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

1. Introducción

La LO 13/2015, de 5 de octubre, *de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*, ha venido a 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 carencias de la Ley de Enjuiciamiento Criminal (en adelante, LECrim) en esta materia se pusieron de manifiesto con motivo de la regulación del secreto de las comunicaciones en el art. 18.3 de la Constitución Española (en adelante, CE). El Tribunal Europeo de Derechos Humanos (en adelante, TEDH) denunció la ausencia de regulación en su sentencia de 30 de julio de 1988, caso Valenzuela Contreras contra España.

La LO 4/1988, de 25 de mayo, *de reforma de la Ley de Enjuiciamiento Criminal,* intentó resolver el problema con la introducción de tres apartados en el art. 579

LECrim regulando las intervenciones telefónicas, previsión que tampoco superó las exigencias del TEDH (STEDH de 18 de febrero de 2003, caso Prado Bugallo contra España).

Tuvieron que ser nuestros tribunales los que generaran un cuerpo jurisprudencial con los estándares y exigencias mínimas para la legalidad de las intervenciones telefónicas, alcanzando con ello, esta vez sí, la aprobación del TEDH (en este sentido, la resolución de inadmisión de 25 de septiembre de 2006, caso Abdulkadir Coban contra España). Ello no obstante, y como muy acertadamente señala el preámbulo de la LO 13/2015, "por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado".

La Ley 13/2015 ha introducido en la LECrim una regulación pormenorizada de la intervención de las comunicaciones telefónicas y telemáticas como diligencia de investigación que limita el derecho fundamental al secreto de las comunicaciones. A esta materia se dedica ahora el Capítulo V del Título VIII del Libro II (arts. 588 ter a a 588 ter m), Título este que concentra todas las medidas de investigación que limitan los derechos reconocidos en el artículo 18 de la Constitución.

De entre todas ellas, las reguladas en los capítulos V a IX vienen precedidas de una serie de disposiciones generales (Capítulo IV) que han sido objeto de análisis en la Circular 1/2019, s*obre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la Ley de Enjuiciamiento Criminal*, cuyas previsiones específicas modularán y precisarán su aplicación, constituyendo la columna vertebral de las que se han venido a denominar diligencias de investigación tecnológica.

Por ello, aunque el presente documento tiene por objeto el análisis de la concreta regulación de la interceptación de las comunicaciones telefónicas y telemáticas, guarda una íntima conexión con la Circular 1/2019, cuyas previsiones deberán ser especialmente observadas en la práctica de las medidas de investigación que ahora se abordan.

Se trata de una regulación cuyo origen se encuentra, como así se preocupa de recordar el Preámbulo de la Ley 13/2015, en la copiosa y rica doctrina jurisprudencial elaborada en los últimos años tanto por el Tribunal Supremo como por el Tribunal Constitucional. En consecuencia, las previsiones que recoge la Ley deberán ser interpretadas conforme al espíritu que preside esa doctrina jurisprudencial, inspirada, a su vez, por la doctrina emanada del TEDH.

2. Alcance de la medida

La LECrim dedica los arts. 588 ter a, a 588 ter m, a la regulación de la interceptación de las comunicaciones telefónicas y telemáticas. En primer lugar, resulta indispensable delimitar el alcance de la regulación precisando cuales de estas comunicaciones podrán ser intervenidas al amparo de la misma para determinar posteriormente la diferencia entre comunicación telefónica o telemática.

Los artículos que se analizan están comprendidos dentro del Título VIII *-de las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución-* del Libro II *-Del sumario-*, LECrim. En consecuencia, será preciso partir de esta primera delimitación, que hace que la regulación sea únicamente aplicable cuando, en la instrucción de las causas penales, se adopten medidas de investigación que limiten los derechos reconocidos en el art. 18 CE. En particular, deberán quedar fuera de la previsión los supuestos contemplados en la LO 2/2002, de 6 de mayo, *reguladora del control judicial previo del Centro Nacional de Inteligencia*; en la LO 4/1981, de 1 de junio, *de los estados de alarma, excepción y sitio.* En el caso de la jurisdicción militar, la regulación de la LECrim resultará

supletoriamente aplicable con las particularidades y en los términos previstos en la Disposición Adicional Primera de la LO 2/1989, de 13 de abril, *Procesal Militar*.

Es importante esta consideración, ya que existirán comunicaciones que, al no afectar a ninguno de estos derechos, quedarán extramuros de la regulación, como son ciertas comunicaciones que se producen en el llamado “Internet de las cosas” (p. ej., la comunicación entre un mando a distancia y el dispositivo que maneja). Deberá tenerse no obstante presente que existen comunicaciones entre máquinas que, puestas en relación con otros datos, sí pueden afectar a alguno de estos derechos, como el derecho a la intimidad (p. ej., la conexión entre los dispositivos móviles de comunicación, las tarjetas SIM insertadas en los mismos y las estaciones BTS. Esta conexión se produce por la mera activación del dispositivo a la red, se trata, por tanto, de una conexión entre maquinas, pero puede resultar esencial para determinar quién es el usuario de un determinado dispositivo o cuál es su localización en el espacio).

La jurisprudencia ha perfilado la naturaleza y características que debe reunir una comunicación para que pueda ser acreedora de la protección dispensada por el texto constitucional. De esta manera, se ha señalado que el secreto de la comunicación es un concepto rigurosamente formal, en el sentido de que “se predica de lo comunicado, sea cual sea su contenido” (SSTC nº 114/1984, de 29 de noviembre, 34/1996, de 11 de marzo y 70/2002, de 25 de abril); que forman parte del derecho fundamental determinados datos externos que se producen como consecuencia de una comunicación, como la identidad subjetiva de los interlocutores y el listado de llamadas (SSTEDH de 2 de agosto de 1984, caso Malone contra Reino Unido y de 3 de abril de 2007, caso Copland contra Reino Unido) o la propia existencia de la comunicación, su momento, duración y destino, tanto en redes públicas como privadas de comunicación y con independencia del medio de trasmisión (SSTC nº 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo; 230/2007, de 5 de noviembre; 249/2008, de 20 de mayo; 776/2008, de 18 de noviembre; y 688/2009, de 18 de junio); que afecta al derecho fundamental el acceso a los mensajes de texto o SMS aun no leídos (STC nº 70/2002, de 3 de

abril y STS nº 1235/2002, de 27 de junio) o a los correos electrónicos enviados y recibidos pero no leídos o en fase de transferencia (STC nº 115/2013, de 9 de mayo); o que vulnera el derecho fundamental cualquier interceptación de la comunicación por un tercero ajeno a la misma, sea un sujeto público o privado (STC nº 114/1984, de 29 de noviembre) y a través de cualquier medio, mientras el proceso de comunicación está teniendo lugar (STC nº 137/2002, de 3 de junio).

Por el contrario, no estarían comprendidas en la previsión constitucional las conversaciones grabadas o difundidas por uno de los interlocutores (SSTC nº 175/2000, de 26 de junio y 56/2003, de 24 de marzo y STS nº 421/2014, de 16 de mayo); las comunicaciones por radio (SSTS nº 209/2007, de 9 marzo; 1397/2011 de 22 de diciembre y 695/2013, de 22 de julio); el acceso a la memoria o contactos de un teléfono móvil (SSTC nº 70/2002, de 3 de abril y 142/2012, de 2 de julio y SSTS nº 1273/2009, de 17 de diciembre); el visionado directo de un número de teléfono entrante (SSTS nº 1040/2005, de 20 de septiembre y 1273/2009, de 17 de diciembre) o la conversación escuchada por agentes policiales a través del manos libres de uno de los interlocutores que accede a ello (STS nº 589/2015, de 28 de septiembre).

La previsión legal se extiende a las comunicaciones telefónicas y telemáticas. La distinción entre ambas clases de comunicación resulta, hoy en día, ciertamente difusa. El legislador, en lugar de regular la interceptación de telecomunicaciones, que incluiría *toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos* (apartado 39 del Anexo II de la Ley 9/2014, de 9 de mayo, *General de Telecomunicaciones*, en adelante, LGT) ha optado por la limitación de la previsión legal a las comunicaciones que se realizan a través de dos medios concretos, que es a lo que alude la diferenciación establecida en la ley.

Si bien el concepto de comunicación telefónica no plantea muchos problemas, no ocurre lo mismo con las comunicaciones telemáticas. La telemática, según la RAE,

es la *aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computerizada*; en consecuencia, pueden definirse las comunicaciones telemáticas como aquellas que emplean la informática para la transmisión de información. Ahora bien, la mera intervención de un equipo o sistema informático en el proceso de transmisión de una comunicación no puede resultar suficiente para catalogar ésta como telemática, ya que, hoy en día, todas las comunicaciones telefónicas utilizan tecnologías digitales, manejadas por sistemas informáticos, para su transmisión y gestión técnica. En consecuencia, el criterio distintivo debe residir en el medio empleado para llevar a cabo la comunicación: telefónica cuando se utilice un teléfono para generar el mensaje que se comunica, y telemática cuando se utilice un sistema informático, aunque nuevamente aquí se encontraría una zona de duda en las comunicaciones generadas a través de los modernos *smartphones* o teléfonos inteligentes, que mezclan en un mismo dispositivo las capacidades de un teléfono y de un ordenador y que podrían ser catalogadas como comunicaciones mixtas.

En cualquier caso, al gozar ambos tipos de comunicación de una misma regulación, el problema de su distinción únicamente se proyecta sobre aquellas formas de comunicación que no tuvieran cabida en ninguna de estas dos, a las que les faltaría la previsión legal que posibilitara su intervención, lo que hoy en día no resulta imaginable aunque sí se plantea como una posibilidad de futuro.

3. Presupuestos

El primer artículo que dedica la LECrim a la regulación de la interceptación de las comunicaciones telefónicas y telemáticas recoge el criterio adoptado por el legislador para establecer los límites del principio de proporcionalidad en relación con esta medida. Efectivamente, la proporcionalidad impone limitar el uso de la medida a la investigación de aquellos hechos que, por su especial gravedad, justifiquen la limitación de los derechos fundamentales.

El art. 588 ter a LECrim dispone que *la autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación*.

Por su parte, el art. 579.1 se refiere a los siguientes delitos:

1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión.
2.º Delitos cometidos en el seno de un grupo u organización criminal.
3.º Delitos de terrorismo.

Es preciso poner de relieve que la delimitación de las conductas delictivas que hace el precepto no elimina ni sustituye los criterios de ponderación que establece, dentro de las disposiciones generales, el art. 588 bis a.5 para justificar la concurrencia del principio de proporcionalidad en un supuesto concreto: 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.

En definitiva, el legislador ha establecido un marco legal mínimo para que sea posible la injerencia, pero dentro de ese marco, es decir, una vez superadas dichas exigencias legales, el órgano judicial ha de valorar la oportunidad concreta en atención a los criterios que menciona en el art. 588 bis a LECrim.

De esta manera, deberá entenderse, con carácter general, que no será posible el recurso a esta medida de investigación tecnológica cuando se trate de la persecución de delitos leves, aunque los mismos hubieran podido ser cometidos en el seno de una organización o grupo criminal o cuando se hayan cometido a través de instrumentos informáticos o tecnologías de la información o comunicación. La

trascendencia social de esta clase de comportamientos delictivos difícilmente alcanzará la gravedad mínima necesaria para culminar las exigencias del principio de proporcionalidad. No obstante lo anterior y como excepción, limitaciones del derecho fundamental leves o menos graves, como podría ser el acceso a determinados datos de tráfico, exigirán también una menor gravedad en el comportamiento delictivo que las justifica, pudiendo resultar proporcionado ese acceso en determinados supuestos de delitos leves, si bien exigiendo siempre una fundamentación reforzada de la decisión judicial (en este sentido, la STJUE (Sala Tercera), de 1 de octubre de 2015 (asunto C-230/14) a la que más adelante se hará referencia).

En cuanto a los delitos conexos que por sí solos no permitirían el recurso a la medida, habrá que remitirse a lo que sobre los hallazgos casuales se expone en la Circular 1/2019: la intervención telefónica o telemática estará justificada mientras se fundamente en el delito principal, no existiendo inconveniente para valorar y considerar el delito conexo casualmente hallado, pero nunca podrá acordarse ni prorrogarse la medida con fundamento en el delito conexo si llega a desaparecer el delito que la justifica.

Es suficiente con la concurrencia de alguno de los supuestos que prevé el art. 588 ter a. De esta manera, se ajustarán a la previsión los casos en los que se investiguen delitos dolosos castigados con pena máxima de, al menos, tres años de prisión, aunque no se comentan en el seno de una organización criminal o terrorista, así como cuando la investigación tenga por objeto delitos cometidos en el seno de una organización o cometidos a través de instrumentos informáticos, aunque sus penas no alcancen la duración máxima de, al menos, tres años de prisión. En estos casos, sin embargo, deberá exigirse un mayor esfuerzo argumentativo en la resolución judicial que se dicte para fundamentar la proporcionalidad de la medida.

En cuanto al primero de los criterios que establece el art. 588 ter a -delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión-, debe

recordarse que no resultarán posibles las intervenciones telefónicas o telemáticas para la investigación de delitos imprudentes, aunque estos pudieran exceder en su pena el límite máximo de tres años que se establece (por ejemplo, el homicidio imprudente del art. 142 CP, castigado con pena de hasta cuatro años de prisión). Este límite máximo de tres años deberá referirse a la pena en abstracto, independientemente del grado de ejecución o posible concurrencia de circunstancias modificativas de la responsabilidad criminal, e incluirá los supuestos en los que el límite máximo punitivo de tres años se alcance por la aplicación de un subtipo agravado (p. ej., en el caso que prevé el art. 327 CP, para los delitos contra los recursos naturales y el medio ambiente), siempre que existan indicios que permitan presumir que la conducta a investigar se encuadra en ese subtipo agravado. Esto mismo se observará en el caso de los delitos masa, a los que se refiere el art. 74.2 CP.

Cuando se trate de delitos cometidos en el seno de un grupo u organización criminal debe tomarse en consideración que la proporcionalidad de la medida se alcanza, no por la gravedad intrínseca del delito cometido, sino *por la potencial eficacia de dichas organizaciones en su embate contra los intereses sociales y públicos garantizados por la legalidad que atacan* (SSTC nº 14/2001, de 29 de enero; 202/2001, de 15 de octubre; 82/2002, de 22 de abril). El preámbulo de la LO 5/2010, de 22 de junio, *por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, señalaba que “la seguridad jurídica, la vigencia efectiva del principio de legalidad, los derechos y libertades de los ciudadanos, en fin, la calidad de la democracia, constituyen objetivos directos de la acción destructiva de estas organizaciones”. Ahora bien, no obstante la consideración del ámbito de producción del delito para llevar a cabo el juicio de proporcionalidad, es preciso reiterar que deberá exigirse una fundamentación reforzada para la adopción de la medida en la investigación de delitos que, en sí mismos, no alcancen la gravedad necesaria para el recurso a este medio de investigación. Se estaría aquí ante una excepción de la regla general que antes se establecía para los delitos leves.

Obsérvese que lo que permite la intervención de las comunicaciones es la investigación de delitos cometidos en el seno de una organización o grupo criminal, no la investigación del propio delito de organización (art. 570 bis CP) o grupo criminal (570 ter CP). Esta precisión cobra especial trascendencia en relación con el delito del art. 570 ter CP, que presenta algunas modalidades típicas que no alcanzan los tres años de prisión como pena máxima. En estos casos, la investigación del grupo criminal deberá ser siempre conexa a la del concreto delito que se cometa en el seno del grupo en los términos que se han expuesto, debiendo igualmente llevarse a cabo un mayor esfuerzo argumentativo en la fundamentación de la resolución que adopte la medida.

Tanto en el caso de los delitos cometidos en el seno de un grupo u organización criminal, como en el de los delitos de terrorismo, la valoración jurídica de los hechos a investigar debe hacerse *ex ante*, en función de los indicios que se puedan tener en el momento de adoptarse la medida. Quiere esto decir que la posterior inexistencia de una condena por esta clase de delitos no tiene que suponer la irregularidad de la medida (en este sentido, pueden considerarse las SSTS nº 575/2013, 28 de junio y 767/2007, 3 de octubre).

Finalmente, por lo que se refiere a los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación, ya señalaba el informe del Consejo Fiscal al Anteproyecto de la LO 13/2015 que el fundamento de su inclusión residía en que *los delitos cometidos a través de las nuevas tecnologías, difícilmente pueden investigarse a través de otros medios*, añadiendo que *la interceptación de las comunicaciones, y en particular las telemáticas, puede ser en ocasiones la única vía de investigación criminal de los ilícitos que se cometen a través de la red*. Este fundamento, además, se ve complementado por “la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito” (STC nº 104/2006, de 3 de abril). Habrá de atenderse, por lo tanto, a estos fundamentos para justificar la proporcionalidad de la medida, debiendo exigirse una mayor motivación a medida que el delito investigado tenga señalada una pena menor, hasta el punto de limitar

al máximo esta forma de investigación cuando se esté en presencia de las formas delictivas de menor entidad.

4. Ámbito objetivo

El art. 588 ter b precisa que el ámbito objetivo de la interceptación de las comunicaciones puede extenderse al contenido de la comunicación en sí y a *los datos electrónicos de tráfico o asociados al proceso de comunicación,* a los que añade *los que se produzcan con independencia del establecimiento o no de una concreta comunicación.* Este amplio ámbito objetivo, sin embargo, no será común para toda medida de interceptación de comunicaciones, sino que será necesario, en cada caso concreto, que el Juez determine el preciso alcance de la interceptación.

Efectivamente, al señalar el precepto que la intervención judicial *podrá autorizar*, deberá interpretarse que el Juez tendrá que exteriorizar una voluntad expresa que determine el mayor o menor alcance de la potestad conferida. De este modo, lo habitual será que el Juez autorice el acceso al contenido de la comunicación, pero si además de dicho contenido considera también oportuno el acceso a cualesquiera otros datos de tráfico o asociados a la comunicación, deberá precisarlo expresamente en la resolución que dicte. Esta ampliación del contenido de la interceptación requerirá, además y lógicamente, que la resolución judicial fundamente y justifique conforme a las exigencias legales la necesidad, proporcionalidad y excepcionalidad del acceso a tales datos. En palabras del preámbulo de la LO 13/2015, *se pretende con ello que sea el propio juez, ponderando la gravedad del hecho que está siendo objeto de investigación, el que determine el alcance de la injerencia del Estado en las comunicaciones particulares.*

Se termina, de esta manera, con una práctica que se había venido generalizando con anterioridad a la reforma LECrim consistente en la inclusión sistemática, en las resoluciones que acordaban la intervención de comunicaciones, de todos los datos

de tráfico o asociados que pudieran ser aportados por el operador telefónico y, todo ello, sin fundamentación alguna que lo justificara. Este indebido modo de proceder, puesto ya de manifiesto por algún pronunciamiento jurisprudencial a partir del voto particular a la STS nº 316/2011, de 6 de abril, resultaba poco respetuoso con los principios esenciales fundamentadores de la limitación del derecho fundamental.

Por lo tanto, deberá precisar el Juez si la intervención queda limitada a las comunicaciones orales que puedan sostenerse a través del terminal telefónico o se incluyen también los intercambios de mensajes cortos (SMS), correo electrónico o mensajes multimedia (MMS). Igualmente deberá precisarse si la intervención se extiende, además de al contenido de la comunicación, a los datos de tráfico o asociados, o a aquellos que se produzcan con independencia del establecimiento de una comunicación. Así se desprende, también, del art. 588 ter d que, al referirse al contenido de la solicitud que haya de dirigirse al Juez, precisa en su apartado segundo:

“Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:
a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.
b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.
c) La localización geográfica del origen o destino de la comunicación.
d) 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 orden a delimitar el alcance de lo que deba entenderse por datos electrónicos de tráfico o asociados, el último párrafo del art. 588 ter b se encarga de precisar que serán “todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad

de la información o comunicación telemática de naturaleza análoga". Para distinguir entre datos de tráfico y datos asociados deberá operarse con las previsiones contenidas en el art. 1 (que define los datos de tráfico) y el art. 18.3 y demás regulación contenida en el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE de 17 septiembre de 2010), al que posteriormente se hará referencia.

En definitiva, se incluyen aquí todos los datos a 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*, así como los que se recogen en el art. 39 de la LGT.

Entre tales datos figuran algunos esenciales para hacer posible técnicamente la comunicación, como el número de abonado, la dirección IP (protocolo de Internet, por sus siglas en inglés), el IMSI (identidad internacional del abonado móvil), el IMEI (identidad internacional del equipo móvil), la DSL (línea digital de abonado), entre otros. Igualmente figuran otros datos técnicos, como son los referidos a la geolocalización de los equipos que intervienen en la comunicación o a las vicisitudes técnicas que se hayan podido producir durante la comunicación (como la causa de su finalización), así como los datos necesarios para la facturación del servicio de comunicación, entre los que se incluyen la identificación del titular del servicio, su domicilio, número de cuenta, dirección de correo electrónico, hora de comienzo y fin de la comunicación, etc. Además, se incluyen, como datos que se generan independientemente del establecimiento de una comunicación concreta, todos aquellos que se producen de manera automática y casi permanente como consecuencia de la comunicación entre los teléfonos móviles y los puntos de conexión a red o estaciones BTS (*Base Transceiver Station*) o los que generan los sistemas de conexión wifi entre dispositivos y redes.

Como puede apreciarse, no se trata de datos que afectan exclusivamente al derecho fundamental al secreto de las comunicaciones (art. 18.3 CE), sino que se incluyen también otros que entrarían en la esfera de la intimidad (art. 18.1 CE) o del

derecho a la protección de datos (art. 18.4 CE). De esta manera, se confirma la precisión que se hacía *ut supra* acerca del ámbito o alcance de la regulación contenida en la LECrim a todos los derechos previstos en el art. 18 CE y no solo al secreto de las comunicaciones. Por otro lado, la regulación contenida en la Ley 25/2007 referente a la cesión de tales datos *a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales* (art. 1), debe entenderse superada por la contenida ahora en la LECrim cuando se trate de una medida de interceptación de comunicaciones, con lo que desaparecen todas las dudas interpretativas que se habían venido planteado, tales como el alcance de la gravedad del delito, el derecho fundamental afectado o la autoridad competente para requerir los datos.

Por último, es preciso señalar que, en atención a esa diferente naturaleza de los datos de tráfico o asociados, al tener en muchos casos el acceso a los mismos una menor incidencia en la esfera de los derechos fundamentales del afectado que la intervención del contenido de la comunicación, deberá también ser menor el grado de exigencia de los principios rectores para acordar su incorporación al proceso. En este sentido, señalaba la STC nº 26/2006, de 30 enero, en relación con la incorporación a un proceso de listados de llamadas, que “aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las escuchas telefónicas, siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad” (en el mismo sentido, la STC nº 123/2002, de 20 de mayo).

5. Ámbito subjetivo y afectación de terceros

5.1. Regulación legal

La LECrim regula en los arts. 588 ter b y 588 ter c la delimitación subjetiva de la medida de interceptación de las comunicaciones telefónicas y telemáticas. En el primero de ellos se incluyen las diversas estrategias que el investigado pudiera utilizar para eludir el control de sus comunicaciones (utilizar ocasionalmente terminales o medios de comunicación ajenos o poner a nombre de terceros la titularidad del terminal o medio de comunicación que habitualmente utilice), mientras que el segundo hace referencia a la posibilidad de intervenir comunicaciones de terceros ajenos a la investigación. Se añade, en el art. 588 ter b, la intervención de los medios de comunicación o terminales de la víctima de un delito. En todos estos supuestos, con las particularidades que prevé el legislador, será lícito el recurso a la medida de interceptación.

La diferencia esencial entre ambos preceptos reside en que, en el primero de ellos, el derecho fundamental que se limita es el del propio investigado, independientemente de los terminales o medios de comunicación que utilice, cuya relación con el investigado y su actividad delictiva deberá ser acreditada, mientras que, en el segundo, lo que se limita es el derecho fundamental de un tercero con fundamento en su relación con el delito a través del investigado. Este último precepto enlaza directamente con el art. 588 bis h que, como se analizaba en la Circular 1/2019, admite de manera genérica que las medidas de investigación tecnológica de la LECrim puedan afectar a terceras personas *en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas*.

5.2. Utilización por el investigado de terminales o medios de comunicación de titularidad ajena

La circunstancia de que el investigado recurra para el mantenimiento de sus comunicaciones a terminales o medios de comunicación que figuren a nombre de terceras personas no supone ningún obstáculo para la adopción de la medida. Ya desde antiguo la doctrina jurisprudencial venía admitiendo sin fisuras esta posibilidad (por todas, la STS nº 474/2012, de 6 de junio). En realidad, lo determinante para fundamentar la medida de interceptación de las comunicaciones no va a ser la relación de titularidad del sujeto investigado con el terminal o medio de comunicación, sino su relación como usuario, aunque sea ocasional. Esta conclusión aparece reforzada, sobre todo, si se tiene en cuenta que, normalmente, va a ser estrategia del delincuente hacer figurar los terminales o medios de comunicación que utilice a nombre de terceros, precisamente, para evitar el control judicial de sus comunicaciones. Esta relación de usuario y no de titular es la que ha llegado a fundamentar, incluso, la intervención de terminales o equipos situados en establecimientos públicos, posibilidad ésta prevista en el art. 39 LGT, exigiéndose, eso sí, la adopción de medidas para limitar en lo posible la afectación del derecho de terceros (SSTS nº 467/1998, de 3 de abril y 1233/1994, de 18 de abril).

En cualquier caso, la intervención de terminales o medios de comunicación que figuren a nombre de terceros va a requerir un especial esfuerzo en la motivación del principio de idoneidad de la medida, que exigirá la exteriorización de indicios que justifiquen esa relación del sujeto investigado con el medio de comunicación de ajena titularidad que se pretende intervenir.

De esta manera, en los supuestos de utilización por el investigado de terminales o medios de comunicación que figuren a nombre de terceros, la necesaria identificación subjetiva de la medida pasará por justificar la relación del investigado con el teléfono y la existencia de indicios que pongan de manifiesto que utiliza ese terminal o medio de comunicación para sus fines delictivos. En estos casos, por lo tanto, la falta de identificación del titular formal del medio no resultará trascendente

para valorar la legalidad de la medida, habiendo señalado la STS nº 48/2013, de 23 de enero: “esa disociación entre el titular o abonado y el usuario de los servicios de telefonía encuentra también reflejo en la Ley 32/2003, 3 de noviembre, en cuyo art. 38.4 se reconoce un estatuto específico a los usuarios que no tengan la condición de abonados, admitiendo el hecho incuestionable de una utilización de las terminales telefónicas disociada de la titularidad del servicio. En consecuencia, el hecho de que en el auto inicial no se especificara quién era el titular de los teléfonos intervenidos, limitándose a hacer mención a uno de los usuarios, identificado como Ramón -otro de los coacusados finalmente condenados-, no afecta a la legitimidad de la medida”.

En cuanto a la intervención de las comunicaciones en las que el investigado aparezca como receptor de las mismas -referidas ahora en el art. 588 ter b-, como ya se indicaba en la Circular 1/2019, la jurisprudencia no ha tenido objeciones en admitir la legalidad de la limitación del derecho fundamental del interlocutor no investigado como consecuencia de la interceptación de las comunicaciones del verdaderamente investigado (“recogida de arrastre”, en palabras de la STS nº 419/2013, de 14 de mayo). De manera muy elocuente señala el Tribunal Constitucional (STC nº 219/2009, de 21 de diciembre): “no puede considerarse constitucionalmente ilegítima la intervención de las conversaciones de las personas que comunican o con las que se comunican aquéllas sobre las que recaen inicialmente los indicios, en la medida en que tales conversaciones estén relacionadas con el delito investigado, correspondiendo al Juez, a través del control de la ejecución de la medida, la identificación de las conversaciones relevantes”.

5.3. Intervención de terminales o medios de comunicación de la víctima

El art. 588 ter b.2 regula también la posibilidad de intervenir *los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad.* Esta previsión no figuraba en la redacción inicial del anteproyecto de ley, habiendo sido sugerida su inclusión en el informe del Consejo Fiscal, que señalaba como fundamento de la misma la necesidad de *conocer la forma de*

comisión del delito, las personas que pudieran ser autoras de los mismos o se pretenda tener noticia del paradero del encartado.

Si bien pudiera parecer que la regulación será únicamente aplicable a aquellos casos en los que la víctima no se encuentre en condiciones de prestar su consentimiento a la intervención de sus comunicaciones, como podrían ser los supuestos de secuestros o desaparición en circunstancias violentas (piénsese en lo determinante que puede resultar para la investigación la interceptación de los datos de geolocalización), nada se opone a considerar también aplicable este artículo a la interceptación de comunicaciones de la víctima con su propio conocimiento y consentimiento. Siempre que se dé el presupuesto del grave riesgo para su vida o integridad y resulte relevante para el desarrollo de la investigación, el Juez podrá acordar la intervención de sus comunicaciones, haya prestado o no su consentimiento, toda vez que la capacidad del Juez no podría verse condicionada por la voluntad de la víctima.

Es cierto, y así se ha indicado, que la grabación de las comunicaciones, sin autorización judicial, por uno de los interlocutores -o por un tercero con el consentimiento de uno de ellos- no llega a limitar el derecho fundamental al secreto de las comunicaciones, al ser ese interlocutor “dueño” del secreto, que podrá o no revelar según su voluntad (SSTC nº 175/2000, de 26 de junio y 56/2003, de 24 de marzo y STS nº 421/2014, de 16 de mayo); pero no es menos cierto que la autorización judicial de la interceptación de esas comunicaciones confiere, sin duda, algunas ventajas al procedimiento.

En primer lugar, inviste de formalismo la medida de investigación, aportando seguridad jurídica a la prueba de este modo obtenida, en atención al control y mayores garantías que rodean el desarrollo de esta medida bajo el control judicial. Pero es que, además, las posibles afecciones del derecho a la intimidad que pudieran derivar de la revelación del contenido de una conversación privada por parte de uno de los interlocutores aparecerían de esta manera amparadas por la cobertura judicial.

En estos casos, sin embargo, las exigencias de motivación de la resolución judicial serán ciertamente diferentes a las de los supuestos ordinarios de interceptación de comunicaciones, al no aparecer controvertido el derecho al secreto de las comunicaciones y aparecerlo mínimamente el derecho a la intimidad, lo que deberá condicionar decisivamente la ponderación de los principios rectores. Además, el consentimiento de la víctima a la interceptación de sus comunicaciones le confiere un efecto legitimador que debería plasmarse en el auto habilitante como garantía que afecta a la ponderación de los principios rectores en el caso concreto. No obstante lo anterior, deberá siempre observarse un escrupuloso respeto a las exigencias legales que rigen la adopción de la medida y, entre ellas, a la concerniente a las modalidades delictivas que admiten el recurso a la misma, conforme al art. 588 ter a.

Cuando la interceptación de comunicaciones se lleve a cabo sin el consentimiento de la víctima, sin embargo, la justificación de la medida, desde la perspectiva de la proporcionalidad, exige una mayor gravedad del delito, al limitar un derecho fundamental de quien ni siquiera es sospechoso de actividad delictiva.

En cualquier caso, nunca debe olvidarse que su aplicación queda limitada a la investigación de actividades delictivas, resultando absolutamente improcedente su uso bajo el amparo de esta regulación legal en aquellos casos en los que no exista indicio alguno de actividad delictiva, como podría ser la desaparición voluntaria de una persona o derivada del padecimiento de una enfermedad psíquica.

5.4. Intervención de terminales o medios de comunicación de terceras personas

La posibilidad de limitar el derecho fundamental al secreto de las comunicaciones de terceras personas no investigadas aparece condicionada por el art. 588 ter c a tres supuestos: que el investigado se sirva de ellas para transmitir o recibir información, que colaboren con el investigado en sus fines ilícitos o se beneficien

de los mismos o que el investigado u otros que también pudieran serlo utilicen maliciosamente el dispositivo por vía telemática sin conocimiento de su titular. Esta posibilidad, como ya se señalaba en la Circular 1/2019 al analizar el alcance subjetivo de la resolución en el caso de las disposiciones generales, ya venía siendo admitida pacíficamente por nuestra doctrina jurisprudencial (STS nº 1839/1994, de 18 de marzo). Se está pensando aquí, fundamentalmente, en la denominada vía indirecta, a la que se hacía referencia.

Las comunicaciones que es posible intervenir en estos casos serán tanto las emitidas como las recibidas, a pesar de que el precepto se refiere expresamente solo a las primeras. Así cabe interpretarlo de la propia redacción del artículo, cuando admite a continuación los supuestos en los que el investigado se sirve del tercero para transmitir o recibir información.

El precepto se refiere a supuestos en los que la colaboración del tercero no resulte suficiente para dirigir también contra él la investigación como cómplice o cooperador necesario de la actividad delictiva del investigado, que justificaría la intervención del terminal o medio de comunicación con fundamento en su propia actividad delictiva y no en la del investigado. Se incluirían aquí, entre otros, aquellos casos en los que existen dudas acerca de la conciencia o voluntariedad de la colaboración del tercero, cuando se trate de familiares del investigado que transmiten datos importantes para el desarrollo de la actividad delictiva estando exentos de responsabilidad por un posible encubrimiento, cuando se trate de menores de 14 años u otras personas exentas de responsabilidad criminal o en el caso de destinatarios de la actividad delictiva, como serían los consumidores, clientes finales de un narcotraficante, por ejemplo.

Finalmente, cuando el artículo hace referencia al uso malicioso del dispositivo por parte de terceros hace alusión, normalmente, a supuestos de vulneración de las medidas de seguridad de redes informáticas para su uso inconsentido o al empleo de cualquier tipo de *malware* para controlar dispositivos ajenos con el fin de utilizarlos para entablar comunicaciones. En estos casos, la previsión por el

legislador de que el uso deba hacerse por vía telemática planteará problemas interpretativos cuando se trate de usos maliciosos de terminales telefónicos mediante técnicas de desvío de llamada o uso fraudulento de la conectividad de los mismos. Incluso, dejaría indebidamente fuera de la previsión los supuestos más simples de uso malicioso de terminales ajenos mediante la interceptación de frecuencias o, simplemente, con la derivación física de la comunicación por medio de cables. En estos casos, sin embargo, la amplitud de la medida que parecen concebir los arts. 588 ter b y c permitiría la interceptación de esta clase de comunicaciones una vez acreditada su relación con el investigado, al amparo del supuesto general que regula el art. 588 ter b: terminales o medios de comunicación habitual u ocasionalmente utilizados por el investigado.

Para concluir, es preciso señalar que en todos los casos de interceptación de comunicaciones emitidas desde terminales o medios de comunicación ajenos, como parece lógico, se impone la necesidad de una mayor motivación de la resolución judicial habilitante pues, realmente, se estará limitando el derecho fundamental de una persona que no es responsable de la actividad delictiva. Por lo tanto, no solo el principio de proporcionalidad, sino también los de necesidad y excepcionalidad, exigen una mayor justificación, debiendo reflejarse indicios suficientes, no solo de la relación del investigado con el medio o la persona que transmite o recibe la comunicación, sino también de la importancia de esa interceptación para los fines de la investigación.

6. Solicitud

El art. 588 ter d regula los extremos que deberá contener la solicitud de autorización judicial de interceptación de las comunicaciones telefónicas o telemáticas. Las exigencias que incluye el precepto deberán añadirse a las que, con carácter general, se prevén en el art. 588 bis b para la solicitud de cualquier medida de investigación tecnológica. La finalidad del precepto, por tanto, no es otra que complementar las disposiciones generales con aquellas menciones específicas que exige la naturaleza de esta concreta medida de investigación tecnológica.

En el apartado primero del artículo se establece que la solicitud habrá de comprender los datos técnicos necesarios para identificar el terminal o medio a intervenir. Su finalidad es hacer posible la interceptación pues, sin un dato que individualice el terminal o medio de comunicación, será imposible técnicamente llevar a cabo la misma. Por eso, las irregularidades o deficiencias que pudiera contener la solicitud en cuanto a este extremo podrán tener trascendencia práctica y no jurídica, al hacer imposible la interceptación. Entre los datos de identificación que recoge el precepto se incluye la etiqueta técnica a la que se refiere el art. 39 LGT en los siguientes términos: "puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso".

El apartado segundo precisa el ámbito objetivo de alcance de la medida que ya se analizaba *ut supra*. Únicamente resulta necesario recordar aquí que cualquier aspecto referido a la comunicación que quiera ser incorporado al procedimiento deberá estar previsto y justificado en la resolución judicial habilitante.

Finalmente, el apartado tercero del artículo incluye una previsión extraña a la solicitud: la posibilidad de que la interceptación de comunicaciones pueda ser autorizada por el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Los términos en los que aparece redactado el precepto remiten a una situación de necesidad justificada por la imposibilidad de recabar autorización judicial ante la urgencia del caso. En estos supuestos pueden distinguirse dos momentos en la interceptación de las comunicaciones: el primero, constituido por la resolución ministerial que ordene la medida y, el segundo, referido al momento de la convalidación judicial de la misma.

En cuanto a la resolución del Ministro o Secretario de Estado acordando la medida debe interpretarse que la misma no está sujeta a las exigencias formales que la LECrim prevé para la autorización judicial habilitante (art. 588 bis c), precisamente, por estar limitada esa previsión a la resolución judicial. Bastará que el acuerdo ministerial contenga los datos técnicos que posibiliten la intervención, la justificación de que la medida se acuerda para la investigación de un delito de terrorismo y los datos que fundamenten la existencia de una situación de urgencia que no pueda esperar a la resolución judicial. La urgencia existirá únicamente en los casos en los que aparezca plenamente justificado que, en el caso concreto, no se pudo acudir al Juez para obtener la autorización. La posterior convalidación judicial de la medida deberá avalar estos extremos, además de culminar la totalidad de las exigencias que, para cualquier medida de interceptación de las comunicaciones, establece la LECrim. Si no aparecieren acreditados los presupuestos que autorizan la intervención por el Ministro del Interior o el Secretario de Estado, la intervención de comunicaciones practicada será nula.

7. Deber de colaboración

Con la finalidad de hacer posible la interceptación de las comunicaciones telefónicas y telemáticas, el art. 588 ter e impone a cualquier persona o entidad que de algún modo contribuya a facilitar las comunicaciones el deber de colaboración con las autoridades. Este precepto deber ser puesto en relación con los arts. 588 bis b.2.8.º y 588 bis c.3.h) que, referido el primero a la solicitud y el segundo a la resolución judicial por la que se acuerde cualquier medida de investigación tecnológica, adelantan ya la necesidad de precisar, tanto en la solicitud como en la resolución judicial habilitante, la identificación del *sujeto obligado que llevará a cabo la medida, caso de conocerse.*

El precepto resulta novedoso, al haber pasado la Ley de considerar sujetos obligados a “los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al

público" (art. 39.1 LGT), a incluir ahora a sujetos ajenos a cualquier forma de explotación de recursos públicos.

Efectivamente, el precepto incluye tres categorías de sujetos obligados.

- Los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, donde habrá que considerar incluidos a los operadores referidos en la LGT.
- Los prestadores de servicios de la sociedad de la información, donde habrá que incluir, según la exposición de motivos de la Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico* (en adelante, LSSICE), además de los anteriores, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice la contratación de bienes y servicios por vía electrónica, el suministro de información (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), entre otros, siempre que represente una actividad económica para el prestador.
- Cualquier otra persona que de algún modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, donde podría incluirse, desde el responsable de una red informática privada, al propietario de un equipo informático que haya sido empleado para el mantenimiento de una comunicación.

Se hacen destinatarios de la obligación, por lo tanto, desde las más importantes compañías de telecomunicaciones hasta el simple particular que intermedie en el proceso de comunicación. El precepto no hace más que enfatizar expresamente para los supuestos de interceptación de comunicaciones la obligación de colaboración con Jueces y Tribunales que, con carácter general, recogen los arts. 118 CE y 17.1 LOPJ, concretando para estos casos el vínculo específico con la

comunicación que justifica ese deber genérico de colaboración con la administración de justicia.

La redacción inicial del Anteproyecto excluía de la obligación “al sospechoso o imputado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional”. Su supresión en el texto definitivo, sin embargo, no debe entenderse como una voluntad deliberada del legislador de incluir una excepción al régimen general de la Ley, sino, más bien, como el resultado de la reordenación de los preceptos en el texto definitivo (esta previsión aparece ahora recogida en el art. 588 sexies c, referida al registro de dispositivos de almacenamiento masivo de información).

En la determinación del alcance de la obligación legal que se analiza pueden llegar a surgir algunos problemas de jurisdicción, sobre todo si se atiende al carácter global que hoy en día tienen las comunicaciones y, especialmente, las compañías prestadoras de servicios. Si bien es cierto que no va a plantear dudas la sujeción al ordenamiento jurídico español de los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, al estar operando con redes públicas ubicadas en territorio español, sí pueden plantearse en relación con los prestadores de servicios de la sociedad de la información, en muchos casos, radicados fuera de las fronteras españolas.

El criterio determinante para que el Juez se dirija directamente a estos operadores apercibiéndoles del deber de colaboración que la ley procesal impone o, por el contrario, remita la solicitud de interceptación de las comunicaciones a través de una comisión rogatoria u orden europea de investigación, tendrá que venir determinado por el establecimiento o no del servicio en España, como así se desprende del art. 2.4 LSSICE cuando señala que “los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de

medios electrónicos para su realización". Este mismo artículo se encarga de precisar cuándo debe entenderse que el servicio está establecido en España, señalando:

"1. Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.
Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.
2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.
Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.
3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.
La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador".

Así cabe interpretarlo, también, a la vista de la STJUE (Sala Tercera), de 1 de octubre de 2015 (asunto C-230/14), que, aunque en materia de derecho administrativo sancionador, parece apuntar en la misma dirección cuando declara que "el artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que permite aplicar la legislación relativa a la protección de los datos

personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que éste ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento" (actualmente, art. 3.2 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*).

En los casos en los que la interceptación de comunicaciones o la obtención de datos de tráfico deban hacerse a través de un operador ubicado en un país de la Unión Europea, se estará a las previsiones contenidas en los arts. 202 y 204 de la Ley 23/2014, de 20 de noviembre, *de reconocimiento mutuo de resoluciones penales en la Unión Europea*.

Son acreedores del deber de colaboración y asistencia, según el precepto, el Juez, el Ministerio Fiscal y los agentes de la Policía Judicial. La referencia al Ministerio Fiscal debe interpretarse conjugando esta previsión con los arts. 588 bis b, 588 ter d, 588 ter m y 588 octies. Efectivamente, si el Ministerio Fiscal está legitimado para instar del Juez la intervención de comunicaciones telefónicas y telemáticas (art. 588 bis b) y en la solicitud de autorización judicial deben incluirse los datos necesarios para identificar el terminal o medio de comunicación a intervenir (art. 588 ter d), cobra sentido que se imponga a los sujetos obligados el deber de asistencia al Ministerio Fiscal cuando éste ejerza las facultades que le reconocen los arts. 588 ter m (identificación de titulares o terminales o dispositivos de conectividad) y 588 octies (orden de conservación de datos). También cobra sentido este deber de asistencia al Ministerio Fiscal cuando en el marco de unas diligencias de investigación propias haga uso de esa facultad prevista en el art. 588 ter m.

Cuando se trate de prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, el contenido de su obligación viene precisado por el art. 39 LGT que, entre otros extremos, establece que "en el caso de que los sujetos

obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles" (art. 39.11 LGT). Igualmente deberán tenerse en cuenta, en estos casos, las previsiones contenidas en los arts. 83 y siguientes del 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 los usuarios*. Ahora bien, el contenido de tales preceptos debe ser interpretado como un mínimo que no impide la exigencia, en función de las circunstancias concurrentes en un caso concreto, de mayores cotas de colaboración, al no poderse ver privilegiados estos sujetos obligados frente a otros respecto de los que no existen previsiones legales acerca del contenido de su colaboración y atendiendo, además, a que el precepto no impone límites a ese deber de asistencia.

Para concluir, debe señalarse que la obligación de asistencia y colaboración viene complementada, en el apartado segundo del precepto, con otra de *guardar secreto acerca de las actividades requeridas por las autoridades*, cuyo conocimiento por las personas afectadas podría, con toda seguridad, frustrar el resultado de la investigación. El incumplimiento de cualquiera de estas dos obligaciones -asistencia y colaboración, y secreto-, conforme al apartado tercero del precepto, podrá dar lugar a un delito de desobediencia. Se reitera, de esta forma, la previsión ya contenida con carácter general para todas las medidas de investigación tecnológica en el art. 588 bis c.3.h, por lo que deberá estarse a lo expuesto sobre este extremo en la Circular 1/2019.

8. Control de la medida

El art. 588 ter f, desarrollando para las interceptaciones telefónicas y telemáticas la previsión general de control judicial que para toda medida de investigación tecnológica contiene el art. 588 bis g, establece concretas medidas para hacerlo efectivo.

Como ya se indicaba al analizar el alcance del art. 588 bis g en la Circular 1/2019, el control judicial de la medida forma parte del derecho fundamental, habiéndose desarrollado una consolidada jurisprudencia que fija el alcance de este control en los supuestos de intervenciones telefónicas y que la Circular 1/2013, *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas,* sintetizaba señalando que "para considerar cumplido el requisito de control judicial es suficiente con que los autos de autorización y prórroga fijen periodos para que la fuerza actuante dé cuenta al Juzgado del resultado de las intervenciones, y que el órgano judicial efectúe un seguimiento de las mismas y conozca los resultados de la investigación, que debe tener en cuenta para autorizar las prórrogas, conocimiento que puede obtenerse a través de las transcripciones remitidas y los informes efectuados por quienes la llevaban a cabo (SSTC nº 25/2011, de 14 de marzo; 72/2010, de 18 de octubre; 205/2005, de 18 de julio; 239/2006, de 17 de julio; 197/2009, de 28 de septiembre; y 26/2010, de 27 de abril)".

El legislador de 2015, recogiendo toda esa doctrina jurisprudencial, que hay que entender plenamente vigente, ha fijado en los arts. 588 bis g y 588 ter f, las siguientes exigencias para el control judicial de la interceptación de las comunicaciones:

- Que la Policía Judicial informe al Juez de Instrucción del desarrollo y resultados de la medida.
- Que el Juez establezca en la resolución judicial habilitante la periodicidad y la forma con la que la Policía Judicial deberá informarle del desarrollo de la medida.
- Que la Policía Judicial ponga a disposición del Juez, en los plazos fijados, dos soportes digitales distintos, uno con la transcripción de los pasajes que considere de interés y otro con las grabaciones íntegras realizadas.
- Que en las grabaciones se indique el origen y destino de cada una de las comunicaciones.

- Que la Policía Judicial asegure *mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.*
- Que la Policía Judicial informe de los resultados de la medida cuando se ponga fin a la misma.

De todos estos requisitos, sin embargo, solamente la falta del efectivo seguimiento y control de la medida por parte del Juez que la haya acordado será lo que invalide la interceptación, generando su nulidad, no así otras posibles deficiencias que no impidan este control, que no pasarán de meras irregularidades procesales sin trascendencia constitucional. Se incluyen, entre estas últimas, por ejemplo, el incumplimiento de los plazos de rendición de cuentas ante el Juzgado (STS nº 250/2017, de 5 de abril), la falta de entrega de dos soportes distintos o el incumplimiento de las garantías de sellado.

Una de las novedades más importantes que ha supuesto la nueva regulación es la exigencia de que la Policía Judicial ponga a disposición del Juez dos soportes digitales distintos de las grabaciones. Esta previsión resultó valorada muy positivamente por el informe del Consejo Fiscal al Anteproyecto, al considerar que, de esta forma, se mantienen intactas las garantías de la defensa, permitiendo al propio tiempo economizar esfuerzo al Juez y Fiscal. Efectivamente, la aportación al procedimiento de las grabaciones íntegras constituye una garantía esencial para la salvaguarda del derecho de defensa, mientras que la selección de comunicaciones relevantes para la investigación en un soporte distinto facilita enormemente el acceso a lo que realmente es importante para el procedimiento.

El adecuado control judicial debe traducirse, además, en la exigencia a la Policía Judicial, no solo de los dos soportes digitales que menciona el precepto, sino también de informes de investigación referidos al periodo de rendición de cuentas, donde se explicarán el contenido, significado y trascendencia de las

comunicaciones intervenidas, así como el resultado del resto de la investigación que aporte datos necesarios para la adecuada interpretación de las comunicaciones intervenidas.

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.

Efectivamente, los soportes digitales aportados por la Policía Judicial serán ordinariamente utilizados, no solo para posibilitar el adecuado control judicial, sino también para introducir la prueba en el acto del juicio oral. Guarda silencio la LECrim acerca de la forma de practicar esta prueba en el plenario, por lo que habrá que estar a la doctrina jurisprudencial existente. En este sentido, señala la STS nº 513/2010, de 2 de junio, que será necesario “la audición o lectura de las mismas en el juicio oral, que da cumplimiento a los principios de oralidad y contradicción, previa petición de las partes, pues si estas no lo solicitan, dando por bueno su contenido, la buena fe procesal impediría invocar tal falta de audición o lectura en esta sede casacional”, añadiendo esta misma sentencia que la transcripción y cotejo bajo la fe del Letrado de la Administración de Justicia únicamente será necesaria en los casos en los que se opte por la lectura y no por la audición. Merece destacarse, especialmente, la plena validez probatoria de las comunicaciones interceptadas que sean introducidas en el juicio oral como prueba

documental que se dé por reproducida, siempre que ninguna de las partes solicite su audición al Tribunal (SSTS nº 789/2011, de 20 de julio y 578/2012, de 26 de junio y STC nº 26/2010, de 27 de abril, entre otras).

Igualmente resulta novedosa la exigencia de que se asegure la *autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas.* Su justificación descansa, según el preámbulo de la LO 13/2015, en la necesidad de homologar el proceso penal a las exigencias de validez de aportación al proceso de documentos en formato electrónico que venía siendo exigida en otras jurisdicciones, lo que ya había sido acogido por una línea jurisprudencial de la Sala Segunda del Tribunal Supremo. La previsión, sin embargo, resultará únicamente aplicable en aquellos supuestos en los que las comunicaciones resulten grabadas en un ordenador central, aportándose al proceso copia de las mismas. Este será el caso más frecuente (SITEL, SILTEC, SIBORG, etc.) pero, junto con él, existirán otras intervenciones que serán practicadas de manera diferente (como será el caso de algunas comunicaciones telemáticas), lo que obligará, en estos casos, a extremar las cautelas para garantizar la integridad y autenticidad de los soportes digitales que se aporten al procedimiento.

9. Duración y prórrogas

Habiéndose abordado ya el análisis de las exigencias y vicisitudes que resultan de la fijación de la duración y prórrogas de las medidas de investigación tecnológica con carácter general en la Circular 1/2019, se hará a continuación referencia a las particularidades que presenta el plazo y sus prórrogas en el caso de la interceptación de comunicaciones telefónicas y telemáticas (arts. 588 ter g y 588 ter h).

Tres son los aspectos específicos que la LECrim regula en relación con la duración y prórrogas de las interceptaciones telefónicas y telemáticas que complementan la regulación general:

- La duración máxima de la autorización de intervención y de sus prórrogas.
- La necesidad de que la Policía Judicial aporte la transcripción de los pasajes relevantes que permitan fundamentar la prórroga.
- La posibilidad de que el Juez, antes de conceder la prórroga, solicite aclaraciones o mayor información.

La duración máxima inicial que se fija para la medida es de tres meses, prorrogables por periodos sucesivos de igual duración hasta un máximo de dieciocho. La extensión de la medida, tanto en su plazo inicial como en el cómputo global, deberá estar fundamentada en los principios rectores del art. 588 bis a. De esta forma, por ejemplo, para fijar un plazo inicial que alcance los tres meses de duración máxima, deberá justificarse la necesidad de esa extensión en el caso concreto, así como su proporcionalidad. El principio de proporcionalidad también deberá ir ganando protagonismo en la fundamentación de las prórrogas a medida que se acerque el plazo máximo de duración de la interceptación, pues solo la gravedad del delito investigado, unido a las necesidades de la investigación, podrá justificar el agotamiento de los plazos máximos de duración.

Los plazos, como dice el precepto, se computarán *desde la fecha de autorización judicial* y no desde la fecha efectiva de la interceptación, objetivando y aportando seguridad jurídica, de esta forma, en una materia en la que, a pesar de las diferentes interpretaciones doctrinales, la jurisprudencia venía pronunciándose desde hacía tiempo en este sentido (entre otras, STC nº 205/2005, de 18 de julio y STS 7/2014, 22 de enero). Resultará irrelevante, por lo tanto, que la efectiva interceptación de las comunicaciones no haya comenzado hasta transcurridos algunos días de su autorización judicial porque, por ejemplo, existan problemas técnicos; el plazo de autorización correrá siempre desde la fecha del auto habilitador.

El cómputo, además, deberá hacerse en relación con cada investigado cuyo derecho fundamental se vea limitado, sin que sea procedente un cómputo total

para todo el procedimiento o un cómputo para cada concreto medio de comunicación intervenido. Así, por ejemplo, el cambio de terminal de teléfono móvil que realice un investigado no debe motivar que se inicie de nuevo el cómputo del plazo, del mismo modo que, si se cesa temporalmente en la medida para después reanudarla, el cómputo no deberá iniciarse de nuevo, sino que continuará el anterior. Por el contrario, si se inicia una nueva investigación sobre el mismo sujeto por hechos diferentes a los que motivaron la intervención de sus comunicaciones, dando lugar a un nuevo procedimiento, deberá reiniciarse el cómputo del plazo de los dieciocho meses, al tener que renovarse también completamente la motivación y fundamentación de la resolución judicial que autorice la medida. Esta circunstancia se dará, por ejemplo, en los supuestos de hallazgos casuales que, conforme al art. 588 bis i, propiciará la formación de un nuevo procedimiento, no afectando al nuevo plazo el tiempo ya transcurrido de intervención telefónica en el procedimiento de origen.

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.

La prórroga de la medida requerirá, según establece el art. 588 ter h, la aportación por parte de la Policía Judicial de *la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.* Mantiene plenamente su vigencia, por lo tanto, lo que se expone en la Circular nº 1/2013 cuando señala que “las exigencias de motivación deben ser igualmente observadas en las prórrogas y las nuevas intervenciones acordadas a partir de datos obtenidos en una primera intervención, debiendo el Juez conocer los resultados de la intervención con carácter previo a acordar su prórroga y explicitar las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión tácita o presunta a la inicialmente obtenida (SSTC nº 25/2011, de 14 de marzo; 261/2005, de 24 de

octubre; y 26/2010, de 27 de abril; y SSTS nº 940/2011, de 27 de septiembre; y 1044/2011, de 11 de octubre)". La falta de aportación de las transcripciones, sin embargo, no tiene por qué invalidar la medida, siendo aplicable la prolija doctrina jurisprudencial a la que ya se hizo referencia acerca del alcance del control judicial en los casos en los que las prórrogas no fueran precedidas de transcripciones o escuchas de grabaciones.

La Ley prevé igualmente la posibilidad de que el Juez, antes de acordar la prórroga, solicite aclaraciones o mayor información acerca del desarrollo de la investigación. Este incidente no suspenderá el plazo de dos días que para resolver sobre las prórrogas establece, con carácter general, el art. 588 bis f. En consecuencia y con el fin de evitar que pudiera expirar el plazo fijado sin haberlo prorrogado, interviniéndose de esta forma conversaciones sin cobertura judicial, es recomendable que las solicitudes de prórroga sean presentadas ante el Juez con, al menos, tres días de antelación a la expiración del plazo fijado para la medida. Debe recordarse que la expiración del plazo sin que se haya acordado la prórroga impedirá que puedan valorarse las conversaciones intervenidas a partir de ese momento y hasta la fecha del auto de prórroga, no siendo posible su convalidación por la posterior prórroga.

Es preciso insistir, por último, en que la fundamentación de la prórroga de una medida de interceptación de las comunicaciones debe centrarse, no en la procedencia de la interceptación, que constituye el objeto de la resolución inicial habilitante, sino en la procedencia de la prórroga. Por lo tanto, será la necesidad de continuar con la medida, en atención al desarrollo de la investigación, su idoneidad, vistos los resultados arrojados y su proporcionalidad, al confirmarse la gravedad del delito, lo que justificará la prórroga (en este sentido la STS nº 497/2016, de 9 de junio) y todo ello sin perjuicio de la heterointegración de la resolución acordando la prórroga con las anteriormente dictadas cuando la motivación del auto así lo exija. De esta manera, por ejemplo, en el caso frecuente de que el investigado haya cambiado de teléfono para dificultar una eventual investigación de sus actividades (que, en puridad, no supondría una prórroga, sino lo que se ha denominado

ampliación instrumental), lo que deberá justificarse y acreditarse indiciariamente es ese cambio de teléfono, así como que persiste la necesidad de la intervención, sin que sea preciso reiterar nuevamente toda la fundamentación del auto inicial (STS nº 446/2012, de 5 de junio).

10. Acceso de las partes a las grabaciones

10.1. Derecho de las partes a acceder a las grabaciones

El derecho de los afectados por una medida de interceptación de sus comunicaciones a conocer que se ha producido la intervención y las concretas comunicaciones intervenidas ha venido siendo reconocido por la jurisprudencia del TEDH. La STEDH de 6 de septiembre de 1978, caso Klass y otros contra Alemania, señalaba ya que la notificación de la interceptación de las comunicaciones, una vez concluida, está indisolublemente vinculada a la de la efectividad de los recursos judiciales y, por tanto, a la existencia de garantías efectivas contra el abuso de los poderes públicos. Como fundamento y finalidad de este derecho pueden señalarse, además del derecho del afectado a conocer el volumen de información que el Estado dispone sobre él, posibilitar que pueda ejercitar sus derechos (como son los de pedir la destrucción de los registros o ejercitar acciones penales por la intromisión, por ejemplo) y, sobre todo, ejercer su derecho de defensa cuando tales comunicaciones vayan a ser utilizadas contra él en un proceso penal.

El reconocimiento de este derecho se ha incluido en el art. 588 ter i LECrim, que comprende, tanto el derecho de las partes a obtener copias de las grabaciones y de las transcripciones -salvo de aquellas que afecten a la vida íntima de las personas-, como el derecho de los terceros, ajenos al proceso, cuyas comunicaciones hayan resultado intervenidas, a conocer la intervención y, eventualmente, obtener copias de las mismas. Las copias que las partes personadas podrán obtener serán tanto de las grabaciones como de sus transcripciones lo que, en la práctica, supondrá darles acceso a las diversas piezas

separadas que se hayan podido formar para la tramitación de la medida de investigación. La falta de notificación de la interceptación a las partes, como ya señalaba la Circular 1/2013, privaría a estas de obtener la tutela de sus derechos fundamentales (ATS de 18 de junio de 1992).

El momento que marca la entrega es doble: expiración de la vigencia de la medida y alzamiento del secreto.

La Ley establece, igualmente, la obligación del Juez, previa a la entrega de copias a las partes, de llevar a cabo un filtro de las comunicaciones intervenidas. Dice el precepto, de manera poco precisa, que el Juez deberá excluir de las copias que entregue los datos referidos a aspectos de la vida íntima de las personas. En realidad, buena parte del contenido de lo grabado incidirá, en mayor o menor medida, en la intimidad de los afectados; el precepto deberá interpretarse, por lo tanto, en el sentido de que el Juez excluya de las copias aquellas grabaciones que, afectando a la intimidad de los investigados, no resulten necesarias a los fines del procedimiento. En consecuencia, las copias a entregar deberán limitarse, únicamente, a aquellas comunicaciones que pudieran tener relevancia para el procedimiento, preservando el resto de la intimidad del afectado del conocimiento ajeno. Esa labor judicial de escrutinio que impone el respeto al derecho fundamental de los afectados por la medida deberá estar guiada por los mismos principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad que presiden la propia medida; la concurrencia y valoración de estos principios deberá reflejarse en la resolución judicial que se dicte, exponiendo en ella, en su caso, las comunicaciones intervenidas que se excluyen de las copias y el fundamento de la exclusión.

A pesar de la imprecisión del precepto, las copias que no deberán ser entregadas por afectar a la vida íntima de las personas serán tanto de las grabaciones como de las transcripciones. Cualquier otra interpretación conduciría a la ineficacia del fin pretendido, preservar el núcleo más íntimo del investigado. Además, deberán excluirse también de las copias las comunicaciones entre el investigado y su

letrado que pudieran haber sido interceptadas, en los términos previstos en el art. 118.4 LECrim.

La decisión del Juez acerca de las comunicaciones que se excluyan de las copias entregadas a las partes puede ser revisada a petición de éstas. Para ello, concederá el Juez un plazo acorde con el volumen de las comunicaciones intervenidas a fin de que las partes puedan examinar las grabaciones, solicitando a continuación las inclusiones que consideren procedentes. Aunque el precepto guarda silencio, deberá entenderse, igualmente, que las partes podrán solicitar también la exclusión de pasajes que hayan sido incluidos en la copia de las transcripciones que, sin aportar nada al procedimiento, afecten a su vida íntima. Este trámite, a diferencia de lo que propugnaban algunas soluciones jurisprudenciales y doctrinales, así como el art. 287.1 del Anteproyecto LECrim de 2011, se desarrollará por escrito y no mediante comparecencia ante el Juez. Concluye el precepto señalando que *el juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.*

Así pues, podrán existir dos resoluciones judiciales razonando las exclusiones; una primera en la que el Juez decida no incluir en las copias determinados pasajes de las grabaciones por afectar a la vida íntima de las personas (art. 588 ter i.1) y, eventualmente, una segunda en la que el Juez admita o rechace la solicitud de inclusión o exclusión que le dirijan las partes (art. 588 ter i.2). Existiendo en la Ley un trámite para que las partes puedan solicitar inclusiones o exclusiones, deberá entenderse que no cabrá recurso contra la primera de estas resoluciones judiciales con fundamento, precisamente, en la necesidad de incluir o excluir determinadas grabaciones en las transcripciones. El trámite correcto será solicitar la inclusión o exclusión, procediendo el recurso, esta vez sí, contra el auto que desestime la solicitud.

Por último, merece destacarse que el precepto no impone al Juzgado la obligación de transcribir, sino que se refiere a la entrega de copia de las transcripciones que, conforme al art. 588 ter f, hubieran sido puestas a disposición del Juzgado por la

Policía Judicial con el fin de posibilitar el control de la medida. En consecuencia, las partes no pueden pedir que sea el Juzgado quien realice una determinada transcripción, puesto que esa es una tarea policial. Lo que sí pueden hacer es discrepar de la transcripción realizada por la Policía, solicitando del Juzgado que, si no se hubiera hecho ya, se proceda al cotejo de las transcripciones con los soportes originales, labor que se llevará a cabo por el Letrado de la Administración de Justicia.

10.2. Derecho de terceros afectados de conocer la intervención de sus comunicaciones

El apartado tercero del art. 588 ter i impone la notificación de la intervención de sus comunicaciones a terceros que, no siendo parte en el procedimiento, hayan sido grabados en algún momento. Se incluyen aquí, también, los investigados que no hayan finalmente adquirido la condición de parte procesal y aquellos otros respecto de los cuales se haya sobreseído el procedimiento. En este caso, el precepto únicamente impone la obligación de informarles de la intervención de sus comunicaciones y de las concretas comunicaciones en las que hayan participado, pero no de entregarles copia, que, en su caso, requerirá, además de la solicitud del interesado, de un nuevo juicio valorativo por parte del Juez, que deberá concluir que la entrega de las copias no afecta al derecho a la intimidad de otras personas ni resulta contrario a los fines del proceso. En consecuencia, si la entrega de copias de las grabaciones supone la entrega de pasajes que desvelan la intimidad de terceros afectados, estará justificada la denegación.

En estos casos, no obstante, establece el precepto diversos supuestos que permitirían excepcionar la medida. El primero de ellos, que la notificación resulte imposible o exija un esfuerzo desproporcionado; la imposibilidad podrá venir derivada, por ejemplo, del desconocimiento de la identidad de las personas que participan en las conversaciones o de su ignorado paradero. Ante esta posibilidad, como regla general, no estará justificada la práctica de diligencias encaminadas a la identificación de tales interlocutores, al resultar ajena a los fines de la instrucción.

Además, la identificación de alguien que no lo estaba, puede suponer una mayor intromisión en su intimidad, al poder relacionar la conversación grabada con una persona concreta.

La segunda excepción se dará en los casos en los que dicha notificación suponga un esfuerzo desproporcionado. Estos supuestos habrá que circunscribirlos a los casos en los que, existiendo numerosos investigados o habiendo durado varios meses la investigación, la tarea de individualizar las conversaciones de todos los afectados y proceder a su citación y notificación, así como a atender sus diversas demandas, suponga un esfuerzo que no esté al alcance racional de la capacidad del Juzgado.

El último de los motivos de excepción a la previsión legal se dará en los casos en los que la notificación de las intervenciones a terceros pueda perjudicar futuras investigaciones. Se incluirán aquí, por ejemplo, aquellas intervenciones de comunicaciones que no hayan culminado finalmente con una imputación, provocando un sobreseimiento provisional del procedimiento y que, por su propia naturaleza, podría volver a reabrirse e impulsarse la investigación ante la aparición de nuevos indicios (en este sentido, STS nº 960/2008, de 26 de diciembre). En estos casos, la notificación de la medida a los investigados frustraría, con toda seguridad, esa eventual futura reapertura. En palabras de la STEDH de 6 de septiembre de 1978 (caso Klass contra Alemania), *una notificación ulterior a cada individuo afectado por una medida ulteriormente levantada podría comprometer el fin a largo plazo que motiva el origen de la vigilancia.* Igualmente podría pensarse en supuestos de terrorismo o criminalidad organizada, en los que la información obtenida con una interceptación de comunicaciones que posteriormente no culminara en una acusación sirve en numerosas ocasiones para el desarrollo de nuevas investigaciones que, de ser alertados los investigados, quedarían frustradas.

La expresa previsión del artículo que se analiza permitirá omitir la notificación a terceros sin necesidad de mantener el secreto de las actuaciones. En cuanto a la

duración del periodo durante el cual podrá mantenerse el silencio sobre la interceptación de las comunicaciones, no dice nada el precepto, a diferencia de lo que preveía el art. 286 del Anteproyecto de LECrim de 2011, que señalaba expresamente, como límite máximo, la duración del propio procedimiento en el que se hubiera adoptado la medida. En consecuencia, el único límite temporal al que ahora aparece sujeta la previsión será la subsistencia de la causa que motivó la excepción de notificación. Por lo tanto, podrá mantenerse esta situación mientras dure la situación de imposibilidad, desproporción del esfuerzo o perjuicio para futuras investigaciones.

Para concluir, es preciso señalar que el incumplimiento de la obligación de notificar la interceptación de sus comunicaciones a los terceros afectados no perjudicará en nada a la validez de la medida. Únicamente podrían verse afectados los derechos del tercero que, por otra parte, dispone del cauce previsto con carácter general en el art. 240 LOPJ para obtener acceso a aquellas partes de un procedimiento que pudieran afectarle. En cualquier caso y con el fin de cumplir adecuadamente la previsión legal, deberá exigirse en todos los procedimientos, una vez concluida la práctica de la medida de interceptación de las comunicaciones, una resolución judicial que acuerde la comunicación a terceros o justifique la exclusión en el caso concreto, resolución ésta que bien pudiera ser la que acuerde el cese de la medida.

11. Incorporación al proceso de datos de tráfico o identificación

11.1. Regulación legal

El Capítulo V, del Título VIII, del Libro II, consagrado a la interceptación de las comunicaciones telefónicas y telemáticas, concluye con dos secciones que comprenden cuatro artículos (588 ter j, a 588 ter m); el art. 588 ter j regula la incorporación al proceso de datos de tráfico o asociados que se encuentren vinculados a procesos de comunicación, que requerirán siempre autorización judicial, y los arts. 588 ter k al 588 ter m abordan el acceso a determinados datos de identificación de usuarios o dispositivos, que no requiere autorización judicial.

A la hora de determinar qué datos aparecen vinculados a procesos de comunicación y cuáles no, suele distinguirse entre datos de naturaleza dinámica y los de naturaleza estática. Los primeros son los que se generan durante un proceso de comunicación, mientras que los segundos aparecen almacenados en las bases de datos de los prestadores de servicios de comunicación para posibilitar esas comunicaciones, pero no se generan como consecuencia de una comunicación concreta. A esta misma conclusión conduce la definición que, sobre los datos de tráfico, ofrece el art. 1.d del Convenio sobre la Ciberdelincuencia, que señala que por datos sobre el tráfico "se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".

El debate en cuanto a la necesidad de autorización judicial, sin embargo, ya no está en la determinación de qué datos afectan al derecho fundamental al secreto de las comunicaciones. A la vista de la nueva regulación de la LECrim pueden ahora distinguirse dos categorías de datos: los vinculados a un proceso de comunicación, cuya incorporación al proceso se regirá por lo previsto en el art. 588 ter j (excepción hecha de la dirección IP en los casos que prevé el art. 588 ter k) y el resto de los datos de tráfico, no vinculados a procesos de comunicación, entre los que el legislador ha destacado, en los arts. 588 ter l y m, la numeración IMSI e IMEI y los datos de identificación del titular de números telefónicos o los números que corresponden a un titular.

Resulta necesario precisar también que, si bien la incorporación al proceso de datos de tráfico o asociados ya aparece prevista como un posible contenido de la interceptación de las comunicaciones en el art. 588 ter b, la regulación que aquí se comprende será aplicable a los supuestos en los que estos datos se incorporen al proceso independientemente de la interceptación del contenido de una comunicación, bien porque ésta ya hubiere concluido, bien porque no hubiere

llegado a existir (en los casos de llamadas frustradas) o bien porque se considere suficiente a los fines de la investigación con los datos de tráfico, sin necesidad de acceder al contenido de la comunicación. Se trata de la incorporación al proceso de datos de tráfico o asociados que hayan sido almacenados o conservados y no intervenidos a tiempo real.

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

Existen determinados datos electrónicos que se generan como consecuencia de una comunicación y cuya incorporación a un procedimiento puede resultar decisiva para la investigación de ciertos comportamientos delictivos. A los mismos se refiere el art. 588 ter j, exigiendo autorización judicial para ello. Dentro de estos datos es posible distinguir entre los conservados por propia iniciativa, motivos comerciales o de otra índole, por cualquier prestador de servicios de Internet (entre ellos, los datos preservados como consecuencia de una orden de conservación emitida por el Ministerio Fiscal, la Policía Judicial, o incluso el propio Juez de Instrucción, al amparo de las previsiones contenidas en el art. 588 octies) y aquellos cuya conservación impone la legislación a los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones. La delimitación e identificación de estos últimos, así como el establecimiento del deber de conservarlos, aparece regulado en el art. 3 de la Ley 25/2007 y en el art. 39 LGT. 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.

El art. 39 LGT, por su parte, incluye, entre otros, la identidad e identificación de los comunicantes, su domicilio, correo electrónico o geolocalización en el momento de la comunicación.

La exigencia de autorización judicial para la incorporación de estos datos al proceso mantiene el sistema instaurado por la Ley 25/2007 y, además, se adecúa a la doctrina sentada por las sentencias del TJUE de 8 de abril de 2014 y 21 de diciembre de 2016 sobre la Directiva 2006/24/CE, que abogaban por el control judicial de dicha cesión a fin de garantizar adecuadamente los derechos fundamentales a la intimidad y a la protección de datos. Ahora bien, no todos los datos que se incluyen en el art. 3 de la Ley 25/2007 y 39 LGT aparecen vinculados a un proceso de comunicación y, en consecuencia, sujetos al régimen del art. 588 ter j, sino que también se incluyen otros datos que, si bien resultan necesarios para el establecimiento de una comunicación, no se vinculan a comunicaciones concretas. Como antes se adelantaba, el legislador ha optado por precisar alguno de ellos en los artículos siguientes de la LECrim, dispensándolos de la autorización judicial. A contrario, para recabar datos incluidos en el art. 3 de la Ley 25/2007 se precisará autorización judicial, a excepción de los expresamente dispensados por la LECrim.

El primer problema que cabe plantearse en relación con la incorporación al proceso de estos datos es el de si únicamente resultará posible cuando se trate de alguno de los delitos que determina el art. 588 ter a o, por el contrario, esa delimitación objetiva solo es predicable de la interceptación de la comunicación en sentido estricto, pero no de la incorporación al proceso de los datos. El problema no tiene una solución clara y ello obliga a actuar con cautela. El análisis de los precedentes legislativos y del proceso de gestación de la LO 13/2015 conduce a inclinarse por la segunda postura. Efectivamente, el Anteproyecto de la Ley de reforma limitaba expresamente la posibilidad de incorporación de los datos al proceso a los delitos

para los que se autorizaba la medida de intervención telefónica. Esta previsión fue objeto de críticas en el informe del Consejo Fiscal, que ponía de relieve que la incorporación de los datos al proceso supone una medida mucho menos invasiva que la interceptación de las comunicaciones. La consecuencia final ha sido la eliminación del art. 588 ter j de toda referencia expresa al catálogo de delitos para los que se permite la interceptación de comunicaciones, por lo que parece que la previsión podría interpretarse en un sentido más amplio. Ahora bien, no debe desconocerse que la incorporación al procedimiento de estos datos de tráfico va a suponer siempre una limitación de los derechos de los investigados que, en atención a su trascendencia, exigirá siempre que se justifique su necesidad para la investigación de delitos que revistan una cierta gravedad. En consecuencia, deberá incluirse siempre una especial motivación de la proporcionalidad de la medida que justifique que el sacrificio de esos derechos no va a resultar superior al beneficio que para el interés público y de terceros haya de resultar de la incorporación de los datos de tráfico al procedimiento.

El art. 588 ter j se limita a establecer la necesidad de autorización judicial para incorporar estos datos al proceso, no de precisar quiénes son los sujetos obligados a la conservación de los datos o a atender el requerimiento judicial. Ello, no obstante, hace extensiva su previsión, no solo a los datos conservados por los prestadores de servicios o personas obligadas por la legislación sobre retención de datos relativos a las comunicaciones electrónicas (los referidos en la Ley 25/2007), sino también, a los conservados por cualquier otra persona o entidad que pueda poseer estos datos por motivos comerciales o de otra índole. Se amplía, de esta forma, el ámbito de los datos que es posible incorporar al procedimiento, más allá de los términos previstos en el referido art. 3 de la Ley 25/2007, a cualesquiera otros datos que aparezcan vinculados a un proceso de comunicación. Se incluirían aquí, por ejemplo, los *log* o registros que el administrador de cualquier página web pudiera tener acerca de concretas comunicaciones que se hayan podido desarrollar a través de la misma (identificación de los comunicantes, fecha y hora de la comunicación, contenido de la comunicación, etc.)

El apartado segundo del precepto se encarga de recordar que la petición de estos datos por el Juez deberá precisar concretamente qué datos requiere y las razones que justifican la petición. Como ya se indicaba al analizar el art. 588 ter b, vuelve la LECrim a incidir en este extremo con el propósito de poner fin a la práctica consistente en la petición generalizada e indiscriminada de todos los datos de tráfico de los que pudiera disponer el prestador de servicios. Será necesario, por tanto, una resolución judicial que justifique, conforme a los principios rectores y, entre ellos, especialmente, el principio de necesidad, la procedencia de la incorporación de tales datos al procedimiento.

11.3. Identificación mediante número IP

El art. 588 ter k regula la forma de proceder en los casos en los que se quiere identificar la persona que se encuentra detrás de una comunicación mantenida a través de Internet que, con carácter general, será el método que se siga para investigar muchos de los delitos cometidos a través de este medio.

El punto de partida, en estos casos, va a ser siempre la determinación de la dirección IP a través de la cual se haya producido la comunicación telemática objeto de investigación y aquí pueden plantearse dos posibilidades: que para la determinación de la dirección IP haya que solicitar el dato a un prestador de servicios de comunicación obligado a su conservación por la Ley 25/2007 o que los investigadores hayan podido obtener la dirección IP sin necesidad de recurrir al prestador de servicios.

En el primer caso, la petición del dato deberá acomodarse a las previsiones del art. 588 ter j, al tratarse de un dato vinculado a un proceso de comunicación. Por lo tanto, sería necesaria autorización judicial. El segundo caso, cuando los investigadores hayan podido obtener la dirección IP sin necesidad de recurrir al prestador de servicios, es el que daría lugar a la aplicación del régimen que contiene el art. 588 ter k.

En este último supuesto, si la Policía Judicial puede determinar una dirección IP a través de la cual se estuviera cometiendo un delito careciendo de información acerca de la identificación y localización del equipo o dispositivo que la estuviera utilizando o de la identidad del usuario del mismo, deberá recabar autorización judicial para obtener de los sujetos obligados, conforme al art. 588 ter e, esos datos de identificación y localización. En realidad, lo que prescribe el precepto es que la Policía Judicial no necesita autorización judicial para determinar la dirección IP si puede hacerlo sin recurrir al operador de comunicaciones electrónicas obligado por la Ley 25/2007 (obteniéndola directamente de Internet, si fuere posible); para lo que sí la necesitará será para relacionar esa dirección IP con un equipo o dispositivo concreto y, en último término, con la persona usuaria del mismo. El fundamento de esta previsión se encuentra en que la dirección IP, por sí sola, no identifica a persona alguna. Su operatividad se pone de manifiesto, únicamente, cuando se interrelaciona esa dirección IP con ciertos datos de identidad conservados por las operadoras de comunicaciones. Es decir, la dirección IP no identifica, pero permite identificar; por lo tanto, su obtención no resultaría extraña a las labores policiales que regula el art. 22.2 de la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente conforme a la disposición transitoria de la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*), que permite la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, pero la identificación final del usuario mediante el cruce de ese dato con los conservados por imposición de la Ley 25/2007, sí precisará de esa autorización judicial.

Ciertamente, esta previsión no hace más que incorporar al articulado de la LECrim la doctrina jurisprudencial elaborada por el Tribunal Supremo en los últimos años y que sintetizaba de manera muy precisa la Circular 1/2013 cuando señalaba que “el Tribunal Supremo considera que estos datos -*la dirección IP*- no se encuentran protegidos ni por el art. 18.1 CE, ni por el art. 18.3 CE (SSTS nº 292/2008, de 28 de mayo; y 776/2008, de 18 de noviembre). Tras la averiguación del IP, las subsiguientes actuaciones de identificación y localización de quién sea la persona

que tiene asignado ese IP se deben llevar a cabo bajo control judicial. No obstante, debe tenerse presente una matización: la jurisprudencia distingue por un lado los casos de rastreo policial del espacio público y por otro lado los supuestos en los que para acceder a una información sobre IP es necesario oficiar a una operadora. En este último supuesto, es necesario obtener autorización judicial conforme a las previsiones de la Ley 25/2007 (SSTS nº 292/2008, de 28 de mayo; nº 236/2008, de 9 de mayo; nº 680/2010, de 14 de julio)".

Conviene precisar que la identificación de los equipos o de la persona que estuviera detrás de los mismos utilizando la dirección IP captada por la Policía Judicial, la acordará el Juez conforme a lo dispuesto en el art. 588 ter j y, por lo tanto, no solo será posible en relación con los delitos incluidos en el art. 588 ter a. Así se desprende, también, de la redacción definitiva de la Ley 13/2015 que, frente a la previsión específica en el Anteproyecto de ley de que se tratara de alguno de los delitos en los que era posible la interceptación de comunicaciones, suprimió esta previsión en el texto definitivo, ante la sugerencia en este sentido del informe del Consejo Fiscal.

11.4. Identificación de terminales mediante captación de códigos

El art. 588 ter l regula un supuesto íntimamente relacionado con el que se acaba de exponer, tanto en su fundamento, como en el tratamiento jurisprudencial dispensado al mismo. El precepto ha incorporado al texto legal una consolidada doctrina jurisprudencial nacida para dar respuesta a una práctica habitual de la Policía Judicial que tiene por finalidad la identificación de líneas telefónicas cuyas comunicaciones se pretende intervenir. Cuando en el desarrollo de una investigación fuera necesario intervenir las comunicaciones telefónicas de una persona cuyo número de abonado se desconozca, uno de los procedimientos utilizados para su determinación consiste en el empleo de diferentes medios técnicos que permiten captar los códigos de identificación o etiquetas técnicas del teléfono que lleve consigo o de alguno de sus componentes, tales como la numeración IMSI o IMEI. Con estos datos y previa consulta con la correspondiente

operadora telefónica, es posible identificar la línea telefónica que utiliza el investigado (su número comercial y titularidad, por ejemplo) y, en definitiva, proceder a su interceptación.

En este proceso, al igual que ocurría con la dirección IP, pueden distinguirse dos momentos; uno, cuando se recogen los datos técnicos de identificación por medio del escáner y, otro, cuando esos datos técnicos, después de ser cruzados con los conservados por las operadoras de telefonía, permiten identificar una línea telefónica y el resto de los datos que ello conlleva. Pues bien, nuevamente aquí, el precepto lo que realmente regula es la posibilidad de que la Policía Judicial pueda obtener los datos técnicos por medio del escáner sin necesidad de recabar previamente autorización judicial. Su fundamento es el mismo que antes se exponía: esos datos técnicos –fundamentalmente el IMSI y el IMEI-, no permiten la identificación de persona alguna. Solo el trámite posterior con la operadora será lo que posibilite esa identificación y de ahí que la autorización judicial sea necesaria para el segundo momento del proceso, pero no para el primero.

Esta solución, como se adelantaba, se encontraba ya plenamente consolidada en nuestra doctrina jurisprudencial desde la STS nº 249/2008, de 20 de mayo, señalando la Circular 1/2013: “El TS tiene declarada la legitimidad de que sea la propia Policía la que los obtenga -*los datos técnicos, concretamente, el IMSI y el IMEI*- por sí misma y por sus medios técnicos en la medida que con ellos se desconoce incluso el número telefónico concernido, y las llamadas que pudieran recibirse y efectuarse, y, por supuesto se desconoce igualmente las conversaciones (SSTS nº 1115/2011, de 17 de noviembre, 79/2011, de 15 de febrero; 249/2008, de 20 de mayo; 776/2008, de 18 de noviembre). Sin embargo, no puede la Policía solicitar tal información de las operadoras”, recordando más adelante el contenido de la STS 249/2008, cuando señalaba que “así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia”.

El precepto aporta una novedad. La Policía Judicial deberá informar al Juez de que ha utilizado artificios técnicos para la obtención de los datos que le presente para posibilitar la intervención telefónica. Se trata de extender el control judicial a todo el proceso de interceptación, incluso a estas actuaciones previas, con la finalidad de garantizar la transparencia y respeto a la Ley de toda la actuación. Ahora bien, el precepto exige que se informe de la utilización de artificios, pero no que se explique el funcionamiento concreto de estos, ni que se desvelen técnicas de investigación policial que, sin duda, podrían perjudicar futuras investigaciones. Únicamente en aquellos casos en los que pudieran suscitarse dudas razonables y fundadas acerca de la legalidad de los métodos o artificios utilizados sería exigible un mayor detalle en la justificación de la Policía Judicial. En cualquier caso, la falta de indicación de este extremo no tiene por qué afectar a la validez de la medida, siempre que no existan indicios de que la actuación policial ha sido ilegal, habiendo señalado la doctrina jurisprudencial que no puede presumirse que las actuaciones policiales "son ilegítimas e irregulares, vulneradoras de derechos fundamentales, mientras no conste lo contrario. Ello supondría la paradoja de que mientras que tratándose de los acusados ha de presumirse su inocencia, en tanto no se prueba su culpabilidad (art. 24.2 CE), a los Jueces y Tribunales, en el mismo marco procesal, ha de presumírseles una actuación contraria a la Constitución y a las Leyes, en tanto no se prueba que han actuado conforme a Derecho" (STS nº 246/2014, de 2 de abril).

En cualquier caso, la previsión que recoge este art. 588 ter l y la interpretación que de él se hace hay que entenderla circunscrita a la captación de códigos encaminada a una posterior interceptación de comunicaciones, pero no cuando lo que se pretende es la identificación de un determinado dispositivo de conectividad no vinculado a una comunicación concreta, supuesto este que caería dentro de la regulación del artículo siguiente que a continuación se analiza.

11.5. Identificación de titulares o terminales o dispositivos de conectividad

El art. 588 ter m regula ahora expresamente la incorporación al proceso de los datos necesarios para conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación que pudiera verse involucrado en una actividad delictiva o que estuviere utilizando una persona investigada. En estos casos, al tratarse de datos que no afectan al derecho fundamental al secreto de las comunicaciones y con la finalidad de facilitar la operatividad y agilidad de las investigaciones, se permite que puedan ser directamente recabados por el Ministerio Fiscal o la Policía Judicial.

En primer lugar, es preciso establecer el alcance objetivo de esta previsión, tanto en relación con los delitos en cuya investigación resultaría aplicable, como en relación con los concretos datos que el Ministerio Fiscal y la Policía Judicial pueden recabar directamente sin necesidad de autorización judicial.

En cuanto al primer extremo, no cabe duda de que la obtención de los datos a que se refiere este precepto resulta completamente extraña a la interceptación de comunicaciones. Es más, la gran mayoría de los casos en los que el Ministerio Fiscal o la Policía Judicial pudieran hacer uso de esta facultad podrían no tener relación, ni siquiera, con la preparación de una ulterior intervención de comunicaciones. En consecuencia, esta facultad no debe entenderse circunscrita a los supuestos de interceptación de comunicaciones que contempla el art. 588 ter a. Serán las disposiciones generales del art. 588 bis a las que deberán presidir la adopción de esta medida y, entre ellas, especialmente, y por lo que a la determinación de las modalidades delictivas a las que resulta aplicable se refiere, el principio de proporcionalidad. En particular, la STJUE de 2 de octubre de 2018 (asunto C-207/16) ha proclamado que, si bien la obtención de estos datos constituye una injerencia en los derechos fundamentales de los ciudadanos, no reviste la gravedad suficiente como para limitarla a la lucha contra la delincuencia

grave, estando justificada “por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general”.

En cuanto a los concretos datos que pueden ser recabados directamente por el Ministerio Fiscal o por la Policía Judicial, la previsión no se agota, simplemente, en la obtención de la titularidad de un número de teléfono o, en sentido inverso, en la obtención del concreto número telefónico que utilice una persona, sino que debe entenderse aquí incluida cualquier petición de datos encaminada a esa identificación del titular o del dispositivo de comunicación, siempre que no se trate de datos vinculados a procesos de comunicación.

Se incluirían aquí, por ejemplo, los supuestos de solicitud del IMSI que aparece asociado a un determinado dispositivo electrónico, con el fin de determinar quién es el usuario de ese dispositivo electrónico. Este supuesto se ha venido planteando con cierta frecuencia en los casos de sustracción de teléfonos móviles con el fin de identificar a la persona que lo tenía en su poder mediante la identificación del IMSI de la tarjeta SIM que estaba siendo utilizada por el usuario del teléfono. El IMSI, en estos casos, no puede ser considerado como un dato de tráfico y, por lo tanto, vinculado a un proceso de comunicación, pues no se genera como consecuencia de una comunicación concreta, sino que se trata, en palabras de la STS nº 249/2008, de 20 de mayo, de un código de identificación de cada dispositivo de telefonía móvil que sirve para posibilitar esa identificación a través de las redes GSM y UMTS; en consecuencia, puede fácilmente encuadrarse en el concepto de “dato identificativo de un medio de comunicación”, que utiliza el art. 588 ter m. Se trata, por lo tanto, de un supuesto diferente al que regula el art. 588 ter l en el que, como antes se analizaba, será necesario recabar autorización judicial para relacionar ese IMSI con otros datos que posibiliten la identificación del usuario.

Para concluir y en cuanto a la delimitación subjetiva de la previsión, debe hacerse referencia a los posibles destinatarios de la solicitud del Ministerio Fiscal o la Policía Judicial. El precepto abarca un amplio ámbito de aplicación, ya que se refiere a cualquier medio de comunicación y a cualquier dato que pueda facilitar el

conocimiento de la titularidad del medio o, en sentido inverso, la identificación del medio de comunicación de un titular ya conocido. Precisamente por eso, no limita el posible destinatario de la solicitud a los operadores obligados por la Ley 25/2007, sino que, por el contrario, se refiere de manera genérica a *los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información*.

12. Cláusula de vigencia

La presente Circular condensa la doctrina de la Fiscalía General del Estado en las materias que aborda, por lo que debe entenderse que quedan sin efecto, en todo aquello que se oponga a lo que en ella se contiene, las previsiones contenidas en otros documentos sobre esta misma materia, como la Circular 1/1999, *sobre la intervención de las comunicaciones telefónicas en el seno de los procesos penales* y la Circular 1/2013, *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas* (con la modificación incluida en la conclusión 7.1 hecha en la comunicación del FGE de 21 de octubre de 2014), sin perjuicio de que sus argumentos puedan ser de interés y complementarios a los que figuran en la presente Circular.

Igualmente, conserva plenamente su vigencia la Instrucción 2/2017, *sobre procesos incoados a raíz de la deducción de testimonios de una causa principal*.

Finalmente, la nueva regulación que se contiene ahora en la LECrim y la interpretación de la misma que se realiza en el presente documento sirven para dar respuesta actualizada al problema que se planteaba en la Consulta nº 1/1999 de 22 de enero, sobre *tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones,* que habrá que entender dejada sin efecto.

13. Conclusiones

1ª La regulación contenida en los arts. 588 ter a, a 588 ter m será únicamente aplicable a la interceptación de comunicaciones telefónicas y telemáticas que se puedan acordar en causas penales reguladas por la LECrim y que pudieran limitar los derechos a la intimidad, la inviolabilidad domiciliaria, el secreto de las comunicaciones y la protección de datos frente al uso de la informática.

2ª La investigación de alguno de los delitos previstos en el art. 588 ter a no resultará suficiente para colmar las exigencias del principio de proporcionalidad en las medidas de interceptación de comunicaciones telefónicas o telemáticas, sino que será preciso, además, justificar en la resolución que la acuerde que la medida resulta proporcionada en atención a la trascendencia social y ámbito tecnológico de producción del delito investigado, intensidad de los indicios existentes y relevancia del resultado perseguido.

Como regla general no procederá la interceptación de comunicaciones cuando se trate de investigar delitos leves, aunque los mismos hayan sido cometidos en el seno de una organización delictiva o se trate de delitos cometidos a través de medios informáticos. Excepcionalmente, la consideración de la especial gravedad del ámbito de producción del delito o de la menor intensidad de la intromisión en el derecho fundamental, permitirán el recurso a esta medida también en estos últimos casos, lo que deberá motivarse especialmente en la resolución que la acuerde.

3ª Las resoluciones que acuerden la interceptación de comunicaciones telefónicas o telemáticas deberán precisar expresamente si la medida se extiende solo al contenido de la comunicación o incluye también algún dato de tráfico o asociado o algún dato producido con independencia de la comunicación, fundamentando conforme a los principios rectores establecidos en la Ley la procedencia de incluir cada uno de esos datos.

4ª Podrán intervenirse las comunicaciones que el investigado mantenga desde terminales o medios de comunicación ajenos, así como las que mantengan terceras personas ajenas al investigado y de las que éste se sirva o que con él colaboren. En estos casos, sin embargo, deberá reforzarse especialmente la fundamentación de la idoneidad, proporcionalidad, excepcionalidad y necesidad de la medida, aportando indicios de la relación del investigado con el terminal o medio de comunicación utilizado o con su titular, su aprovechamiento para la comisión del delito y la relevancia de la medida para la investigación en el caso concreto.

5ª La intervención de los terminales o medios de comunicación de la víctima podrá acordarse tanto con su consentimiento como sin él. Esta medida solo podrá adoptarse con la finalidad de investigar infracciones penales en las que se acredite un previsible grave riesgo para la vida o integridad de la víctima y con la observancia del resto de las exigencias que se establecen con carácter general para la interceptación de comunicaciones.

6ª Tendrán obligación de prestar la asistencia y colaboración necesaria para llevar a cabo las intervenciones de comunicaciones que se acuerden así como de guardar secreto acerca de las actividades requeridas, no solo los prestadores de servicios de telecomunicaciones y de acceso a redes de telecomunicaciones, sino también los prestadores de servicios de la sociedad de la información, así como toda persona que de cualquier otro modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

7ª En el caso de los prestadores de servicios de la sociedad de la información deberá entenderse que quedan sujetos a las obligaciones impuestas por el ordenamiento jurídico español cuando se encuentren establecidos en territorio español, conforme a los criterios establecidos en el art. 2 LSSICE.

8ª El control judicial de la interceptación de las comunicaciones forma parte del

derecho fundamental, por lo que deberá asegurarse el efectivo seguimiento de la medida por parte del Juez que la haya acordado mediante la información que la Policía Judicial deberá remitirle en los periodos que hubieran sido fijados en la resolución judicial habilitante.

9ª La transcripción de los pasajes de interés que la Policía Judicial habrá de remitir al Juez en formato digital podrán ser literales o en extracto. Será imprescindible su cotejo con las grabaciones originales en los supuestos en los que las transcripciones vayan a ser utilizadas como prueba en el juicio, aunque resulta aconsejable que se realice también durante la sustanciación de la instrucción.

10ª Cuando la interceptación de las comunicaciones se lleve a cabo a través de ordenadores centrales deberá asegurarse la autenticidad e integridad de las copias en formato digital que se aporten al procedimiento mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración fiable. En los demás casos deberán extremarse las cautelas para garantizar la autenticidad e integridad de los soportes digitales que se aporten al procedimiento.

11ª La duración del plazo inicial de una medida de interceptación de las comunicaciones, así como de sus prórrogas, deberá estar justificada por la necesidad, idoneidad y proporcionalidad de esa duración, debiendo reflejarse así en la resolución judicial por la que se acuerde la medida o su prórroga. El cómputo del plazo total de duración se hará en relación con cada investigado cuyos derechos se vean limitados y no en relación con cada medio de comunicación intervenido o en relación con la duración total del procedimiento.

12ª Cesada la medida, el Juez deberá entregar a las partes copia de la totalidad de las grabaciones y de las transcripciones. No obstante, podrá omitir la entrega de aquellas que, no siendo relevantes para el procedimiento, pudieran afectar a la vida íntima de las personas, debiendo razonar la exclusión conforme a los mismos principios de especialidad, idoneidad, excepcionalidad, necesidad y

proporcionalidad que presiden la medida.

13ª Quienes no siendo parte en el procedimiento se vieran afectados por la medida deberán ser informados de la misma a su cese, pudiendo obtener la entrega de copias de las grabaciones únicamente en aquellos casos en los que no resulte afectada la intimidad de terceros.

14ª Las excepciones a la entrega de copias a terceros afectados por la medida subsistirán mientras siga existiendo la causa que las motivó, y ello, aunque haya concluido el procedimiento y sin necesidad de acordar el secreto de las actuaciones.

15ª Los datos vinculados a un proceso de comunicación que requieren autorización judicial para su incorporación al proceso según el art. 588 ter j, serán todos los datos a los que se refiere la Ley 25/2007 en su art. 3. La LECrim excluye expresamente de la autorización judicial los casos comprendidos en los arts. 588 ter k a 588 ter m.

La incorporación al procedimiento de datos, tanto los vinculados como los no vinculados a un proceso de comunicación, podrá acordarse en relación con cualquier comportamiento delictivo, siempre que la medida aparezca justificada por la ponderación de los principios rectores en el caso concreto

16ª La Policía Judicial no necesita autorización judicial para obtener la dirección IP correspondiente a cualquier comunicación telemática, salvo en los casos en los que recabe este dato de operadores de comunicaciones obligados por la Ley 25/2007. Sí se requiere autorización judicial, sin embargo, para relacionar esa dirección IP con un equipo o dispositivo concreto y, en último término, con la persona usuaria del mismo.

17ª Cuando se trate de posibilitar una intervención de comunicaciones la Policía

Judicial no necesita autorización judicial para obtener, a través de artificios técnicos, los códigos de identificación, tales como el IMSI o IMEI, de cualquier dispositivo de comunicación telefónica. En estos casos, sin embargo, sí será necesaria autorización judicial para relacionar dichos códigos con un equipo o dispositivo de comunicación concreto y, en último término, con la persona usuaria del mismo.

18ª La facultad del Ministerio Fiscal y de la Policía Judicial de obtener directamente, sin autorización judicial, la titularidad de cualquier medio de comunicación o, en sentido inverso, la identificación del medio de comunicación que utilice una persona determinada, se extiende a cualquier dato que facilite esa identificación sin estar vinculado a un proceso de comunicación. Esta facultad podrá ejercitarse en relación con cualquier clase de comportamiento delictivo, siempre que los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad lo justifiquen.

Madrid, 6 de marzo de 2019

LA FISCAL GENERAL DEL ESTADO

María José Segarra Crespo

EXCMOS/AS E ILMOS/AS SRES/AS FISCALES DE SALA, FISCALES SUPERIORES, FISCALES JEFES PROVINCIALES Y DE ÁREA