver afectada, de manera asegurada, la investigación si la persona investigada tuviera conocimiento. El incumplimiento de estas obligaciones dará lugar a un delito por desobediencia.

5.6. Solicitud de autorización judicial

Cuando a instancia del Ministerio Fiscal o de la Policía Judicial se solicite al Juez de instrucción la adopción de la medida de investigación tecnológica, esta debe contener, además del hecho y la identidad del sujeto investigado, otros requisitos específicos establecidos en el art. 588 ter d) 1 de la Ley de Enjuiciamiento Criminal:

En primer lugar, la identificación del número de abonado, del terminal o de la etiqueta técnica.

En segundo lugar, la identificación de la conexión con el objeto de la intervención.

Y por último, en el apartado c) se mencionan los datos necesarios para la identificación del medio de comunicación de que se trate.

Por otro lado, el art. 588 ter d.2 LECrim determina la extensión de la medida, pudiendo contener la solicitud como objeto:

→ El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.

→ El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

→ La localización geográfica del origen o destino de la comunicación.

→ El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos.

En caso de urgencia, dice ARMENTA DEU: *"Cuando las investigaciones afecten a delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible el registro o cualquiera de las medidas acabadas de citar, podrá ordenarla el Ministro del Interior o en su defecto el Secretario de Estado de Seguridad, comunicándolo inmediatamente al juez competente, y en todo caso en el máximo de 24 horas, haciendo constar las razones que justifican la adopción de la medida y la forma en que se ha efectuado, así como su resultado.*

El juez competente revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fuera ordenada la medida".[21]

5.7. Control judicial de la medida

El artículo 588 ter f) de la Ley de Enjuiciamiento Criminal, en relación con el control judicial de la medida y su previsión general establecida en el art. 588 bis g), dispone unas medidas concretas para hacerlo efectivo:

- Información por parte de la Policía Judicial al Juez de Instrucción del desarrollo y resultados de la medida, así como cuando se ponga fin a la causa.
- La Policía Judicial deberá informar al Juez del desarrollo de la medida con la periodicidad y forma que este determine.
- La Policía Judicial pondrá a disposición del Juez, soportes digitales distintos; uno con la transcripción de los pasajes que considere de interés y el otro, con las grabaciones íntegras realizadas.
- En las grabaciones se señalará el origen y destino de cada una.

[21] ARMENTA DEU, T., Lecciones de derecho procesal penal, ed. Marcial Pons, Madrid, 2019, págs. 198-199.

- Por último, la Policía Judicial deberá asegurar la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.

Cabe destacar la Circular de la FGE cuando hace referencia al contenido de cada soporte digital: "*El precepto establece diferente contenido para cada uno de los dos soportes digitales; las grabaciones íntegras en uno (tanto de conversaciones como SMS u otras formas de comunicación intervenidas) y solamente las de interés en el otro, aunque, en este último caso, no necesariamente en formato de audio, siendo suficiente y necesaria su transcripción. Con ello, al propio tiempo, está excluyendo la transcripción de la totalidad de las grabaciones. La transcripción de los pasajes de interés, que será lo que va a tener relevancia en el procedimiento, podrá cotejarse, en su caso, con las grabaciones recogidas en el otro soporte. Además, ante el silencio del precepto, la transcripción podrá ser literal o en extracto, de ahí la importancia del cotejo en aquellos casos en los que vayan a ser utilizadas como prueba en el proceso, toda vez que, por mucho que se certifique la autenticidad de los soportes digitales, la transcripción es una labor no automatizada, que llevarán a cabo los agentes encargados de la investigación".*[22] Los soportes digitales mantienen un papel fundamental a la hora de la adopción de la medida pues, no solo servirán para hacer efectivo el control judicial de esta sino que también, introducirá la prueba en el acto del juicio oral.

Es necesaria además, la homologación judicial cuando el legislador se refiere a asegurar *"la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas"* y, presentar copia de estas.

Finalmente, hacemos referencia al sistema más conocido para la interceptación de las comunicaciones, el cual será desarrollado más adelante: "Sistema Integrado de Interceptación Telefónica" o "SITEL".

[22] FISCALÍA GENERAL DEL ESTADO, "Circular 2/2019 sobre la interceptación de comunicaciones telefónicas y telemáticas", BOE, Nº 70, 22 de marzo de 2019, págs. 30091-30120.

5.8. Duración de la medida y su prórroga

En este apartado se llevará a cabo el desarrollo de la perdurabilidad o duración de la medida y su solicitud de prórroga y su relación con los arts. 588 bis e) y f) y los artículos 588 ter g) y h) de la Ley de Enjuiciamiento Criminal.

Con respecto a la duración de la medida, el art. 588 bis g) no establece un tiempo delimitado sino que, será aquel que se especifique para cada una de ellas y el necesario para el esclarecimiento de los hechos. Sin embargo, el art. 588 ter g) si proporciona un límite de 3 meses prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses, contando desde la fecha de autorización judicial.

Dicha extensión de la medida estará basada en los principios rectores del art. 588 bis a) de la LECrim, tomando más importancia aún el principio de proporcionalidad pues, dependiendo de la gravedad del asunto investigado junto al desarrollo de la investigación, esta podrá sobrepasar los plazos de duración establecidos.

Además, el cómputo del plazo se deberá iniciar desde la fecha en la cual el Juez autoriza la interceptación y no desde la fecha efectiva de esta.

Por último, en relación con la perdurabilidad de la medida, la FGE menciona que: "*No quiere esto decir, sin embargo, que los procedimientos en los que se utilice esta medida de investigación deban concluir a los dieciocho meses de su adopción. La duración que se fija es para la medida de intervención de las comunicaciones, no para la tramitación del procedimiento".*[23]

Por otro lado, en cuanto a la solicitud de prórroga que indican los arts. 588 bis f) y 588 ter h) de la LECrim, dice SANCHÍS CRESPO:

"*La solicitud de prórroga, según indica el art. 588 bis f), núm. 1, LECrim, se dirigirá al juez competente con la antelación suficiente a la expiración del plazo concedido y deberá incluir un informe detallado del resultado de la medida y las razones que justifiquen la continuación de la misma.*

[23] FISCALÍA GENERAL DEL ESTADO, "Circular 2/2019 sobre la interceptación de comunicaciones telefónicas y telemáticas", BOE, Nº 70, 22 de marzo de 2019, págs. 30091-30120.

El art. 588 ter h) da cuenta de cuáles pueden ser los fundamentos que aconsejen prorrogar la interceptación:

1) La transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.

2) Las aclaraciones que eventualmente solicite el juez que pueden incluir el contenido íntegro de las conversaciones intervenidas".[24]

Con anterioridad a la aprobación de la prórroga, se encuentra prevista en la Ley la posibilidad de que el Juez pida ciertas aclaraciones o mayor contenido de la información referente al transcurso de la intervención, siendo necesario presentar ante este, la solicitud con al menos tres días de antelación para evitar así el cumplimiento del plazo de dos días para la aprobación de la misma, como establece el artículo 588 bis f).2.

5.9. Acceso de las partes a las grabaciones

El acceso a las partes de las grabaciones se encuentra regulado en el artículo 588 ter i) de la LECrim, último precepto elaborado de la Sección Primera del Capítulo V de esta.

Este artículo regula el derecho de las partes a obtener acceso a las grabaciones, siempre y cuando se den las dos condiciones exigidas: el alzamiento del secreto y la expiración de la vigencia de la medida. Aquellos sujetos que hayan sido parte de la práctica de la injerencia, se les proporcionará copia tanto de las grabaciones como de las transcripciones realizadas. En ningún caso, las transcripciones podrán ser exigidas al Juez de Instrucción pues de estas se hace cargo la Policía Judicial.

Cuando coincidan varias interceptaciones, se levantará el secreto una vez acabada la última medida. A partir de ese momento, podrán ser recurridos los autos que la concedieron o prorrogaron.

En el caso de que en las grabaciones se encontrasen datos referidos a la vida íntima de los sujetos investigados, solo serán entregados las partes que no se refieran a ellos, debiendo constar que no se proporciona la totalidad de la grabación o transcripción. Serán

[24] SANCHÍS CRESPO, C., "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas", La Ley penal: revista de derecho penal, procesal y penitenciario, Nº 125, 2017.

excluidas también, las copias de toda aquella comunicación establecida entre el investigado y letrado (art. 118.4 LECrim).

Por otro lado, es posible que por el alto contenido de información almacenado en los soportes, las partes puedan solicitar la incorporación de datos que consideren relevantes y no se encuentren en las copias de las grabaciones. El juez de instrucción examinará por sí mismo las comunicaciones, decidiendo su exclusión o inclusión en la causa.

Finalmente, el apartado tercero del artículo 588 ter i) dispone que aquellas terceras personas interceptadas en las comunicaciones tendrán derecho de ser notificadas por el juez de la práctica llevada a cabo y sus participaciones en ellas. Además, será posible la entrega de una copia de la grabación o transcripción si la parte informada lo solicita siempre que no afecte a la intimidad de los demás sujetos o resulte contrario a la finalidad del proceso en que hubiera sido adoptada la medida.

5.10. Incorporación al proceso de datos electrónicos de tráfico o asociados

La incorporación al proceso de datos electrónicos de tráfico o asociados se encuentra regulada en la Sección Segunda del Capítulo V del Libro II, introducidos por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. En dicha sección se establece el artículo 588 ter j) sobre los "datos obrantes en archivos automatizados de los prestadores de servicios".

Debemos tener presente que la intención del precepto es simplemente, la incorporación de estos datos en el proceso penal pues en su apartado primero se limita a establecer la necesidad de autorización judicial y no de distinguir los sujetos que se encuentran obligados a preservar los datos, como pueden ser los prestadores de servicios, las personas obligadas por la legislación sobre retención de datos relativos a las comunicaciones electrónicas o cualquier otra persona o entidad que pueda poseerlos por motivos comerciales o de otra índole.

Otros preceptos para tener en cuenta para la delimitación e identificación de algunos datos de tráfico son el art. 3 de la Ley 25/2007, de 18 de octubre, "*de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"* y el art. 39 LGT.

Menciona la Circular 2/2019 sobre "la interceptación de comunicaciones telefónicas y telemáticas", en particular el art. 3 de la Ley 25/2007:

"En particular, el art. 3 de la Ley 25/2007 enumera los datos respecto de los que establece el deber de conservación distinguiendo seis categorías: a) Datos necesarios para rastrear e identificar el origen de una comunicación. b) Datos necesarios para identificar el destino de una comunicación. c) Datos necesarios para determinar la fecha, hora y duración de una comunicación. d) Datos necesarios para identificar el tipo de comunicación. e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación. f) Datos necesarios para identificar la localización del equipo de comunicación móvil".[25]

Por último, el art. 588 ter j 2) LECrim, determina la necesidad de precisar los datos que resulten indispensables para la investigación y para la solicitud que será presentada ante el juez competente para recabar la información contenida en los archivos automatizados de los prestadores de servicios.

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

El siguiente y último apartado del Capítulo V, lo encontramos en la Sección 3ª, concretamente en los artículos 588 ter k), l) y m) de la Ley de Enjuiciamiento Criminal, teniendo como rúbrica *"el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad".*

Para la prevención y descubrimiento de aquellos delitos cometidos a través de las comunicaciones telefónicas y telemáticas, es necesaria la identificación de los usuarios que los llevan a cabo. Para ello, la LECrim establece diferentes métodos de investigación siempre y cuando no se interfiera en los derechos fundamentales del sujeto y cumpliendo la normativa, los principios establecidos en el art. 588 bis a).

[25] FISCALÍA GENERAL DEL ESTADO, "Circular 2/2019 sobre la interceptación de comunicaciones telefónicas y telemáticas", BOE, Nº 70, 22 de marzo de 2019, págs. 30091-30120.

El artículo 588 ter k) regula la identificación mediante número IP. Antes de adentrarnos en la regulación legal de este, me gustaría explicar de qué se trata un número o dirección IP.

→ "Dirección IP" o "Dirección del Protocolo de Internet": se trata de un conjunto de números o normas para poder establecer una comunicación a través de una red, cualquiera que sea el medio utilizado para ello. A través de ella, se puede llegar a identificar una red o un dispositivo en Internet.

Una vez analizado el concepto de IP, encontramos regulado en el precepto nombrado que si la Policía Judicial no pudiera tener acceso a esa dirección para la identificación del sujeto que está cometiendo el delito a través de sus propios medios, podrá solicitar al Juez de Instrucción que requiera a los sujetos obligados el deber de colaboración proporcionando los datos de identificación y localización del terminal o dispositivo.

Otro de los métodos para obtener acceso a los datos de identificación por parte de la Policía Judicial cuando no le haya sido posible la identificación de un número de abonado a través de los medios utilizados comúnmente, es la utilización de "artificios técnicos", como el IMSI o IMEI para conseguir los códigos necesarios (art. 588 ter l).

Ya obtenidos los códigos, la Policía Judicial deberá seguir el proceso de solicitud de autorización judicial establecido en el art. 588 ter d), debiendo dictar el tribunal una resolución motivada con la decisión a adoptar, siguiendo los plazos del art. 588 bis c).

Antes de analizar el precepto siguiente, veo necesario adentrarnos un poco más en los dos casos particulares nombrados recientemente. En concreto vamos a hablar del IMSI y el IMEI.

→ IMSI (International Mobile Subscriber Identity): Se trata de un número único asignado a la tarjeta SIM con una longitud de 15 dígitos habitualmente, a través del cual podemos averiguar el país y la red móvil.

LÓPEZ-BARAJAS PEREA considera que la jurisprudencia oscila entre dos situaciones respecto a la naturaleza jurídica del IMSI, sobre todo en base al art. 18.3 CE, *"quedando protegido por el secreto de las comunicaciones, puesto que a través de dicho código alfanumérico, se produce el mismo efecto que la propia injerencia en el ámbito del secreto". En segundo lugar entiende que no está protegido por el secreto de las comunicaciones debido a que se trata de "una técnica que no afecta al núcleo del 18.3 CE, ya que a priori, no permite conocer la identidad del comunicante, la propiedad del teléfono, ni la relación de llamadas efectuadas, entre otros, además de que dicho dato puede obtenerse con posterioridad a la comunicación".*[26]

→ IMEI (International Mobile Equipment Identity): Numeración única asignada a cada teléfono móvil en su interior. Se configura también de 15 dígitos. El problema de este método es que no siempre se obtienen los datos esperados pues, solo prueba la autenticidad del teléfono y no el titular de este.

La Circular 1/2013, de 11 de enero, concluye sobre ambos conceptos con una simple relación: *"Tanto el IMEI como el IMSI carecen de capacidad de información sobre la identidad del usuario, teniendo valor probatorio únicamente si se asocia a otros datos en poder de las operadoras".*[27]

Acabamos el apartado con la regulación del art. 588 ter m) sobre la *"identificación de titulares o terminales o dispositivos de conectividad",* el cual solo muestra la facultad tanto del Ministerio Fiscal como de la Policía Judicial para obtener los datos identificativos de cualquier número telefónico o medio de comunicación a través de los prestadores de servicios de telecomunicaciones, ya que tienen el deber de colaborar con la justicia.

[26] LÓPEZ-BARAJAS PEREA, I., "El derecho al secreto de las comunicaciones y las nuevas tecnologías", en la intervención de las comunicaciones electrónicas, Ed. LA LEY, Madrid, Marzo 2011, págs. 27

[27] FISCALÍA GENERAL DEL ESTADO, "Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas", Madrid, 11 enero de 2013.

Dispone finalmente OTAMENDI ZOZAYA una comparación de este precepto con la antigua regulación establecida: *"Este nuevo precepto legal ha superado el criterio establecido en la ley 25/2007, pues en esta norma la obtención de dichos datos estaba sometida a la previa autorización judicial mientras que en este nuevo precepto de la Ley de Enjuiciamiento Criminal la policía o el Ministerio Fiscal podrán obtener dichos datos directamente de las operadoras, sin necesidad de solicitarlos al juez. Conforme a la disposición derogatoria única de la Ley Orgánica 13/2015, las disposiciones de la ley 25/2007 que exigían autorización judicial en estos casos deben entenderse tácitamente derogadas".*[28]

6. EL SISTEMA INTEGRADO DE INTERCEPTACIÓN LEGAL DE LAS COMUNICACIONES (SITEL)

Uno de los grandes avances establecidos en la interceptación de las comunicaciones telefónicas y telemáticas es, sin duda alguna, el Sistema Integrado de Interceptación de las Comunicaciones o también conocido como SITEL.

Según LÓPEZ-BARAJAS, el SITEL *"es un sistema que utiliza un software o aplicación informática instalada en los proveedores de servicios de las redes de telecomunicaciones, una vez introducidos los parámetros de interceptación, no se precisa de intervención humana para realizarla y transmitirla en tiempo real a un centro de interceptación. Esta tecnología permite sustituir la presencia personal usada anteriormente con el magnetófono, por un sistema de grabación provisto de una serie de medidas de seguridad que a juicio de nuestro Tribunal Supremo impiden de manera fehaciente la manipulación de la información interceptada con mayores garantías que en el sistema tradicional de cintas analógicas".*[29]

Este nuevo sistema fue implantado con la intención de solucionar la falta de seguridad en las intervenciones telefónicas y telemáticas realizadas con los antiguos métodos "tradicionales".

---

[28] OTAMENDI ZOZAYA, F., "La ansiada regulación de las llamadas medidas de investigación tecnológica", Ed. Dykinson, Madrid, 2017, pág. 37.

[29] LÓPEZ-BARAJAS PEREA, I., "El procedimiento de intervención: el sistema integrado de interceptación de las comunicaciones (SITEL) y sus garantías" en la intervención de las comunicaciones electrónicas, ed. la ley, 2011, págs. 203-227.

El SITEL consta de un sistema central de almacenamiento, el cual una vez recogida la información que resulta necesaria y ha sido solicitada, la transfiere a un CD/DVD, con el fin de garantizar la autenticidad e integridad de la información. Además, tampoco es posible una modificación o eliminación del contenido porque como establece la Circular 1/2013, de 11 de enero: *"El contenido de las conversaciones y datos asociados queda íntegramente grabado en el Servidor Central del SITEL, y no es posible su borrado sin autorización judicial específica, sin que sea posible su alteración porque queda registrado en el sistema cualquier intento de manipulación y ello de forma indeleble".*[30]

A falta de norma propia, muestra también la fiabilidad y seguridad de este sistema de interceptación, la jurisprudencia del Tribunal Supremo como lo podemos ver reflejado en su Sentencia 573/2012, de 28 de junio de 2012, cuando expresa *"los procedimientos propios del sistema denominado* ***SITEL****, ha de recordarse que, tras un intenso debate acerca del mismo, la mayoría de esta Sala ha considerado dicho modo de proceder como técnicamente fiable, por encima incluso del sistema "tradicional" de grabación de esas comunicaciones".*[31] Además, la Sentencia 250/2009, de 13 de marzo de 2009 lo considera *"un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones"*[32], pues tradicionalmente el método de grabación es totalmente distinto, donde anteriormente las grabaciones se registraban en cintas, ahora son volcadas en CD/DVD automáticamente, sin la necesidad de realizarlo de forma manual. Dispone también la misma Sentencia del Tribunal Supremo que dicho sistema cumple con las garantías constitucionales a través de tres principios de actuación: *"1. Centralización: El servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Guardia Civil, distribuyendo la información aportada por las operadoras de comunicaciones a los distintos usuarios implicados.*

2. Seguridad: El sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio anterior. Existen 2 ámbitos de seguridad:

---

[30] FISCALÍA GENERAL DEL ESTADO, "Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas", Madrid, 11 enero de 2013.

[31] STS (Sala de lo Penal) núm. 573/2012, de 28 de junio de 2012 (RJ 2191/2011).

[32] STS (Sala de lo Penal) núm. 250/2009, de 13 de marzo de 2009 (RJ 10624/2008).

**Nivel central: Existe un ordenador central del sistema para cada sede reseñada, dotado del máximo nivel de seguridad, con unos operarios de mantenimiento específicos, donde se dirige la información a los puntos de acceso periféricos de forma estanca. La misión de este ámbito central es almacenar la información y distribuir la información.*

**Nivel periférico: El sistema cuenta con ordenadores únicos para este empleo en los grupos periféricos de enlace en las Unidades encargadas de la investigación y responsables de la intervención de la comunicación, dotados de sistema de conexión con sede central propio y seguro. Se establece codificación de acceso por usuario autorizado y clave personal, garantizando la conexión al contenido de información autorizado para ese usuario, siendo necesario que sea componente de la Unidad de investigación encargada y responsable de la intervención.*

3. Automatización: El sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándole de mayor nivel de garantía y seguridad, reduciendo costes y espacio de almacenamiento, así como adaptarse al uso de nuevos dispositivos de almacenamiento".[33]

Como hemos comentado, el Sistema Integrado de Interceptación Legal de las Comunicaciones o SITEL, carece de una regulación legal propia o específica, es por ello por lo que en un principio se dudaba de su fiabilidad y validez.

En la actualidad podemos encontrar su regulación en algunas de las siguientes normas jurídicas:

1) Ley 9/2004, de 9 de mayo, General de Telecomunicaciones.
2) Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
3) Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios.

[33] STS (Sala de lo Penal) núm. 250/2009, de 13 de marzo de 2009 (RJ 10624/2008).

7. CONCLUSIONES

I. La interceptación de las comunicaciones telefónicas y telemáticas en el proceso penal es un medio de investigación llevado a cabo por la Policía Judicial en el momento en el que encuentran evidencias fundamentadas y demostrables de la comisión de un delito. Para efectuar la medida de intervención, se necesitan diversos aparatos electrónicos.

Actualmente, su régimen jurídico se basa en la Ley de Enjuiciamiento Criminal principalmente.

II. La aplicación de esta diligencia puede llegar a afectar a distintos derechos fundamentales. Es por eso por lo que nuestra Constitución recoge en su artículo 18.3, la protección del derecho al secreto de las comunicaciones, donde además, nos ofrece ciertas garantías constitucionales como la dignidad de la persona y el libre desarrollo de la personalidad.

Esta protección es reconocida también en el ámbito jurídico europeo e internacional, concretamente en la Declaración Universal de Derechos Humanos o en el Convenio Europeo de Derechos Humanos y Libertades Fundamentales.
En cuanto a su titularidad, recaerá en toda persona física o jurídica, nacional o extranjera, incluso en los menores de edad.

III. Para una mejora en la regulación de las intervenciones, se hizo necesario el desarrollo de un concepto más exacto de la interceptación de las comunicaciones telefónicas y telemáticas. En la elaboración de este TFG, citamos el dado por la jurisprudencia del Tribunal Supremo o bien, la distinción entre comunicaciones telefónicas o telemáticas ya que, en la primera nos estaríamos refiriendo a una conversación entre dos o más sujetos a través de un terminal telefónico y de forma oral; y en la segunda, en comunicaciones orales o intercambio de datos e imágenes empleando otros medios electrónicos.

Por otro lado, debemos tener claro cuándo podemos aplicar esta de medida de intervención. Tras la reforma de la LECrim, en su art. 579 se hayan los delitos que pueden ser investigados, siempre y cuando tengan por objeto lo estipulado por el artículo 588 ter a) de la misma.

IV. El apartado cuarto de este trabajo recoge, bajo la rúbrica *"Disposiciones comunes a medios de investigación tecnológica",* la regulación introducida por la Ley Orgánica 13/2015 por la que se reforma la Ley de Enjuiciamiento Criminal.
Encontramos en Capítulo IV, Título VIII del Libro II, las disposiciones comunes, desde el artículo 588 bis a) hasta el 588 bis k).

Para el cumplimiento de estas diligencias es necesario que estén fundadas primordialmente en los principios rectores. Estos son el principio de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad.

Por otro lado, se hace referencia a la solicitud de la autorización y resolución judicial de la medida donde se establece la necesidad de presentar una previa valoración de las pruebas recabadas respetando los principios rectores, siendo el juez instructor el que acuerde las medidas de investigación y, en cuanto a la resolución judicial, se concretan los extremos a tener en cuenta para la autorización de la medida.

Además, el subapartado 4.3. del trabajo pone de manifiesto la relación entre el secreto y la afectación de terceras personas en las comunicaciones existentes entre el/los investigado/s y otro/s sujeto/s ya que, es necesario guardar secreto a las terceras personas implicadas como a su identidad.

En cuanto a la duración, será la específica para cada una de las medidas pudiendo ser prorrogadas por el Juez competente mediante auto motivado. Será adoptada a instancia del Ministerio Fiscal o de la Policía Judicial antes de que acabe el plazo a través de una petición razonada (arts. 588 bis e) y f)).

Para que la diligencia sea llevada a cabo correctamente, es necesario un control judicial pues, ante la intromisión en los derechos fundamentales supone un riesgo en este tipo de medidas. Para ello, la Policía Judicial se encargará de informar al juez del transcurso de la investigación y, en el caso de desaparecer los indicios que llevaron a su adopción, este podrá cesar la medida.

Finalmente, se regula el descubrimiento casual de comunicaciones entre sujetos con un contenido posiblemente ilícito y para ello se aplicará el art. 579 bis de la Ley. Por otro lado, en relación con la finalización de la medida, para salvaguardar y proteger los derechos de los investigados, a través de una resolución firme se acordará la destrucción de registros acumulados en la causa.

V. El apartado quinto, en a sus once subapartados, lleva consigo un análisis más detallado de la regulación de las medidas de investigación de la interceptación de las comunicaciones.

El Capítulo V de la LECrim se encuentra dividido en tres secciones, comprendidas desde el art. 588 ter a) hasta el 588 ter m).

Grosso modo, se exige para poder autorizar la medida, que la investigación verse sobre algunos de los delitos del art. 579.1. En cuanto al ámbito de aplicación, hemos distinguido entre ámbito material u objetivo y subjetivo y su relación con la afectación a terceros. El ámbito de aplicación material será aquel en el que el sujeto actúe como emisor o receptor de la comunicación ilícita mientras que, el subjetivo será los medios utilizados para establecerla (art. 588 ter b).

En relación con la afectación de terceros se añade la protección de los derechos fundamentales de sujetos afectados totalmente ajenos a la causa cuando el investigado use algún terminal que no sea de su propiedad.

Por consiguiente, hemos explicado el deber de colaboración donde se enumeran los sujetos obligados a colaborar con la Justicia y por otro lado, el de guardar secreto para no afectar al desarrollo de la investigación.

Cuando mencionamos la solicitud de la autorización judicial, hemos añadido en esta, otros requisitos para la identificación del terminal por el que se intercambia la comunicación y además, para extensión de la medida. Con respecto al control judicial de la medida, será la Policía Judicial la encargada de informar al Juez de Instrucción sobre el transcurso de la investigación, las grabaciones y transcripciones obtenidas a través de diferentes soportes, asegurando la autenticidad de estas.

La duración de la intervención es de 3 meses siendo posible su prórroga en períodos de otros tres meses hasta un alcance máximo de año y medio. Acto seguido toda persona afectada en la investigación tiene derecho a una copia de las grabaciones y transcripciones realizadas una vez alzado el secreto de la causa.

Ya hemos visto que algunos de los sujetos obligados a colaborar son los prestadores de servicios de las comunicaciones, pues bien, estos también deberán aportar los datos que sean relevantes para el transcurso de la investigación aún cuando se encuentren en un ámbito distinto.

Finalmente, el acceso para adquirir los datos necesarios para poder identificar a los sujetos o terminales, es posible conseguirlo a través del número IP y así llegar a la red o dispositivo utilizado; el IMSI o IMEI, para la obtención de la red móvil, país en el que se encuentra, o el titular directo o indirecto del terminal.

VI. En la actualidad y con el continuo avance tecnológico, se llegó a establecer el SITEL: un sistema más avanzado y seguro en las intervenciones telefónicas y telemáticas.

Este medio utiliza un sistema central en el cual se recopila toda la información necesaria que, posteriormente será desglosada en un CD/DVD, examinado y proporcionado íntegramente por la Policía Judicial como prueba en el juicio oral.

Para concluir, existe un inconveniente ante este sistema y es la falta de una regulación propia en nuestro régimen jurídico.

8. BIBLIOGRAFÍA

- ÁGUILA SÁNCHEZ, C., "La interceptación de las comunicaciones telefónicas y
- telemáticas en el proceso penal", Diario La Ley, Nº 9303, 2018.
- ARMENTA DEU, T., *Lecciones de derecho procesal penal,* ed. Marcial Pons, Madrid, 2019.
- DÍAZ REVORIO F. J., "El derecho fundamental al secreto de las comunicaciones", en Revista de la Facultad de Derecho, Pontificia Universidad Católica del Perú, 2007, núm. 59, pág. 159-173.
- ELVIRA PERALES, A., "Titularidad y eficacia del derecho" en El derecho al secreto de las comunicaciones, Breviarios jurídicos, Madrid, 2007.
- FISCALÍA GENERAL DEL ESTADO, *"Circular 1/2013 sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*", Madrid, 11 enero de 2013.
- FISCALÍA GENERAL DEL ESTADO, *"Circular 2/2019 sobre la interceptación de comunicaciones telefónicas y telemáticas",* BOE, Nº 70, 22 de marzo de 2019.
- GÓMEZ COLOMER, J.L., BARONA VILAR, S., MONTERO AROCA, J., ESPARZA LEIBAR, I., ETXEBERRÍA GURIDI, J.F., *"Derecho jurisdiccional III, Procesal Penal",* ed. Tirant lo Blanch, Valencia, 2019.
- LÓPEZ-BARAJAS PEREA, I., *"Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley",* ed. UNED, Revista de Derecho Político, Nº 98, Enero de 2017.
- LÓPEZ-BARAJAS PEREA, I., "El procedimiento de intervención: el sistema integrado de interceptación de las comunicaciones (SITEL) y sus garantías" en la intervención de las comunicaciones electrónicas, ed. La Ley, Madrid, 2011.
- MORENO CATENA, V., CORTÉS DOMÍNGUEZ, V., "*Derecho Procesal Penal",* ed. Tirant lo Blanch, Valencia, 2019.
- OTAMENDI ZOZAYA, F., "La ansiada regulación de las llamadas medidas de investigación tecnológica", Ed. Dykinson, Madrid, 2017.

- PALOP BELLOCH, M., *"Las medidas de investigación tecnológica",* ed. VLex, Revista de Derecho Procesal, Nº 2, Diciembre 2017.
- RICHARD GONZÁLEZ, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», Diario La Ley, nº. 8808, 2016.
- SANCHÍS CRESPO, C., "Puesta al día de la instrucción penal: la interceptación de las comunicaciones telefónicas y telemáticas", La Ley penal: revista de derecho penal, procesal y penitenciario, Nº 125, 2017.
- SANTANA LÓPEZ, S., "La interceptación de las comunicaciones telefónicas y telemáticas", Martell Abogados, de 16 de marzo de 2021.