Las medidas de investigación tecnológica[*]

Jaime Vegas Torres
Catedrático de Derecho Procesal
Universidad Rey Juan Carlos

I. Introducción

La primera aparición de las medidas de investigación tecnológica en la legislación procesal penal española tuvo lugar con las leyes dictadas a finales de los años setenta y durante los ochenta para combatir el terrorismo. El Real Decreto-ley 21/1978, de 30 de julio contemplaba, en su artículo 4º, la medida de "observación postal, telegráfica o telefónica", a fin de establecer que dicha medida pudiera ser adoptada por la "autoridad gubernativa" para personas de las que se pudiera estimar racionalmente que "puedan estar relacionadas o integradas" en grupos o bandas terroristas. La Ley 56/1978, de 4 de diciembre, que sustituye al Real Decreto-ley anterior, mantiene la previsión de la observación postal, telegráfica y telefónica como medida que podría adoptarse respecto a las mismas personas, si bien atribuyendo su adopción, no genéricamente a la "autoridad gubernativa", sino de manera concreta al Ministro del Interior. La Ley Orgánica 11/1980, de 1 de diciembre, ya postconstitucional, regulaba asimismo la observación postal, telegráfica o telefónica exigiendo, como regla general, resolución judicial motivada para la adopción de la medida, en consonancia con lo dispuesto en el artículo 18.3 de la Constitución sobre el secreto de las comunicaciones. Ahora bien, con apoyo en las previsiones del artículo 55.2 del texto constitucional, la citada Ley Orgánica permitía que, en casos de urgencia, la observación de comunicaciones fuese acordada por el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado. La Ley Orgánica 9/1984, de 26 de diciembre, que sustituyó a la de 1980, contemplaba igualmente la medida de investigación que nos ocupa, regulándola en términos similares. Sobre esta regulación se pronunció la STC 199/1987, de 16 de diciembre, declarando que no era contraria a la Constitución.

Finalmente, con la Ley Orgánica 4/1988, de 25 de mayo, dictada también en el marco de la legislación especial antiterrorista, el control de las comunicaciones telefónicas con fines de investigación penal entra, por primera vez, en la Ley de Enjuiciamiento Criminal (L.e.cr.). La Ley de 1988 opta por regular las especialidades de los procesos sobre delitos de terrorismo en la ley procesal común, mediante las correspondientes reformas de los preceptos afectados por dichas especialidades en la Ley de Enjuiciamiento Criminal. De ahí que el desarrollo legal de la suspensión del derecho al secreto de las comunicaciones prevista para las investigaciones sobre delitos de terrorismo en el artículo 55.2 de la Constitución, se articule mediante una reforma del artículo 579 de la L.e.cr. Ahora bien, para regular la especialidad, antes se tenía que establecer la regla general, esto es, la posibilidad misma de emplear el control de las comunicaciones telefónicas como medida de investigación penal, ya que esta medida no

[*] Publicado en CEDEÑO HERNÁN, M. (coord.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, 2017, págs. 21-47.

estaba prevista en la L.e.cr. De ahí que la reforma del artículo 579 L.e.cr. realizada por la Ley Orgánica 4/1988 incorpore una regulación de carácter general sobre el control de las comunicaciones telefónicas en la instrucción penal, hasta entonces inexistente en la L.e.cr.

La regulación de 1988 se ha mantenido vigente durante más de veintisiete años, hasta la Ley Orgánica 13/2015, de 5 de octubre[1]. Durante este tiempo, las previsiones del artículo 579 L.e.cr. en materia de intervención y observación de las comunicaciones telefónicas han sido objeto de muchas críticas, especialmente por su parquedad, que dejaba sin respuesta cuestiones muy importantes[2].

Por otro lado, en los últimos años el mundo ha experimentado una verdadera revolución tecnológica que ha afectado tanto a las comunicaciones (telefonía móvil, correo electrónico, mensajería a través de internet) como a los medios técnicos que pueden ser utilizados para la investigación de hechos de apariencia delictiva[3]. La Ley de Enjuiciamiento Criminal no tenía normas especialmente adaptadas a la investigación con estos nuevos medios que, sin embargo, eran efectivamente utilizados en la instrucción de las causas penales, con la consiguiente inseguridad jurídica.

Partiendo de esta situación, la Ley Orgánica 13/2015, de 5 de octubre, por un lado, ha venido a completar la regulación legal de la intervención de comunicaciones en la instrucción penal y, por otro, a regular por primera vez en la L.e.cr. la utilización de medios tecnológicos avanzados en la investigación judicial de los hechos delictivos. Todo esto se hace mediante la introducción en el Título VIII de la L.e.cr. de siete nuevos capítulos que regulan las que la propia Ley denomina "medidas de investigación tecnológica".

---

[1] Sobre esta reforma, y la llevada a cabo paralelamente mediante la Ley 41/2015, de 5 de octubre, cfr. MUERZA ESPARZA, J., "La reforma procesal penal de 2015", *Aranzadi digital*, num. 1/2015; BUENO DE MATA, F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", en *Diario La Ley*, nº 8627, Sección Doctrina, 19 de Octubre de 2015.

[2] La insuficiencia de la regulación motivó que el TEDH, en la sentencia de 18 de febrero de 2003, caso Prado Bugallo contra España, apreció vulneración del artículo 8 del CEDH, por entender que no se cumplían las exigencias que el Tribunal vincula al requisito de que la injerencia de la autoridad pública en el derecho al respeto a la vida privada y familiar esté "prevista por la ley". Concretamente, el TEDH echaba de menos, en la regulación del artículo 579 L.e.cr., la determinación de la naturaleza de las infracciones que podían dar lugar a las escuchas, la fijación de un límite a la duración de la ejecución de la medida, las condiciones de la transcripción de la conversaciones interceptadas por el Secretario Judicial y la comunicación de las grabaciones, intactas y completas, a fin de un eventual control por el juez y por la defensa. El Tribunal Constitucional, por su parte, en la Sentencia 184/2003, de 23 de octubre, puso de manifiesto "que el art. 579 LECrim adolece de vaguedad e indeterminación en aspectos esenciales, por lo que no satisface los requisitos necesarios exigidos por el art. 18.3 CE para la protección del derecho al secreto de las comunicaciones, interpretado, como establece el art. 10.2 CE, de acuerdo con el art. 8.1 y 2 CEDH"; cfr. LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, ed. La Ley, Madrid, 2011, cap. II.

[3] Cfr. LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, cit., cap. I.

En el presente trabajo se examinará la regulación de estas medidas, poniendo especial atención en su incidencia en los derechos fundamentales de los sujetos afectados (que no son solamente los investigados). Se comprobará que, además de la directa repercusión en el derecho al secreto de las comunicaciones propia de la intervención de las comunicaciones, las medidas de investigación tecnológica suponen –cada una de ellas individualmente, pero especialmente consideradas en conjunto- fuertes limitaciones a la intimidad[4].

II. Contenido de las medidas de investigación tecnológica

Bajo la rúbrica general de "medidas de investigación tecnológica" la Ley de Enjuiciamiento Criminal contempla y regula las siguientes actuaciones, que pueden ser acordadas por el juez durante la instrucción del proceso penal:

1) La interceptación de las comunicaciones telefónicas y telemáticas.

2) La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.

3) La utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen.

4) El registro de dispositivos de almacenamiento masivo de información.

5) Registros remotos sobre equipos informáticos.

Como ya se ha indicado, la interceptación de las comunicaciones telefónicas ya estaba regulada en la L.e.cr., aunque muy insuficientemente. El resto de las medidas señaladas han sido introducidas en la L.e.cr. mediante la reforma de la Ley Orgánica 13/2015, si bien se trata de actuaciones que ya se venían realizando con sujeción a los criterios generales establecidos —principalmente por vía jurisprudencial— en materia de actuaciones de investigación limitativas de derechos fundamentales[5].

En la nueva regulación de la L.e.cr. se precisa el contenido de cada una de estas medidas, los presupuestos para su adopción y los procedimientos para su realización y control.

---

[4] En sentido muy crítico al respecto, RICHARD GONZÁLEZ, M., "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización", en *Diario La Ley*, nº 8808, Sección Tribuna, 21 de Julio de 2016.

[5] Se echa de menos una regulación legal de la obtención de información mediante interceptación de los datos que circulan por una red Wi-Fi, que plantea problemas específicos a los que no da respuesta la regulación de la interceptación de comunicaciones telefónicas o telemáticas; sobre esto, cfr. RODRÍGUEZ LAINZ, J.L., "Análisis del espectro electromagnético de señales inalámbricas: rastreo de dispositivos Wi-Fi", *Diario La Ley*, Nº 8588, Sección Doctrina, 22 de Julio de 2015.

1. Interceptación de las comunicaciones telefónicas y telemáticas

Puede acordarse la interceptación de comunicaciones en que participe el investigado como emisor o receptor (art. 588 ter b L.e.cr.).

Como regla, la medida afectará a comunicaciones realizadas por medio de terminales o dispositivos de los que sea titular o usuario el investigado (art. 588 ter b L.e.cr.). No obstante, cabe también interceptar comunicaciones realizadas por medio de terminales o dispositivos de terceras personas, cuando concurran determinadas circunstancias.

Así, en primer lugar, se pueden intervenir terminales o dispositivos de personas distintas del investigado cuando éste se sirva de la persona titular para transmitir o recibir información; asimismo, cuando el titular del terminal o dispositivo intervenido colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad; o, finalmente, cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular (art. 588 ter c L.e.cr).

La interceptación puede tener uno o varios de los siguientes contenidos (art. 588 ter d.2 L.e.cr.):

a) El registro y la grabación del contenido de la comunicación afectada.

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[6].

La Ley regula también la obtención de los datos necesarios para identificar el terminal o dispositivo cuya intervención interesa, a partir de los rastros que la actividad realizada con los mismos deja en las redes de comunicaciones. Por una parte, cuando las comunicaciones se realizan a través de internet, dejan como rastro la dirección IP del equipo utilizado. En este caso, se puede requerir a las empresas prestadoras del servicio de internet que identifiquen al usuario a quien estuviera asignada la dirección IP utilizada en las comunicaciones investigadas.

Por otro lado, las comunicaciones realizadas mediante el uso de teléfonos móviles dejan como rastro los identificadores IMSI e IMEI. El primero identifica un terminal móvil y el segundo una tarjeta SIM. La Policía, en el marco de la investigación de las comunicaciones de algún sujeto sospechoso, puede obtener estos números mediante el

[6] Sobre la nueva regulación de la interceptación de comunicaciones tras la Ley Orgánica 13/2015, RODRÍGUEZ LAINZ, J.L., "La intervención de las comunicaciones en el proceso penal", en *La Ley Penal*, 24 de noviembre de 2015.

uso de los adecuados artificios técnicos. Para ello no es necesaria la autorización judicial. Una vez conocidos esos datos, la Policía o el Ministerio Fiscal pueden requerir directamente a la empresa de telefonía que identifique el número de teléfono correspondiente y el titular del número.

Aunque el mecanismo es parecido, la Ley exige autorización judicial para solicitar a las empresas prestadoras del servicio de internet que identifiquen al usuario de una determinada IP (art. 588 ter k L.e.cr.), y no requiere, sin embargo, dicha autorización para pedir a las operadoras de telefonía móvil que identifiquen al usuario de un determinado terminal partiendo de los números IMSI o IMEI[7].

En cualquier caso, conocidos los datos anteriores, se podrá solicitar al juez que autorice la interceptación de las comunicaciones que se realicen con los terminales, tarjetas o números previamente identificados (art. 588 ter l L.e.cr.).

Se contempla también la obtención de los datos electrónicos conservados por los operadores de telefonía en cumplimiento de una obligación legal o por propia iniciativa, que sólo podrán reclamarse con autorización judicial (art. 588 ter j L.e.cr.).

2. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos

Esta medida consiste en la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados[8]. Puede limitarse a la grabación de sonido o extenderse también a la obtención de imágenes (art. 588 quáter a L.e.cr.). La posibilidad de que las escuchas se realicen incluso dentro del domicilio, y que pueda extenderse la grabación no solamente al sonido, sino también a la imagen, suponen una injerencia en el ámbito de la intimidad de intensidad máxima[9].

Solamente se contempla la captación y grabación de encuentros concretos del investigado con otras personas. No cabe autorizar la colocación de dispositivos para la

---

[7] La detección de los códigos IMSI e IMEI, así como a la obtención de direcciones IP suscitaban muchos interrogantes antes de la Ley Orgánica 13/2015; cfr. LÓPEZ-BARAJAS PEREA, I., *La intervención de las comunicaciones electrónicas*, cit., cap. I.

[8] Sobre los problemas que suscitaba, antes de la Ley Orgánica 13/2015, la ausencia de regulación legal de esta medida, ARAGONÉS SEIJO, S. y FERNÁNDEZ SERRA, L., "La ausencia de previsión legal para las escuchas en vehículos", en *Diario La Ley*, nº 8570, Sección Tribuna, 26 de Junio de 2015.

[9] En este sentido, CASANOVA MARTÍ, R., "La captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", en *Diario La Ley*, nº 8674, Sección Doctrina, 4 de Enero de 2016, considera que "la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos constituye muy probablemente la más limitativa y gravosa diligencia de investigación susceptible de practicarse en el marco del proceso penal, debido a la cualitativa y cuantitativa afectación de derechos fundamentales que conlleva su realización."

grabación de todas las conversaciones que pudiera mantener el investigado durante un periodo de tiempo (art. 588 quáter b.1 L.e.cr.).

Antes de la Ley Orgánica 13/2015, el Tribunal Constitucional había declarado que era contraria al artículo 18.3 de la Constitución, por falta de previsión legal, la grabación de las conversaciones orales mantenidas por dos detenidos en dependencias policiales (STC 145/2014, de 28 de octubre).

3. Utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen.

Bajo esta rúbrica general, la Ley regula en realidad dos medidas diferentes. Por una parte, se contempla la obtención y grabación, por cualquier medio técnico, de imágenes de la persona investigada cuando se encuentre en un lugar o espacio público. Estas grabaciones pueden hacerse por la Policía sin necesidad de autorización judicial (art. 588 quinquies a L.e.cr.).

Cuando la persona investigada se encuentre en un domicilio, sin embargo, la obtención y grabación de imágenes requiere autorización judicial, aunque se lleve a cabo utilizando medios que no requieran la entrada en el domicilio. En este sentido, la STS 2ª de 20-4-2016, ECLI:ES:TS:2016:1709, ha considerado lesiva de la inviolabilidad del domicilio la observación mediante unos prismáticos, a través de las ventanas, de lo que sucedía en el interior de un domicilio.

Además de lo anterior, se prevé y se regula también la utilización de dispositivos o medios técnicos de seguimiento y localización, para lo que sí se requiere autorización judicial, si bien en casos de urgencia los dispositivos podrán ser colocados por la Policía dando cuenta al juez con posterioridad (art. 588 quinquies b L.e.cr.)[10].

Antes de la Ley Orgánica 13/2005, la jurisprudencia había admitido la colocación de balizas para hacer un seguimiento mediante GPS de los desplazamientos del sujeto investigado. De acuerdo con esta jurisprudencia no era necesaria siempre y en todo caso la autorización judicial para la adopción de esta medida (STS 2ª de 7-7-2016, ECLI: ES:TS:2016:3621; STS 5-11-2013, ECLI: ES:TS:2013:5313).

4. Registro de dispositivos de almacenamiento masivo de información.

La medida consiste en el acceso a la información contenida en ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o en repositorios telemáticos de datos accesibles a través de dichos dispositivos[11].

---

[10] Sobre esta medida, cfr. REYES LÓPEZ, J. I., "Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la L.O.13/2015", en *Revista Aranzadi Doctrinal* num.4/2016.

[11] Un completo estudio sobre la nueva regulación legal de esta medida, en DELGADO MARTÍN, J., "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015",

La Ley parte de la distinción entre la aprehensión o incautación de los ordenadores y otros dispositivos (teléfonos inteligentes, tabletas, discos duros, pendrives, etc.), y el acceso a la información contenida en ellos. La incautación se lleva a cabo conforme a las reglas generales en materia de recogida de piezas de convicción, incluyendo, en su caso, las disposiciones en materia de registros domiciliarios. Pero para el acceso a la información es necesaria una *autorización judicial especial*, tanto si los dispositivos son aprehendidos en el domicilio del investigado (en este caso la simple autorización judicial del registro domiciliario legitima la incautación, pero no el acceso a la información) como si la incautación se lleva a cabo en un espacio no protegido (en este caso no es necesaria autorización judicial para la incautación del dispositivo, pero sí para acceder a su contenido) (art. 588 sexies a y b L.e.cr.).

Ya antes de la Ley Orgánica 13/2015, la jurisprudencia había establecido la necesidad de autorización judicial para el acceso al contenido de los dispositivos de almacenamiento de datos en el curso de una investigación penal. Así, el Tribunal Constitucional, en su sentencia 173/2011, de 7 de noviembre, establece que el acceso a los datos almacenados en un ordenador personal afecta al derecho a la intimidad y requiere, por ello, como regla general, previa autorización judicial:

> *Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) —por lo que sus funciones podrían equipararse a los de una agenda electrónica—, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona (STC 173/2011, FJ 3; en*

Diario La Ley, nº 8693, Sección Doctrina, 2 de Febrero de 2016; con referencia a la situación anterior a la reforma y los problemas que suscitaba la ausencia de regulación legal, BONILLA CORREA, J.A., "Los avances tecnológicos y sus incidencias en la ejecución de la diligencia de registro en domicilio", en *Diario La Ley*, nº 8522, Sección Doctrina, 20 de Abril de 2015.

el mismo sentido, STC 170/2013, de 7 de octubre, FJ 5; STC 142/142, de 30 de julio, FJ 3).

El Tribunal Supremo precisó, además, que la autorización para efectuar el registro domiciliario no llevaba implícita la habilitación para el acceso a los dispositivos de almacenamiento de datos que pudieran ser hallados en el registro:

> *Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional ha de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejercen los derechos individuales más elementales, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías (STS 2ª de 10-3-2016, ECLI: ES:TS:2016:1218; STS 2ª de 24-2-2105, ECLI: ES:TS:2015:823; STS 2ª de 17-4-2013, ECLI: ES:TS:2013:2222).*

La autorización judicial ha de ser previa al registro, como regla general, pero en casos de urgencia se permite que la Policía examine el contenido del dispositivo incautado, dando cuenta de inmediato al juez, quien confirmará o revocará la actuación policial (art. 588 sexies c.4 L.e.cr.).

Autorizado el registro de la información contenida en un dispositivo, podrá extenderse a datos que estén en otro sistema informático, siempre que se trate de datos a los que se pueda acceder lícitamente desde el dispositivo inicialmente registrado (art. 588 sexies c.3 L.e.cr.). Se permite, por tanto, el acceso a información del usuario que se encuentre en servicios de almacenamiento en internet (Dropbox, Google Drive, Onedrive y similares), así como en redes sociales, a través de las aplicaciones que den acceso a dichos servicios desde el dispositivo de que se trate[12].

La incautación del dispositivo a efectos de su registro puede evitarse cuando se pueda realizar una copia de la información que contenga en condiciones que garantice la autenticidad e integridad de los datos. En estos casos el dispositivo se dejará a disposición de su propietario y la investigación se llevará a cabo sobre la copia obtenida (art. 588 sexies c.2 L.e.cr.)[13].

---

[12] Sobre los servicios que se prestan en internet, COTINO HUESO, L., "Algunas cuestiones clave de protección de datos en la nube. Hacia una «regulación nebulosa»", en *Revista Catalana de Dret Públic*, nº 51, 2015.

[13] La clonación del dispositivo de almacenamiento investigado, con obtención del hash de dicho dispositivo y de la copia sirve, además, como elemento de garantía de que la investigación se proyecta sobre información no manipulada. Este aspecto y, en general, todos los relacionados con la cadena de custodia

5. Registros remotos sobre equipos informáticos.

La medida consiste en la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos (art. 588 septies a.1 L.e.cr.).

Se contempla, en definitiva, la instalación de *programas espía* o *troyanos* en el ordenador o dispositivo investigado, lo que permite a la Policía acceder desde un equipo remoto a todo el contenido almacenado en (o accesible desde) el ordenador o dispositivo de que se trate y seguir en tiempo real la actividad que se realice con el mismo, todo ello sin conocimiento del usuario[14].

Es una medida muy invasiva de la privacidad que solamente está justificada para la investigación de delitos muy graves[15]. En otros países la introducción de este tipo de medidas ha sido objeto de fuertes debates y se ha llevado a cabo con sujeción a límites más estrictos[16].

III. Iniciativa para la adopción de las medidas. La solicitud

Siguiendo la regla general de los actos de investigación de la instrucción penal, las medidas de investigación tecnológica se pueden acordar por el Juez de Instrucción de oficio o a instancia del Ministerio Fiscal. Pero la Ley también contempla que estas medidas se adopten a instancia de la Policía Judicial (art. 588 bis b.1 L.e.cr.).

La Policía judicial, una vez incoado el proceso, debería actuar, según la Ley, siguiendo las instrucciones del juez (art. 287 L.e.cr.). Hay que entender, por tanto, que la "instancia" de la Policía Judicial a que se refiere el artículo 588 bis b.1 L.e.cr. es más bien un "informe" que los agentes que realizan la investigación bajo las órdenes del juez

---

han sido descuidados en la nueva regulación, como pone de manifiesto RUBIO ALAMILLO, J., "La informática en la reforma de la Ley de Enjuiciamiento Criminal", en *Diario La Ley*, nº 8662, Sección Tribuna, 10 de Diciembre de 2015.

[14] Esta medida entraña riesgos para las garantías procesales, ya que no se establece ninguna cautela que impida que los propios agentes que realizan el registro remoto puedan enviar archivos ilegales al equipo investigado, archivos que posteriormente podrían ser utilizados para incriminar al usuario de ese equipo; cfr. RUBIO ALAMILLO, J., "La informática en la reforma de la Ley de Enjuiciamiento Criminal", cit.

[15] En este sentido, DELGADO MARTÍN, J., "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015", cit., apunta que "los registros remotos prolongan en el tiempo la injerencia en los diferentes contenidos del dispositivo, por lo que suponen una afectación de elevada intensidad en los derechos a la intimidad y al secreto de las comunicaciones de la persona investigada, aunque también en el denominado derecho a la autodeterminación informativa del art. 18.4 Constitución."

[16] ORTIZ PRADILLO, J.C., "El 'remote forensic software' como herramienta de investigación contra el terrorismo", en *ENAC e-Newsletter en la lucha contra el cybercrimen*, nº 4, octubre 2009.

presentan a éste, informe cuyo papel hay que entender limitado a ilustrar al juez a fin de que valore la conveniencia, en el ejercicio de sus funciones como director de la investigación, de adoptar o no, de oficio, las medidas de que se trate. La resolución judicial que, en su caso, se dicte a la vista del informe policial podrá ser, en su caso, recurrida por el Ministerio Fiscal o por las partes personadas, pero en ningún caso por la Policía, que no es parte en el proceso ni puede serlo, lo que demuestra que no se trata en realidad de una resolución dictada "a instancia" de la Policía Judicial. Es más, en caso de "solicitud" policial, el Juez únicamente debería dictar auto cuando considerase procedente la adopción de la medida, ya que en este caso, por lo dicho, hay que entender que la decisión sobre la medida se produce de oficio, y no tendría sentido que el Juez dictara de oficio una resolución denegatoria.

Se regula de manera muy detallada el contenido de la solicitud del Ministerio Fiscal o de la Policía Judicial. De acuerdo con el artículo 588 bis b.2 L.e.cr., la solicitud debe hacer referencia a los siguientes puntos:

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

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida, atendiendo a los principios del art. 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

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

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

6.º La forma de ejecución de la medida.

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

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

Cuando se solicite la *interceptación de comunicaciones telefónicas o telemáticas*, la solicitud deberá expresar, además de lo anterior, la identificación del número de abonado, del terminal o de la etiqueta técnica; la identificación de la conexión objeto de la intervención o los datos necesarios para identificar el medio de telecomunicación de que se trate (art. 588 ter d.1 L.e.cr.).

IV. La resolución judicial sobre medidas de investigación tecnológica

1. Principios rectores de la resolución judicial sobre medidas de investigación tecnológica

Las medidas de investigación tecnológica requieren, como regla, autorización judicial. Esta exigencia tiene un importante valor como garantía de validez constitucional de la injerencia en derechos fundamentales que estas medidas comportan. Así lo ha destacado la jurisprudencia, con referencia a la intervención de las comunicaciones. En este sentido, la Sala Segunda del Tribunal Supremo se ha pronunciado en numerosas ocasiones en el sentido siguiente:

> *En nuestro ordenamiento la principal garantía para la validez constitucional de una intervención telefónica es, por disposición constitucional expresa, la exclusividad jurisdiccional de su autorización, lo que acentúa el papel del Juez Instructor como Juez de garantías, ya que lejos de actuar con criterio inquisitivo impulsando de oficio la investigación contra un determinado imputado, la Constitución le sitúa en el reforzado y trascendental papel de máxima e imparcial garantía de los derechos fundamentales de los ciudadanos, de manera que la investigación, impulsada por quienes tienen reconocida legal y constitucionalmente la facultad de ejercer la acusación, no puede, en ningún caso ni con ningún pretexto, adoptar medidas que puedan afectar a dichos derechos constitucionales, sin la intervención absolutamente imparcial del Juez, que en el ejercicio de esta función constitucional, atribuida con carácter exclusivo, alcanza su máxima significación de supremo garante de los derechos fundamentales (STS 2ª de 1-12-2106, ROJ: STS 5282/2016; STS 2ª de 18-12-2015, ROJ: STS 5747/2015; STS 2ª de 2-10-2014, ROJ: STS 4297/2014; STS 2ª de 5-12-2013, ROJ: STS 6211/2013 y STS 2ª de 12-4-2012, ROJ: STS 2513/2012, entre otras).*

Tratándose de medidas que afecten al secreto de las comunicaciones del artículo 18.3 de la Constitución, la exigencia de resolución judicial que autorice la injerencia está expresamente prevista en el precepto constitucional. Para este tipo de medidas, solamente cuando la causa se refiera a delitos relacionados con la actuación de bandas armadas o elementos terroristas, podrá prescindirse de la autorización judicial. Concretamente, en las causas por delitos de terrorismo la interceptación de comunicaciones telefónicas y telemáticas puede llevarse a cabo sin necesidad de autorización judicial, por acuerdo del Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, siempre que se den las condiciones previstas en el artículo 588 ter d.3 L.e.cr. Esta posibilidad se basa en las previsiones del art. 55.2 de la Constitución sobre suspensión individual de los derechos fundamentales en la investigación de delitos de terrorismo.

Los criterios con arreglo a los cuales ha de decidirse si se concede o no la autorización judicial vienen expresados en la Ley como "principios rectores" que son comunes a todas las medidas de investigación tecnológica (art. 588 bis a L.e.cr.). Se trata, en general, de la plasmación legal de criterios que ya habían sido establecidos por la jurisprudencia.

1) *Principio de especialidad y descubrimientos casuales*

De acuerdo con este principio, sólo podrá autorizarse una medida de investigación tecnológica si está relacionada con la investigación de un delito concreto. Se excluye, por tanto, la adopción de medidas de investigación tecnológica con el fin de prevenir o descubrir delitos o despejar sospechas sin base objetiva.

Se contempla, no obstante, que las medidas acordadas para la investigación de un delito den lugar al *descubrimiento casual* de otro delito, o que dichas medidas proporcionen información que pudiera ser relevante en una causa penal distinta[17]. Cuando así suceda, el resultado de las medidas podrá incorporarse al proceso que se abra para la investigación del nuevo delito descubierto (art. 588 bis i L.e.cr.).

Este principio de especialidad estaba ya firmemente asentado en la jurisprudencia anterior a la Ley Orgánica 13/2015. Así, de acuerdo con la jurisprudencia del Tribunal Supremo:

> *(...) cuando se trata de investigaciones realizadas mediante intervenciones telefónicas, entre los requisitos que deben ser observados se encuentra el de la especialidad de la medida, en el sentido de que la intervención debe de estar orientada hacia la investigación de un delito concreto, sin que sean lícitas las observaciones encaminadas a una prospección sobre la conducta de una persona en general. Lo que no excluye que los hallazgos casuales sugerentes de la posible comisión de otros delitos distintos no sean válidos, sino que la continuidad en la investigación de ese hecho delictivo nuevo requiere de una renovada autorización judicial (STS 2ª de 12-1-2017, ECLI: ES:TS:2017:47; STS 2ª de 27-9-2016, ECLI: ES:TS:2016:4173; STS 2ª de 10-11-2015, ECLI: ES:TS:2015:4803; STS 2ª de 21-10-2014, ECLI:ES:TS:2014:4829 y STS 2ª de 22-7-2013, ECLI: ES:TS:2013:4300, entre muchas otras).*

Aunque no se permitan medidas de investigación tecnológica de carácter prospectivo, la posibilidad de utilizar en la investigación de un delito los descubrimientos casuales que se hubieran producido en la ejecución de medidas adoptadas para la investigación de otro delito ha sido admitida por la jurisprudencia del Tribunal Constitucional. En este sentido, la STC 41/1998, de 24 de febrero, dice lo siguiente:

> *(...) la Constitución no exige, en modo alguno, que el funcionario que se encuentra investigando unos hechos de apariencia delictiva cierre los ojos ante los indicios de delito que se presentaren a su vista, aunque los hallados casualmente sean distintos a los hechos comprendidos en su investigación oficial, siempre que ésta no sea utilizada fraudulentamente para burlar las garantías de los derechos fundamentales (en el mismo sentido, STC 104/2006, de 3 de abril).*

---

[17] Un completo estudio sobre la nueva regulación legal de los hallazgos casuales, en NADAL GÓMEZ, I., "El régimen de los hallazgos casuales en la Ley 13/2015, de modificación de la Ley de Enjuiciamiento Criminal", en *Revista General de Derecho Procesal,* nº 40 (2016).

La utilización de los resultados de una medida de investigación tecnológica en procedimientos distintos a aquel en que se hubiese adoptado está sujeta a los requisitos establecidos en el artículo 579 bis de la L.e.cr. A tal efecto, en el procedimiento en el que se hubiese practicado la medida se tendrá que expedir un testimonio para su incorporación al procedimiento que se siga por el delito diferente casualmente descubierto o sobre el que la medida haya proporcionado alguna información relevante. Se exige que este testimonio incluya los particulares necesarios para acreditar la legitimidad de la injerencia, particulares que comprenderán, en todo caso, la solicitud inicial de la medida, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen. Al remitir el testimonio se informará si las diligencias continúan declaradas secretas, en cuyo cado dicha declaración deberá ser respetada en el otro proceso penal, hasta que se acuerde el alzamiento del secreto.

La medida puede continuar en el procedimiento al que se haya remitido el testimonio, para lo que se requiere autorización del juez que conozca de este proceso. Para decidir si se autoriza o no la continuación de la medida, la Ley exige que se compruebe la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento.

2) *Principio de idoneidad: extensión subjetiva, objetiva y temporal de la medida*

Este principio condiciona la autorización de la medida a que ésta resulte útil para el esclarecimiento del hecho delictivo investigado. En particular la medida no debe tener una extensión objetiva, subjetiva o temporal mayor de la necesaria para lograr el esclarecimiento del hecho punible.

Respecto a la *extensión subjetiva*, las medidas pueden afectar a terceras personas distintas del investigado cuando sea necesario a los fines de la investigación (art. 588 bis h L.e.cr.). En cuanto a la *extensión objetiva*, la aplicación del principio de idoneidad tendrá que acomodarse al contenido concreto de la medida de cuya autorización se trate: limitar la intervención de las comunicaciones a aquellas cuyo previsible contenido pueda ser de interés para la investigación; limitar el registro de dispositivos de almacenamiento a aquellos que previsiblemente puedan contener datos relevantes, etc. Finalmente, respecto a la *extensión temporal*, se ha de entender que el principio de idoneidad exige al juez no prolongar la medida más allá del tiempo necesario para alcanzar los fines de la investigación, sin apurar necesariamente los plazos máximos establecidos en la Ley.

Por otra parte, y también en relación con la extensión temporal, cabe entender que el principio de idoneidad se opone a la adopción de una medida de investigación tecnológica cuando la obtención de resultados útiles para la investigación previsiblemente requeriría prolongar la medida durante un tiempo que exceda de los límites temporales legalmente establecidos.

3) Principios de excepcionalidad y necesidad

De estos principios, que la Ley presenta unidos, derivan dos consecuencias. Por una parte, la improcedencia de las medidas de investigación tecnológica cuando la investigación pueda realizarse con otras medidas menos gravosas para los derechos

fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho. Por otra parte, los principios que nos ocupan requieren que, sin el recurso a la investigación tecnológica, se vieran gravemente dificultados el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito.

4) *Principio de proporcionalidad*

La Ley exige, finalmente, que la adopción de la medida de investigación tecnológica sea proporcionada. El juicio de proporcionalidad requiere poner en relación el sacrificio de los derechos e intereses afectados por la medida con el beneficio que la adopción de la medida suponga para el interés público y de terceros. No deberá autorizarse la medida cuando aquel sacrificio sea superior a este beneficio.

La valoración del beneficio para el interés público que derivaría de la adopción de la medida ha de realizarse, conforme a la Ley, atendiendo a los siguientes elementos: la gravedad del hecho (a mayor gravedad, mayor interés público); la trascendencia social del hecho (cuanto mayor sea, mayor será el interés público); el ámbito tecnológico de producción (a mayor relación del delito con el ámbito tecnológico, mayor interés público en la adopción de la medida); la intensidad de los indicios existentes (a mayor intensidad, más peso tendrá el interés público en la adopción de la medida); y, finalmente, la relevancia del resultado perseguido con la restricción del derecho (a mayor relevancia, más intensidad tendrá el interés público).

Sobre el principio de proporcionalidad existe una muy consolidada doctrina del Tribunal Constitucional que distingue tres aspectos o vertientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (STC 43/2014, de 27 de marzo; STC 23/2014, de 13 de febrero; STC 16/2014, de 30 de enero; STC 199/2013, de 5 de diciembre y STC 173/2011, de 7 de noviembre, entre otras).

En relación con las medidas de investigación tecnológica, la Ley Orgánica 13/2015 ha desgajado, presentándolos como principios distintos, los tres juicios que el Tribunal Constitucional vincula al principio de proporcionalidad. Así, la referencia al principio de proporcionalidad en el artículo 588 bis a de la L.e.cr. ha de entenderse referida a lo que el Tribunal Constitucional denomina "juicio de proporcionalidad en sentido estricto".

5) *La gravedad del delito investigado*

Las medidas de *interceptación de comunicaciones telefónicas y telemáticas* y de *captación y grabación de comunicaciones orales* mediante la utilización de dispositivos electrónicos pueden acordarse en investigaciones por delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión. El límite de gravedad no es excesivamente exigente ya que basta un rápido repaso a la parte especial del código penal

para comprobar que hay muy pocas figuras delictivas que no alcancen dicho límite, si no en su tipo básico, sí al menos en alguna modalidad agravada.

Con todo, la propia Ley permite que la interceptación de comunicaciones telefónicas o telemáticas y la grabación de conversaciones orales se puedan acordar, aunque el delito investigado no alcance la gravedad señalada, cuando se trate de delitos cometidos en el seno de un grupo u organización criminal o de delitos de terrorismo (art. 579.1 en relación con arts. 588 ter a y 588 quáter b.2.a) L.e.cr.).

La interceptación de comunicaciones telefónicas o telemáticas puede acordarse también, con independencia de la gravedad de la pena, en la investigación de delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación (art. 588 ter a L.e.cr.).

Para la medida de *registro remoto sobre equipos informáticos* se establece un régimen más restrictivo, ya que no se contempla la posibilidad de que esta medida sea adoptada en la investigación de cualquier delito que alcance determinada gravedad, sino únicamente en causas que se sigan por una lista cerrada de delitos: delitos cometidos en el seno de organizaciones criminales, delitos de terrorismo, delitos cometidos contra menores o personas con capacidad modificada judicialmente, delitos contra la Constitución, de traición y relativos a la defensa nacional y delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación (art. 588 ter a L.e.cr.)[18]. En investigaciones por delitos distintos a los mencionados, por muy graves que pudieran ser, no cabe el registro remoto de equipos informáticos.

Hay que precisar, en cualquier caso, que no es suficiente para justificar la adopción de cualquiera de las medidas anteriores que el delito de cuya investigación se trate cumpla las condiciones requeridas por la Ley. El cumplimiento de estas condiciones no elimina la necesidad de comprobar, atendiendo a las circunstancias del caso, que la adopción de la medida es conforme con las exigencias generales de proporcionalidad y los demás principios arriba señalados, sin que proceda la adopción de la medida en otro caso.

Para las medidas *de utilización de dispositivos técnicos de captación de la imagen,* de *seguimiento y de localización* y de *registro de dispositivos de almacenamiento masivo de información* la Ley no exige una gravedad mínima ni limita su procedencia a determinadas figuras delictivas, por lo que estas medidas pueden acordarse en la investigación de cualquier tipo de delito, siempre que se cumplan las exigencias generales de proporcionalidad.

---

[18] Sobre el empleo del registro remoto de equipos informáticos en la investigación de delitos cometidos a través de internet, cfr. FERNÁNDEZ LÓPEZ, M., "Algunas propuestas para regular la investigación del cibercrimen", en *La reforma del proceso penal*, editorial La Ley, Madrid, 2011; en cuanto a la delimitación de los delitos que pueden considerarse comprendidos en el ámbito de la ciberdelincuencia tiene interés BARRIO ANDRÉS, M., "Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010", en *La Ley Penal*, nº 86, Sección Legislación aplicada a la práctica, Octubre 2011.

2. Procedimiento y contenido de la resolución

La resolución debe dictarse en el plazo máximo de 24 horas desde la presentación de la solicitud. Antes de resolver, el Juez debe oír al Ministerio Fiscal, si no es quien ha solicitado la medida (art. 588 bis c.1 L.e.cr.).

También está previsto que el juez requiera ampliación o aclaración de la solicitud cuando lo estime necesario. En este caso, se interrumpe el plazo de 24 horas hasta que se realice la ampliación o aclaración (art. 588 bis c.2 L.e.cr.).

La solicitud, en su caso, la resolución judicial autorizando la medida, y las actuaciones posteriores de ejecución de la misma se sustancian en una pieza separada que tiene carácter secreto sin necesidad de que se acuerde expresamente el secreto de las actuaciones (art. 588 bis d L.e.cr.).

Cuando resulte procedente acordar la medida de investigación tecnológica de que se trate, el Juez de Instrucción lo hará mediante *auto motivado* que deberá tener, al menos, los siguientes contenidos (art. 588 bis b.3 L.e.cr.):

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

De acuerdo con la jurisprudencia del Tribunal Constitucional, los indicios racionales exigidos para que sea procedente la medida han de ser algo más que simples sospechas, si bien no es necesario que lleguen a tener la solidez que se exige a los indicios racionales que han de concurrir para el procesamiento (STC 145/2014, de 22 de septiembre; STC 25/2011, de 14 de marzo; STC 72/2010, de 18 de octubre; STC 197/2009, de 28 de septiembre, entre otras).

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

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

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

e) La duración de la medida.

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

g) La finalidad perseguida con la medida.

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

i) Cuando se acuerde la *captación y grabación de comunicaciones orales* la resolución debe precisar el lugar o dependencias, así como los encuentros del investigado que van a ser sometidos a vigilancia (art. 588 quáter c L.e.cr.).

j) La resolución que autorice el *registro de dispositivos de almacenamiento masivo de información* fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial (art. 588 sexies c.1 L.e.cr.).

k) Cuando se autorice el registro remoto de equipos informáticos, la resolución judicial deberá identificar el ordenador, dispositivo o sistema informático afectado y precisar cómo se realizará el acceso y el software que se empleará para obtener la información, así como otros extremos a que se refiere el artículo 588 septies a.2 L.e.cr.

La regulación legal recoge, así, las exigencias que la jurisprudencia había venido estableciendo en cuanto a la extensión de la motivación de la resolución que autoriza medidas limitativas de derechos fundamentales. Así, por ejemplo, la STC 145/2014, de 22 de septiembre (FJ 2), resume la doctrina del Tribunal Constitucional al respecto:

> *En relación con el derecho al secreto de las comunicaciones telefónicas, nuestra doctrina ha venido reiterando que las exigencias de motivación de las resoluciones judiciales que autorizan la intervención o su prórroga forman parte del contenido esencial del art. 18.3 CE. Dicho sintéticamente, éstas deben explicitar, en el momento de la adopción de la medida, todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Por ello, el órgano judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo; indicios que han de ser algo más que simples sospechas (SSTC 167/2002, de 18 de septiembre, FJ 2; 184/2003, de 23 de octubre, FJ 11; y 197/2009, de 28 de septiembre, FJ 4). Tiene además que determinar con precisión el número o números de teléfono y personas cuyas conversaciones han de ser intervenidas, el tiempo de duración de la intervención, quiénes han de llevarla a cabo y cómo, y los periodos en los que deba darse cuenta al Juez (por todas, SSTC 261/2005, de 24 de octubre, FJ 2; y 219/2009, de 21 de diciembre, FJ 4).*

La jurisprudencia viene admitiendo que la expresión de los indicios en que se basa la adopción de la medida se pueda efectuar mediante remisión al contenido del oficio policial. En este sentido, con referencia a las medidas de intervención de las comunicaciones, es jurisprudencia consolidada que:

> *(...) aunque es deseable que la resolución judicial contenga en sí misma todos los datos o hechos objetivos que puedan considerarse indicios de la existencia del delito y la conexión de la persona o personas investigadas con el mismo, nuestra jurisprudencia ha admitido la motivación por remisión, de modo que la resolución judicial puede considerarse suficientemente motivada si, integrada con la solicitud policial, a la que puede remitirse, contiene todos los elementos*

necesarios para llevar a cabo el juicio de proporcionalidad (STS 2ª de 16-6-2016, ECLI: ES:TS:2016:2950; STS 2ª de 10-7-2015, ECLI:ES:TS:2015:3377; STS 2ª de 24-6-2014, ECLI: ES:TS:2014:2906; STS 2ª de 14-6-2013, ECLI: ES:TS:2013:3258 y STS 2ª de 5-11-2009, ECLI: ES:TS:2009:6864, entre otras).

V. Ejecución de la medida

1. Duración

La duración de la medida se fija por el Juez en el auto de autorización. Existe un límite general y limitaciones específicas para las distintas medidas. Con carácter general, ninguna medida de investigación tecnológica puede durar más del tiempo imprescindible para el esclarecimiento de los hechos (art. 588 bis e.1 L.e.cr.).

Para algunas medidas se establecen, además, unos límites de duración que no pueden sobrepasarse aunque no se hubiese conseguido el esclarecimiento de los hechos. Así, la *interceptación de las comunicaciones telefónicas y telemáticas* y la *utilización de dispositivos técnicos de seguimiento y de localización* están sujetas a un plazo máximo inicial de tres meses, con posibles prórrogas por periodos sucesivos de tres meses hasta un máximo de 18 meses (art. 588 ter g L.e.cr. y art. 588 quinquies c L.e.cr.).

Los *registros remotos sobre equipos informáticos* pueden acordarse, en principio, por el tiempo máximo de un mes, con posibles prórrogas por periodos sucesivos de un mes hasta un máximo de tres meses (art. 588 septies c L.e.cr.).

El *dies a quo* de estos plazos es la fecha de la autorización judicial, y no la del efectivo comienzo de la aplicación de la medida. Así se prevé expresamente para la interceptación de comunicaciones y el seguimiento y localización, pero ha de entenderse que el mismo criterio debe aplicarse para el cómputo del plazo máximo del registro remoto de equipos informáticos. Se trata, por lo demás, de un criterio que ya había sido establecido por la jurisprudencia (STS 2ª de 11-1-2017, ECLI:ES:TS:2017:40; STS 2ª de 25-3-2015, ECLI: ES:TS:2015:1977 y STS 2ª de 1-10-2013, ECLI: ES:TS:2013:4944, entre otras).

La medida de *captación y grabación de comunicaciones orales* mediante la utilización de dispositivos electrónicos no está sujeta a límites temporales pues no tiene carácter continuo, sino que ha de referirse a encuentros concretos del investigado, sobre la base de indicios resultantes de la investigación que hagan previsibles dichos encuentros (art. 588 quáter b L.e.cr.). Tampoco afectan los límites temporales a la medida de registro de dispositivos de almacenamiento masivo de información, que tampoco tiene carácter continuo.

La Ley procura evitar el automatismo de las prórrogas, que se pueden acordar de oficio o previa petición razonada del solicitante (Ministerio Fiscal o Policía Judicial). La solicitud de prórroga se debe efectuar con antelación suficiente a la expiración del plazo.

La solicitud deberá incluir los datos que sean necesarios para que el juez pueda valorar la necesidad de prorrogar la medida. Concretamente, exige la Ley que se incluya en la solicitud un informe detallado del resultado de la medida y se expresen las razones

que justifiquen la continuación de la misma (art. 588 bis f.1 L.e.cr.). Además, tratándose de interceptación de las comunicaciones telefónicas y telemáticas, la Policía Judicial aportará, en su caso, la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida (art. 588 ter h L.e.cr.).

El Juez debe resolver sobre la prórroga por medio de auto motivado en el plazo de dos días. Antes de dictar la resolución puede solicitar aclaraciones o mayor información (art. 588 bis f.2 L.e.cr.). Si se trata de interceptación de las comunicaciones telefónicas y telemáticas, podrá requerir el contenido íntegro de las conversaciones intervenidas (art. 588 ter h L.e.cr.). Se acordará la prórroga siempre que subsistan las causas que motivaron la adopción de la medida (art. 588 bis e.2 L.e.cr.).

La jurisprudencia subraya la necesidad de que las prórrogas se motiven, partiendo de una previa valoración de los resultados obtenidos. En este sentido, el Tribunal Constitucional ha señalado que:

> *Tales exigencias de motivación se reproducen en las prórrogas y en las nuevas escuchas acordadas a partir de datos obtenidos en una primera intervención, debiendo el Juez conocer los resultados de ésta con carácter previo al acuerdo de prórroga, explicitando las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión tácita o presunta a la inicial (STC 145/2014, de 22 de septiembre; STC 26/2010, de 27 de abril; STC 261/2005, de 24 de octubre y STC 202/2001, de 15 de octubre).*

La prórroga comienza a computarse desde la fecha de expiración del plazo inicial (o de la prórroga anterior) (art. 588 bis f.3 L.e.cr.). Si por cualquier causa no se acuerda la prórroga solicitada antes de la expiración del plazo (o de la prórroga anterior), la medida cesa a todos los efectos (art. 588 bis e.3 L.e.cr.).

2. Control judicial de la ejecución de la medida

Con carácter general, para todas las medidas de investigación tecnológica, se dispone que la Policía presente informes al juez de instrucción del desarrollo y los resultados de la medida, en la forma y con la periodicidad que éste determine y, en todo caso, cuando por cualquier causa se ponga fin a la misma (art. 588 bis g L.e.cr.).

Tratándose de interceptación de comunicaciones telefónicas o telemáticas, o de captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, además de lo anterior, la Policía Judicial deberá entregar al juez, con la periodicidad que éste determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas (arts. 588 ter f y 588 quáter d L.e.cr.).

El control ha de ser efectivo, pero esto no supone que el juez de instrucción deba necesariamente oír íntegramente las grabaciones, a medida que se van efectuando. En este sentido, la jurisprudencia viene considerando que:

(...) el control efectivo judicial del contenido de la intervención, se puede efectuar, y así se hace de ordinario, bien a través de los propios informes policiales en los que se va dando cuenta de los datos relevantes de la investigación, complementados con las transcripciones más relevantes, con independencia de que, además se envíen las cintas íntegras para su introducción, si se solicitase en el Plenario, por lo que no es preciso la audición directa de las cintas por el Sr. Juez Instructor (STS 2ª de 12-1-2017, ECLI:ES:TS:2017:81; STS 2ª de 8-6-2016, ECLI:ES:TS:2016:2557; STS 2ª de 24-7-2015, ECLI: ES:TS:2015:3811; STS 2ª de 9-12-2014, ES:TS:2014:5198 y STS 2ª de 18-6-2013, ECLI: ES:TS:2013:4069).

Las eventuales irregularidades que puedan producirse en el control judicial a posteriori de los resultados de las medidas de investigación tecnológica pueden tener efectos invalidantes en relación con el valor probatorio de dichos resultados, pero no entrañan lesión de los derechos fundamentales afectados por la medida (secreto de las comunicaciones, intimidad). En este sentido, la jurisprudencia del Tribunal Constitucional viene manteniendo que:

(...) no constituyen una vulneración del derecho al secreto de las comunicaciones las irregularidades cometidas en el control judicial a posteriori del resultado de la intervención telefónica, pues no tienen lugar esos defectos durante la ejecución del acto limitativo de derechos, sino, antes al contrario, en la incorporación de su resultado a las actuaciones sumariales. En definitiva, lo relativo a la entrega y selección de las cintas grabadas, a la custodia de los originales y a la transcripción de su contenido, no forma parte de las garantías del art. 18.3 CE, sin perjuicio de su relevancia a efectos probatorios, pues es posible que la defectuosa incorporación del resultado de una intervención telefónica legítimamente autorizada no reúna las garantías de control judicial y contradicción suficientes como para convertir la grabación de las escuchas en una prueba válida para desvirtuar la presunción de inocencia (art. 24.2 CE) (STC 145/2014, de 22 de septiembre; STC 167/2002, de 18 de septiembre y STC 126/2000, de 16 de mayo, entre otras).

3. Incorporación al proceso de los resultados de la medida

Durante la vigencia de la medida, los resultados que se vayan obteniendo se incorporan al proceso mediante los correspondientes soportes (grabaciones, transcripciones, etc.), si bien se mantienen en una pieza separada y secreta para las partes, a fin de no perjudicar el resultado de la investigación (arts. 588 bis d; 588 quáter d y 588 quinquies c.2 L.e.cr.).

Una vez acordado el cese de la medida se alza el secreto y se entrega a las partes copia de las grabaciones y transcripciones (art. 588 ter i L.e.cr.).

Tratándose de *interceptación de comunicaciones telefónicas y telemáticas*, no se incorporarán al proceso ni se entregará copia a las partes de las comunicaciones grabadas que no sean relevantes para la investigación. Por otra parte, si en la grabación de una comunicación relevante hubiera datos referidos a aspectos de la vida íntima de las

personas, se omitirán estos datos en las copias y transcripciones que se entreguen a las partes (art. 588 ter i, apartados 1 y 2 L.e.cr.)[19].

4. Deber de colaboración

A fin de facilitar la ejecución de las medidas de investigación tecnológica, la Ley establece un deber de colaboración de todas las empresas y sujetos que proporcionan o gestionan los medios tecnológicos a que se refiera la medida acordada (prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, etc.) (art. 588 ter e L.e.cr.). La colaboración de las empresas prestadoras de los servicios de telecomunicaciones es imprescindible para la interceptación de las comunicaciones por medio del sistema SITEL[20].

La colaboración puede requerirse por el Ministerio Fiscal o por la Policía Judicial, antes de la autorización judicial de las medidas, a fin de que se conserven y protejan los datos contenidos en un sistema informático hasta que el juez autorice el acceso a los mismos. El deber de conservar los datos en estos casos puede extenderse hasta un máximo de 180 días (art. 588 octies L.e.cr.).

En particular, tratándose del *registro de dispositivos de almacenamiento masivo de información*, las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona (salvo al investigado y a las personas exentas del deber de declarar) que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado (art. 588 sexies c.5 L.e.cr.)[21].

Hay que entender que este requerimiento puede incluir el de revelar las claves que se hayan empleado para encriptar la información, en los casos en que la gestión de estas claves se confía a la empresa que presta el servicio de almacenamiento.

Los prestadores de servicios y los titulares o administradores de los sistemas informáticos pueden ser obligados también a colaborar para facilitar la instalación del

---

[19] Cfr. TOMASELLI ROJAS, A.L., "Actuación del Secretario Judicial: conservación, transcripción y cotejo de las grabaciones", *Diario La Ley*, Nº 8615, Sección Tribuna, 29 de Septiembre de 2015.

[20] VIDAL MARÍN, T. y RUIZ DORADO, M., "Análisis de la constitucionalidad del SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal", en *Revista Aranzadi Doctrinal* num. 9/2016; López-Barajas Perea, I., *La intervención de las comunicaciones electrónicas,* cit., cap. V.

[21] Sobre este deber de colaboración para registros de dispositivos de almacenamiento masivo, poniéndolo en relación con un conocido caso suscitado ante los tribunales de los EEUU., se hacen interesantes reflexiones en RODRÍGUEZ LAINZ, J.L., "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?", *Diario La Ley*, Nº 8729, Sección Doctrina, 28 de Marzo de 2016.

software espía que permita el *registro remoto de equipos informáticos*, en los términos previstos en el artículo 588 septies b L.e.cr.

VI. Cese de la medida

El juez acordará el cese de la medida cuando haya transcurrido el plazo para el que hubiera sido autorizada. Ahora bien, incluso antes del agotamiento de dicho plazo deberá acordarse el cese de la medida en cuanto, atendidas las circunstancias, deje de estar justificado su mantenimiento. A estos efectos, la Ley ordena que se ponga fin a las medidas de investigación tecnológica en el momento en que desaparezcan las circunstancias que justificaron su adopción o cuando resulte evidente que a través de ellas no se están obteniendo los resultados pretendidos (art. 588 bis j).

Al cesar la medida, como regla, se debe comunicar a las personas afectadas la práctica de la injerencia y entregarles copia de las grabaciones o transcripciones de sus comunicaciones, si así lo pidieran. No obstante, esta sensata regla se ve notablemente debilitada al establecerse que su cumplimiento pueda eludirse cuando sea imposible, exija un esfuerzo desproporcionado o pueda perjudicar futuras investigaciones (art. 588 ter i.3 L.e.cr.). Estas excepciones a la regla, dada su amplia formulación, podrían conducir a que, en la práctica, cuando la investigación hubiese arrojado como resultado la carencia de relevancia penal de los hechos investigados, no se comunicara a los sujetos afectados la injerencia en sus derechos fundamentales. Se produciría así el paradójico y rechazable resultado de que solamente aquellas personas que, conforme a la investigación, pudieran haber incurrido en una conducta delictiva tendrían asegurado conocer las medidas de investigación tecnológica adoptadas frente a ellas, con la consiguiente posibilidad de defenderse frente a eventuales irregularidades o abusos; ahora bien, aquellas personas a las que la investigación precisamente exonere de toda responsabilidad penal no tendrían garantizado conocer la injerencia de las autoridades en sus derechos fundamentales ni podrían, por tanto, reaccionar frente a abusos o irregularidades.

VII. Destrucción de los registros

La Ley contempla la destrucción de los registros de las medidas de investigación tecnológica en dos fases. En primer lugar, al *finalizar el procedimiento* por resolución firme se ordena el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida, pero se conservará una copia bajo custodia del secretario judicial. No obstante, cuando el proceso haya terminado con sobreseimiento libre o sentencia absolutoria firme respecto del investigado, no se conservará copia salvo que el tribunal lo considere preciso (art. 588 bis k.2 L.e.cr.).

En un segundo momento, se destruirán también las copias conservadas por el tribunal. La destrucción de estas copias se producirá cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o, antes de los cinco años, cuando el delito o la pena hayan prescrito (art. 588 bis k.2 L.e.cr.).

Nada garantiza, en cualquier caso, que se destruyan las copias entregadas a las partes.