



**VNiVERSIDAD
D SALAMANCA**

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

Curso 2015/2016

LA NUEVA REGULACIÓN DE LA INTERVENCIÓN DE LAS COMUNICACIONES EN EL PROCESO PENAL ESPAÑOL

Nombre de la estudiante: Eloísa Victoria González

Tutora: Alicia González Monje

Junio 2016

TRABAJO FIN DE GRADO

GRADO EN DERECHO

Departamento: Derecho Administrativo, Financiero y Procesal

Área de conocimiento: Derecho Procesal

**LA NUEVA REGULACIÓN DE LA
INTERVENCIÓN DE LAS
COMUNICACIONES EN EL
PROCESO PENAL ESPAÑOL**

**THE NEW REGULATION OF THE
COMMUNICATIONS INTERVENTION
IN THE SPANISH CRIMINAL
PROCEEDING**

Nombre de la estudiante: Eloísa Victoria González
e-mail de la estudiante: elovicgon@usal.es

Tutora: Alicia González Monje

RESUMEN

Recientemente la Ley de Enjuiciamiento Criminal ha sufrido una modificación muy relevante, pues a través de LO 13/2015 de 5 de octubre, se procede a la incorporación de diversas diligencias de investigación relativas a la intervención en las comunicaciones, poniendo fin a la situación de inexistencia de regulación legal con respecto a esta materia en la que nos encontrábamos con anterioridad. Esta incorporación era, como podemos observar, muy necesaria, pues son muchos los avances tecnológicos que han tenido lugar en los últimos años y en consecuencia, han surgido nuevas modalidades a la hora de delinquir, nos referimos a la ciberdelincuencia, y a su vez nuevos instrumentos en manos de la autoridad judicial para proceder a la investigación de los delitos para así contribuir a la justicia. En el presente trabajo realizaremos un análisis de las nuevas diligencias de investigación incorporadas a la Ley de Enjuiciamiento Criminal, así como un breve estudio del derecho fundamental implicado principalmente en este tipo de supuestos, el derecho al secreto de las comunicaciones.

PALABRAS CLAVE: diligencias de investigación, nueva regulación, comunicaciones, ciberdelincuencia, derecho fundamental, secreto.

ABSTRACT

Recently the Criminal Procedure Law has suffered a very significant modification, because through LO 13/2015 of October 5, is come to the incorporation of various diligence investigations relating to the intervention in communications thus ending the situation of nonexistence legal regulation regarding this matter in which we were previously. This incorporation was like we can observe very necessary because there are many technological advances that have taken place in recent years and consequently, at the time new forms of committing a crime have emerged, we are referring to cyber crime, and in turn new instruments in the hands of the judicial authority to proceed to the investigation of crimes in order to contribute to justice. In the present paperwork we'll carry out an analysis of the new diligence investigations incorporated into the Criminal Procedure Law and a brief study of the fundamental right involved mainly in these types of cases, the right to secrecy of communications.

KEYWORDS: diligence investigations, new regulation, communications, cibercrime, fundamental right, secret.

INDICE

| | |
|--|----|
| ABREVIATURAS..... | 6 |
| 1. INTRODUCCIÓN..... | 7 |
| 2. NUEVA REGULACIÓN DE LA INTERVENCIÓN EN LAS COMUNICACIONES..... | 8 |
| 2.1. BREVE REFERENCIA A LAS NOVEDADES INTRODUCIDAS POR LA LO 13/2015 DE 5 DE OCTUBRE..... | 8 |
| 2.2. INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS..... | 17 |
| 2.2.1. Concepto y características..... | 17 |
| 2.2.2. Contenido..... | 18 |
| 2.2.3. Breve referencia a SITEL (Sistema Integral de Interceptación de las Comunicaciones Electrónicas)..... | 24 |
| 2.2.4. Hallazgos causales..... | 24 |
| 3. EL DERECHO AL SECRETO DE LAS COMUNICACIONES..... | 27 |
| 3.1. CONCEPTO..... | 27 |
| 3.2. MARCO JURÍDICO..... | 29 |
| 3.3. FINALIDAD..... | 30 |
| 3.4. TITULARIDAD..... | 30 |
| 3.5. GARANTÍAS DEL DERECHO AL SECRETO DE LAS COMUNICACIONES..... | 32 |
| 3.6. REGULACIÓN DE LA INTERVENCIÓN: RESOLUCIÓN JUDICIAL HABILITANTE..... | 32 |
| 3.7. DERECHO AL SECRETO DE LAS COMUNICACIONES EN EL ÁMBITO DE LAS ESCUCHAS TELEFÓNICAS Y TELEMÁTICAS..... | 35 |
| 4. EVOLUCIÓN DEL CONCEPTO DE COMUNICACIÓN Y NECESIDAD DE ADAPTACIÓN LEGAL..... | 39 |
| 4.1. CONCEPTO DE COMUNICACIÓN..... | 39 |
| 4.2. NECESIDAD DE REFORMA DE LA LEY DE ENJUICIAMIENTO CRIMINAL..... | 42 |
| 4.3. NUEVAS DILIGENCIAS DE INVESTIGACIÓN INCORPORADAS EN LA LEY CRIMINAL..... | 44 |

| | |
|--|----|
| 4.3.1. Utilización de dispositivos técnicos de seguimiento y localización... | 44 |
| 4.3.2. Captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos..... | 47 |
| 4.3.3. Registro de dispositivos informáticos de almacenamiento masivo..... | 50 |
| 4.4.4. El registro remoto de equipos informáticos..... | 51 |
| 5. CONCLUSIONES..... | 53 |
| BIBLIOGRAFÍA | 56 |

ABREVIATURAS

Art: Artículo

CE: Constitución Española

CEDH: Convenio Europeo de Derechos Humanos

CP: Código Penal

IMEI: International Mobile Station Equipment Identity (identidad internacional de equipo móvil)

IMSI: *International Mobile Subscriber Identity* (Identidad Internacional del Abonado a un Móvil)

LECrím: Ley de Enjuiciamiento Criminal.

LO: Ley Orgánica

MF: Ministerio Fiscal

STC: Sentencia del Tribunal Constitucional

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

STS: Sentencia del Tribunal Supremo

TC: Tribunal Constitucional

TEDH: Tribunal Europeo de Derechos Humanos

TS: Tribunal Supremo

UE: Unión Europea

1. INTRODUCCIÓN.

En el presente trabajo trataremos de exponer de forma concisa las principales novedades introducidas en la Ley de Enjuiciamiento Criminal a través de la LO 13/2015, de 5 de octubre, en relación con la intervención en las comunicaciones. Es bien sabido que la investigación de un hecho delictivo en un Estado de Derecho como el nuestro no es ilimitada pues trae consigo la posible vulneración de ciertos derechos fundamentales. En relación con esta cuestión, analizamos en las siguientes páginas el derecho implicado en estas situaciones, el derecho al secreto de las comunicaciones, recogido en el art. 18.3 CE, pues no toda intromisión e interceptación de una comunicación ajena en la investigación goza de licitud. Son diversos requisitos los exigidos en la nueva redacción de la LECrim, de los que podemos destacar el respeto a los principios constitucionales de necesidad, idoneidad, proporcionalidad, especialidad y excepcionalidad. A su vez, incidir en el hecho de que en nuestro ordenamiento la principal garantía para la validez constitucional de una intervención en las comunicaciones particulares, por disposición constitucional expresa, es la exclusividad jurisdiccional de su autorización.

¿Cuál es el objeto de este trabajo? Principalmente tratamos de resaltar la escasa previsión legal existente con anterioridad a la reciente reforma de la LECrim en relación con los medios de investigación relativos a la intervención de las comunicaciones para proceder a la persecución de nuevas modalidades delictivas, pues las clásicas intervenciones telefónicas resultan insuficientes para abarcar todos los supuestos que han ido surgiendo en los que se precisa una intromisión del poder estatal en las comunicaciones llevadas a cabo por el sujeto investigado. Los avances tecnológicos han traído consigo una necesaria adaptación del derecho a los nuevos tiempos, pues ya en cierto modo hemos dejado a un lado el correo postal pasando a la mensajería instantánea a través de la red o el terminal móvil.

Así, era notable el incremento de la dificultad en las tareas policiales la hora de proceder a la investigación de delitos de cierta envergadura como puede ser la desarticulación o persecución de una organización criminal en base a la legislación anterior. No obstante los citados avances han facilitado la tarea del delincuente y traen consigo nuevas modalidades de delincuencia, haciendo en definitiva necesaria la creación de nuevos medios en manos de las autoridades competentes para la investigación de las mismas.

Se ha tratado por tanto de regular las diversas diligencias de investigación encaminadas a investigar las distintas situaciones que van teniendo lugar a raíz de los avances

tecnológicos. Con la nueva redacción se incorpora la regulación de: la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes; y el registro de dispositivos de almacenamiento masivo de información.

Ante la ausencia de regulación normativa, ha sido a través de la doctrina y la jurisprudencia como se ha procurado suplir los vacíos legales, sin embargo, ha llegado un punto en el que resultaba inaceptable seguir aplicando el método de la analogía pues son muchas las actuaciones delictivas cuya intervención no encuentra base alguna en el único precepto existente en la anterior LECrim, el art.579, y de ahí la gran ventaja que ha supuesto esta regulación que en las páginas siguientes analizaremos.

2. NUEVA REGULACIÓN DE LA INTERVENCIÓN EN LAS COMUNICACIONES

2.1. BREVE REFERENCIA A LAS NOVEDADES INTRODUCIDAS POR LA LO 13/2015 DE 5 DE OCTUBRE.

En primer lugar, procede aludir a la definición de intervención en las comunicaciones, y es que se trata de “un acto de captación en tiempo real del contenido de comunicaciones tanto telefónicas, por vía de correo electrónico, por vía internet o cualquier otro tipo de comunicación”¹.

Era necesaria una adaptación de la normativa actual con respecto al surgimiento de las nuevas tecnologías. Así, la reforma de la Ley de Enjuiciamiento Criminal llevada a cabo en el año 2015 ha supuesto la remodelación de varias cuestiones, como son el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (LO 13/2015 de 5 de octubre). Observamos que se ha procedido a la tramitación mediante Ley Orgánica, en la medida que la nueva regulación incide sobre derechos fundamentales recogidos en la Constitución, del que destacamos el derecho al secreto de las comunicaciones consagrado en el art.18 CE².

¹ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal”, *I Jornada del Boletín del Ministerio de Justicia: «Las reformas del proceso penal»*, *Boletín del Ministerio de Justicia*, núm. 2186, febrero 2016, p. 29.

² Artículo 18 CE: “1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las

El legislador se ha visto en la necesidad de adaptarse a los nuevos tiempos puesto que, entre otras cosas, los avances tecnológicos han conllevado el surgimiento de una nueva metodología a la hora de proceder a la investigación mediante el recurso a la interceptación de las comunicaciones, deviniendo en consecuencia ineficaces los medios tradicionales de investigación³. Se han desarrollado, por tanto, múltiples herramientas de carácter electrónico que favorecen la actuación de los poderes públicos a la hora de proceder a la investigación del delito y averiguación del delincuente, así como nuevas modalidades de medios de comunicación en manos de los investigados.

Siguiendo a GONZÁLEZ MONJE, “entre estos medios destacan, la autorización de actividades de vigilancia electrónica de las comunicaciones mediante medios técnicos y de grabación de las conversaciones o de seguimiento y videovigilancia de personas; las medidas dirigidas a facilitar las investigaciones financieras en el patrimonio de la organización criminal, mediante el levantamiento del secreto bancario y el establecimiento de obligaciones de colaboración obligatoria de los operadores financieros y de la propia Administración; el uso de la figura del agente encubierto y del agente provocador; equipos conjuntos de investigación; y, finalmente, la autorización de la circulación o entrega vigilada de determinados efectos delictivos”⁴.

Sin embargo, debemos precisar que esta actuación del poder público en la investigación de un determinado hecho delictivo no es ilimitada, por lo que la cuestión a plantearse es ¿hasta dónde puede llegar esa investigación mediante la interceptación de las comunicaciones?, o lo que es lo mismo, ¿cuándo se entienden vulnerados los derechos de la persona investigada? En consecuencia resulta necesario establecer un equilibrio entre la actuación del Estado a la hora de proceder a la investigación criminal y los derechos constitucionalmente garantizados a todos los ciudadanos, que posteriormente analizaremos.

Como sabemos, nuestro ordenamiento jurídico hasta esta última reforma ha carecido de regulación suficiente referente a la interceptación de las comunicaciones del investigado y los jueces han tenido que actuar basándose en la jurisprudencia desarrollada a lo largo

comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

³ Para un análisis del tema: GONZÁLEZ MONJE, A., “Nuevas tecnologías e investigación penal. La superación de los métodos tradicionales”, *FODERTICS 3.0. Estudios sobre nuevas tecnologías y Justicia*, Comares, Granada, 2015, pp. 149-158.

⁴ GONZÁLEZ MONJE, A., “Nuevas tecnologías...”, op., cit., p. 154.

de estos últimos años por nuestros Altos Tribunales, TS y TC. Procede afirmar que la creación jurisprudencial ha suplido la regulación relativa a esta materia que depende en gran medida de las evoluciones tecnológicas que van aconteciendo con el paso del tiempo.

Así, esta nueva regulación ha sido demandada tanto por el Tribunal Supremo como por el Tribunal Constitucional⁵, que por su parte ha manifestado la necesidad de abordar esta materia, siendo muchas las cuestiones carentes de cobertura legal y sobre las que no procedía la aplicación del método de la analogía en base a la escasa regulación existente⁶.

Un ejemplo de ello lo encontramos en una reciente resolución del Tribunal Constitucional, la STC de 22 de septiembre de 2014, en la que declaró la vulneración del derecho fundamental al secreto de las comunicaciones en un supuesto de grabación de conversaciones de los detenidos en las dependencias policiales, a pesar de haber sido autorizada por resolución judicial expresa. El TC manifiesta la insuficiencia legislativa para habilitar “la intervención en las comunicaciones directas entre detenidos en dependencias judiciales”, puesto que el antiguo art. 579 LECrim sólo hacía referencia a intervenciones telefónicas y no a otro tipo de escuchas. Así, el TC declaró que “*las grabaciones en dependencias policiales resultaron contrarias al art. 18.3 CE, deviniendo nula la prueba obtenida por ese cauce para todos aquellos que resultaron perjudicados penalmente por ella*”⁷. Tras este pronunciamiento, se observa de forma clara la necesidad urgente de llevar a cabo una reforma legal.

Procede describir brevemente en qué ha consistido la reforma objeto de estudio para posteriormente hacer un análisis más exhaustivo de algunas de las diligencias recogidas en la misma, concretamente la interceptación de las comunicaciones telefónicas y telemáticas.

⁵ RODRÍGUEZ LAINZ, J. L., “Peculiaridades de la intervención judicial de comunicaciones electrónicas”, *Diario La Ley*, 2 de Marzo de 2009, pp. 2 y ss.

⁶ Las insuficiencias de nuestro marco legal han sido puestas de manifiesto tanto por el TC (SSTC núm. 26/2006, de 30 de enero, 184/2003, de 23 de octubre, 49/1999, de 5 de abril) como por el TEDH (SSTEDH de 18 de febrero de 2003, Prado Bugallo contra España y de 30 de julio de 1998, Valenzuela Contreras contra España).

⁷ Para un análisis de la misma: GONZÁLEZ MONJE, A., “Sentencia del Tribunal Constitucional (Sala Segunda), 145/2014, de 22 de septiembre [BOE n.º 261, de 28-X-2014]: Intervención de comunicaciones en dependencias policiales”, *AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, Vol. 3, núm. 1, 2015, pp. 355-357.

Así, en primer lugar la reforma de la LECrim actualiza el artículo 579 LECrim, añadiendo la detención y apertura de la correspondencia escrita y telegráfica y delimitando su ámbito material de aplicación, así como los plazos de duración y las excepciones a la necesidad de autorización judicial para proceder a la investigación⁸.

Por otra parte, la nueva regulación carece de un listado de delitos expreso sobre los que cabe realizar la investigación mediante este tipo de interceptaciones, por lo que se ha impuesto la exigencia de que concurren de forma no cumulativa concurrencia tres requisitos: el primero de los requisitos se refiere a la gravedad de la pena y exige que se trate de delitos dolosos con pena con límite máximo superior a tres años de prisión. El segundo hace alusión a que el delito haya sido cometido en el seno de una organización criminal y el tercero y último a que se trate de delitos de terrorismo⁹.

Debemos destacar a su vez la introducción del artículo 579 bis referido entre otras cuestiones al tratamiento de los “hallazgos causales”, es decir al cómo proceder ante el surgimiento de indicios sobre la comisión de un nuevo delito en el transcurso de la investigación del delito previsto en la resolución habilitante. Se establece que la persecución de este hallazgo tendrá que ser autorizada por la autoridad judicial de forma expresa (art. 579 bis 3 por remisión del art. 588 bis i)¹⁰.

En el Capítulo IV LECrim se han incorporado por tanto una serie de disposiciones que van a ser aplicables sobre el resto de medidas de investigación tecnológicas albergadas en los siguientes capítulos, concretamente entre los Capítulos V y VIII de la LECrim.

No debemos obviar la existencia y exigencia normativa de los principios constitucionales básicos¹¹ para que el acto de intromisión en la comunicación sea válido y estos son:

- Principio de especialidad, que exige que la medida esté relacionada con la investigación de un concreto hecho delictivo. No podrán autorizarse medidas de investigación cuya finalidad sea descubrir delitos sin una base objetiva.
- Principio de idoneidad, que exige que la injerencia en las comunicaciones sea apta para lograr el fin perseguido.

⁸ Exposición de Motivos de Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Punto IV, p. 4.

⁹ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación...”, op., cit., pp. 30 y 31.

¹⁰ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación...”, op., cit., pp. 34 y 35.

¹¹ Art. 588 bis a) LECrim.

- Principio de excepcionalidad: conforme a este solo podrá autorizarse la ejecución de la medida cuando no sea posible el empleo de otras medidas menos gravosas para los derechos fundamentales del investigado e igualmente útiles para el esclarecimiento del hecho.

- Principio de necesidad: solo podrá aprobarse la medida cuando se agrave la dificultad de la investigación del hecho delictivo en cuestión en caso de no recurrir a la misma, es decir, que la misma tiene que ser indispensable.

- Principio de proporcionalidad de la medida: se refiere al equilibrio que debe existir entre el sacrificio de los derechos del investigado y el beneficio que implica la adopción de la medida con respecto al interés público y de terceros. Se debe realizar por tanto una ponderación de los intereses en conflicto teniendo en cuenta que el sacrificio de los derechos del investigado no podrá ser superior al beneficio que implicaría la adopción de la medida para el interés general ¹².

Respecto a la interceptación de las comunicaciones telefónicas y telemáticas, se incorpora el art. 588 ter LECrim, precepto dedicado exclusivamente a la regulación de esta cuestión y del mismo podemos destacar varios aspectos principales como es la incorporación de ciertos delitos en el ámbito material de la medida como son los cometidos por medio de instrumentos informáticos, tecnológicos u análogos. A su vez, destacar como gracias a la reforma se le otorga sustantividad propia a otras formas de comunicación telemática que anteriormente no gozaban de regulación.

En consecuencia, con la nueva regulación se permite la intervención y registro de las comunicaciones de cualquier clase realizadas mediante el teléfono o cualquier otro medio de comunicación telemática, lógica o visual, una actuación que sin embargo estará sometida a los principios generales recogidos legalmente.

¿Qué implica esto último? Pues que al autorizar la intervención telefónica o de cualquier otro medio de comunicación, el juez deberá precisar en la resolución habilitante el ámbito objetivo y subjetivo de la misma, y tendrá que hacerlo ponderando la intromisión del Estado en las comunicaciones de los particulares y la gravedad del presunto hecho delictivo objeto de la investigación.

¹² VELASCO NUÑEZ, E., “Investigación tecnológica de delitos: disposiciones comunes e interceptaciones telefónicas y telemáticas”, *Jornadas de especialistas en criminalidad informática*, Centro de Estudios Jurídicos, CEJ, 2016, p. 3. Disponible en: http://www.cej-justicia.es/cej_dode/flash/ebook/assets/img/cejponencia1462865634628/cejponencia1462865634628.pdf

En el art. 588 ter g LECrim se establece además un plazo de duración máxima inicial de tres meses, susceptible de prórroga, previa petición razonada por períodos sucesivos de igual duración, hasta un máximo temporal de 18 meses. Por otra parte, se exige que la solicitud policial de la intervención esté suficientemente motivada.

A su vez, se impone la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central al sistema digital de grabación de las comunicaciones con el fin de asegurar la autenticidad e integridad de los soportes puestos a disposición del juez¹³. Además, se fija cómo debe procederse al borrado y eliminación de las grabaciones originales una vez que finalice el procedimiento.

Debemos resaltar el otorgamiento de un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, y todo ello en base a la continua y ya consolidada jurisprudencia del Tribunal Supremo. Se regula a su vez, el supuesto de la cesión de datos desvinculados de los procesos de comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal (MF) o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial¹⁴.

En la gran mayoría de las ocasiones, para una idónea investigación en ciertos tipos delictivos es precisa e incluso resulta determinante la grabación de comunicaciones orales abiertas a través de dispositivos electrónicos. Sin embargo, esta actuación debe ser autorizada por el juez de instrucción y es necesario que dicha autorización esté basada y justificada conforme a los principios procesales de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad.

Así, no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas pues esta medida solo podrá acordarse para encuentros concretos que vaya a mantener el investigado, debiéndose identificar con precisión el lugar o dependencias sometidos a vigilancia. Debemos señalar en

¹³ Art. 588 ter f LECrim: “la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, 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”.

¹⁴ Exposición de Motivos de Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Punto IV, p. 5.

consecuencia que este tipo de medidas son de carácter excepcional y tienen que estar perfectamente delimitadas en cuanto a espacio y tiempo (art. 588 quater c).

Además, en la reforma se trata la cuestión relativa a la utilización de dispositivos de seguimiento y localización, cuestión muy polémica pues es una medida que repercute de forma directa sobre la intimidad de las personas y es por eso que la autorización de su práctica corresponde al Juez de Instrucción (art. 588 quinquies b).

El fin de esta diligencia es el de seguir los movimientos de una persona en concretos espacios de tiempo, así como descubrir los periodos de tiempo en los que permanece en un espacio en concreto.

En el art. 588 quinquies b) 4 se prevé la posibilidad de que la policía se anticipe a la práctica de la medida cuando la investigación se pueda ver frustrada en caso de retrasar la intervención. Sin embargo, en el momento en el que se conceda la autorización judicial, la actuación de la policía quedará sometida a las indicaciones de la autoridad judicial¹⁵.

Se permite a su vez la grabación visual en espacio público sin autorización judicial siempre y cuando no se vulneren los derechos albergados en el art.18 CE (intimidad, honor y propia imagen, secreto de las comunicaciones etc)¹⁶.

Con la nueva redacción de la ley se ha pretendido acabar con otro vacío normativo, el relativo al registro de dispositivos informáticos de almacenamiento masivo.

Así, la nueva regulación establece una diferenciación entre el supuesto de incautación en el transcurso de la ejecución de una medida de entrada y registro domiciliario (art. 588 sexies a), y la de cualquier otra actuación policial ajena al registro domiciliario (art. 588 sexies b).

El precepto exige que se prevea específicamente en la resolución de la medida la justificación del acceso policial a la información contenida en los dispositivos objeto de investigación. El descubrimiento ocasional en el curso de un registro domiciliario o de práctica de cualquier otra diligencia policial, si bien no impedirá su incautación, exigirá de una previa autorización judicial específica.

¹⁵ RODRÍGUEZ LAINZ, J. L., “Las nuevas medidas de investigación tecnológica de la Ley Orgánica 13/2015”, *SEPIN*, Enero de 2016, p. 9. Disponible en: [webs\Artículo Monográfico. Enero 2016.htm](https://www.sepin.es/web/Articulo_Monografico_Enero_2016.htm)

¹⁶ Art. 588 quinquies a) LECrim: “1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos”.

En el art. 588 sexies c) se exige que la resolución habilitante determine los límites concretos a los que deberá ceñirse el análisis de contenidos. Se establece a su vez como regla general que se evite incautar soportes originales, siempre y cuando sea posible.

Como novedad en la LECrim destacamos la posibilidad de expandir el examen de los contenidos almacenados en el dispositivo de almacenamiento masivo en cuestión, a otros dispositivos físicos o virtuales accesibles lícitamente por medio del sistema inicial o que se encuentren disponibles para el mismo.

El art. 586 sexies c) 4, por su parte, autoriza a la Policía Judicial y siempre cuando se trate de razones de urgencia, realizar el examen directo de los datos almacenados en el dispositivo objeto de investigación o incautado¹⁷.

Se introduce asimismo el art. 588 septies, en el que se regula el llamado registro remoto sobre equipos informáticos. En dicho precepto se recoge un *numerus clausus* de delitos para los que procede la práctica de esta medida y la exigencia de especificar en la resolución judicial habilitante el ámbito objetivo de la misma de la intervención. Por lo que se refiere al ámbito de aplicación temporal, éste es de un mes de duración máxima, prorrogable por iguales períodos hasta un máximo de tres meses.

En el art. 588 octies se fija como medida de aseguramiento, en lo que se refiere a las diligencias de investigación tecnológica, la orden de conservación de datos con el objetivo de asegurar la preservación de la información y datos concretos de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente para su cesión.

Se establece un plazo de vigencia máximo de la orden de noventa días prorrogable hasta que se autorice la cesión o se cumplan ciento ochenta días.

Finalmente procede resaltar la figura del agente encubierto y su importancia de cara a la investigación de ciertos delitos. Con la reforma se actualizan los instrumentos que puede emplear el agente encubierto de cara a la realización de las tareas que le han sido encomendadas, como la grabación de conversaciones o la obtención de imágenes. Debemos señalar como el marco de actuación del agente encubierto debe ser autorizado por la autoridad judicial.

¹⁷ RODRÍGUEZ LAINZ, J. L., “Las nuevas...”, op., cit., p. 12.

Además es preciso mencionar la nueva figura del agente encubierto informático, pues su actuación contribuye a una mayor eficacia en la persecución de las actividades propias de la delincuencia organizada. El mismo precisará de autorización judicial para actuar en canales cerrados de comunicación aunque ciertas actuaciones como el intercambio o envío de archivos ilícitos por razón de su contenido quedarán sujetas a la emisión de una nueva autorización expresa¹⁸.

Descritas brevemente las medidas anteriores, debemos preguntarnos cuáles han sido en definitiva las novedades introducidas por la LO 13/2015 en relación a la intervención en las comunicaciones.

Con la reforma, el 579 LECrim dedica su regulación a las comunicaciones postales y telegráficas, mientras que se crea un Capítulo IV en el Título VIII del Libro II para las nuevas tecnologías, dividido en:

- interceptación de las comunicaciones telefónicas y telemáticas;
- captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos;
- utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes;
- registro de dispositivos de almacenamiento masivo de información¹⁹.

Así, con la modificación del art. 579, la redacción del art. 579 bis LECrim y la suma de nuevas medidas de investigación tecnológica a los Capítulos V-VIII del Título VIII del Libro II de la LECrim se ha procedido a la adaptación de la legislación a las nuevas formas de delinquir mediante el uso de las nuevas tecnologías.

Para perseguir algunos delitos, en ocasiones, la incorporación en la investigación de ciertos datos de carácter electrónico de tráfico o asociados puede ser clave y decisivo.

La reforma incorpora el criterio establecido en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas

¹⁸ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación...”, op., cit., p. 38.

¹⁹ GIMENO BREVIÁ, J., “Principales novedades de la reforma de la LECrim 2015”, Dossier reforma de la Ley de Enjuiciamiento Criminal, Thomson Reuters-Aranzadi, 2015, p. 17. Disponible en: http://www.aranzadi.es/sites/aranzadi.es/files/creatividad/Marketing/email_dossieres_LEC_LECrim/imagenes/Dossier_Ref_LECrim_min.pdf

de comunicaciones²⁰, y en consecuencia establece que para que puedan incorporarse esos datos al procedimiento y ser cedidos a los agentes facultativos, es requisito ineludible que el juez emita una autorización.

Por último es preciso resaltar la adaptación del lenguaje empleado en la LECrim a los tiempos actuales, eliminando ciertos términos o expresiones que carecían de rigor conceptual. Aparecen así los términos de investigado y encausado, el primero referido a la persona que es objeto de investigación por la presunta comisión de un determinado delito y el segundo una vez concluida la instrucción de la causa, cuando la persona es imputada por haber participado en la comisión del delito²¹.

2.2. INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS Y TELEMÁTICAS.

2.2.1. Concepto y características.

En cuanto al concepto de intervención telefónica por parte de la doctrina, podemos aludir a la dispuesta por LÓPEZ FRAGOSO que las definió: “(...) como aquellas medidas instrumentales restrictivas del derecho fundamental al secreto de las comunicaciones privadas, ordenadas y ejecutadas en la fase instructora de un proceso penal bajo la autoridad del órgano jurisdiccional competente frente a un imputado –u otros sujetos de los que éste se sirva para comunicarse-, con el fin de, a través de la captación del contenido de lo comunicado o de otros aspectos del proceso de comunicación, investigar determinados delitos, averiguar el delincuente y, en su caso, aportar al juicio oral determinados elementos probatorios”²².

Esta diligencia de investigación tiene por objeto los terminales o sistemas de comunicación que de forma habitual son utilizados por el investigado. Precisar que dicha intervención podrá realizarse tanto sobre el contenido de las comunicaciones y los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una llamada, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales de los que el investigado sea titular o usuario de los mismos.

²⁰ Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (BOE nº. 251, de 19 –X-2007).

²¹ GIMENO BREVIÁ, J., “Principales novedades...”, op., cit., p. 16.

²² LÓPEZ-FRAGOSO ALVÁREZ, T., *Las intervenciones telefónicas en el proceso penal*, Colex, Madrid, 1991, pp.14 y ss.

Se dice que las intervenciones telefónicas gozan de una doble naturaleza, pues pueden actuar como fuente de investigación y a su vez como medio de prueba.

Es preciso señalar como este medio de investigación debe respetar el contenido del art. 18 de nuestra Constitución relativo al derecho al secreto de las comunicaciones.

Así, esa intromisión en el ámbito de la intimidad personal de los investigados debe ser constitucionalmente correcta. Debe existir por tanto un equilibrio entre esa necesidad de salvaguardar el orden social y la seguridad ciudadana investigando y destapando la comisión de delitos, y los derechos de las personas objeto de investigación (STS n°1424/1993, de 18 de junio)²³.

Con anterioridad a la reforma, esta diligencia estaba prevista con carácter exclusivo en el art. 579 LECrim, reformado tras la entrada en vigor de la LO 4/1988, de 25 de mayo, y en el mismo se establecía la posibilidad por parte del juez de aprobar la detención de la correspondencia privada, postal y telegráfica del investigado; la intervención de las comunicaciones telefónicas del mismo y la observación de las comunicaciones postales, telegráficas o telefónicas²⁴.

A raíz del progresivo avance en las nuevas tecnologías, esta norma resultó insuficiente y en defecto de regulación aplicable al resto de supuestos que iban surgiendo, se optó por la vía de la analogía para solucionar esta cuestión. Así, en los últimos años se han ido integrando estas lagunas legislativas a través de la interpretación jurisprudencial.

Finalmente, y tal y como mencionamos en el punto anterior, a través de la aprobación de la Ley Orgánica 13/2015 se ha llevado a cabo la incorporación en la Ley de Enjuiciamiento Criminal de una serie de disposiciones relativas a la intervención en las comunicaciones. En lo que se refiere a las intervenciones telefónicas, debemos resaltar la reforma del art. 579, así como la incorporación de los arts. 579 bis y 588 bis y ss.

2.2.2. Contenido.

Como ya hemos señalado anteriormente, destaca GONZÁLEZ-CUELLAR SERRANO, que "la intervención de comunicaciones prevista por el muy defectuoso artículo 579 no puede decirse que se encuentre amparada por una normativa que cumpla las mínimas

²³ Circular de la Fiscalía General del Estado 1/ 2013 *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*.

²⁴ GONZÁLEZ-MONTES SÁNCHEZ, J. L., "Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", *Revista electrónica de ciencia penal y criminología*, 2015, p. 21.

garantías exigibles en un Estado de Derecho”²⁵. Y es que dicho precepto no especificaba tan siquiera el procedimiento de intervención en la comunicación telefónica, cuestión que tuvo que ser solventada por la jurisprudencia del TS, de la que destacamos la STS de 25 de junio de 1993²⁶. Lo anterior fue constatado tanto por el Tribunal Europeo de Derechos Humanos (TEDH) así como por el Tribunal Constitucional que ha señalado que dicho precepto “no es inconstitucional por lo que dice, sino por lo que no dice”²⁷.

Se introduce el art. 588 bis LECrim, en el que se recogen una serie de disposiciones generales aplicables a todas las medidas de intervención en las comunicaciones previstas en los preceptos siguientes. De las mismas destacamos, en primer lugar, la exigencia del respeto a los principios rectores enunciados en el art. 588 bis a), principios de idoneidad, excepcionalidad, proporcionalidad y necesidad.

Por otro lado, hace referencia al contenido de la solicitud de la medida emitida por el Ministerio Fiscal o por la Policía Judicial, en la que deberá contener de forma detallada el objeto de la medida e identidad del investigado en caso de ser conocida, así como la justificación expresa de la necesidad de adoptar dicha medida e indicios de criminalidad que hayan surgido de forma previa a la elaboración de esta solicitud. Deberá explicitar además, la extensión del acto de injerencia, especificando su contenido y su forma de ejecución, los medios de comunicación que serán utilizados para llevarlo a cabo, la duración del mismo y la unidad investigadora de la Policía Judicial que procederá a su ejecución.

Por su parte, el juez de instrucción, tras recibir la solicitud y aceptarla, dictará, previa audiencia al Ministerio Fiscal, la resolución habilitante y en la misma deberá precisar las mismas cuestiones previstas para el caso de la solicitud por parte de la Policía o Ministerio Fiscal, y además, conforme al art. 588 bis c, las siguientes:

- calificación jurídica de los hechos,
- forma y periodicidad con la que el solicitante informará al juez sobre los resultados de la medida,

²⁵ GONZÁLEZ-CUELLAR SERRANO, N., “La reforma de la Ley de Enjuiciamiento Criminal: Necesidad de su reforma y examen de las sucesivas reformas parciales”, Centro de Estudios Jurídicos, CEJ, 2004, p. 11. Disponible en: webs\Centro de Estudios Jurídicos_Descarga de ponencias.htm

²⁶ Véase: <webs\noticias jurídicas.htm>

²⁷ STC 184/2003, de 23 de octubre, en la que reitera la doctrina ya afirmada en STC 49/1999, de 5 de abril: “el Alto Tribunal ha decidido no plantearse su inconstitucionalidad, lo cual justifica básicamente con el argumento de que el precepto no es inconstitucional por lo que dice, sino por lo que no dice, de forma que su anulación no serviría para remediar la lesión constitucional y simultáneamente privaría de un medio necesario de investigación de los delitos”.

- finalidad perseguida con la medida y,

- expresa mención del deber de colaboración y de guardar secreto por parte del obligado a llevarla cabo, con apercibimiento de incurrir en un delito de desobediencia.

El juez tendrá que ponderar la gravedad de los hechos objeto de investigación, para así determinar hasta qué punto podrá llegar esa intromisión del Estado en la intimidad del investigado en cuestión.

Conforme al art. 588 bis j) LECrim, se pondrá fin a la medida, bien cuando se cumpla el plazo fijado en la resolución judicial, o bien cuando cesen los hechos que justificaron su adopción o se acredite que no se están obteniendo los resultados esperados con su ejecución.

Tras la finalización del proceso, se impone la destrucción de los registros originales que puedan persistir en los sistemas informáticos empleados para la ejecución de la medida, manteniendo una copia en manos del secretario judicial. Esta copia conservada, será a su vez eliminada una vez transcurridos cinco años desde la ejecución de la pena o desde la prescripción del delito o declaración de sobreseimiento libre o declaración de sentencia absolutoria de carácter firme con respecto al investigado, todo ello siempre y cuando no considerara lo contrario el Tribunal²⁸.

Dejando a un lado las disposiciones generales, es el contenido del art. 588 ter LECrim el encargado de regular de forma específica la diligencia de intervención en las comunicaciones telefónicas, indicando en primer lugar los presupuestos que deben darse para proceder a la práctica de esta diligencia.

Así, se establece que la autorización de dicha medida queda subordinada al hecho de que el objeto de la investigación sea alguno de los delitos descritos en el art. 579.1 LECrim o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la comunicación.

Se concreta por tanto el ámbito material de aplicación de esta diligencia recurriendo a dos criterios, según CABEZUDO RODRÍGUEZ, por un lado cualitativo al tener en cuenta el tipo de delito sobre el que se va a autorizar y por otro cuantitativo pues se atiende a la gravedad de la pena de dicho delito. Debemos destacar por tanto, lo que este hecho ha supuesto en la actualidad, pues con anterioridad a la reforma no había unos

²⁸ Art. 588 bis k) LECrim.

criterios legalmente preestablecidos sobre los que basarse a la hora de autorizar la intervención, sino que de nuevo ha sido objeto de interpretación jurisprudencial que por su parte, no solo entendía que había que basarse en que se tratara de un delito grave y la pena que llevase aparejada, sino que además tenía en cuenta la influencia del bien jurídico protegido y su repercusión a nivel social²⁹.

Así, en virtud del criterio cuantitativo, el art. 588 ter a) establece que deberá tratarse de delitos dolosos con pena cuyo límite máximo sea de, al menos, tres años de prisión. En lo que respecta al criterio cualitativo, debe tratarse de “delitos cometidos en el seno de un grupo u organización criminal, delitos de terrorismo” o “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) por remisión al art. 579.1 LECrim).

En cuanto al ámbito de actuación, se especifica que los instrumentos a intervenir deberán ser aquéllos que sean utilizados por el investigado de forma regular³⁰.

En lo que se refiere al objeto de la medida, se distinguen varios componentes de la comunicación sobre los que cabe la posibilidad de intervenir; así el precepto aclara que podrá ser objeto de interceptación tanto el contenido del acto de comunicación, los datos de tráfico³¹ individuales o asociados al proceso de comunicación, o la información personal del usuario que, supuestamente, efectúa la transmisión. Así, es posible diferenciar entre el término *interceptación* referido a la captación del contenido de la comunicación, y *observación* referido a identificar la procedencia e identidad de los partícipes de la comunicación o algunos datos de tráfico anexos a la misma³².

Por otro lado se prevé la posibilidad de efectuar la intervención sobre un terminal del que sea titular la víctima cuando se entienda que sobre la misma recae un grave riesgo.

En el art. 588 ter c) LECrim se establece la posibilidad de autorizar la intervención de un terminal perteneciente a una tercera persona distinta del investigado, siempre que se acredite que éste último emplea dicho instrumento para transmitir información o que el

²⁹ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación..., op., cit., p. 30.

³⁰ Art. 588 ter b) LECrim.

³¹ La Ley Orgánica 13/2015, los define como “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”, (art. 588 ter I.III).

³² CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación..., op., cit., p. 29.

titular del mismo participa en la actividad delictiva en la que se ve inmerso el investigado o se beneficie de la misma.

Asimismo procederá la ejecución de la medida cuando el terminal sea objeto de utilización maliciosa por parte de terceros sin conocimiento de su titular.

Además de los datos exigidos por el art. 588 bis LECrim, la Policía Judicial o en su caso el Ministerio Fiscal, por mandato expreso del art. 588 ter d) LECrim, deberán adjuntar en la solicitud los siguientes:

- 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.

En cuanto a la determinación de la extensión de la medida, el precepto citado, en su apartado segundo, establece que la solicitud podrá tener por objeto distintos tipos de datos: el contenido de la comunicación con indicación *de la forma o tipos de comunicaciones a que afecta*, su origen o destino, la localización geográfica del origen o destino u otros datos de tráfico *asociados o no asociados*. Gracias a ello, según CABEZUDO RODRÍGUEZ, “se pone término a la práctica forense de proceder a la intervención indiferenciada de todas las comunicaciones, sin parar en el medio utilizado, y de los datos adjuntos o asociados con ocasión de cualquier interceptación, debiendo optarse por aquellos que supongan un sacrificio menor de los derechos del afectado siempre que resulte idónea para la consecución del fin pretendido. Los solicitantes habrán de justificar tales extremos y el instructor ponderar esas razones antes de acordar la intervención”³³.

Pese a lo anterior, el art. 588 ter d) 3 LECrim alberga una excepción a la regla general de necesidad de una autorización previa para la celebración de la intervención (principio de reserva jurisdiccional de las medidas de investigación), y es que recoge la posibilidad de que en circunstancias excepcionales, la Policía Judicial o el Ministerio Fiscal adopten la medida en cuestión sin autorización judicial previa. Procede aplicar lo anterior siempre y cuando se trate de actuaciones de carácter urgente en el marco de la averiguación de *delitos relacionados con la actuación de bandas armadas o elementos terroristas* y *existan razones fundadas que hagan imprescindible la medida*. No

³³ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación...”, op., cit., p. 32.

obstante, deberán comunicar la realización de esta actuación en un plazo máximo de veinticuatro horas a la autoridad judicial y justificar de forma motivada las razones por las que se decidió adoptarla, así como el modo de proceder y el resultado alcanzado con la misma. Ante esto, el juez posteriormente manifestará la aprobación o desestimación de la misma en un plazo máximo de setenta y dos horas desde que fue ordenada la medida.

En la nueva regulación se prevé a su vez un deber de colaboración por parte de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información o cualquier otra persona que pueda facilitar las comunicaciones a través de cualquier medio de comunicación, hacia la autoridad judicial, el MF o agentes de la Policía Judicial, con el fin de lograr una mayor eficiencia del transcurso de la investigación facilitando el cumplimiento de la medida autorizada.

Sobre los colaboradores pesará la obligación de conservar el secreto en relación con las actividades que le fueron requeridas por las autoridades previamente indicadas, pudiendo incurrir en caso contrario en un delito de desobediencia³⁴.

La Policía Judicial tendrá que proporcionar al juez en los plazos que este último determine, y mediante diferentes soportes digitales, la transcripción de los pasajes que estime de interés y las grabaciones íntegras realizadas, indicando el origen y destino de cada una de ellas y asegurando “la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas” mediante un sistema de sellado o firma electrónica.

Finalmente, en lo que respecta al plazo de la intervención, se fija un plazo máximo de tres meses de intervención, prorrogable por periodos de igual duración hasta un máximo de 18 meses.

Para proceder a la prórroga se exige una previa petición motivada en periodos sucesivos de igual duración y siempre que persistan las causas que justificaron en su día la ejecución de la intervención

Con esto se logra, por un lado, una mejora en la investigación, y por otro, se asegura que no va a haber una prolongación innecesaria de la intromisión en la vida privada de los sujetos implicados en la investigación o más bien afectados por esta medida.

³⁴ Art. 588 ter e) LECrim.

2.2.3. Breve referencia a SITEL (Sistema Integral de Interceptación de las Comunicaciones Electrónicas).

Se trata de un sistema informático que ofrece un espionaje íntegro de comunicaciones de carácter electrónico. Desde hace unos años, la intervención de las comunicaciones telefónicas en España se lleva a cabo por medio de este mecanismo, configurado con un sistema de enlaces punto a punto con las operadoras de telefonía, que transmiten directamente las intervenciones autorizadas, y estas son almacenadas automáticamente y de forma íntegra bajo firma digital, en el mismo formato remitido. Posteriormente estos archivos se plasman en un soporte físico y son entregados a la autoridad judicial competente. Este sistema, además de facilitar la escucha de las conversaciones telefónicas del terminal objeto de intervención, aporta otros datos complementarios como la localización de dicho terminal mediante la ubicación de la BTS (repetidor) desde el que se está realizando dicha comunicación³⁵.

Este sistema proporciona "un amplio material probatorio electrónico basado en la interceptación y en la grabación digital de conversaciones a través de móviles o dispositivos electrónicos tanto en formato oral como en escritura digital, y que deberán ser aportadas posteriormente en un determinado juicio. (...) hasta hoy no teníamos una regulación que amparaba el amplio de espectro de comunicaciones que podía interceptar SITEL, ni una ley orgánica que refrendara su uso. Para solventar este vacío legal nos remitíamos a la jurisprudencia establecida por el TC sobre las intervenciones telefónicas en numerosas sentencias y extraer de ellas los presupuestos mínimos de interceptación; por lo que nos movíamos en un claro terreno marcado por una palpable inseguridad jurídica"³⁶.

2.2.4. Hallazgos causales.

Implican la aparición en la ejecución de una determinada intervención de indicios acerca de la comisión de otros hechos delictivos no contemplados en la resolución

³⁵ LLAMAS FERNÁNDEZ, M., GORDILLO LUQUE, J.M., "Medios técnicos de vigilancia", *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, núm.2, 2007, pp. 209 y ss.

³⁶ BUENO DE MATA, F., "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", *Diario La Ley*, 2015, p. 1.

habilitadora inicial, cuya posterior persecución deberá ser autorizada de forma expresa por el juez³⁷.

Ésta ha sido la postura adoptada jurisprudencialmente en los últimos años y finalmente ha sido introducida en la LECrim mediante la incorporación del art. 579 bis.

Se trata por tanto de una cuestión polémica que también ha sido finalmente abarcada por la LO 13/2015, y es que cabe la posibilidad de que en el transcurso de la interceptación de un dispositivo de carácter electrónico o de otra índole se obtengan de forma inesperada otras pruebas para las que no había autorización judicial expresa, es decir, para las que no se había previsto la medida.

Cuando esto ocurre, debemos preguntarnos: ¿Cuál es el tratamiento de estos hallazgos? ¿Se incorporan al procedimiento o hay que iniciar un nuevo proceso? ¿Ha habido una vulneración de derechos al no haber autorización expresa para tales hallazgos?

Es preciso señalar que, en base al principio de especialidad, no está permitido acordar una intervención para tratar de descubrir la comisión de un hecho delictivo de forma general, sin concreción alguna. Se exige por tanto, tal y como hemos expresado en reiteradas ocasiones, que el juez concrete en la resolución el ámbito objetivo y subjetivo de la medida en cuestión, es decir, el objeto de la intervención.

Por otra parte, hay que tener presente que en ningún lugar se establece que el sujeto encargado de la investigación pueda o deba ignorar la aparición de otros hechos delictivos en el transcurso de la investigación de otro delito, esté o no relacionado con el mismo³⁸.

Tal y como apunta BUENO DE MATA, procede hacer una distinción entre lo que serían pruebas derivadas de una prueba inicialmente ilícita, es decir, derivadas de una actuación sin autorización judicial, y los hallazgos causales que son por su parte la aparición de nuevos hechos delictivos no incluidos en la resolución judicial habilitante de la medida de intervención y que surgen a raíz de la intervención que se está llevando a cabo.

³⁷ Art. 579 bis 3 por remisión del art. 588 bis i) LECrim.

³⁸ Circular de la Fiscalía General del Estado 1/2013, *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, p. 37.

Así, ¿cómo determinar la extensión de la ilicitud de las pruebas derivadas de la principal para las que no existía previa autorización judicial?³⁹ En lo que se refiere a las escuchas telefónicas, cuando el juez tenga conocimiento del hallazgo causal de un hecho delictivo distinto al investigado tendrá que valorar si ese hecho está relacionado con el inicialmente investigado o si por el contrario constituye un delito completamente distinto y ajeno al mismo.

Por su parte, BAÑULS GÓMEZ estima que si el hallazgo está relacionado con el hecho que inicialmente se está investigando, procede la emisión de una orden judicial que amplíe el ámbito de la intervención continuando así con la investigación. En el caso de constituir un delito completamente distinto, el Juez tendrá que dictar una autorización judicial expresa que permita la continuación de la escucha e iniciar una nueva investigación ajena en relación con el hallazgo⁴⁰.

La LO 13/2015 establece que en el caso de los hallazgos causales corresponde al juez tomar la decisión de si se les debe otorgar o no valor probatorio. Con anterioridad a la promulgación de la ley indicada y en definitiva a la reforma de la LECrim, jurisprudencialmente se determinó la validez de los hallazgos causales y la continuidad en la investigación de un hecho delictivo nuevo con previa autorización judicial⁴¹.

En definitiva el tratamiento de los hallazgos causales tal y como hemos señalado, está íntimamente relacionado con el principio de especialidad y trae consigo la aparición de indicios de la comisión de un nuevo hecho delictivo para el que no estaba prevista la intervención recogida en la resolución judicial habilitante. Así, corresponde al juez la valoración de esta cuestión, es decir, será este el que decida si procede continuar con la investigación del mismo o no. Esta última ha sido la postura jurisprudencial adoptada por el TS y finalmente ha sido recogida en la LECrim, concretamente en los arts. 579 bis 3 por remisión del art. 588 bis i), según el cual, “el juez debe comprobar la diligencia de la actuación, evaluando el marco en que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal

³⁹ BUENO DE MATA, F., “Comentarios y reflexiones...”, op. cit., p. 4.

⁴⁰ BAÑULS GOMEZ, F., “Las intervenciones telefónicas a la luz de la jurisprudencia más reciente”, Portal Web Noticiasjurídicas.com, 2007. Disponible en: [webs/Las intervenciones telefónicas a la luz de la jurisprudencia más reciente · Noticias Jurídicas.htm](http://webs/Las%20intervenciones%20telef%C3%B3nicas%20a%20la%20luz%20de%20la%20jurisprudencia%20m%C3%A1s%20reciente%20-%20Noticias%20Jur%C3%ADdicas.htm)

⁴¹ Entre otras, STS 740/2012, de 10 de octubre.

declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce”.

3. EL DERECHO AL SECRETO DE LAS COMUNICACIONES

3.1. CONCEPTO.

El derecho al secreto de las comunicaciones se recoge en el art.18.3 CE, dentro de la Sección 1ª del Capítulo II del Título Primero de la Constitución, por lo que goza de las máximas garantías legales.

Se encuentra recogido en dicho precepto junto a otros derechos: honor, intimidad y propia imagen, inviolabilidad del domicilio y protección de datos personales. Podemos afirmar que en todos ellos el bien jurídico protegido es la intimidad personal, aunque en el caso del derecho al secreto de las comunicaciones la protección podríamos decir que va más allá, pues no solo se protegen las comunicaciones que sean de carácter personal o íntimo, sino que puede tratarse de comunicaciones de otra índole.

Se podría hablar, por tanto, de una cierta autonomía del derecho al secreto de las comunicaciones con respecto a los otros derechos recogidos en el citado art. 18 CE, tal y como afirma la STC 123/2002, de 20 de mayo, cuyo FJ5 señala: “[...] el fundamento del carácter autónomo y separado del reconocimiento de este derecho fundamental y de su específica protección constitucional reside en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación”.

En definitiva, el secreto de las comunicaciones pretende proteger la comunicación entre personas en la distancia, aproximándola a lo que sería una comunicación directa, y garantizando en todo caso la privacidad de la misma.

Si leemos la letra del art.18.3 CE⁴² concluimos que se trata de un enunciado abierto, es decir, de contenido puramente formal, pues a pesar de mencionar expresamente una concreta tipología de comunicaciones (postales, telegráficas o telefónicas), su protección se extiende a cualquier otro tipo, como puede ser el correo electrónico,

⁴² Art. 18.3 CE: “Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”.

mensajería instantánea, es decir tanto a los medios de comunicación existentes como a los venideros⁴³.

Hablamos de una protección especial basada en la vulnerabilidad del sujeto que emplea tales medios de comunicación cuando estos pueden verse afectados por una intromisión de un tercero (el prestador del servicio u otros). La clave para diferenciar el derecho al secreto de las comunicaciones y el derecho a la intimidad reside en el ámbito de protección material de los mismos pues en el primer caso se exige la intromisión mediante algún artificio técnico, mientras que en el segundo se trataría de una intervención directa. Así, señala RODRÍGUEZ LAINZ que “la sola comunicación entre dos personas, aun con la intervención de un tercero, como intérprete, colaborador, o simple emisario, para hacer llegar una noticia o documento a un tercero, no se haría merecedora de la protección formal del secreto de las comunicaciones”⁴⁴.

El derecho al secreto es independiente del contenido de la comunicación, puesto que debe respetarse aunque la información transmitida no se integre en el ámbito de la privacidad. Este derecho no es de carácter absoluto, pues en toda sociedad democrática existen determinados valores que pueden justificar con las debidas garantías su limitación, como la prevención del delito⁴⁵.

Se trata, por tanto, de una garantía relativa a la protección de las comunicaciones entre las personas, de forma que cualquier supuesto de interceptación de las mismas se considera excepcional, limitado, y sometido a requisitos, puesto que esa práctica implica una afeción a un derecho fundamental y sólo el respeto de tales garantías y requisitos permitirá que no constituya una vulneración⁴⁶.

La comunicación constituye el contenido del derecho, siendo innecesario que se plasme en palabras aunque sí que al menos se manifieste mediante el empleo de algún tipo de símbolo que permita la comunicación entre el emisor y receptor del mensaje.

⁴³ REBOLLO DELGADO, L., “El secreto de las comunicaciones: problemas actuales”, *Revista de Derecho Político*, 2000, pp. 351-382.

⁴⁴ RODRÍGUEZ LAINZ, J. L., “Sobre el ámbito objetivo de la protección constitucional del secreto de las comunicaciones en la STC 107/2012, de 21 de mayo”, *Diario La Ley*, 2012, p. 7.

⁴⁵ REYES LÓPEZ, J. I., “Las intervenciones de las comunicaciones en el derecho español. Alcance y valoración de la noticia anónima. Cooperación judicial internacional. Información de inteligencia”, *Boletín Científico ESMPU*, Brasilia, núm. 40, junio 2013, pp. 135-147.

⁴⁶ DÍAZ REVORIO, F. J., “El derecho fundamental al secreto de las comunicaciones”, *Revista de la Facultad de Derecho*, Pontificia Universidad Católica del Perú (PUCP), n° 59, 2007, p. 159. Disponible en: revistas.pucp.edu.pe/index.php/derechopucp/article/viewFile/3040/2887

En ocasiones el simple hecho de desvelar la identidad de los interlocutores o conocer la duración de la comunicación, se considerará una vulneración del derecho. Así lo ha manifestado el TC, declarando que “sea cual sea el ámbito objetivo del concepto de “comunicación”, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia “erga omnes”) ajenos a la comunicación misma. La presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado”⁴⁷.

El bien constitucionalmente protegido es la libertad de las comunicaciones, pues el derecho objeto de análisis exige el secreto de las comunicaciones estableciendo la antijuridicidad del conocimiento de las comunicaciones ajenas. Puede vulnerarse tanto si se lleva a cabo una interceptación en sentido estricto a través del uso de algún mecanismo que capte el soporte del mensaje, o por el simple conocimiento de lo comunicado, según establece nuestro Tribunal Constitucional⁴⁸.

3.2. MARCO JURÍDICO.

Se encuentra regulado en el art.18. 3 de nuestra Constitución tal y como precisé con anterioridad. A su vez, al tratarse de un derecho fundamental, el mismo se haya reconocido en la Declaración Universal de Derechos Humanos de 10 de diciembre de 1948⁴⁹, así como en el Pacto Internacional de Derechos Civiles y Políticos de 19 de diciembre de 1966⁵⁰, del que forma parte España.

También en el ámbito convencional, en el Convenio de Roma del 4 de noviembre de 1950, para la protección de los Derechos Humanos y de las Libertades Fundamentales⁵¹.

Por su parte, el artículo 7 de la Carta de los Derechos Fundamentales de la Unión

⁴⁷ STC 114/1984, de 29 de noviembre.

⁴⁸ STC 123/2002, de 20 de mayo.

⁴⁹ Art. 12: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

⁵⁰ Art. 17: “Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación”.

⁵¹ Art. 8: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”.

Europea, afirma que “...toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones”.

3.3. FINALIDAD.

Desde la perspectiva del Derecho Constitucional sería suficiente con que la finalidad, la decisión de adoptar una medida de interceptación de las comunicaciones, no fuese contraria a la propia Constitución, ni a los requisitos legalmente exigidos.

No obstante, el art. 8. 2 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales recoge de forma expresa los objetivos que puede perseguir dicha medida, constitutiva de una injerencia en el derecho al secreto de las comunicaciones, para considerarse admisible:

- la seguridad nacional,
- la seguridad pública,
- el bienestar económico del país,
- la defensa del orden y la prevención del delito,
- la protección de la salud o de la moral, o la protección de los derechos y
- las libertades de los demás.

De dichos objetivos debemos destacar el relativo a la persecución de los delitos, pues en la práctica la mayoría de las intervenciones en las comunicaciones que se llevan a cabo se realizan en el ámbito de los procesos penales, con el fin de investigar delitos. Así, es en la Ley de Enjuiciamiento Criminal donde se recogen los requisitos legales que deben concurrir para que dicha intervención goce de legitimidad⁵².

3.4. TITULARIDAD.

La cuestión relativa a la determinación de quiénes gozan de la protección de un derecho, trae consigo mayor importancia cuando se trata de un derecho fundamental.

En este caso, puesto que se trata de un derecho que protege la esfera privada, la titularidad corresponde a cualquier persona, sea cual sea su nacionalidad. Así, es titular de este derecho cualquier persona, ya sea física o jurídica, nacional o extranjera.

⁵² Arts. 579 y 588 bis LECrim.

A su vez, debemos apuntar la especial precaución que debe existir cuando se procede a la autorización de una intervención en las comunicaciones en determinados supuestos en los que el derecho al secreto de las comunicaciones concurre con el respeto de otro tipo de secretos como puede ser el secreto profesional o el secreto de la correspondencia profesional, por ejemplo el existente entre abogado y cliente, reconocidos por los órganos jurisdiccionales europeos⁵³.

Por otro lado, podemos cuestionarnos si se trata de un derecho que efectúa una protección con respecto a los poderes públicos en exclusiva o si por el contrario éste también puede ser vulnerado con la actuación de particulares. Con respecto a esta cuestión el Tribunal Constitucional ha manifestado la eficacia erga omnes del derecho al secreto de las comunicaciones⁵⁴. Las intromisiones llevadas a cabo por particulares deben atender a las previsiones de la L.O. 1/1982, de 5 de mayo, de protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en la que se contiene cuándo se entienden dichas intromisiones contrarias a derecho⁵⁵.

Sin embargo, el Tribunal Supremo por su parte, ha considerado que en el caso de intromisiones llevadas a cabo por particulares se entiende que la vulneración se produce con respecto al derecho a la intimidad, y no al derecho al secreto de las comunicaciones, lo cual se produce cuando es el poder público el que se inmiscuye en la esfera privada de un sujeto particular⁵⁶.

Y por último, en relación a esta cuestión, el Código Penal tipifica aquellos supuestos en los que la intervención ilegítima se lleva a cabo por parte de un funcionario público o agente, y se prevé la pena de inhabilitación, cuya extensión depende de la divulgación o no de los hechos interceptados⁵⁷.

⁵³ STEDH de 25 de marzo de 1998, caso Koop; (STJCE de 18 de mayo de 1982, A.M.S. v. Comisión).

⁵⁴ STC 114/1984 de 29 de noviembre de 1984.

⁵⁵ Arts. 7. 1 y 2 LO 1982: “el emplazamiento en cualquier lugar de aparatos de escucha [...] o de cualquier otro medio para grabar o reproducir la vida íntima de las personas” o “la utilización de aparatos de escucha [...] para el conocimiento de la vida íntima de las personas o de ...cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción”.

⁵⁶ STS de 14 de mayo de 2001.

⁵⁷ Art. 536 CP: “La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses”.

3.5. GARANTÍAS DEL DERECHO AL SECRETO DE LAS COMUNICACIONES.

Se trata de un derecho fundamental, contenido en la Sección 1ª del Capítulo II del Título Primero de nuestra Constitución, en consecuencia, forma parte del conjunto de derechos a los que nuestra norma superior concede un grado extra de protección y un plus de garantías que podemos resumir en las siguientes⁵⁸:

- a) El desarrollo del mismo debe ser efectuado mediante ley orgánica (artículos 53 y 81 CE).
- b) La normativa destinada a su regulación debe respetar su «contenido esencial» (artículo 53.1).
- c) Procedimiento sumario y de carácter preferente en los Tribunales ordinarios (artículo 53. 2).
- d) Puede ser objeto de recurso de amparo ante el Tribunal Constitucional (artículo 53. 2).
- e) En cuanto a su reforma debe ser efectuada conforme al procedimiento agravado (artículo 168 CE).
- f) Es apto para ser tutelado mediante el recurso y la cuestión de inconstitucionalidad (arts.53.1, 161.1ª y 163 CE) , así como por el defensor del pueblo (art. 54 CE).

3.6. REGULACIÓN DE LA INTERVENCIÓN: RESOLUCIÓN JUDICIAL HABILITANTE.

Partimos de la exigencia manifestada expresamente por el TC de que “por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal”⁵⁹.

A su vez, en lo que a nosotros nos compete, el art. 18.3 CE garantiza el secreto de las comunicaciones “salvo resolución judicial”, es decir, es *conditio sine qua non* que exista una autorización expresa por parte de la autoridad judicial para proceder a la

⁵⁸ DÍAZ REVORIO, F. J.,”El derecho ...op., cit., p. 180.

⁵⁹ STC 49/1999, de 5 de abril.

intervención de las comunicaciones. Con este hecho se plasma la idea, presente en el constitucionalismo contemporáneo, de la legitimación exclusiva del Poder Judicial para autorizar las intromisiones en los derechos fundamentales cuya titularidad corresponde a todos los ciudadanos⁶⁰.

Así, corresponde al juez analizar en cada caso concreto si se cumplen los requisitos para proceder a la interceptación de la comunicación y facilitar en consecuencia la investigación criminal.

A su vez, dicha resolución debe reunir una serie de requisitos, que con la nueva redacción de la LECrim⁶¹, en lo que se refiere a la interceptación en las comunicaciones, vienen recogidos de forma genérica en su art. 588 bis c) 3 y en el art. 579 LECrim.

Con anterioridad a la reciente reforma, tales requisitos fueron establecidos por vía jurisprudencial del TEDH, Tribunal Supremo y Tribunal Constitucional, y a modo general, podemos citar los siguientes:

- 1) Motivación de la resolución judicial.
- 2) Establecimiento de un plazo.
- 3) La intervención debe referirse a personas concretas y determinadas, y respecto de delitos también concretos.
- 4) Comunicación de la intervención a los afectados una vez finalizada.

En la actualidad, los requisitos que deben darse para que la ejecución de la medida sea óptima y no vulnere el derecho al secreto de las comunicaciones, se recogen en los artículos 579, con respecto a la interceptación de la *correspondencia escrita o telegráfica* y 588 bis c) 3 en relación a *interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*.

⁶⁰ DIAZ REVORIO, F. J., “El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español”, *Derechos Humanos México*, 2006, pp. 139-140.

⁶¹ Ley Orgánica 13/2015, de 5 de octubre. *BOE* núm. 239, de 6 de octubre de 2015, pp. 90192 a 90219.

Así, en el art. 588 bis c) 3 se recogen las cuestiones que deberá precisar el juez en su resolución, que textualmente son:

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

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

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

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

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”.

Podemos concluir que toda interceptación que no cumpla con los requisitos previamente señalados, implicaría una vulneración del derecho al secreto de las comunicaciones.

La consecuencia procesal de esa actuación de carácter ilegítimo, sería la nulidad de cualquier prueba que hubiera podido obtenerse a consecuencia de dicha intervención ilícita⁶².

Esta consecuencia deriva, entre otras cosas, de la posición de preferencia de la que gozan los derechos fundamentales y de su inviolabilidad tal y como ha manifestado el propio Tribunal Constitucional en STC 49/1999.

El derecho al secreto de las comunicaciones, probablemente será objeto de un gran desarrollo jurídico principalmente a consecuencia del gran avance que está llevándose a

⁶² Esta consecuencia ha sido reiterada por la jurisprudencia en múltiples ocasiones. Entre otras, la STC 299/2000, del 11 de diciembre y STC 184/2003, del 23 de octubre.

cabo en el ámbito tecnológico, desarrollando numerosas novedades en cuanto a los medios de comunicación, lo cual era impensable hace unos años. Y así lo ha afirmado el propio Tribunal Constitucional en la STC 132/2002, de 20 de mayo, al señalar que “en una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo”.

3.7. DERECHO AL SECRETO DE LAS COMUNICACIONES EN EL ÁMBITO DE LAS ESCUCHAS TELEFÓNICAS Y TELEMÁTICAS.

Debemos partir de la base de que no solo se protege constitucionalmente (art.18 CE) el contenido de la comunicación, sino también otros aspectos de la misma, como pueden ser el listado de llamadas contenido en el terminal u otros datos externos como la identidad de los interlocutores.

Destaca en este sentido la STEDH de 2 de agosto de 1984, Malone contra Reino Unido, que reconoce la violación del art. 8 CEDH al acceder a un listado de números telefónicos marcados y no al contenido de la comunicación en sí.

Así, no todo el contenido está bajo la protección del art. 18 CE; es preciso por tanto, llevar a cabo un análisis previo para determinar su funcionalidad y encajarlo cuando proceda bajo el marco protector del derecho a la intimidad (art. 18.1), derecho a la inviolabilidad de las comunicaciones (art. 18.3) o el derecho a la protección de datos.

El Tribunal Constitucional determinó que el concepto de secreto de comunicación no solo cubre su contenido, sino que alcanza la identidad subjetiva de los interlocutores⁶³.

Se puede afirmar y apuntar como dato que nuestro ordenamiento jurídico es de los más estrictos en este campo de intervenciones telefónicas en lo que se refiere al derecho comparado, puesto que se exige para su puesta en práctica tanto la autorización judicial como la motivación de la misma⁶⁴.

En lo que respecta a la interceptación del listado de llamadas del terminal objeto de investigación, jurisprudencialmente se determinó que sí entra dentro del contenido de la

⁶³ STC 114/1984, de 29 de noviembre.

⁶⁴ Circular de la Fiscalía General del Estado 1/2013 *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, p. 15.

interceptación telefónica y que en consecuencia por orden judicial se puede efectuar su reclamación⁶⁵.

Es obvio que tiene mayor peso grabar una conversación, que identificar llamadas y números telefónicos, de modo que la intromisión en el primer caso es claramente superior. Y así lo ha manifestado el TC, al señalar que “...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”⁶⁶.

Podemos concluir por tanto que jurisprudencialmente se ha determinado que la relación de llamadas emitidas o recibidas por un terminal telefónico es materia que afecta al derecho que garantiza el art. 18.3 CE, siendo necesario a tales efectos, la autorización judicial correspondiente habilitadora de la intervención en defecto de consentimiento de los sujetos comunicantes. Dicha autorización resultará necesaria a su vez para acceder al registro de llamadas entrantes y salientes grabadas en un teléfono móvil⁶⁷.

En lo que respecta al acceso a la agenda de contactos del móvil, jurisprudencialmente se ha determinado que la simple utilización del contenido de un terminal con el objetivo de obtener los números de otros sujetos no resulta ilícito, y por tanto no constituye una vulneración del derecho al secreto de las comunicaciones. No obstante, sí que implicaría un intromisión en el derecho a la intimidad de la persona en cuestión⁶⁸.

Debemos precisar que en el caso del derecho a la intimidad, no es precisa una autorización judicial previa como ocurre en el caso del derecho al secreto de las comunicaciones, y en consecuencia se ha admitido, que de forma excepcional “la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad”⁶⁹.

⁶⁵ STC 123/2002, de 20 de mayo.

⁶⁶ STC 56/2003, de 24 de marzo.

⁶⁷ SSTS 142/2002, de 2 de julio; 707/2009 de 22 de junio y 230/2007, de 5 de noviembre; STEDH de 3 de abril de 2007, caso Copland contra Reino Unido).

⁶⁸ STC 70/2002, de 3 de abril.

⁶⁹ Circular de la Fiscalía General del Estado 1/2013 *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, p. 28.

Es preciso, a su vez, advertir sobre la diferenciación existente entre lo que sería el acceso a la agenda de contactos de un terminal y el acceso al listado de llamadas del mismo. Así, en el primero no se obtiene ningún dato acerca de la comunicación llevada a cabo a través del terminal, mientras que con el listado de llamadas se obtiene información relativa a las comunicaciones llevadas a cabo por el titular de dicho teléfono y en consecuencia implica una injerencia del derecho al secreto de las comunicaciones (art.18.3 CE).

Lo determinante por tanto para la delimitación del contenido de los derechos fundamentales, concretamente el derecho a la intimidad y el derecho al secreto de las comunicaciones, es el carácter de la información a la que se accede⁷⁰.

¿Qué ocurre cuando el contenido de la comunicación es revelado por uno de los intervinientes?

En tal caso no se produce una vulneración del derecho al secreto de las comunicaciones sino del derecho a la intimidad. En consecuencia, tal información puede emplearse como prueba, aun careciendo de autorización judicial expresa. Solo se entiende vulnerado el derecho al secreto de las comunicaciones cuando la conversación es grabada por un tercero ajeno a la comunicación.

Un ejemplo de lo anterior lo encontramos en la STC 56/2003, de 24 de marzo de 2003, en la que el TC manifiesta lo siguiente “...en el presente caso, no existe vulneración del derecho al secreto de las comunicaciones. Es, precisamente, uno de los interlocutores en la comunicación telefónica (el denunciante del chantaje al que se encontraba sometido) quien autorizó expresamente a la Guardia Civil a que registrara sus conversaciones para poder determinar así el número desde el que le llamaban, al no contar con aparato técnico para ello”.

En definitiva, el deber del secreto no recae sobre los comunicantes, pues la garantía del secreto de las comunicaciones solo procede cuando la intromisión, la interceptación de la comunicación es llevada a cabo por una tercera persona, ajena al proceso de comunicación⁷¹.

⁷⁰ STS 142/2002, de 2 de julio.

⁷¹ Circular de la Fiscalía General del Estado 1/2013 *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas*, p. 23. Tal y como declaró el TC en STC 114/1984, de 29 de noviembre “...sobre los comunicantes no pesa el deber de secreto”.

No obstante, la posibilidad de que los agentes de Policía procedan a intervenir una comunicación con el consentimiento de uno de los comunicantes se trata de algo excepcional, pues se requiere de autorización judicial expresa para proceder a la ejecución de la medida.

Otra cuestión que merece entrar a valorar es la relativa a la posible afección de los derechos del comunicante ajeno a la investigación penal, es decir, aquel que participa en la comunicación interceptada pero que por su parte no es objeto de investigación. Debemos partir del hecho de que la propia naturaleza de la intervención trae consigo que se vean afectados no solo el titular de la línea interceptada sino también los terceros que con el mismo se comunican⁷².

Así, jurisprudencialmente se ha determinado que no resulta ilegítima la intervención de las conversaciones de las personas con las que se comunica la persona objeto de investigación puesto que las mismas pueden guardar relación con el delito investigado, y corresponde al juez identificar las conversaciones relevantes⁷³.

¿Qué ocurre cuando el terminal es usado por persona distinta al titular o usuario?

En estos casos, la intervención sigue siendo legítima en tanto en cuanto la autorización judicial cubre las comunicaciones llevadas a cabo mediante el terminal interceptado aunque este sea utilizado por otras personas distintas a las recogidas en la resolución habilitante. Por otro lado, si es el propio sujeto investigado el que utiliza otro teléfono del que no es titular, sería legítima la intervención si la autorización judicial emitida esté justificada por el hecho del uso⁷⁴.

En lo que respecta al supuesto en el que un mismo terminal sobre el que recae la medida de intervención es utilizado por varias personas, no se exige una nueva autorización judicial puesto que sería ilógico. Lo importante para que la intervención sea correcta es que conste la identidad del titular del móvil junto con el cumplimiento del resto de requisitos⁷⁵.

El acceso al contenido de los mensajes de texto de un teléfono móvil también está restringido, y es que de forma tajante se puede afirmar que los mensajes enviados a un sujeto y no leídos aún por éste están protegidos por el derecho al secreto de las

⁷² STS 1001/2005, de 19 de julio.

⁷³ STS 712/2012, de 26 de septiembre.

⁷⁴ STS nº84/2010, de 18 de febrero.

⁷⁵ STS 905/2003, de 18 de junio.

comunicaciones al constituir “auténticas y genuinas comunicaciones personales, similares a las que se remiten y reciben por correo o telégrafo, pero cuyo vehículo de transmisión en este supuesto es el teléfono, por lo que, de hecho, se trata de una especie de comunicación de una misiva personal efectuada vía telefónica, que no se "oye" por su destinatario, sino que se "lee" al aparecer en la pantalla del aparato y mediante esa lectura conoce el contenido del mensaje o de la misiva, por lo que resulta incuestionable que esta clase de comunicaciones se encuentran tuteladas por el secreto que establece el art.18.3 CE”⁷⁶.

4. EVOLUCIÓN DEL CONCEPTO DE COMUNICACIÓN Y NECESIDAD DE ADAPTACIÓN LEGAL

4.1. CONCEPTO DE COMUNICACIÓN.

¿Qué es realmente lo que define el proceso comunicativo?

Es preciso hacer un breve análisis acerca de las cuestiones que realmente se acogen dentro del concepto de comunicación y en consecuencia quedan dentro del ámbito de protección constitucional.

Como sabemos, en la actualidad se ha producido una notoria evolución en el campo de las comunicaciones, lo que ha traído consigo una necesidad de adaptación por parte del Derecho, estableciendo una normativa destinada a la regulación de esas nuevas formas de comunicación que analizaremos con posterioridad. Tal y como indicamos en puntos anteriores, recientemente se ha llevado cabo la esperada reforma de la Ley de Enjuiciamiento Criminal en la que se han añadido preceptos dedicados a la intervención en las comunicaciones a través de distintos instrumentos que posteriormente analizaremos. El concepto de comunicación ha evolucionado con el transcurso de los años y por ello debe matizarse a qué hace referencia el término comunicación en la actualidad.

Para ello podemos partir del art.6 4 c) del RD 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios (RLGT), en el que se define la comunicación electrónica como “cualquier información

⁷⁶ STS 1235/2002, de 27 de junio.

intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público”⁷⁷.

Por otro lado, si nos referimos a la comunicación en el ámbito de la correspondencia postal, el art. 3.3 de la Ley 43/2010, de 30 de diciembre, del servicio de postal universal, de los derechos de los usuarios y del mercado postal (LSPU) define el envío de correspondencia como “...la comunicación materializada en forma escrita sobre un soporte físico de cualquier naturaleza, que se transportará y entregará en la dirección indicada por el remitente sobre el propio envío o sobre su envoltorio”.

RODRÍGUEZ LAINZ por su parte, introduce un concepto de comunicación en el que abstrae ese carácter electrónico o físico del objeto de la comunicación, para así abarcar todas las posibilidades que hoy en día precisan las nuevas tecnologías. Así, entiende que comunicación es “la transmisión, compartición o intercambio de información entre dos o más sujetos determinados o determinables, dirigida a través de determinados canales de comunicaciones que son gestionados por terceras personas o entidades, en quienes se confía no solo su buen fin, sino también la confidencialidad en su gestión frente al conocimiento ajeno”⁷⁸.

De dicha definición extrae tres componentes: la transferencia de información; la participación entre intercomunicantes y la intermediación de un tercero prestador del servicio sobre el que pesa el deber de confidencialidad.

En consecuencia, en lo que respecta a la transferencia de información, sería el contenido de la comunicación, el objeto de protección constitucional. No obstante es preciso resaltar como se trata de un objeto mediato, puesto que lo principal es el instrumento, el derecho recogido en el art. 18.3 CE mediante el cual se ejercita el poder de excluir aquello que comunicamos de la intromisión de terceros. La protección ofrecida por la Constitución es independiente de la trascendencia de la información transmitida. No resulta importante la información que se transmite si partimos de la concepción formal del derecho al secreto de las comunicaciones, pues su protección recae también sobre los elementos externos de la comunicación como los datos de tráfico, los cuales

⁷⁷ Es exacta a la contenida en el art. 2 d) Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

⁷⁸ RODRÍGUEZ LAINZ, J. L., “En torno al concepto de comunicación protegida por el art. 18.3 de la Constitución”, *Diario La Ley*, 5 Sep. 2013, p. 2.

pueden revelar la identidad de los interlocutores, la duración de la comunicación, la propia existencia de la comunicación etc.

La problemática surge en el ámbito de las comunicaciones electrónicas cuando hay que distinguir entre metadatos y datos de tráfico. El metadato puede definirse como “...toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto, que tiene la finalidad de facilitar su recuperación, autenticación, evaluación, preservación y/o interoperabilidad”⁷⁹.

Conforme al art. 588 ter b los datos de tráfico son “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”. Así, pese a que aparentemente el metadato puede entenderse que se trata de contenido propio de la comunicación, lo cierto es que no es así, pues son los datos de tráfico los que tienen por finalidad facilitar el tránsito de la comunicación y contienen información incluida en el concepto de comunicación antes descrito, pues permiten identificar a los intervinientes en un proceso de comunicación, así como el lugar, tiempo y los aparatos empleados⁸⁰.

Si nos referimos a la participación de un tercero prestador del servicio de comunicaciones y su deber de confidencialidad, hay que decir que el surgimiento del derecho a la inviolabilidad de la correspondencia privada surgió a consecuencia de la necesidad de que determinadas comunicaciones fueran transmitidas por medio de un tercero. Esto trajo consigo el deber de confidencialidad, por parte del prestador del servicio puesto que su participación en ocasiones resulta inevitable, así es preciso que este asuma el compromiso de no desvelar el contenido de la comunicación que debe remitir.

En definitiva, no se trata solo de evitar la intromisión por parte de terceros, sino también el acceso al contenido de la comunicación por parte del prestador del servicio de

⁷⁹ MÉNDEZ E. y SENSO, J. A, *Unidad de Autoformación*, SEDIC, 2004. Disponible en: <http://www.sedic.es/autoformacion/metadatos/tema1.htm>

⁸⁰ RÍOS PINTADO, J. F., “La reforma procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la ley de enjuiciamiento criminal)”, *Jornadas de especialistas en criminalidad informática*, Centro de Estudios Jurídicos, CEJ, 2016, pp. 4 y ss. Disponible en: http://www.cejjusticia.es/cej_dode/flash/ebook/assets/img/cejponencia1462865552415/cejponencia1462865552415.pdf

comunicación, aunque hay supuestos en los que dicho acceso será una consecuencia necesaria de la propia naturaleza del servicio que se demanda.

Por lo que respecta a los interlocutores de la comunicación, debemos hacer una alusión a la gran evolución del mundo de las tecnologías de la información, sobre todo el surgimiento de internet, y es que antiguamente lo natural es que hubiera al menos un emisor y un receptor en el transcurso de una actividad comunicativa, sin embargo, con la aparición de las comunicaciones electrónicas, pasamos a hablar de intercomunicantes.

En relación a las nuevas redes de comunicación, es necesario puntualizar que solo se considera objeto de protección aquella información, comunicación que se manifieste en un círculo cerrado de usuarios, es decir, que no sean de carácter público, pues quién no muestra preocupación en restringir el acceso a la información que transmite no puede pretender exigir posteriormente el respaldo constitucional del art. 18 CE. No se requiere autorización para acceder a aquello que es público⁸¹.

4.2. NECESIDAD DE REFORMA DE LA LEY DE ENJUICIAMIENTO CRIMINAL.

Observamos cómo el mundo de las comunicaciones ha sufrido una gran evolución y se han dado multitud de supuestos en los que se ha puesto de manifiesto la escasez de cobertura legal con respecto a la intervención en las comunicaciones. En relación a esta cuestión tenemos que citar la STC 145/2014, de 22 de septiembre, que constituyó un toque de atención sobre la necesidad de proceder a una reforma de la legislación preexistente, puesto que se estaba llevando a cabo una actividad jurisprudencial contraria a la CE, al aplicar el art. 579 LECrim mediante el método de la analogía a muchos casos que realmente no podían enmarcarse en el contexto de dicho precepto.

La citada sentencia resolvía un recurso de amparo 6157-2010 (y CJ 140049/2014) relativo a la vulneración del derecho al secreto de las comunicaciones por proceder a la instalación de artificios técnicos de escucha, grabación de sonido e imagen en los calabozos de la Comisaría de Policía ocupados por los detenidos. La intervención fue previamente validada por el TS⁸² pues entendió conforme al principio de proporcionalidad, que si resultaba lícita la intervención de una persona "libre" cómo no iba a estar justificada la intervención en las comunicaciones llevadas a cabo por una

⁸¹RODRÍGUEZ LAINZ, J. L., "En torno al concepto...", op., cit., p. 3.

⁸² STS 513/2010, de 2 de junio.

persona detenida, imputada por un delito grave como un asesinato. El recurso de amparo, se fundamentaba principalmente en la carencia de previsión legal que hiciera de soporte a la citada diligencia de investigación, pues como sabemos en ese momento sólo existía el art. 579 LECrim, precepto en el que se fundamentaron las resoluciones anteriores⁸³. El recurrente alegaba la ilicitud de la interpretación extensiva de dicho precepto llevada a cabo por el Tribunal Supremo en una materia tan sensible como esta. El Tribunal Supremo entendió que la ausencia legal podría ser suplida por la jurisprudencia del Tribunal Constitucional, así como por la Sala Segunda del Tribunal Supremo y las previsiones de la Ley General Penitenciaria y el Reglamento Penitenciario.

El Tribunal Constitucional por su parte, sentenció que al tratarse de una injerencia estatal en materia de derechos fundamentales deben concurrir una serie de garantías como es la existencia de una habilitación legal expresa que contenga los límites de la actuación por parte del estado, y que en consecuencia contribuya a una mayor seguridad jurídica del individuo. Conforme a esto, el Tribunal Constitucional determinó que ninguna de las normas alegadas en las resoluciones judiciales impugnadas contenían la habilitación de la intervención de las comunicaciones verbales directas en las dependencias policiales. No se debe entender como un rechazo a la posibilidad de que sea el propio Tribunal Supremo el que se encargue de contrarrestar los déficits existentes en la regulación actual, sino que en este caso, como en muchos otros, la norma en la que se fundamenta la medida no se corresponde en absoluto con la misma, más bien no hay un precepto que regule esta situación, hay una ausencia total de regulación, pues el citado artículo se refiere de forma exclusiva a las intervenciones telefónicas, no alude por tanto a las comunicaciones llevadas a cabo en dependencias policiales⁸⁴.

Este pronunciamiento pone fin a la doctrina de la Sala Segunda sobre las escuchas ambientales puesto que no estamos ante la enésima insuficiencia de la LECrim, sino ante la ausencia de previsión legal al respecto⁸⁵.

⁸³ Art. 579.2 LECrim, según el cual “asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa”.

⁸⁴ GONZÁLEZ MONJE, A., “Intervención de comunicaciones en dependencias policiales”, *Ars Iuris Salmanticensis*, 2015, pp. 358-360.

⁸⁵ ARAGONÉS SEIJO, S., y FERNÁNDEZ SERRA L., “La ausencia de previsión legal para las escuchas en vehículos”, *Diario La Ley*, 26 de Junio de 2015, p. 3.

¿Qué podemos extraer de lo anterior? Pues que una cosa es suplir deficiencias legales y otra muy distinta es que la doctrina jurisprudencial pretenda proceder a la regulación de situaciones en las que se produce una intromisión estatal en el derecho al secreto de las comunicaciones y sobre las que no existe previsión legal de ningún tipo. En este caso en concreto, la conclusión es que las grabaciones en dependencias policiales resultan contrarias al art. 18.3 CE al carecer de previsión legal que justifique dicha intervención.

4.3. NUEVAS DILIGENCIAS DE INVESTIGACIÓN INCORPORADAS EN LA LECRIM.

A raíz de pronunciamientos como el descrito anteriormente, además de otros factores, el legislador procede a modificar la Ley de Enjuiciamiento Criminal, incluyendo en la misma una serie de diligencias de intervención en las comunicaciones inexistentes previamente, tal y como indicamos en apartados previos. Éstas son las siguientes:

4.3.1. Utilización de dispositivos técnicos de seguimiento y localización.

Los dispositivos técnicos de seguimiento y localización permiten situar a una persona en el espacio pero no reproducen la imagen y el sonido del lugar sino que afectan por al conocimiento de la ubicación espacial de la persona objeto de investigación.

Hasta hace unos meses no existía precepto alguno destinado a la regulación de la vigilancia a través de dispositivos de seguimiento y localización, adheridos a objetos utilizados por la persona sometida a la investigación. La única norma que podía contener en cierto modo la situación descrita era el art. 263 bis, apartado 2 LECrim, relativa a la entrega controlada, no obstante no aportaba cobertura total a la misma⁸⁶.

La regulación de la intervención mediante este tipo de dispositivos, ha sido muy importante, puesto que su uso es habitual al facilitar de forma notable las tareas de seguimiento que son llevadas a cabo por la Policía Judicial sobre las personas investigadas.

Esta medida de “tecnovigilancia” sustituye por tanto las labores de seguimiento que anteriormente tenían que desempeñar funcionarios de policía consistentes en la

⁸⁶ RODRÍGUEZ LAINZ, J. L., “Los dispositivos electrónicos de posicionamiento global (GPS) en el Proceso Penal”, *Diario La Ley*, 17 Oct. 2012, p. 14.

realización de vigilancias físicas personalizadas y presenciales que requerían entre otras cosas grandes cantidades de efectivos policiales⁸⁷.

La incorporación de estos medios tecnológicos ha supuesto a su vez para el Estado una reducción de costes pero además la garantía de una mayor seguridad y precisión en la investigación⁸⁸.

El objetivo de la medida es al fin y al cabo la realización de un seguimiento continuo de los movimientos de una persona u objeto durante determinados espacios de tiempo y del mismo modo averiguar los concretos espacios de tiempo en los que permanece en una concreta ubicación, estableciendo en ambos casos su localización. La puesta en marcha de esta intervención, por tanto, trae consigo el poder controlar personalmente los movimientos de una persona sospechosa de la comisión de un delito e incluso obtener la localización del lugar donde se encuentra el centro de operaciones, dejando a un lado el posible riesgo personal que pudiera sufrir el sujeto investigador⁸⁹.

Para el desempeño de la misma se pueden emplear dispositivos físicos como puede ser el GPS o bien virtuales instalando por ejemplo un software en un teléfono móvil que sirva para transmitir de forma automática información sobre la localización del investigado.

Esta medida se incorpora en la Ley de Enjuiciamiento Criminal con la creación del Capítulo VII en el Título III del Libro II que recoge el art. 588 quinquies.

Al igual que indicamos en relación con la intervención en escuchas telefónicas, en el Capítulo IV se recogen una serie de disposiciones comunes aplicables a esta diligencia de investigación, concretamente nos referimos al art. 588 bis.

Los arts. 588 quinquies b) y quinquies c) dedican su redacción de forma exclusiva a regular esta medida de seguimiento y localización. Conforme a los mismos, se exige la autorización expresa del juez competente para la puesta en marcha de esta medida y la misma deberá basarse en los principios rectores descritos en su momento y recogidos en el art. 588 bis a) LECrim.

⁸⁷ VELASCO NÚÑEZ, E., “Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica”, *Diario La Ley*, 4 Nov. 2013, p. 18.

⁸⁸ Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, pp. 106 y ss.

⁸⁹ RODRÍGUEZ LAINZ, J. L., “Los dispositivos electrónicos...”, op., cit., p. 10.

El juez deberá precisar el ámbito objetivo de la medida especificando el instrumento tecnológico que va a ser empleado por los agentes facultativos. A su vez, al igual que ocurría en el caso de las intervenciones telefónicas, se exige la colaboración por parte de otros sujetos tales como prestadores de servicios de comunicaciones, agentes o terceras personas con el fin de facilitar el desarrollo de la diligencia, pesando sobre ellos la obligación de guardar secreto para evitar incurrir en un delito de desobediencia.

Asimismo se prevé en el art. 588 quinquies b) 4 LECrim, la posibilidad de anticipación policial cuando se trate de situaciones en las que demorar el inicio de la medida por el sometimiento a la previa autorización judicial podría traer consigo la frustración de la investigación. Así, en tal situación, la Policía Judicial podrá actuar de forma inmediata aunque deberá informar de tales actuaciones a la autoridad judicial en un plazo máximo de veinticuatro horas. El juez por su parte podrá proceder a la ratificación de dicha actuación o por el contrario desestimarla⁹⁰.

En cuanto a la duración, se fija un plazo máximo de tres meses a contar tras la emisión de la autorización por parte de la autoridad judicial, siendo posible una prorrogación del mismo hasta un máximo de dieciocho meses y siempre y cuando sea justificado. Al igual que ocurría con la información recogida tras las interceptaciones telefónicas, se exige la entrega de la misma al juez por parte de la Policía Judicial una vez finalizada la investigación, y con anterioridad si este lo solicita.

Frente a la situación anterior a la reforma, observamos cómo se exige la conservación de los datos generados por el sistema de tecnovigilancia, los cuales podrán ser así sometidos a un control efectivo por la autoridad judicial, y facilitar a las partes un examen con garantías de contradicción de la propia fuente de información. No se especifica nada sobre los requisitos a cumplir de cara a la conservación de tales datos y las garantías con respecto a la salvaguardia de la autenticidad de la información obtenida. Sin embargo, la norma se preocupa de que la unidad policial actuante custodie debidamente la información obtenida con el fin de evitar su uso indebido⁹¹.

⁹⁰ RODRÍGUEZ LAINZ, J.L., "Las nuevas...", op., cit., p. 9.

⁹¹ Artículo 588 quinquies c.3 LECrim.

4.3.2. Captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos.

Con anterioridad a la reforma, la utilización de cámaras ocultas como medio de investigación criminal no estaba prevista legalmente⁹². Sin embargo, su uso no estaba completamente vetado pues se permitía siempre y cuando no fuese contrario a los límites y principios establecidos en la Constitución. Un ejemplo de lo anterior lo encontramos en la STC 10 de julio de 2000 en la que el Tribunal Constitucional consideró admisible la captación de imágenes en una empresa a través de un circuito cerrado de televisión con el fin de probar que una de las empleadas sustraía dinero de la caja registradora de su lugar de trabajo⁹³.

La LO 13/2015 de reforma de la Ley de Enjuiciamiento Criminal introduce el art. 588 quinquies a) destinado específicamente a la regulación de esta diligencia de investigación.

De dicha regulación destaca la ausencia de una previa autorización judicial para la puesta en marcha de la medida, pues dicha intervención en lo que se refiere a espacios públicos ha sido en cierto modo considerada como algo ajeno a la protección de privacidad⁹⁴.

Con la regulación de esta medida y su sometimiento a límites, el legislador combate las controversias que surgían con anterioridad en relación al empleo de la misma. El art. 588 quinquies a) LECrim, autoriza la grabación de imágenes de personas objeto de una investigación situadas en un espacio de carácter público.

En lo que se refiere al objeto de la intervención, se trata de facilitar con la misma la identificación del investigado, localizar instrumentos del delito así como obtener datos importantes de cara al esclarecimiento de los hechos acontecidos.

RODRIGUEZ LAINZ por su parte, pone de manifiesto el cuestionamiento de la ausencia de autorización judicial en aquellos supuestos en los que los medios técnicos empleados permiten una visión más allá de cualquier margen de previsibilidad, expectativa razonable de privacidad del investigado, con independencia de encontrarse en un lugar público. El magistrado manifiesta que “*en aquellos parajes públicos en los*

⁹² STS 474/2012 de 6 de junio

⁹³ VELASCO NÚÑEZ, E., “Investigación procesal...”, op., cit., p. 16.

⁹⁴ Así lo manifiestan tanto el TEDH como el TC, en las STEDH de 28 de enero de 2003 (caso Peck v. Reino Unido; asunto 44647/98) y la STC 12/2012, de 30 de enero respectivamente.

*que el sujeto pudiera sentirse amparado por una expectativa razonable de estar completamente fuera del alcance de visión de terceras personas, podría cuestionarse seriamente la innecesariedad del respaldo judicial a este tipo de medidas de investigación*⁹⁵.

Por otro lado, el legislador se preocupa de reducir conforme a los principios de necesidad y proporcionalidad de la intervención, la posible afectación de la misma sobre terceras personas, o prevenir, la posible involucración de dichas personas con el hecho delictivo⁹⁶.

En lo que respecta a la grabación de comunicaciones orales, tal y como indiqué en apartados anteriores, el Tribunal Constitucional manifestó la ausencia de regulación legal con respecto a dicha intervención en el supuesto de grabación de comunicaciones orales en dependencias policiales⁹⁷. La jurisprudencia constitucional ha enumerado de forma reiterada los requisitos para proceder a la restricción de cualquier derecho fundamental, y son los ya descritos principios de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad de la medida⁹⁸.

En la nueva regulación se concretan de forma específica los requisitos relativos al contenido de la solicitud policial o del Ministerio Fiscal, así como la resolución judicial habilitante de la medida, la prórroga, el secreto automático y la necesidad de pieza separada y los hallazgos causales.

Anteriormente, como hemos podido comprobar, los órganos judiciales han tenido que juzgar conforme al único precepto existente en cuanto a intervención en comunicaciones, el artículo 579 LECrim, y ello ha sido objeto de crítica puesto como ponen de manifiesto ARAGONÉS SEIJO y FERNÁNDEZ SIERRA “Los Tribunales no están llamados a crear milagros del parco art. 579 LECrim., es al legislador al que corresponde delimitar cada medio de investigación penal”⁹⁹.

⁹⁵ RODRÍGUEZ LAINZ, J. L., “Las nuevas...”, op., cit., p. 6.

⁹⁶ Artículo 588 quinquies a) 2 LECrim: “La medida podrá ser llevada a cabo aun cuando afecte a personas diferentes del investigado, siempre que de otro modo se reduzca de forma relevante la utilidad de la vigilancia o existan indicios fundados de la relación de dichas personas con el investigado y los hechos objeto de la investigación”.

⁹⁷ STC 145/2014, de 22 de septiembre de 2014.

⁹⁸ SSTC 89/2006, de 27 de marzo y 173/2011, de 7 de noviembre.

⁹⁹ ARAGONÉS SEIJO, S., y FERNÁNDEZ SERRA L., “La ausencia de..., op., cit., p. 5.

En el art. 588 quater a) se establece la posibilidad de emplear y colocar dispositivos electrónicos aptos para proceder a la grabación de las comunicaciones orales directas llevadas a cabo por el sujeto investigado, ya sea en espacios públicos o privados.

En este último supuesto, se especifica que para proceder a la entrada de ese espacio privado, como puede ser el domicilio, deberá motivarse en la resolución habilitante de la medida.

Asimismo, una de las novedades a destacar de la reforma de la LECrim, es que no solo se permite la captación de las conversaciones que mantenga el investigado en lugares cerrados sino que esta se podrá complementar con “la obtención de imágenes cuando expresamente lo autorice la resolución que la acuerde”.

Para proceder a la autorización de la puesta en marcha de la medida, el juez deberá comprobar que los hechos objetos de investigación constituyen alguno de los delitos previstos legalmente, concretamente en el art. 588 quater b) 2 LECrim: “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”.

En el citado precepto se exige, a su vez, el cumplimiento de los principios de proporcionalidad y necesidad de la medida, poniendo de manifiesto que para proceder a la puesta en marcha de la medida el juez deberá asegurarse de que la misma traerá consigo la obtención de datos relevantes para el esclarecimiento de los hechos e identificación del autor de los mismos.

En cuanto al contenido de la resolución judicial, se establece que en la misma se deberá especificar el lugar concreto y momentos en los que el sujeto investigado va a ser sometido a la medida¹⁰⁰.

La Policía Judicial encargada de la ejecución de la medida deberá adjuntar a la autoridad judicial competente un informe en el que se especifique qué agentes han participado y por otro lado deberá presentar las grabaciones e imágenes en un soporte físico así como una transcripción de las conversaciones más relevantes¹⁰¹.

¹⁰⁰ Art. 588 quater c) LECrim.

¹⁰¹ Art. 588 quater d) LECrim.

Cuando llega a su fin la ejecución de la medida, para proceder a posteriores grabaciones es precisa una nueva autorización judicial¹⁰².

4.3.3. Registro de dispositivos informáticos de almacenamiento masivo.

Se trata de una medida consistente en el acceso a la información albergada en ordenadores, *pens drives*, móviles, discos duros y el resto de dispositivos de almacenamiento masivo.

Su regulación la encontramos en el nuevo capítulo VIII del Título Octavo de la LECrim, y en la misma destaca la exigencia de necesidad de autorización judicial para proceder a la ejecución de la medida. Lo anterior se justifica tal y como señala la exposición de motivos de la LO 13/2015, en el sentido de que la reforma “descarta cualquier duda acerca de que esos instrumentos de comunicación y, en su caso, almacenamiento de información son algo más que simples piezas de convicción. De ahí la exigente regulación respecto del acceso a su contenido”¹⁰³.

Tal y como establecen los artículos 588 sexies a) y b) LECrim, la autorización judicial será condición ineludible en aquellos supuestos en los que se proceda a la interceptación de tales elementos en el transcurso de un registro domiciliario así como en los casos en los que se incauten fuera del domicilio del sujeto investigado.

Se exige por tanto una autorización judicial independiente a la autorización emitida para proceder al registro domiciliario para el caso de pretender el acceso al contenido de tales dispositivos incautados.

Conforme al art. 588 sexies c) LECrim, la autorización judicial debe a su vez especificar si se van a efectuar copias de los datos informáticos analizados en el registro, pues dicho registro debe realizarse en un principio sin la incautación de los dispositivos, es decir sobre una copia del mismo, salvo que constituya objeto del delito o se den razones que justifiquen dicha sustracción¹⁰⁴.

Así, la resolución judicial habilitadora de la medida deberá fijar el ámbito objetivo de la misma, es decir los términos en los que se va a proceder al registro y su alcance, así

¹⁰² Art. 588 quater e) LECrim.

¹⁰³ Ley Orgánica 13/2015, de 5 de octubre.

¹⁰⁴ CONDE-PUMPIDO TOURÓN, C., “La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies Lecrim)”, *Jornadas de especialistas en criminalidad informática*, Centro de Estudios Jurídicos, CEJ, 2016, p. 8. Disponible en: http://www.cejmjusticia.es/cej_dode/flash/ebook/assets/img/cejponencia1462865212704/cejponencia1462865212704.pdf

como las condiciones para garantizar la preservación de los datos registrados. Se permite asimismo la ampliación del registro con previa autorización judicial en aquellos casos en los que existan razones fundadas para entender que los datos buscados se encuentran en otro sistema informático siempre y cuando se pueda acceder de forma lícita a los mismos conforme al sistema inicial.

La nueva regulación prevé al igual que en otro tipo de intervenciones, la posibilidad de una actuación de carácter excepcional por parte de la Policía Judicial, sin previo consentimiento del juez competente, en aquellos supuestos en los que por razones de urgencia e interés constitucional legítimo se entienda necesaria la intervención y examen directo de los datos contenidos en los dispositivos incautados.

No obstante, tras dicha actuación deberá comunicarlo de forma inmediata a la autoridad judicial y aportar un escrito donde se justifiquen las razones que le llevaron a actuar, así como el modo de proceder y el resultado de la actuación. Ante esto, el juez emitirá su conformidad o disconformidad en un plazo máximo de setenta y dos horas desde que fue ordenada la medida¹⁰⁵.

Destacar que generalmente el registro supondrá una afección de datos referidos al investigado sino irrelevante si el dispositivo donde se contienen pertenece a él mismo o a un tercero, no obstante es posible limitar el alcance de intervención¹⁰⁶. Es posible asimismo que surjan descubrimientos causales y en tal caso, será de aplicación la regla general prevista en el art. 579 bis.

4.4.4. El registro remoto de equipos informáticos.

Se trata de una medida procesal destinada principalmente a la investigación del crimen organizado. Destaca en ese sentido, la conveniencia de su incorporación legal como instrumento de lucha frente al terrorismo *yihadista*, puesto que internet ha pasado a ser una especie de campo de entrenamiento virtual de los integrantes del mismo, en el que se procede a su reclutamiento, adoctrinamiento y formación, así como una fuente de financiación¹⁰⁷.

La regulación de esta medida la encontramos en el art. 588 septies LECrim, y de la misma podemos destacar su carácter de “arma” en manos de las fuerzas de seguridad

¹⁰⁵ Art. 588 sexies c) LECrim.

¹⁰⁶ CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación...”, op., cit., p. 45.

¹⁰⁷ CONDE-PUMPIDO TOURÓN, C., “La reforma procesal...”, op., cit., pp. 12 y ss.

del Estado, pues la Policía Judicial conforme a la misma podrá proceder a la instalación de troyanos en los ordenadores de los sujetos investigados con el fin de acceder a su contenido, con previa autorización judicial.

Se permite por tanto, la instalación de un programa malicioso en el ordenador del investigado con el fin de controlar su contenido sin que este sea consciente de ello, y todo ello de forma legítima.

Son diversas las formas en las que se puede proceder a la instalación del software malicioso: por un lado, de forma directa, penetrando físicamente en el ordenador para lo que será necesaria una autorización judicial especial, pues se daría por ejemplo en la situación de actuación en el domicilio del investigado, o bien de forma indirecta, por envío remoto, enviando el software al ordenador en cuestión, cuando el usuario proceda a la apertura de un correo electrónico aprovechando las deficiencias en seguridad que poseen multitud de programas de dicha naturaleza.

Esta modalidad de intervención tiene por tanto dos rasgos determinantes: en primer lugar, la actuación secreta del agente interviniente y en segundo lugar, el carácter remoto de la técnica de acceso, rasgos que implican una clara invasión en la privacidad de la persona investigada.

El legislador establece un listado de categorías delictivas sobre las que cabe el empleo de esta medida, y se trata del mismo listado que el referido a las injerencias sobre telecomunicaciones añadiendo los delitos cometidos contra menores o personas con capacidad modificada judicialmente y los delitos contra la Constitución, de traición y relativos a la defensa nacional¹⁰⁸.

En el apartado 2 del art. 588 septies se concreta que la resolución judicial habilitante deberá acotar los ámbitos objetivo e instrumental de la medida, garantizando así el cumplimiento de los principios de proporcionalidad y necesidad.

El juez debe proceder a la descripción minuciosa de los dispositivos o ubicaciones virtuales que van a ser objeto de investigación así como la técnica que será empleada para proceder a la misma.

Se exige, a su vez, autorización judicial para llevar a cabo la realización y conservación de copias de los datos informáticos cuando proceda, y las medidas precisas para la

¹⁰⁸ Art. 588 septies LECrim.

preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso. Sin embargo, esa garantía de la integridad e inaccesibilidad o inalterabilidad de los datos incautados introduce un factor distorsionador de compleja solución jurídica. Pues la esencia de esta técnica de investigación se basa en la discreción, y esto se ve tergiversado al emplear las citadas vías de conservación y preservación ya que el investigado podría tener conocimiento de la ejecución de la intervención al descubrir por ejemplo que no puede modificar ni eliminar documentos contenidos en su ordenador.

RODRÍGUEZ LAINZ, por su parte considera preciso “establecer un protocolo de actuación que permitiera la obtención de copias de seguridad de aquellos documentos o archivos inspeccionados que quedaran conservadas independientemente del soporte del dispositivo o alojamiento investigado a disposición de la autoridad judicial; y dotar a esta extracción de información y conservación en soporte externo de las máximas garantías de complitud, inalterabilidad y preservación frente a accesos ilícito”¹⁰⁹.

Al igual que sucede en los registros de dispositivos de almacenamiento masivo de datos, se prevé la posibilidad de que, constatada o deducida racionalmente la realidad de que parte o toda la información objeto de búsqueda está almacenada en otro sistema informático o una parte del mismo, se pueda instar del Juez autorizante a una ampliación de los términos del registro.

La nueva regulación en el art. 588 septies b) establece un amplio deber de colaboración que recaerá, además de las personas referidas en el art. 588 ter e), sobre titulares o responsables del sistema informático o base de datos objeto de registro. Finalmente se establece un plazo máximo de duración de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

5. CONCLUSIONES

La LO 13/2015 de modificación de la Ley de Enjuiciamiento Criminal española sobre medidas de investigación tecnológica supone un considerable avance, más bien pone fin a la situación de inexistencia normativa en la que nos encontrábamos hasta hace unos meses. Se trata por tanto de una reforma con un claro carácter de urgencia y necesidad pues el progreso tecnológico ha traído consigo entre otras cosas la aparición de los

¹⁰⁹ RODRÍGUEZ LAINZ, J. L., “Las nuevas medidas..., op., cit., p. 14.

“ciberdelitos” y en el sistema judicial preexistente los jueces no disponían de instrumentos suficientes para combatirlos.

Podemos afirmar que con esta nueva regulación se han podido colmar las distintas lagunas jurídicas y vacíos legales que surgieron en el transcurso de la investigación de diversos delitos en los que se precisaba la intervención de las comunicaciones por parte de las autoridades competentes, y ello implicaba una gran inseguridad jurídica. Anteriormente el cumplimiento del principio de legalidad a la hora de poner en práctica, de autorizar, las diversas medidas de investigación, era de una dificultad elevada.

Constituye por tanto una normativa muy necesaria puesto que al fin alberga un conjunto de diligencias de investigación destinadas a la interceptación de comunicaciones, tanto las tradicionales telefónicas como las de carácter electrónico.

Observamos a su vez la evolución que ha sufrido el concepto de comunicación, en el que no solo podemos incluir la realizada por medio del soporte escrito sino también las efectuadas a través de medios tecnológicos como el correo electrónico o mensajería instantánea a través del teléfono móvil.

Se trata de una aportación a través de ley orgánica puesto que tal y como apuntamos, las diligencias incorporadas a la LECrim traen consigo un claro enfrentamiento con los derechos fundamentales de la persona investigada, de los cuales destacamos el derecho al secreto de las comunicaciones cuya vulneración lícita debe estar fundamentada y ello viene desarrollado para cada medida de intervención en los nuevos preceptos incorporados. Hablamos por tanto de una ventaja con respecto a la protección de esos derechos y sobre todo ventaja en relación a la incorporación de las posibilidades de proceder a la ejecución de tales diligencias a través del uso de diversos dispositivos para los cuales con anterioridad no encontrábamos respaldo legal a nivel de ley orgánica.

El nuevo texto legal es a su vez acertado en lo que respecta a la determinación explícita de las situaciones para las que se prevén las distintas medidas de investigación y los delitos sobre los cuales procede su autorización. Asimismo especifica en cada supuesto el contenido objetivo que debe albergar la resolución judicial habilitante.

Es preciso resaltar como aspecto negativo o más bien indeterminado el hecho de no fijar con precisión los plazos de ciertas medidas como puede ser la relativa a la captación de imagen, pues se permite el alargamiento constante de la misma, y esto puede traer

consigo la inseguridad de pensar que se está continuamente siendo objeto de investigación.

Ventajoso a su vez es la redacción de los distintos preceptos pues su carácter abierto da lugar a su posible adaptación a los diversos avances tecnológicos que puedan ir aconteciendo con el transcurso del tiempo.

Personalmente considero acertada esta nueva regulación en la medida en que contempla numerosas situaciones para las que no se preveía la posibilidad de intervención por parte de las autoridades competentes, y a su vez supone un claro ejemplo de adaptación a los nuevos tiempos en los que la tecnología es en definitiva uno de los pilares básicos, incidiendo sobre los métodos de delinquir y aquellos encaminados a la investigación por parte del Estado.

Era al fin y al cabo necesaria y a grandes rasgos podemos afirmar que es apta para dar cobertura a multitud de supuestos que puedan surgir, favoreciendo en definitiva la actuación de las autoridades competentes en las tareas de investigación.

BIBLIOGRAFÍA

Doctrina

ARAGONÉS SEIJO, S., y FERNÁNDEZ SERRA L., “La ausencia de previsión legal para las escuchas en vehículos”, *Diario La Ley*, 26 de Junio de 2015.

BAÑULS GOMEZ, F., “Las intervenciones telefónicas a la luz de la jurisprudencia más reciente”, Portal Web Noticiasjurídicas.com, 2007.

BUENO DE MATA, F., “Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica”, *Diario La Ley*, 2015.

CABEZUDO RODRÍGUEZ, N., “Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal”, *I Jornada del Boletín del Ministerio de Justicia: «Las reformas del proceso penal»*, *Boletín del Ministerio de Justicia*, núm. 2186, febrero 2016.

CONDE-PUMPIDO TOURÓN, C., “La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas. El registro remoto de dispositivos informáticos (arts. 588 sexies y 588 septies Lecrim”, *Jornadas de especialistas en criminalidad informática*, Centro de Estudios Jurídicos, CEJ, 2016.

DÍAZ REVORIO, F. J., “El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español”, *Derechos Humanos México*, 2006.

DÍAZ REVORIO, F. J., “El derecho fundamental al secreto de las comunicaciones”, *Revista de la Facultad de Derecho*, Pontificia Universidad Católica del Perú (PUCP), nº 59, 2007.

GIMENO BREVIÁ, J., GIMENO BREVIÁ, J., “Principales novedades de la reforma de la LECrim 2015”, Dossier reforma de la Ley de Enjuiciamiento Criminal, Thomson Reuters-Aranzadi, 2015.

GONZÁLEZ-CUELLAR SERRANO, N., “La reforma de la Ley de Enjuiciamiento Criminal: Necesidad de su reforma y examen de las sucesivas reformas parciales”, Centro de Estudios Jurídicos, CEJ, 2004.

GONZÁLEZ MONJE, A., “Nuevas tecnologías e investigación penal. La superación de los métodos tradicionales”, *FODERTICS 3.0. Estudios sobre nuevas tecnologías y Justicia*, Comares, Granada, 2015.

GONZÁLEZ MONJE, A., “Sentencia del Tribunal Constitucional (Sala Segunda), 145/2014, de 22 de septiembre [BOE n.º 261, de 28-X-2014]: Intervención de comunicaciones en dependencias policiales”, *AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, Vol. 3, núm. 1, 2015.

GONZÁLEZ-MONTES SÁNCHEZ, J. L., “Reflexiones sobre el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas”, *Revista electrónica de ciencia penal y criminología*, 2015.

LLAMAS FERNÁNDEZ, M., GORDILLO LUQUE, J.M., “Medios técnicos de vigilancia”, *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia*, Cuadernos de Derecho Judicial, núm.2, 2007.

LÓPEZ-FRAGOSO ALVÁREZ, T., *Las intervenciones telefónicas en el proceso penal*, Colex, Madrid, 1991.

REBOLLO DELGADO, L., “El secreto de las comunicaciones: problemas actuales”, *Revista de Derecho Político*, 2000.

REYES LÓPEZ, J. I., “Las intervenciones de las comunicaciones en el derecho español. Alcance y valoración de la noticia anónima. Cooperación judicial internacional. Información de inteligencia”, *Boletín Científico ESMPU*, Brasilia, núm. 40, junio 2013.

RÍOS PINTADO, J. F., “La reforma procesal. Incorporación al proceso de datos de tráfico; preservación específica de datos informáticos (arts. 588 ter j y 588 octies de la ley de enjuiciamiento criminal)”, *Jornadas de especialistas en criminalidad informática*, Centro de Estudios Jurídicos, CEJ, 2016.

RODRÍGUEZ LAINZ, J. L., “Sobre el ámbito objetivo de la protección constitucional del secreto de las comunicaciones en la STC 107/2012, de 21 de mayo”, *Diario La Ley*, 2012.

RODRÍGUEZ LAINZ, J. L., “Los dispositivos electrónicos de posicionamiento global (GPS) en el Proceso Penal”, *Diario La Ley*, 17 Oct. 2012.

RODRÍGUEZ LAINZ, J. L., “En torno al concepto de comunicación protegida por el art.18.3 de la Constitución”, *Diario La Ley*, 5 Sep. 2013.

RODRÍGUEZ LAINZ, J.L., “Las nuevas medidas de investigación tecnológica de la Ley Orgánica 13/2015”, *SEPIN*, Enero de 2016.

VELASCO NÚÑEZ, E., “Investigación procesal penal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba tecnológica”, *Diario La Ley*, 4 Nov. 2013.

Legislación

Constitución Española. (BOE nº. 311, de 29-XII-1978).

Circular de la Fiscalía General del Estado 1/ 2013 *sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.*

Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.

Ley Orgánica 10/1995, de 23 de noviembre, de Código Penal (BOE nº.281, de 24-XI-1995)

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. (BOE nº. 251, de 19 –X-2007).

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. (BOE nº. 239, de 6-X-2015)

Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (BOE nº.260, de 17-IX-1882).

Jurisprudencia

España. Tribunal Constitucional (Pleno). Sentencia núm. 184/2003 de 23 de octubre.

España. Tribunal Constitucional (Pleno) Sentencia núm. 184/2003 de 23 de octubre

España. Tribunal Constitucional (Sala Segunda). Sentencia núm. 114/1984 de 29 de noviembre.

España. Tribunal Constitucional (Sala Segunda). Sentencia núm.145/2014 de 22 de septiembre.

España. Tribunal Constitucional (Sala Primera). Sentencia núm. 89/2006 de 27 de marzo.

España. Tribunal Constitucional (Sala Segunda). Sentencia núm. 173/2011 de 7 de noviembre.

España. Tribunal Constitucional (Sala Primera). Sentencia núm. 123/2002 de 20 de mayo.

España. Tribunal Constitucional (Sala Primera). Sentencia núm. 123/2002 de 20 de mayo.

España. Tribunal Constitucional (Sala Segunda). Sentencia núm. 56/2003 de 24 de marzo.

España. Tribunal Constitucional (Sala Primera). Sentencia núm. 70/2002 de 3 de abril.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm.707/2009 de 22 de junio.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 1001/2005 de 19 de julio.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 712/2012 de 26 de septiembre

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 84/2010 de 18 de febrero.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 905/2003 de 18 de junio.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 1235/2002 de 27 de junio.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 513/2010 de 2 de junio

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 740/2012, de 10 de octubre.

España. Tribunal Supremo (Sala de lo Penal) Sentencia núm. 474/2012 de 6 de junio

Tribunal Europeo de Derechos Humanos (Sección 4ª). Caso Copland contra Reino Unido. Sentencia de 3 de abril 2007.

Tribunal Europeo de Derechos Humanos (Sección 2ª). Caso Koop contra Suiza. Sentencia de 25 de marzo 1998.

Recursos electrónicos

Aranzadi: <webs\Aranzadi.htm>

Boletín Oficial del Estado: <webs\BOE.es - Agencia Estatal Boletín Oficial del Estado.htm>

Centro de Estudios Jurídicos: <webs\CEJ. Centro de Estudios Jurídicos - Página de inicio.htm>

Noticias Jurídicas: <webs\Noticias Jurídicas.htm>

Sepin: <webs\Editorial Jurídica Sepín.htm>