



Universidad de Valladolid

Facultad de Ciencias Sociales, Jurídicas y de la Comunicación

Grado en Derecho

**Las medidas de investigación tecnológica en el proceso penal
español: una década marcada por la Ley Orgánica 13/2015**

Presentado por:

Javier Martín de Frutos

Tutelado por:

María Luisa Escalada López

Segovia, a 6 de diciembre de 2025

RESUMEN

A una década de la entrada en vigor de la Ley Orgánica 13/2015, resulta hoy más imprescindible que nunca analizar en profundidad las diligencias de investigación tecnológica, pues el transcurso del tiempo ofrece una perspectiva especialmente valiosa para esta tarea.

Por este motivo, es objeto del presente trabajo examinar el catálogo de medidas previsto en la Ley de Enjuiciamiento Criminal, todo ello con la finalidad de extraer importantes conclusiones que nos permitan comprender su verdadero alcance. Al mismo tiempo, se detectan los problemas más significativos que, en la práctica, plantea la adopción de estas medidas, así como el impacto que las mismas tienen para los derechos fundamentales del investigado o encausado.

Palabras clave

Medidas de investigación tecnológica, derechos fundamentales, interceptación de las comunicaciones telefónicas y telemáticas, intimidad.

ABSTRACT

A decade after the entry into force of Organic Law 13/2015, it is more necessary than ever to conduct an in-depth analysis of technological investigation measures, as the passage of time offers an especially valuable perspective for this task.

For this reason, the present work aims to examine the catalog of measures established in the Criminal Procedure Law, with the purpose of drawing important conclusions that allow us to understand their true scope. At the same time, it identifies the most significant problems that, in practice, arise from the adoption of these measures, as well as the impact they have on the fundamental rights of the investigated or accused person.

Key words

Measures of technological investigation, fundamental rights, interception of telephone and telematic communications, privacy.

ÍNDICE

I. INTRODUCCIÓN	6
I.I. Justificación del estudio.....	6
I.II. Metodología empleada.....	6
II. DISPOSICIONES COMUNES A LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA.....	8
II.I. Principios rectores	8
a) <i>Principio de especialidad</i>	8
b) <i>Principio de idoneidad</i>	9
c) <i>Principios de excepcionalidad y de necesidad</i>	10
d) <i>Principio de proporcionalidad</i>	11
II.II. Solicitud de autorización judicial	12
II.III. Duración y cese de la medida.....	14
II.IV. Afectación a terceras personas como consecuencia de su aplicación	15
II.V. Control de la medida y destrucción de registros	15
III. DERECHOS FUNDAMENTALES AFECTADOS POR LA ADOPCIÓN DE MEDIDAS DE INVESTIGACIÓN TENOLÓGICA.....	17
III.I. Consideraciones previas	17
III.II. Derecho fundamental a la intimidad personal y familiar (art. 18.1 CE)	18
III.III. Derecho fundamental al secreto de las comunicaciones (art. 18.3 CE)	20
IV. CATÁLOGO DE MEDIDAS	22
IV.I. Interceptación de las comunicaciones telefónicas y telemáticas.....	23
IV.II. Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.....	28
IV.III. Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.....	31
a) <i>Captación de imágenes en lugares o espacios públicos</i>	31

<i>b) Utilización de dispositivos o medios técnicos de seguimiento y localización</i>	<i>32</i>
IV.IV. Registro de dispositivos de almacenamiento masivo de información	34
IV.V. Registros remotos sobre equipos informáticos.....	36
IV.VI. Medidas de aseguramiento.....	38
VI. CONCLUSIONES	40
VII. BIBLIOGRAFÍA.....	42
VIII. JURISPRUDENCIA	44

ÍNDICE DE ABREVIATURAS

Art./-s: Artículo/-s.

CE: Constitución española.

FJ: Fundamento jurídico.

Ibid.: *Ibidem*.

LECrim: Ley de Enjuiciamiento Criminal.

LO: Ley Orgánica.

MF: Ministerio Fiscal.

Ob. cit.: Obra citada.

RD: Real Decreto.

SITEL: Sistema Integrado de Interceptación Telefónica.

STC: Sentencia del Tribunal Constitucional.

STS: Sentencia del Tribunal Supremo.

TC: Tribunal Constitucional.

TS: Tribunal Supremo.

Vid.: Véase.

I. INTRODUCCIÓN

I.I. Justificación del estudio

Como se evidenciará más adelante, la investigación de los delitos en el contexto actual únicamente es posible mediante métodos tecnológicos, pues, de otro modo, su persecución se vuelve prácticamente inviable, especialmente si se considera que gran parte de la actividad delictiva se desarrolla precisamente a través de estos medios. En consecuencia, el hecho de que el presente trabajo tenga por objeto el estudio de las medidas de investigación tecnológica obedece a la necesidad de abordar una materia de absoluta actualidad.

Sin embargo, ello no quiere decir que la regulación prevista para estas diligencias en la LECrim no adolezca de notabilísimas carencias, pues en numerosas ocasiones el surgimiento de nuevas formas de criminalidad desborda con creces las posibilidades de una regulación todavía incompleta.

En efecto, es el examen del catálogo de medidas lo que permitirá identificar con mayor claridad sus principales inconvenientes, al mismo tiempo que se analiza hasta qué punto se ven afectados, por un lado, el derecho fundamental a la intimidad personal y familiar (art. 18.1 CE), y por otro, el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE).

I.II. Metodología empleada

En la elaboración del presente trabajo se ha seguido, en síntesis, la siguiente metodología:

En primer lugar, se aborda el Capítulo IV del Título VIII del Libro II de la LECrim, dedicado a las disposiciones comunes aplicables a las medidas de investigación tecnológica, pues resulta imprescindible conocer, antes de nada, los principios que rigen su adopción, así como los requisitos que debe reunir la resolución judicial que autorice su práctica, entre otros aspectos relevantes.

A partir de estas nociones preliminares, se procede a analizar con cierto detalle el modo en que la ejecución de estas diligencias incide en los derechos fundamentales del investigado, con especial atención al derecho a la intimidad personal y familiar y al derecho al secreto de las comunicaciones, sin perjuicio de advertir que pueden verse comprometidos otros bienes constitucionalmente protegidos, como la inviolabilidad del domicilio.

Por último, se aborda el que constituye el núcleo esencial de este trabajo: el análisis pormenorizado del catálogo de medidas de investigación tecnológica. En este apartado se examinan, entre otras diligencias, la interceptación de las comunicaciones telefónicas y telemáticas, así como la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos.

II. DISPOSICIONES COMUNES A LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

II.I. Principios rectores

El acceso por parte del Estado al contenido de comunicaciones de las que no posee el consentimiento de sus titulares supone, naturalmente, una restricción que vulnera en todo punto el ejercicio del derecho fundamental al secreto de las comunicaciones consagrado en el art. 18.3 CE.

Por ello, el art. 588 *bis* a LECrim, bajo la rúbrica de “*principios rectores*”, establece las condiciones para la adopción de medidas de investigación tecnológica. De este modo, además de la preceptiva autorización judicial, será necesaria la observancia de una serie de principios:

a) Principio de especialidad

El principio de especialidad se constituye como una barrera material de carácter ineludible en lo referente a las diligencias de investigación tecnológica. Dicho principio, hoy expresamente plasmado en el apartado segundo del art. 588 *bis* a LECrim, exige que toda medida esté estrictamente supeditada a indicios racionales que apunten a la comisión de un delito concreto, cortando de raíz cualquier autorización de naturaleza genérica o prospectiva.

Así, el TS ha expresado de manera categórica que “*no cabe decretar la intervención telefónica para propiciar el descubrimiento genérico de posibles infracciones penales, lo que supondría conceder autorizaciones en blanco*” (STS 393/2012). Esta doctrina jurisprudencial ha sido ratificada y reforzada por la STS 272/2017, de 18 de abril, que delimita con notable claridad el contenido del principio al establecer que “*la prohibición de intervenciones prospectivas es consecuencia del principio de especialidad vigente en la materia, que significa que los poderes públicos no pueden inmiscuirse en la intimidad de los sospechosos, interceptando sus comunicaciones, con el exclusivo propósito u objeto de indagar a ciegas su conducta, por lo que la decisión jurisdiccional de intervención de las comunicaciones telefónicas tiene que estar siempre relacionada con la investigación de un delito concreto al menos en el plano indiciario*”.

No obstante, conviene precisar que la aplicación estricta del principio de especialidad no impide la validez de los hallazgos casuales obtenidos durante la ejecución legítima de una intervención inicialmente autorizada. Tal como recuerda la STC 41/1998, de 24 de febrero, “*que se estén investigando unos hechos delictivos no impide la persecución de*

cualesquiera otros distintos que sean descubiertos por casualidad al investigar aquellos, pues los funcionarios de Policía tienen siempre el deber de poner en conocimiento de la autoridad penal competente los delitos de que tuvieran conocimiento, practicando incluso las diligencias de prevención que fueran necesarias por razón de urgencia”. Esta excepción, sin comprometer el núcleo del principio de especialidad, garantiza que la investigación penal no permanezca obstaculizada ante descubrimientos imprevistos que revisten importancia criminal.

En definitiva, el principio de especialidad reafirma la proscripción de diligencias basadas en meras conjeturas o sospechas genéricas sin sustrato fáctico mínimamente razonable.

b) Principio de idoneidad

El art. 588 *bis* a LECrim, en su apartado tercero, establece la idoneidad como uno de los principios rectores que, junto a los demás, “*deberían entenderse aplicables a todas las formas de investigación (de hecho, en la actualidad la investigación o es tecnológica o no es investigación)*” PÉREZ GIL.¹

Dicho precepto impone que la diligencia ha de estar orientada de forma precisa al objeto de la investigación, limitando su ámbito objetivo —delitos concretos susceptibles de ser investigados—; ámbito subjetivo —sujetos que podrán ser investigados—; y duración a lo estrictamente necesario, a fin de evitar intrusiones e injerencias desmedidas en la esfera del derecho fundamental al secreto de las comunicaciones. Por consiguiente, el órgano judicial ha de valorar en cada caso concreto si la medida resulta adecuada para obtener pruebas que contribuyan efectivamente al avance de la instrucción penal.²

El propio art. 588 *bis* e LECrim, al preceptuar que las medidas “*no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos*” o que la prórroga de las mismas exigirá auto motivado del juez competente, pone de manifiesto, junto con el art. 588 *bis* f LECrim,

¹ PÉREZ GIL, Julio. “Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución”. *“Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli”*. 2018, pág. 2.

² CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, págs. 304-305.

relativo al control judicial de aquellas, el carácter dinámico que se desprende del principio de idoneidad, pues la utilidad de las medidas cuya adopción se pretenda ha de ser evaluada no solo en el momento de su autorización, sino también durante su ejecución. Por eso mismo, la solicitud de prórroga de una medida requiere que “*subsistan las causas que la motivaron*” (art. 588 bis e LECrim). Estas revisiones contribuyen a asegurar que las medidas continúen siendo pertinentes y ajustadas a los fines de la investigación, de tal forma que se adapten a las circunstancias cambiantes del proceso penal en su fase de instrucción.

c) Principios de excepcionalidad y de necesidad

En lo que a los principios de excepcionalidad y de necesidad se refiere, el art. 588 bis a 4 LECrim dispone que únicamente puede acordarse una medida cuando: (1) “*no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho*”; (2) “*el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida*”.

Por tanto, en virtud del principio de excepcionalidad, “*si puede obtenerse, en síntesis, la misma información mediante la utilización de dos medidas de investigación tecnológicas, con distinta intensidad invasiva en los derechos fundamentales de los investigados, el Juez o Jueza optará siempre por la menos agresiva, en cumplimiento del principio de especialidad, que impondrá seleccionar, de entre las varias medidas posibles, cuál sea la más idónea en función de dos parámetros a conciliar: el éxito de la investigación y el menor menoscabo posible de los derechos fundamentales del investigado*” CALAZA LÓPEZ.³

Por otro lado, respecto al principio de necesidad, en palabras de NIEVA FENOLL, “*aunque lo correcto sería que la ley exigiera que el seguimiento fuera imprescindible para la investigación, la norma se contenta con que se justifique que sin la medida ‘se vea gravemente dificultada’ la investigación (art. 588 bis a 4 b LECrim)*”.⁴

³ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 305.

⁴ NIEVA FENOLL, Jordi. “Tema 6: La instrucción”. “*Derecho Procesal III (Proceso Penal) Adaptado a la Ley Orgánica 1/2025*”. Valencia: Tirant lo Blanch, 2025, pág. 215.

En consecuencia, la exigencia de seleccionar siempre la diligencia menos taxativa para los derechos fundamentales, unida al hecho de que únicamente se lleve a cabo cuando resulte indispensable para alcanzar los fines de la instrucción penal, cumple con una función tuitiva que trata de evitar, nuevamente, intromisiones ilegítimas y arbitrarias.

d) Principio de proporcionalidad

Los actos de naturaleza procesal, y de manera singular aquellos desplegados en el marco de la fase de instrucción, comportan un potencial impacto sobre los derechos fundamentales de las personas investigadas, por lo que su validez requiere un escrupuloso examen conforme al principio de proporcionalidad, de acuerdo con la reiterada doctrina del TC. Conforme a este principio, se lleva a cabo un control indispensable en todo Estado de Derecho frente a posibles injerencias arbitrarias.

Desde esta perspectiva, toda medida de investigación que suponga una vulneración de un derecho fundamental únicamente puede reputarse legítima si satisface determinados presupuestos: en primer término, la previsión expresa en una norma con rango de ley, en observancia del principio de legalidad; en segundo lugar, la concurrencia de una justificación objetiva que permita apreciar su idoneidad para la finalidad perseguida; y, finalmente, la exposición razonada y detallada de la restricción impuesta, a través de una motivación suficiente en la que se incorpore el denominado juicio de necesidad, del que se derive la inevitabilidad del sacrificio del derecho afectado en aras de los fines legítimos de la investigación penal.⁵

La aplicación del principio de proporcionalidad exige al órgano jurisdiccional realizar una valoración integral de las circunstancias concurrentes en el supuesto concreto, con el objeto de verificar que la utilidad o el beneficio derivado de la medida acordada no resulte inferior al sacrificio que esta comporta para los derechos fundamentales o intereses legítimos afectados. Como ha señalado el TC, *“la adopción de medidas restrictivas de derechos fundamentales exige una ponderación entre la intensidad de la injerencia y la relevancia del fin que se persigue, en términos de proporcionalidad”* (STC 70/2002, de 3 de abril). Este mismo criterio ha sido el adoptado por la jurisprudencia del TS, que ha insistido en que la proporcionalidad

⁵ GIMENO SENDRA, Vicente. “Lección 2: El principio de proporcionalidad. Los Derechos fundamentales de Derecho Judicial Orgánico. Los Derechos fundamentales materiales a la legalidad y al *non bis in idem*”. *“Manual de Derecho Procesal Penal”*, 2ª Edición, 2025, pág. 33.

opera como parámetro rector judicial sobre las medidas de investigación tecnológica, especialmente por tratarse de técnicas que, por su naturaleza invasiva, pueden vulnerar gravemente el ámbito de intimidad de los investigados.

Por su parte, el art. 588 *bis* a LECrim, en su apartado quinto, proporciona algunos parámetros que pueden guiar al juzgador en la realización de ese ejercicio de ponderación al que aludíamos anteriormente: “*para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho*”. Por ende, en comparación con el contexto normativo previo a la entrada en vigor de la LO 13/2015, puede advertirse un incremento en los criterios para valorar cuándo una actuación resulta o no proporcionada, así como una mejor adaptación de los mismos a la realidad.⁶

Conviene señalar, además, que el principio de proporcionalidad, como resulta evidente, no es una novedad introducida con la reforma de la LECrim del año 2015, sino que “*se encuentra implícitamente contenido en el art. 25 CE (que, al consagrar el principio de ‘legalidad’, no solo establece el de ‘tipicidad’, sino también el de ‘proporcionalidad’ entre la medida y la sanción*”. GIMENO SENDRA.⁷ De esta manera, el acatamiento del principio de proporcionalidad en la adopción de medidas de investigación tecnológica permite que la vulneración de los derechos fundamentales afectados sea legítima no solo desde el punto de visto legal, sino también acorde con los parámetros fijados por el marco constitucional.

II.II. Solicitud de autorización judicial

La existencia de autorización judicial deviene un requisito *sine qua non* para la práctica de cualquiera de las diligencias de investigación legalmente previstas. Dicha autorización judicial adoptará la forma de auto, el cual será debidamente motivado, dictado

⁶ GÓMEZ COLOMER, Juan Luis. “Lección 11ª: Los actos de investigación garantizados basados en las nuevas tecnologías”. “*Proceso Penal. Derecho Procesal III*”. Valencia: Tirant lo Blanch, 2025, pág. 256.

⁷ GIMENO SENDRA, Vicente. “Lección 2: El principio de proporcionalidad. Los Derechos fundamentales de Derecho Judicial Orgánico. Los Derechos fundamentales materiales a la legalidad y al *non bis in idem*”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 33.

tras la estricta observancia de los principios rectores que se recogen en el art. 588 *bis* a LECrim.⁸

El juez encargado de la instrucción podrá acordar las medidas tanto de oficio como a instancia del MF o de la Policía Judicial, si bien en el caso de que la solicitud se realice por parte de estos dos últimos, la petición habrá de contener, conforme a lo establecido por el art. 588 *bis* b LECrim, los extremos siguientes:

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

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

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

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

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

6º) La forma de ejecución de la medida.

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

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

De lo anteriormente expuesto se infiere que, en aquellos supuestos en los que la medida se ordene de oficio, no será preceptivo que el auto haga mención expresa a tal enumeración. Ahora bien, con independencia de que la medida sea autorizada o denegada, el auto habrá de dictarse, previa audiencia del MF, en el plazo máximo de veinticuatro horas siguientes a la presentación de la correspondiente solicitud (art. 588 *bis* c LECrim).⁹

Por otra parte, aunque el análisis detallado de la interceptación de las

⁸ LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, pág. 248.

⁹ Ibid., pág. 251.

comunicaciones telefónicas y telemáticas se abordará en un momento ulterior, resulta especialmente pertinente subrayar que la LECrim contempla expresamente la posibilidad de que, en determinados supuestos, el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad dispongan la práctica de dicha diligencia. En concreto, la norma hace referencia a casos de urgencia, “*cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida*” (art. 588 *ter* d 3 LECrim). En cualquier caso, la medida acordada habrá de ser puesta en conocimiento inmediato del juez competente dentro del límite temporal máximo de veinticuatro horas, quien, de forma motivada, la revocará o confirmará en un plazo máximo de setenta y dos horas desde que tuvo lugar la ordenación de la medida.¹⁰

Cabe añadir, respecto a la solicitud y a las actuaciones posteriores relacionadas con la medida, que, de conformidad con lo dispuesto en el art. 588 *bis* d LECrim, “*sustanciarán en una pieza separada y secreta*”, si bien es cierto que ello no implicará necesariamente decretar el secreto de la causa.

II.III. Duración y cese de la medida

En cuanto al tiempo de vigencia de la medida, bastémonos señalar que esta tendrá la duración que se indique para cada una de ellas en la LECrim, de tal forma que, dependiendo de la medida concreta a la que apuntemos y de las circunstancias concurrentes de cada caso, su extensión en el tiempo será mayor o menor. No obstante, en ningún caso podrá la medida exceder del tiempo que se considere imprescindible para el esclarecimiento de los hechos, sin perjuicio de su posible prórroga siempre que subsistan las causas que la motivaron.

De acuerdo con ARRABAL PLATERO, es importante tener presente que “*hay diligencias no sujetas a un plazo determinado por su naturaleza puntual y no continua, como la captación y grabación de comunicaciones orales o el registro de dispositivos de almacenamiento masivo de información*”.¹¹ Tampoco debe ignorarse el hecho de que las disposiciones comunes no hacen ninguna

¹⁰ Art. 588 *ter* d 3 LECrim.

¹¹ ARRABAL PLATERO, Paloma. “Capítulo III: Obtención de la prueba tecnológica”. “*La Prueba Tecnológica: Aportación, Práctica y Valoración*”. Valencia: Tirant lo Blanch, 2020, pág. 184.

referencia en lo que al cómputo de las medidas se refiere, por lo que ha de entenderse que resulta aplicable el criterio que se establece para la interceptación de las comunicaciones telefónicas y telemáticas, es decir, se tomará como referencia la fecha de la autorización judicial.¹²

En cuanto al cese de la medida, este se acordará, de conformidad con el art. 588 bis j LECrim, “*cuando desaparezcan las causas que justificaron su adopción*”, pero también cuando se evidencie que con su aplicación no se obtienen los resultados deseados. En todo caso, el cese de la medida tendrá lugar cuando se produzca el transcurso del plazo para el que fue inicialmente autorizada.

II.IV. Afectación a terceras personas como consecuencia de su aplicación

Resulta incuestionable que la aplicación de medidas restrictivas conlleva, de manera inevitable, la eventual incidencia sobre personas distintas de aquel que ostenta la condición de investigado. Sin embargo, “*ello no permite hacer uso de medidas de intervención de las comunicaciones de un sujeto al que se pretende investigar, mediante el uso de aparatos o instrumentos titularidad de otro u otros, si no es tras la atribución al primero de la condición de investigado —que es la que corresponde, y no la de tercero— y el estatuto jurídico a esta inherente*” LÓPEZ YAGÜES.¹³

II.V. Control de la medida y destrucción de registros

Tal y como se expuso al tratar el principio de idoneidad, el control judicial de estas medidas reviste un carácter esencialmente dinámico, en cuanto no permanece inmutable durante toda su vigencia, si no que exige la constante verificación o constatación de su utilidad y necesidad, so pena de que deban cesar de forma inmediata. En este sentido, en palabras de LÓPEZ YAGÜES, “*la garantía o exigencia de jurisdiccionalidad, lejos de agotarse en el acuerdo de la medida, se extiende al control de su desarrollo*”.¹⁴

Por otro lado, toda vez que el procedimiento termine mediante resolución firme, “*se ordenará el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e*

¹² Ibid.

¹³ LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, págs. 250-251.

¹⁴ Ibid., pág. 252.

informáticos utilizados en la ejecución de la medida” (art. 588 *bis* k LECrim); si bien es cierto que el LAJ conservará una copia bajo su custodia. No obstante, transcurrido el plazo de cinco años en los supuestos previstos en el apartado segundo del art. 588 *bis* k LECrim, se decretará la destrucción de las copias conservadas, salvo que, a juicio del tribunal, se estime necesaria su conservación. En cualquier caso, corresponde a la Policía Judicial llevar a efecto la referida destrucción de registros.¹⁵

¹⁵ Art. 588 *bis* k 3 LECrim “*Los tribunales dictarán las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción contemplada en los anteriores apartados*”.

III. DERECHOS FUNDAMENTALES AFECTADOS POR LA ADOPCIÓN DE MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

III.I. Consideraciones previas

El art. 18 CE reconoce diversos derechos relativos a la esfera privada —derecho a la intimidad, derecho al secreto de las comunicaciones o derecho a la protección de datos de carácter personal, entre otros— que pueden verse limitados con mayor o menor incidencia por la práctica de determinadas diligencias de investigación tecnológica.¹⁶

Naturalmente, los derechos que adquieren una mayor relevancia en el asunto que aquí nos ocupa son el derecho fundamental a la intimidad (art. 18.1 CE) y el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE) —sin perjuicio, claro está, de que puedan verse afectados otros bienes constitucionalmente protegidos como, por ejemplo, la inviolabilidad del domicilio si se colocan aparatos de escucha o grabadoras de audio y vídeo dentro de la vivienda—. Ahora bien, aun cuando ambos derechos convergen en la tutela de un mismo bien jurídico, resulta necesario enfatizar en la idea de que cada uno de ellos posee autonomía respecto al otro. En otras palabras, se trata de derechos distintos, aunque estrechamente vinculados entre sí, en virtud de la naturaleza complementaria que los caracteriza dentro del marco constitucional.¹⁷

En este sentido, la STC 123/2002, de 20 de mayo, en su FJ núm. 5, determina, en relación con el derecho fundamental al secreto de las comunicaciones, que *“este reconocimiento autónomo del derecho no impide naturalmente que pueda contribuir a la salvaguarda de otros derechos, libertades o bienes constitucionalmente protegidos, como el secreto del sufragio activo, la libertad de opinión, ideológica y de pensamiento, de la libertad de empresa, la confidencialidad de la asistencia letrada o, naturalmente, también, el derecho a la intimidad personal y familiar”*. Así pues, el TC subraya que la autonomía del secreto de las comunicaciones no debe entenderse en un sentido aislado o

¹⁶ ESPÍN LÓPEZ, Isidoro. “Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual”. *“Boletín del Ministerio de Justicia”*, núm. 2244, 2021, pág. 26.

¹⁷ OCÓN GARCÍA, Juan. “Capítulo I: Delimitación del derecho fundamental del art. 18.3 CE”. *“El derecho fundamental al secreto de las comunicaciones ante nuevos escenarios tecnológicos”*. Programa de doctorado en Derecho y cambio social, 2020, Universidad de La Rioja, págs. 25-29.

excluyente, por cuanto opera como garantía de otros derechos fundamentales que, sin confundirse con él, se ven reforzados por su observancia.

En las líneas siguientes se llevará a cabo un análisis pormenorizado de los derechos fundamentales anteriormente mencionados, al objeto de evaluar la forma en que los mismos pueden resultar comprometidos o restringidos por la implementación de medidas de investigación de carácter tecnológico.

III.II. Derecho fundamental a la intimidad personal y familiar (art. 18.1 CE)

La positivación del derecho a la intimidad, en tanto manifestación de los derechos de la personalidad, es de aparición relativamente tardía, pues el primer texto que lo reconoce es la Declaración Universal de Derechos Humanos de 1948, que establece, en su art. 12, una protección explícita frente a “*injerencias arbitrarias*” en la esfera privada. Con posterioridad, diferentes ordenamientos jurídicos incorporarán este derecho en sus respectivos textos constitucionales, dotándolo así de una tutela reforzada en el plano interno de los Estados.¹⁸

Conforme a lo expuesto por MORENO BOBADILLA, la promulgación de la CE de 1978 resulta un hecho absolutamente trascendental en la configuración jurídica del derecho a la intimidad en nuestro país. No solo implica su consagración expresa en el texto constitucional, sino también su inserción dentro de la estructura de los derechos fundamentales —concretamente en la Sección 1ª del Capítulo II del Título I—, lo que le otorga el más elevado rango de protección dentro del ordenamiento jurídico español. Indudablemente, el poder constituyente fue plenamente consciente de la significación jurídica que revestía garantizar de manera efectiva el ejercicio del referido derecho.¹⁹

En concreto, el art. 18.1 CE consagra el derecho a la intimidad personal y familiar con el siguiente tenor: “*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*”.

¹⁸ MARTÍNEZ DE PISÓN CAVERO, José María. “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”. “*Anuario de filosofía del derecho*”, núm. 32, 2016, Universidad de La Rioja, pág. 410.

¹⁹ MORENO BOBADILLA, Ángela. “El derecho a la intimidad en España”. “*Arx Boni et Aequi*”, Vol. 12, núm. 1, 2016, pág. 38.

En lo que al desarrollo legislativo del derecho a la intimidad se refiere, encontramos que la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, ha sido la encargada de llevar a cabo la configuración legal del mismo, labor especialmente compleja si tenemos en cuenta que el texto constitucional no alberga una definición normativa que delimite qué aspectos han de entenderse englobados en el concepto de intimidad. A este respecto, ha sido se suma trascendencia el papel desempeñado por el TC en sus múltiples resoluciones, en virtud de las cuales se han ido perfilando los contornos del citado derecho hasta alcanzar la plena articulación jurídica con que cuenta hoy día.

Concretamente, el mencionado texto legal “*se preocupa fundamentalmente de establecer el ámbito de protección de la intimidad, definiendo para ello qué se consideran intromisiones legítimas e ilegítimas*” MORENO BOBADILLA.²⁰ De este modo, conforme al tenor literal del art. 8.1 LO 1/1982, de 5 de mayo, “*no se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley*”. De ello se desprende que, tal y como ya se explicó al abordar los principios rectores, las injerencias que inciden en el ámbito de los derechos fundamentales —en este caso, las diligencias de investigación de carácter tecnológico que puedan adoptarse en el curso de la instrucción penal— tan solo pueden reputarse legítimas cuando en ellas concurren determinados presupuestos previstos legalmente.

Conviene señalar, además, que, tal y como cabría anticipar, no resulta infrecuente que en la aplicación práctica del ordenamiento constitucional se planteen situaciones de conflicto entre los distintos derechos fundamentales. De ahí que la tesis defendida mayoritariamente por la doctrina sea, precisamente, la que entiende que el ordenamiento jurídico español no reconoce derechos de carácter absoluto, pues su ejercicio ha de ser coherente, dentro de un entramado jurídico que preserve el núcleo esencial de cada uno de ellos en relación con los demás.²¹

Por otra parte, en virtud del reconocimiento autónomo que media entre los diferentes derechos enunciados en el art. 18 CE, se da la circunstancia de que en determinadas actuaciones o diligencias de investigación de naturaleza tecnológica limitan el

²⁰ Ibid., pág. 41.

²¹ Ibid., pág. 39.

derecho a la intimidad personal y familiar (art. 18.1 CE) sin que, por ello, se produzca simultáneamente la afectación o vulneración de otros, como bien pudiera ser el derecho al secreto de las comunicaciones (art. 18.3 CE). Tal es el caso de la utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización (arts. 588 *quinquies* a, b y c LECrim). [Vid. STS 141/2020]²²

Lo manifestado en el párrafo anterior es de importantísima utilidad práctica, pues tal y como aduce CALAZA LÓPEZ, “*la diferencia entre la lesión de un derecho fundamental u otro es muy relevante, por cuanto, entre tanto la intromisión en el derecho al secreto de las comunicaciones requiere, en todo caso, una previa y expresa autorización judicial; la inmersión en el derecho a la intimidad, en una primera incautación a cargo de la policía judicial, y, a saber, por extensión, en el entorno virtual, podrá acometerse sin esta previa autorización, en caso de urgencia*” (art. 588 *sexies* c 4 LECrim).²³

En definitiva, tal y como concluye la autora anteriormente citada, “*la injerencia en el secreto de las comunicaciones requiere, sin duda ni excepción, previa autorización judicial, por exigencia del art. 18.3 CE, mientras que la diligencia que afecta a la intimidad se encuentra, sin embargo, legalmente conferida a la propia autoridad de las fuerzas del orden, siempre que resulte justificada con arreglo a los criterios de urgencia y necesidad y que cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto*”.²⁴

III.III. Derecho fundamental al secreto de las comunicaciones (art. 18.3 CE)

El derecho fundamental al secreto de las comunicaciones constituye una garantía objetiva, es decir, extiende su protección con independencia del contenido o el soporte en que tenga lugar la comunicación misma. Sin embargo, la tutela que otorga el art. 18.3 CE no es, como ya adelantábamos en el epígrafe anterior, absoluta, pues la concede “*salvo*

²² STS 141/2020, de 13 de mayo. “*El conocimiento por los poderes públicos, en el marco de una investigación penal, de la ubicación espaciotemporal del sospechoso, encierra una injerencia de menor intensidad que otros actos de investigación perfectamente imaginables*”.

²³ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, págs. 301-302.

²⁴ Ibid., pág. 302.

resolución judicial”.²⁵ Sin perjuicio de lo anterior, de acuerdo con la STC 114/1984, existe “*la presunción iuris et de iure de que lo comunicado es secreto*”.²⁶ En consecuencia, aun cuando el contenido de una conversación carezca de relevancia o no se revele en ella información alguna relativa a la esfera privada de los interlocutores, la mera captación de dicha comunicación supondría, por sí misma, una vulneración del secreto de las comunicaciones.²⁷

En lo que respecta a los medios objeto de protección, el art. 18.3 CE opta por emplear el término “*comunicaciones*” en un sentido amplio, pues la mención expresa que hace a las de índole postal, telegráfica y telefónica no debe entenderse en un sentido restrictivo, sino meramente ejemplificativo. De este modo, la tutela que dispensa el referido precepto constitucional se extiende a todos los medios de comunicación conocidos en el momento de su aprobación, así como a aquellos que han surgido o puedan desarrollarse con posterioridad.²⁸

Por último, en lo que se refiere a la vulneración del referido derecho, y siguiendo a DÍAZ REVORIO, “*desde el punto de vista constitucional, bastaría en principio una finalidad no contradictoria con la norma fundamental para adoptar una medida de interceptación de las comunicaciones, con el cumplimiento de los demás requisitos aplicables*”.²⁹ Estarían comprendidos, en este punto, fines como la seguridad nacional o la protección de los derechos y las libertades de los demás.

²⁵ DÍAZ REVORIO, F. Javier. “El derecho fundamental al secreto de las comunicaciones”. “*Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*”, núm. 59, 2006, pág. 162.

²⁶ STC 114/1984, de 29 de noviembre, FJ núm. 7.

²⁷ ESPÍN, Eduardo. “Lección 10: Los derechos de la esfera personal”. “*Manual de Derecho Constitucional*”, Vol. I, 2022, pág. 232.

²⁸ DÍAZ REVORIO, F. Javier. Ob. cit. pág. 162.

²⁹ Ibid., pág. 168.

IV. CATÁLOGO DE MEDIDAS

La reforma operada por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, trajo consigo la incorporación, en el Título VIII —“*De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución*”— del Libro II —*Del sumario*—, diversos y novedosos capítulos orientados al análisis y examen de las mencionadas diligencias. El primero de ellos, esto es, el Capítulo IV —relativo a las disposiciones comunes y que ya fue objeto de estudio en el presente trabajo—, prefigura la regulación de las medidas que, a lo largo de los capítulos inmediatamente siguientes, son desglosadas y desarrolladas con cierta exhaustividad.³⁰

No obstante, como bien sostiene CALAZA LÓPEZ, “*debido a la velocidad, práctica fugacidad, de las TICs, no resulta fácil mantener actualizado*” el catálogo de medidas.³¹ En este sentido, algunos autores como PÉREZ GIL, que tilda al repertorio de medidas de “*inacabado*”,³² estiman insuficiente la reforma efectuada por la ley orgánica antes mencionada. Incluso se ha llegado a afirmar que la norma, a pesar de que su aprobación se hacía absolutamente necesaria para colmar la deficitaria regulación existente hasta el momento, “*solo es comprensible como solución provisional y parcial para una necesidad acuciante del proceso penal español: una anhelada reforma integral de la LECrim (¡que data de 1882!)*” PÉREZ GIL.³³

En cualquier caso, con independencia de que su amplitud pueda reputarse suficiente o no, el elenco de medidas contempladas se articula conforme a la siguiente sistematización:

³⁰ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 303.

³¹ Ibid.

³² PÉREZ GIL, Julio. “Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución”. “*Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli*”. 2018, pág. 3.

³³ Ibid., pág. 2.

Capítulo V arts. 588 <i>ter a</i> / 588 <i>ter m</i>	Interceptación de las comunicaciones telefónicas y telemáticas
Capítulo VI arts. 588 <i>quater a</i> / 588 <i>quater e</i>	Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos
Capítulo VII arts. 588 <i>quinquies a</i> / 588 <i>quinquies c</i>	Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización
Capítulo VIII arts. 588 <i>sexies a</i> / 588 <i>sexies c</i>	Registro de dispositivos de almacenamiento masivo de información
Capítulo IX arts. 588 <i>septies a</i> / 588 <i>septies c</i>	Registros remotos sobre equipos informáticos
Capítulo X arts. 588 <i>octies</i>	Medidas de aseguramiento

IV.I. Interceptación de las comunicaciones telefónicas y telemáticas

Este invasivo acto de investigación se revela como un instrumento de singular eficacia en la averiguación de ciertos ilícitos y en la identificación de sus responsables. Su operativa consiste, esencialmente, en la interceptación de lo comunicado a través de cualquier dispositivo susceptible de facilitar comunicaciones telefónicas o telemáticas, que comprende tanto al sujeto presuntamente implicado en la conducta delictiva —para lo cual es imprescindible que ostente la condición de investigado— como a los terceros que se vean involucrados en un acto de comunicación con él.³⁴

El ámbito objetivo de aplicación de esta diligencia de investigación, a pesar de su elevado grado de intromisión, en modo alguno puede extenderse de manera ilimitada o considerarse desprovisto de condicionamiento alguno, pues su alcance se halla estrictamente circunscrito a aquellas actuaciones que se encuentren expresamente tipificadas dentro de alguno de los cuatro bloques de ilícitos penales que se exponen a continuación: 1.º “*Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión*” (art. 579.1 LECrim); 2.º “*Delitos cometidos en el seno de un grupo u organización criminal*” (art. 579.1 LECrim); 3.º “*Delitos de terrorismo*” (art. 579.1 LECrim); 4.º “*Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o*

³⁴ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, págs. 308-309.

servicio de comunicación” (art. 588 *ter a* LECrim).³⁵ La inclusión de este último supuesto, tal y como acertadamente expone LÓPEZ FERIA, obedece al hecho de que *“los delitos cometidos a través de las nuevas tecnologías difícilmente pueden investigarse a través de otros medios, de suerte que, la interceptación de las comunicaciones y, en particular, las telemáticas, puede ser en ocasiones la única vía de investigación criminal de los ilícitos que se cometen a través de la red, de manera que, en este caso, el fundamento de la proporcionalidad no es la gravedad del delito, sino el medio a través del cual se comete el mismo”*.³⁶

Por su parte, el art. 588 *ter b* LECrim preceptúa, en relación a los dispositivos que pueden ser inspeccionados, que estos *“han de ser aquellos habitual u ocasionalmente utilizados por el investigado”*, tanto si ostenta su titularidad como si es un mero usuario. Asimismo, el precepto dispone que *“podrán intervenir los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad”*. Incluso se contempla la posibilidad de intervenir la infraestructura técnica de comunicación perteneciente a una tercera persona siempre que concurren los requisitos siguientes (art. 588 *ter c* LECrim): *“1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o 2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad”*. Cabe igualmente la autorización de la medida cuando el dispositivo objeto de investigación sea utilizado de forma maliciosa por personas ajenas a su titular por vía telemática y sin conocimiento de aquel.

En función del medio empleado para efectuar la comunicación, estaremos bien ante la *“comunicación telefónica”*, bien ante la *“comunicación telemática”*. La primera tendrá lugar cuando el mensaje que se comunica sea generado desde un teléfono, mientras que la segunda se producirá cuando se utilice un sistema informático. *“No obstante, nos encontramos con que hoy en día los teléfonos inteligentes (‘smartphones’) mezclan en un mismo dispositivo las capacidades de un teléfono y de un ordenador y, por tanto, podrían ser catalogadas como comunicaciones mixtas”* LÓPEZ FERIA.³⁷

³⁵ Ibid., pág. 309.

³⁶ LÓPEZ FERIA, Alfonso. “Nuevas tecnologías e interceptación de las comunicaciones telefónicas y telemáticas”. “*Revista española de derecho militar*”, núm. 111-112, 2019, pág. 224.

³⁷ Ibid., pág. 216.

Especial mención merece la interceptación de aquellas comunicaciones que se desarrollan por radio, cuya naturaleza presenta ciertas singularidades desde la perspectiva del control judicial. Tal y como razona la STS 695/2013, “*las captaciones de conversaciones radiotelegráficas, en frecuencia de uso público, no precisan autorización judicial, porque precisamente por ser de uso público y siendo esto conocido por los usuarios, ello implica una implícita aceptación de la posibilidad de captación*”.³⁸

Por otro lado, respecto a los requisitos que habrá de reunir la solicitud de la autorización judicial que pretenda la adopción de esta medida, encontramos que el art. 588 *ter* d LECrim, dispone que, además de las exigencias contenidas en el art. 588 *bis* b LECrim, la solicitud comprenderá:

- “a) la identificación del número de abonado, del terminal o de la etiqueta técnica,*
- b) la identificación de la conexión objeto de la intervención o*
- c) los datos necesarios para identificar el medio de telecomunicación de que se trate”.*

A su vez, el apartado segundo del referido artículo establece que “*para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos:*

- a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta.*
- b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.*
- c) La localización geográfica del origen o destino de la comunicación.*
- d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos”.*

En consecuencia, de lo anterior se infiere que los datos obtenidos en el seno de una intervención como la que es objeto de análisis en el presente epígrafe afectan a la esfera del derecho a la intimidad del art. 18.1 CE y/o al derecho a la protección de datos de carácter personal del art. 18.4 CE, y no únicamente al secreto de las comunicaciones consagrado en el art. 18.3 CE, puesto que cabe la posibilidad de orientar o dirigir la medida a la recopilación de información ajena al contenido comunicativo principal.

³⁸ STS 695/2013, de 22 de julio.

Según se desprende de lo preceptuado por el art. 588 *ter* e LECrim, existe, además, un deber de colaboración para garantizar la eficacia de las diligencias consistentes en la interceptación de las comunicaciones. En primer lugar, la norma impone, tanto a los prestadores de servicios de telecomunicaciones como a quienes contribuyan a facilitar las mismas a través del teléfono o cualquier otro medio o sistema de comunicación telemática, lógica o virtual, la obligación de proporcionar al Juez, al MF y a los agentes de la Policía Judicial que llevan a cabo la investigación toda la asistencia necesaria para la ejecución de la medida. El mencionado artículo dispone, en segundo lugar, una obligación de secreto para todos los sujetos requeridos a prestar colaboración, a fin de preservar la confidencialidad de la investigación. En último lugar, se advierte que quienes “*incumplieren los anteriores deberes podrán incurrir en delito de desobediencia*”.³⁹

En lo que se refiere al desarrollo de la diligencia, concretamente la captación de la comunicación telefónica, encontramos que corresponde a los órganos de la Policía Judicial la ejecución material del seguimiento de las comunicaciones intervenidas, así como su grabación o consignación en soportes magnéticos o electrónicos. Los originales de dichas grabaciones deben remitirse a la Sección de instrucción del Tribunal de instancia del que penda el procedimiento de que se trate, “*bien para su escucha por el juzgador, bien para su transcripción bajo la fe del LAJ*” LÓPEZ YAGÜES.⁴⁰ Sin embargo, tales actuaciones resultan, en la práctica, de muy difícil asunción cuando el volumen de las conversaciones intervenidas alcanza proporciones cuantitativamente inabarcables. Por ello, ante la inviabilidad del sistema de audición personal por parte de los funcionarios antes aludidos, los arts. 588 *ter* e y f LECrim otorgan plena legitimación normativa al modelo operativo que venía aplicándose *de facto*: el denominado SITEL.⁴¹ Dicho sistema se basa “*en la gestión de*

³⁹ Art. 588 *ter* e LECrim.

⁴⁰ LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 262.

⁴¹ <https://www.iberley.es/temas/sistema-sitel-interceptacion-las-comunicaciones-telefonicas-telematicas-proceso-penal-63164> “El Sistema Integrado de Interceptación Telefónica (SITEL) es un sistema utilizado por el Ministerio del Interior —específicamente por la Policía Nacional, la Guardia Civil y el Servicio de Vigilancia Aduanera— para la interceptación legal de las comunicaciones telefónicas y telemáticas en el marco de las investigaciones penales.” [RD 424/2005, de 15 de abril]

un archivo centralizado en el Ministerio del Interior en el que son consignadas las comunicaciones objeto de intervención, sin margen de manipulación —si no es dejando rastro de la misma en el disco duro central— y cuyos resultados son consignados en soporte DVD” LÓPEZ YAGÜES.⁴²

En atención a los indicado por el ya mencionado art. 588 *ter f* LECrim, la Policía Judicial ha de remitir al instructor, con la periodicidad que este determine, tanto las grabaciones completas de las comunicaciones intervenidas como las transcripciones de aquellos fragmentos que se considere que revisten de especial relevancia para la investigación. Dichos materiales se presentarán en soportes digitales diferenciados, a fin de mantener un control preciso de la información que los mismos contienen. En cada caso se expresará claramente el origen y destino de las comunicaciones incluidas. Paralelamente, se adoptarán las medidas técnicas necesarias —como la aplicación de un sistema de sellado o firma electrónica avanzada o cualquier otro sistema de verificación suficientemente fiables— para garantizar que los datos trasladados desde el ordenador central a los soportes digitales conserven plenamente su autenticidad e integridad.

En lo que atañe al lapso temporal de eficacia de la medida, el art. 588 *ter g* LECrim delimita con precisión su extensión al fijar un término inicial máximo de tres meses, prorrogable por periodos sucesivos de igual duración hasta alcanzar un tope total de dieciocho meses. Aunque el precepto no explicita el modo en que tales prórrogas han de acordarse, una interpretación sistemática del mismo conduce sin dificultad a afirmar que toda ampliación temporal requiere un pronunciamiento judicial formalmente adoptado y suficientemente razonado, en el que se expongan con notable claridad las circunstancias concretas que legitiman la prolongación de la medida. No puede obviarse, en este extremo, que cuanto mayor es la proyección en el tiempo de la medida, más se incrementa el potencial intrusivo de la misma y, por ende, mayor es el riesgo de inobservancia del principio de proporcionalidad.⁴³

Por último, resulta pertinente dedicar unas líneas al tratamiento que el art. 588 *ter i* LECrim hace respecto al acceso de las partes a las grabaciones obtenidas durante la ejecución de la medida. De acuerdo con el tenor literal del referido artículo, “*alzado el secreto*

⁴² LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 262.

⁴³ Ibid., págs. 263-264.

y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas". Naturalmente, lo dispuesto responde a la exigencia de asegurar la igualdad de armas, garantizándose con ellos que las partes puedan conocer, examinar y valorar el contenido de las comunicaciones intervenidas una vez finalizada la restricción, en aras del respeto a las garantías procesales. No obstante, para aquellos supuestos en los que las grabaciones contuvieran datos referidos a aspectos de la vida íntima de las personas, se prevé que *"solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos"*. En cualquier caso, la eventual omisión de parte del contenido de la grabación en la transcripción facilitada deberá hacerse constar de forma expresa.

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

La intensidad atribuible a esta medida alcanza su expresión máxima a la luz de lo previsto en el art. 588 *quater* a LECrim, que autoriza su despliegue tanto en espacios abiertos o de acceso público como en lugares cerrados, pues la norma se refiere expresamente a estos últimos, incluyendo el domicilio de los sujetos investigados. De esta suerte se vislumbra un horizonte de injerencia que alcanza el reducto más sagrado de la privacidad, pues el precepto no parece sustraer de su campo de aplicación ni siquiera aquellas estancias o dependencias del domicilio donde transcurren las manifestaciones más intensas de la intimidad personal. Con mayor razón aún, si cabe, habida cuenta de que *"la captación sonora se complementa con la posible captación y consignación de imágenes que permitirán reflejar la escena que se desarrolla en el interior de la vivienda o lugar en el que se hallen los comunicantes"* LÓPEZ YAGÜES.⁴⁴

En lo que concierne a los presupuestos habilitantes para la adopción de esta medida, cabe afirmar que su acuerdo exige, de manera insoslayable, la concurrencia de indicios racionales de criminalidad referidos a un sujeto concreto, derivados de su potencial implicación en alguno de los delitos contemplados en el art. 588 *quater* b LECrim. A ello ha de sumarse la existencia de razones sólidas y debidamente acreditadas que permitan anticipar, con fundamento, que la persona investigada busca reunirse y comunicarse con otros encausados e, incluso, con terceros ajenos al procedimiento.⁴⁵

⁴⁴ Ibid., pág. 265.

⁴⁵ Ibid.

En concreto, el apartado segundo del art. 588 *quater* b LECrim requiere, en primer lugar, que los actos objeto de pesquisa sean subsumibles en alguna de las siguientes categorías delictivas:

“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.”⁴⁶

Asimismo, ha de resultar racionalmente previsible que la utilización de los dispositivos técnicos proporcionará “datos esenciales y de relevancia probatoria para el esclarecimiento de los hechos y la identificación de su autor”.⁴⁷

No obstante, el elenco de ilícitos que habilita la adopción de esta medida —así como, en su caso, la interceptación de las comunicaciones telefónicas y telemáticas—, es calificado, en palabras de LÓPEZ YAGÜES, como un marco “*extraordinariamente amplio y que el legislador debiera haber recortado, reservando la posible adopción de una medida [...] a las solas causas por delito de terrorismo o criminalidad organizada*”.⁴⁸ Todo ello por considerar que la ejecución de tales medidas en aquellas conductas delictivas para las que se prevé una pena de prisión de, al menos, tres años, difícilmente puede superar el juicio de la proporcionalidad.⁴⁹

Por su parte, en lo concerniente al contenido de la resolución judicial que autorice la medida, el art. 588 *quater* c LECrim exige, además de lo previsto en el art. 588 *bis* c LECrim —disposiciones comunes a cualquier resolución judicial que ordene la práctica, sea cual sea, de las diligencias previstas—, “una mención concreta al lugar o dependencias, así como a los

⁴⁶ Se constata, en este extremo, que la enumeración contenida en el apartado segundo del art. 588 *quater* b LECrim reproduce literalmente el mismo espectro de ilícitos penales previstos en el art. 579.1 LECrim —que ya fueron expuestos al abordar la interceptación de las comunicaciones telefónicas y telemáticas—.

⁴⁷ Art. 588 *quater* b 2 b) LECrim.

⁴⁸ LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 265.

⁴⁹ Ibid.

encuentros del investigado que van a ser sometidos a vigilancia".⁵⁰ Es por eso por lo que, a pesar del amplio margen que, en una lectura inicial, parece conferir el art. 588 *quater* LECrim, su ámbito de aplicación no se proyecta de manera indiscriminada sobre el conjunto de las comunicaciones mantenidas por la persona investigada, sino que se limita al específico acto de comunicación objeto de la intervención autorizada. En consecuencia lógica con lo anterior, *"la grabación de conversaciones en otros encuentros o la captación de imágenes en esos momentos precisarán de una nueva autorización judicial"* MORENO CATENA.⁵¹

En lo que atañe al control judicial de la medida, cabe destacar que el art. 588 *quater* d LECrim, en estricta observancia de lo establecido por el art. 588 *bis g* LECrim, dispone que la Policía Judicial consignará ante la autoridad judicial el soporte original o, en su defecto, una copia electrónica auténtica, de las grabaciones e imágenes obtenidas, acompañándolo, asimismo, de una transcripción de aquellos fragmentos de las conversaciones que resulten de interés. En este punto, y de acuerdo con lo sostenido por MORENO CATENA, *"sorprende que la ley exija a la Policía remitir al juez una copia, lo que supone que los originales se conservarán o se podrán mantener, en las propias dependencias y archivos policiales sin ningún control judicial"*.⁵²

En suma, tal como se ha evidenciado a lo largo de este epígrafe y conforme a lo señalado por la STS, Sala Segunda, núm. 718/2020, de 28 de diciembre, resulta evidente que *"la utilización de un dispositivo de esta naturaleza desnuda al investigado de su propia vida familiar, lo coloca a merced de los investigadores, que se convierten así en privilegiados conocedores de una información generada en el día a día y que desborda con creces aquello que pueda resultar de interés para el delito investigado"*.⁵³

⁵⁰ Art. 588 *quater c* LECrim.

⁵¹ MORENO CATENA, Víctor. "Lección 18: Actos de investigación que afectan a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones". *"Derecho Procesal Penal"*. Valencia: Tirant lo Blanch, 2025, pág. 328.

⁵² Ibid., pág. 329.

⁵³ STS 718/2020, de 28 de diciembre, FJ 2.1.2

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

Ante todo, conviene destacar que lo previsto en el Capítulo VII del Título VIII del Libro II de la LECrim no configura una única modalidad de diligencia, sino que articula, en puridad, dos medidas de investigación claramente diferenciadas, cuya distinción reviste especial trascendencia práctica. Así, de un lado, se contempla la captación y grabación de la imagen del investigado en espacios de acceso público mediante dispositivos técnicos, actuación que no requiere autorización judicial de ninguna clase —en la medida en que el sujeto no puede albergar una legítima expectativa de reserva respecto a su conducta en lugares públicos—. De otro lado, se regula una medida de mayor alcance, consistente en el seguimiento y localización del investigado mediante la colocación de dispositivos técnicos de rastreo, cuya adopción, de acuerdo con el art. 588 *quinquies* b LECrim, queda condicionada a la concurrencia de acreditadas razones de necesidad.⁵³

a) Captación de imágenes en lugares o espacios públicos

En cuanto a la primera de las diligencias antes mencionada, esto es, la captación de imágenes, por cualquier medio técnico, del investigado, encontramos que su ejecución compete a la Policía Judicial sin que resulte preceptiva, como ya se ha indicado al comienzo del presente epígrafe, autorización judicial alguna —siempre que, claro está, la persona investigada se halle en lugares o espacios públicos—. No sería admisible, por consiguiente, su práctica —sin habilitación— en entornos cerrados como, por ejemplo, lo es el propio domicilio.⁵⁴

Asimismo, dicha actuación podrá autorizarse y llevarse a cabo, conforme dispone expresamente el art. 588 *quinquies* a LECrim, incluso cuando incida sobre personas ajenas al investigado, siempre que la omisión de tal proceder denote una rebaja significativa en la

⁵³ RAYÓN BALLESTEROS, María Concepción. “Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015”. *“Anuario Jurídico y Económico Escurialense”*, LII (2019), págs. 198-199.

⁵⁴ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, pág. 315.

eficacia de la vigilancia o cuando existan indicios sólidos que acrediten la vinculación de aquellas personas con el sujeto sometido a investigación y con las circunstancias que motivan el procedimiento.⁵⁵

b) Utilización de dispositivos o medios técnicos de seguimiento y localización

En un primer examen de la previsión contenida en el art. 588 *quinquies* b LECrim, se advierte que esta diligencia de investigación se concibe, en su planteamiento inicial, como un instrumento orientado preferentemente al seguimiento y/o localización de personas. Aun así, se impone reconocer que no subsiste inconveniente alguno que excluya su posible utilización para la vigilancia de objetos o elementos materiales relacionados con el hecho delictivo.⁵⁶

Llegados a este punto, tal como acertadamente señala LÓPEZ YAGÜES, la cuestión que cabe plantearse entonces no es otra que determinar si, cuando la medida se orienta a localizar o seguir cosas u objetos, resulta o no exigible la autorización judicial prevista para los supuestos en que la vigilancia incide sobre personas.⁵⁷

En efecto, de acuerdo con la STS, Sala Segunda, núm. 798/2013, de 5 de noviembre, la utilización de dispositivos técnicos para localizar o seguir, por ejemplo, una embarcación o vehículo que transporta sustancias o mercancías ilegales, “*no vulnera el derecho fundamental al secreto de las comunicaciones o supone una inferencia excesiva sobre el derecho fundamental a la intimidad a los efectos de exigir un control jurisdiccional previo*”.⁵⁸

Ahora bien, en aquellos supuestos en los que resulte preceptivo el control judicial previo, la resolución habilitante —esto es, el auto que autorice la práctica de la medida— deberá determinar con precisión el medio técnico concreto que se empleará para llevar a cabo las labores de seguimiento y localización respecto del sujeto sometido a investigación, siempre que, desde luego, se acrediten fundadas razones que justifiquen su necesidad, idoneidad y proporcionalidad.⁵⁹

⁵⁵ Ibid.

⁵⁶ LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, pág. 269.

⁵⁷ Ibid.

⁵⁸ STS 798/2013, de 5 de noviembre, FJ 11.

En cambio, cuando concurren circunstancias de urgencia que permitan inferir razonablemente que, de no procederse rápidamente a la instalación del dispositivo o medio técnico de seguimiento y localización, la investigación podría resultar irremediablemente comprometida, la Policía Judicial podrá ejecutar dicha colocación, quedando obligada a informar a la autoridad judicial de manera tan inmediata como sea posible y, en todo caso, en el plazo máximo de veinticuatro horas (art. 588 *quinquies* b 4 LECrim).

De forma análoga a lo previsto para la interceptación de las comunicaciones telefónicas y telemáticas, el art. 588 *quinquies* b 3 LECrim establece un deber específico de colaboración para los prestadores de servicios, agentes y demás posibles intervinientes, consistente en facilitar al Juez, al MF y a los funcionarios de la Policía Judicial, la asistencia necesaria para su correcta implementación, so pena de incurrir en un delito de desobediencia.⁶⁰

En cuanto a la temporalidad de la medida, cabe afirmar que esta no se concibe, naturalmente, como un instrumento de duración indefinida, sino que su vigencia queda taxativamente limitada a un plazo máximo de tres meses, computados desde la fecha en que se dicte la pertinente resolución judicial. No obstante, de forma excepcional, podrán concederse prórrogas sucesivas por el mismo o inferior plazo, de modo que la duración total acumulada no supere los dieciocho meses. Dichas prórrogas excepcionales, conforme a la lógica inherente a su naturaleza, habrán de justificarse sobre la base de una evaluación fundada a la vista de los resultados obtenidos con la medida (art. 588 *quinquies* c 1 LECrim).

Finalmente, el art. 588 *quinquies* c LECrim dispone que la Policía Judicial habrá de entregar al Juez, a su solicitud o, en todo caso, al concluir las actuaciones de investigación, los soportes originales o copias electrónicas auténticas que contengan los datos obtenidos. Asimismo, la información recabada mediante los dispositivos técnicos de seguimiento y localización deberá ser objeto de una custodia rigurosa a fin de impedir su uso indebido.

⁵⁹ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 316.

⁶⁰ Ibid., pág. 317.

IV.IV. Registro de dispositivos de almacenamiento masivo de información

Al abordar esta diligencia de investigación —prevista en el Capítulo VIII del Título VIII del Libro II de la LECrim—, resulta imprescindible señalar, en primer lugar, que nos hallamos ante dispositivos capaces de albergar volúmenes de información verdaderamente amplios y de la más variada naturaleza, cuyo examen puede adquirir una relevancia singular en la tarea de reconstrucción y esclarecimiento de los hechos sometidos a investigación. En concreto, por dispositivos de almacenamiento masivo de información ha de entenderse el conjunto de soportes materiales destinados a la concentración y preservación sistemática de datos digitales, esto es, “*los discos de ordenador, internos y externos, memorias, DVD o CD, pen drive, dispositivos telefónicos, etc.*” MORENO CATENA.⁶¹

Ahora bien, aunque esta actuación se enmarca en el contexto del registro domiciliario, por así preverlo el art. 588 *sexies* a LECrim, —ámbito en el cual el legislador exige una resolución judicial específica que habilite el acceso al contenido de los dispositivos intervenidos—, lo cierto es que “*los agentes de la Policía Judicial pueden encontrarse ante un dispositivo de este tipo en cualquier situación, incluido un cacheo en la vía pública, y en este caso la ley manda que se ponga el hecho en conocimiento del juez con el fin de que este otorgue la autorización para acceder a la información del dispositivo si lo considera indispensable*” MORENO CATENA.⁶² Concretamente, el art. 588 *sexies* b LECrim dispone que la aprehensión de tales dispositivos podrá llevarse a cabo “*con independencia de un registro domiciliario*”.

En cuanto a los presupuestos que ha de reunir la resolución judicial mediante la que se autorice la práctica de la medida, encontramos que el art. 588 *sexies* c LECrim establece que el juez de instrucción “*fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos*”. Del mismo modo, la resolución deberá establecer las condiciones oportunas para garantizar tanto la conservación íntegra de la información como su adecuada custodia, de manera que, en su caso, sea posible la práctica de un dictamen pericial (art. 588 *sexies* c 1 LECrim).

En este punto, a diferencia de lo previsto para otras diligencias de igual grado de

⁶¹ MORENO CATENA, Víctor. “Lección 18: Actos de investigación que afectan a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 330.

⁶² Ibid.

injerencia, y de acuerdo con lo expuesto por MORENO CATENA, “*llama la atención que la ley no se refiera a ningún tipo delictivo concreto ni que establezca un rango mínimo de pena a partir del cual resulte procedente la adopción de esta medida*”.⁶³ En efecto, la entidad o gravedad del ilícito objeto de investigación resulta, en principio, un factor secundario, toda vez que la habilitación judicial de esta medida queda determinada por los juicios de necesidad y proporcionalidad.⁶⁴

Por su parte, el apartado tercero del art. 588 *sexies* c LECrim contempla la posibilidad de que los encargados de ejecutar el registro o quienes tengan acceso al sistema informático —o a una parte de él— puedan ampliar o extender su actuación a la búsqueda de datos ubicados en otro sistema informático. Para ello es necesario, indudablemente, que existan razones fundadas y que dichos datos resulten “*lícitamente accesibles por medio del sistema inicial o estén disponibles para este*”. Tal ampliación del registro habrá de ser autorizada por el instructor, salvo que tal facultad ya hubiese sido expresamente concedida en la resolución inicial.

No obstante, al igual que ocurre con otras medidas de investigación tecnológica —por ejemplo, la utilización de dispositivos o medios técnicos de seguimiento y de localización—, “*cuando existan razones de urgencia y haya un interés constitucional legítimo (concepto jurídico indeterminado, que se podría concretar en la investigación y persecución de un hecho delictivo) que haga imprescindible la medida, la Policía Judicial podrá examinar directamente los datos contenidos en el dispositivo, dando cuenta a la autoridad judicial a la mayor brevedad, y en todo caso en veinticuatro horas*” MORENO CATENA.⁶⁵

Por último, conviene tener presente que el art. 588 *sexies* c 2 LECrim busca evitar la privación de tales dispositivos al interesado, pues dispone que su incautación se abstendrá “*cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos*”.

⁶³ Ibid., pág. 331.

⁶⁴ Ibid.

⁶⁵ Ibid.

IV.V. Registros remotos sobre equipos informáticos

La inclusión de esta singular diligencia de investigación en el repertorio de medidas era, prácticamente, ineludible para la reforma operada por la LO 13/2015. Era lógico prever que el registro de equipos informáticos mediante su acceso físico exigía también la posibilidad de acceder a ellos mediante su registro remoto. Pese a ello, una década después, *“la instalación de ‘spyware’ para acceder de manera remota a equipos informáticos es una medida que todavía resulta muy controvertida debido al grado de intromisión que implica en la esfera de privacidad de las personas”* BACHMAIER WINTER.⁶⁶

En realidad, lo que incrementa notablemente el potencial intrusivo de esta medida en comparación con cualesquiera otras distintas es, entre otros aspectos, que *“a diferencia del registro domiciliario y del registro físico de un ordenador hallado durante la entrada en un domicilio o en otro lugar público, en el registro remoto el afectado no es conocedor del acceso a sus datos”*. BACHMAIER WINTER.⁶⁷ La razón de que el investigado permanezca totalmente ajeno al dispositivo de vigilancia no es otra, como resulta fácilmente deducible, que preservar la eficacia de la medida, *“pues de otro modo carecería de utilidad”* CALAZA LÓPEZ.⁶⁸

Exactamente, esta gravosa medida consiste en la instalación remota —esto es, sin necesidad de acceso físico al dispositivo— *“en cualquier equipo informático, dispositivo electrónico o sistema digital de almacenamiento de datos, del investigado, de un ‘software’ o programa informático —coloquialmente conocido como un ‘troyano’ en homenaje al caballo de Troya, usado, según cuenta la mitología, por los aqueos como una estrategia para introducirse en la ciudad fortificada de Troya—, que permite acceder, secretamente, a su contenido”* CALAZA LÓPEZ.⁶⁹ Todo ello, naturalmente, con el exclusivo propósito de recabar datos relevantes y directos sobre el hecho delictivo.

⁶⁶ BACHMAIER WINTER, Lorena. “Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015”. *“Boletín del Ministerio de Justicia”*, núm. 2195, 2017, pág. 6.

⁶⁷ Ibid., págs. 6-7.

⁶⁸ CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, pág. 320.

⁶⁹ Ibid.

Por supuesto, la adopción de esta medida tan agresiva exige que la investigación persiga delitos incluidos en alguno de los cinco bloques de ilícitos penales que aparecen recogidos en el art. 588 *septies* a 1 LECrim, y que son, a saber, los siguientes: a) “*Delitos cometidos en el seno de organizaciones criminales*”; b) “*Delitos de terrorismo*”; c) “*Delitos cometidos contra menores o personas con capacidad modificada judicialmente*”; d) “*Delitos contra la Constitución, de traición y relativos a la defensa nacional*”; e) “*Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación*”.

Por otro lado, en cuanto a los extremos que habrá de especificar la resolución judicial que autorice la medida, el art. 588 *septies* a 2 LECrim establece los siguientes:

“a) *Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.*

b) *El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el ‘software’ mediante el que se ejecutará el control de la información.*

c) *Los agentes autorizados para la ejecución de la medida.*

d) *La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.*

e) *Las medidas precisas para la 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”.*

De forma similar a lo que ocurría con el registro de dispositivos de almacenamiento masivo de información, el art. 588 *septies* a 3 LECrim contempla la posibilidad de extender el registro a la búsqueda de datos almacenados en otro sistema informático, para lo que será imprescindible que los agentes encargados de ejecutar la medida pongan este hecho en conocimiento del juez, quien podrá autorizar la ampliación.

Por su parte, el art. 588 *septies* b LECrim —rubricado “*deber de colaboración*”— obliga a “*los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro*” a proporcionar a los agentes que llevan a cabo la investigación toda la asistencia técnica y operativa necesaria para acceder al sistema, así como facilitar las labores de examen y visualización de los datos obtenidos. Ante este deber de colaboración “*solo quedan exceptuados el propio investigado o encausado, las personas que*

*están dispensadas de la obligación de declarar por razón de parentesco, y aquellas que no pueden declarar en virtud del secreto profesional” CALAZA LÓPEZ.*⁷⁰

Por último, el Capítulo IX del Título VIII del Libro II de la LECrim concluye con la disposición contenida en el art. 588 *septies* c, relativa a la duración de la medida. En efecto, la diligencia tendrá una duración inicial máxima de un mes, susceptible de ser prorrogada por iguales periodos, hasta alcanzar un límite máximo de tres meses.

IV.VI. Medidas de aseguramiento

La orden de conservación de datos se integra en el Capítulo X del Título VIII del Libro II de la LECrim, el cual consta de un único precepto —el art. 588 *octies*— destinado a regular un instrumento procesal cuyo propósito no es otro que preservar fuentes de prueba de naturaleza electrónica.⁷¹ Esta *“herramienta jurídica de gran utilidad práctica y que contribuye notablemente a mejorar la eficacia de las investigaciones relacionadas con los ciberdelitos, halla su origen y configuración en la llamada diligencia de conservación rápida de datos informáticos almacenados prevista en los arts. 16 y 17 del Convenio del Consejo de Europa sobre Ciberdelincuencia de 23 de noviembre de 2001”* MONTORO SÁNCHEZ.⁷² En consecuencia, se trata de una medida especialmente útil cuando los datos contenidos en un sistema informático se revelen especialmente proclives a sufrir una pérdida o alteración inminente.⁷³

De acuerdo con lo preceptuado por el art. 588 *octies* LECrim, tanto el MF como la Policía Judicial están facultados para requerir u ordenar, de manera autónoma y sin necesidad de previa autorización judicial, a cualquier persona física o jurídica *“la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes”*.

⁷⁰ Ibid., pág. 321.

⁷¹ MONTORO SÁNCHEZ, Juan Alejandro. “La orden de conservación de datos: una medida de aseguramiento de fuentes de prueba imprescindible para la investigación de los delitos de odio cometidos en línea”. *“Informática y Derecho: Revista Iberoamericana de Derecho Informático”*, núm. 13, 2023, págs. 125-126.

⁷² Ibid., pág. 126.

⁷³ Ibid.

En cualquier caso, la norma establece que los datos habrán de preservarse durante un plazo máximo de noventa días, susceptible de una única prórroga hasta que se autorice su entrega o, en su defecto, hasta alcanzar un límite total de ciento ochenta días. Asimismo, la persona requerida estará obligada a colaborar y a guardar secreto del desarrollo de esta medida, quedando sometida al régimen de responsabilidad previsto en el apartado tercero del art. 588 *ter* e LECrim (posibilidad de incurrir en delito de desobediencia).

VI. CONCLUSIONES

El análisis detallado de las medidas de investigación tecnológica a lo largo del presente trabajo ha permitido comprobar que, a pesar de haberse colmado la mayor parte de las lagunas existentes en esta materia, persisten algunas deficiencias que, aun habiendo transcurrido una década desde la entrada en vigor de la LO 13/2015, siguen generando ciertas dificultades en la práctica.

En síntesis, podríamos destacar, como principales problemas derivados de la adopción de estas diligencias, los tres siguientes:

1.º En el caso del registro de dispositivos de almacenamiento masivo de información —previsto en los arts. 588 *sexies* a, b y c LECrim— es especialmente llamativo, como ya se indicó en el epígrafe correspondiente a esta medida, el hecho de que la norma no especifique un tipo delictivo concreto ni un umbral mínimo de pena a partir del cual pueda ser autorizado dicho registro. La ausencia, por parte del legislador, de parámetros específicos para esta medida —que sí se establecen en otras diligencias de la misma intensidad— solo resulta comprensible si consideramos que los principios rectores pueden suplir esta carencia y orientar al juez de instrucción a la hora de decidir sobre la procedencia de su adopción (juicios de necesidad y proporcionalidad).

2.º Del mismo modo, sorprende que, en el caso de la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, el art. 588 *quater* d LECrim permita que la Policía Judicial entregue al juez únicamente una copia electrónica de las grabaciones e imágenes obtenidas. El hecho mismo de que los originales puedan permanecer en las dependencias policiales implica la ausencia de un control judicial efectivo sobre unos materiales especialmente sensibles desde el punto de vista de los derechos fundamentales del investigado. Además, esta previsión resulta un tanto contradictoria, pues, si se requiere autorización judicial para llevar a cabo la medida, carece de todo sentido que, una vez ejecutada, no exista un control judicial pleno en todos los casos.

3.º En relación con la interceptación de las comunicaciones telefónicas y telemáticas, encontramos que, como ya se advirtió en su momento, el listado de delitos que autorizan esta medida es sumamente extenso, ya que en la mayoría de conductas delictivas que llevan aparejada una pena mínima de tres años de prisión no concurren las notas de necesidad y proporcionalidad. Al igual que las penas, las medidas han de ser coherentes, en términos de proporcionalidad, con el hecho que se imputa, pues en caso contrario el

beneficio que se persigue con su adopción en modo alguno superará la lesión producida en los derechos fundamentales del investigado.

A pesar de estos y otros aspectos pendientes, puede concluirse que la reforma de 2015 arrojó más luces que sombras, si bien es cierto que se trataba de un objetivo relativamente fácil de lograr dado el casi inexistente marco normativo previo a la entrada en vigor de la LO 13/2015.

VII. BIBLIOGRAFÍA

ARRABAL PLATERO, Paloma. “Capítulo III: Obtención de la prueba tecnológica”. *“La Prueba Tecnológica: Aportación, Práctica y Valoración”*. Valencia: Tirant lo Blanch, 2020, pág. 184.

BACHMAIER WINTER, Lorena. “Registro remote de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015”. *“Boletín del Ministerio de Justicia”*, núm. 2195, 2017, pág. 6.

CALAZA LÓPEZ, Sonia. “Lección 16: Los actos de investigación (III): los actos de investigación restrictivos de Derechos fundamentales en el ámbito electrónico”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, págs. 304-305.

DÍAZ REVORIO, F. Javier. “El derecho fundamental al secreto de las comunicaciones”. *“Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú”*, núm. 59, 2006, pág. 162.

ESPÍN, Eduardo. “Lección 10: Los derechos de la esfera personal”. *“Manual de Derecho Constitucional”*, Vol. I, 2022, pág. 232.

ESPÍN LÓPEZ, Isidoro. “Los derechos fundamentales a la vida privada afectados por la investigación tecnológica y el fenómeno del entorno virtual”. *“Boletín del Ministerio de Justicia”*, núm. 2244, 2021, pág. 26.

GIMENO SENDRA, Vicente. “Lección 2: El principio de proporcionalidad. Los Derechos fundamentales de Derecho Judicial Orgánico. Los Derechos fundamentales materiales a la legalidad y al *non bis in idem*”. *“Manual de Derecho Procesal Penal”*, 2ª Edición, 2025, pág. 33.

GÓMEZ COLOMER, Juan Luis. “Lección 11ª: Los actos de investigación garantizados basados en las nuevas tecnologías”. *“Proceso Penal. Derecho Procesal III”*. Valencia: Tirant lo Blanch, 2025, pág. 256.

LÓPEZ FERIA, Alfonso. “Nuevas tecnologías e interceptación de las comunicaciones telefónicas y telemáticas”. *“Revista española de derecho militar”*, núm. 111-112, 2019, pág. 224.

LÓPEZ YAGÜES, Verónica. “Tema 11: Los actos de investigación (II)”. *“Derecho Procesal Penal”*. Valencia: Tirant lo Blanch, 2025, pág. 248.

MARTÍNEZ DE PISÓN CAVERO, José María. “El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional”. “*Anuario de filosofía del derecho*”, núm. 32, 2016, Universidad de La Rioja, pág. 410.

MONTORO SÁNCHEZ, Juan Alejandro. “La orden de conservación de datos: una medida de aseguramiento de fuentes de prueba imprescindible para la investigación de los delitos de odio cometidos en línea”. “*Informática y Derecho: Revista Iberoamericana de Derecho Informático*”, núm. 13, 2023, págs. 125-126.

MORENO BOBADILLA, Ángela. “El derecho a la intimidad en España”. “*Ars Boni et Aequi*”, Vol. 12, núm. 1, 2016, pág. 38.

MORENO CATENA, Víctor. “Lección 18: Actos de investigación que afectan a la intimidad, a la inviolabilidad del domicilio y al secreto de las comunicaciones”. “*Derecho Procesal Penal*”. Valencia: Tirant lo Blanch, 2025, pág. 328.

NIEVA FENOLL, Jordi. “Tema 6: La instrucción”. “*Derecho Procesal III (Proceso Penal) Adaptado a la Ley Orgánica 1/2025*”. Valencia: Tirant lo Blanch, 2025, pág. 215.

OCÓN GARCÍA, Juan. “Capítulo I: Delimitación del derecho fundamental del art. 18.3 CE”. “*El derecho fundamental al secreto de las comunicaciones ante nuevos escenarios tecnológicos*”. Programa de doctorado en Derecho y cambio social, 2020, Universidad de La Rioja, págs. 25-29.

PÉREZ GIL, Julio. “Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución”. “*Informatica giuridica e informatica forense al servizio della società della conoscenza: scritti in onore di Cesare Maioli*”. 2018, pág. 2.

RAYÓN BALLESTEROS, María Concepción. “Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015”. “*Anuario Jurídico y Económico Escurialense*”, LII (2019), págs. 198-199.

VIII. JURISPRUDENCIA

Sentencias del TC

STC 41/1998, de 24 de febrero | ECLI:ES:TC:1998:41 | BOE núm. 77, de 31 de marzo de 1998.

STC 70/2002, de 3 de abril | ECLI:ES:TC:2002:70 | BOE núm. 99, de 25 de abril de 2002.

STC 123/2002, de 20 de mayo | ECLI:ES:TC:2002:123 | BOE núm. 146, de 19 de junio de 2002.

STC 114/1984, de 29 de noviembre | ECLI:ES:TC:1984:114 | BOE núm. 305, de 21 de diciembre de 1984.

Sentencias del TS

STS 393/2012, de 29 de mayo | ECLI:ES:TS:2012:3789 |

STS 272/2017, de 18 de abril | ECLI:ES:TS:2017:1594 |

STS 141/2020, de 13 de mayo | ECLI:ES:TS:2020:881 |

STS 695/2013, de 22 de julio | ECLI:ES:TS:2013:4490 |

STS 718/2020, de 28 de diciembre | ECLI:ES:TS:2020:4436 |

STS 798/2013, de 5 de noviembre | ECLI:ES:TS:2013:5313 |