http://doi.org/10.22370/rcs.2020.76.2812

LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA EN EL PROCESO PENAL ESPAÑOL

TECHNOLOGICAL INVESTIGATION PROCEDURES IN THE SPANISH CRIMINAL PROCEEDING

PALOMA ARRABAL PLATERO*

Resumen

A finales del año 2015 el legislador español modificó su vetusta Ley de Enjuiciamiento Criminal (el texto original data de 1882) para introducir diligencias de investigación tecnológica en pro de una instrucción más moderna, actual, digital y, en todo caso, respetuosa con los derechos fundamentales de los ciudadanos. Este trabajo presenta una panorámica expositiva de estos actos de instrucción, cuya regulación, si bien necesaria, pudo ser más depurada. Así, la norma procesal penal incorpora unos preceptos comunes a medidas heterogéneas, algunas de las cuales resultan contradictorias y a ello añade la regulación de siete diligencias con distintos niveles de afectación a garantías constitucionales útiles en la investigación penal policial.

Palabras Clave

Proceso penal, diligencias de investigación, nuevas tecnologías, derechos fundamentales.

Abstract

At the end of 2015, the Spanish legislator modified its Law of Criminal Procedure (the original text dates from 1882) to introduce technological investigation procedures in favor of a more modern, current, digital

instruction and, in any case, respectful of rights fundamentals of citizens. This paper analyzes these acts of instruction, the regulation of which, although necessary, could have been more refined. Thus, the criminal procedural norm incorporates common precepts to heterogeneous measures, some of which are contradictory and the regulation of seven proceedings with different levels of affectation of fundamental rights useful in the criminal police investigation.

Keywords

Criminal proceedings, technological investigation procedures, fundamental rights.

I. INTRODUCCIÓN.

La investigación policial de los delitos se encuentra, desde hace ya tiempo, con una realidad, más tecnológica que analógica y necesita de las herramientas digitales y del marco legal adecuado para una instrucción eficaz a la vez que garantista. En este sentido, el legislador español introdujo la regulación de nuevas diligencias de investigación en la vigente Ley de Enjuiciamiento Criminal[1]. Esta reforma que, de nuevo, parchea una norma de 1882, resulta un conjunto de preceptos que, si bien permiten a los investigadores policiales tener un régimen jurídico habilitante en el entorno digital, incurre en duplicidades e incoherencias que ponen de relieve no

Artículo recibido para su evaluación el 30 de mayo de 2020, y aprobado para su publicación el 15 de julio de 2020.

* Doctora en Derecho. Profesora Ayudante de Derecho procesal (acreditada a la figura de Profesora Contratada Doctora). Universidad Miguel Hernández. Departamento de Ciencia Jurídica, Alicante, España. Email: p.arrabal@umh.es. Publicación resultado del proyecto "Estudio comparado de modelos procesales desde la perspectiva de los ODS. Una mirada a la inteligencia artificial" realizada en el marco del proyecto de investigación de carácter internacional para la consecución de los Objetivos de Desarrollo Sostenible de la agenda 2030 de las Naciones Unidas (convenio UMH-GVA 2019). El contenido no refleja necesariamente la opinión de la Generalitat Valenciana.

1 Con la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

pocas dudas doctrinales debido, en gran medida, a las modificaciones que sufrió el texto en el trámite parlamentario[2].

II. LAS DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICA

Las diligencias de investigación son los actos policiales tendentes al descubrimiento del hecho punible, su posible autoría y demás circunstancias relevantes para su calificación y la determinación de culpabilidad de los investigados[3]. Aunque Pérez Gil señala que "en la actualidad la investigación o es tecnológica o no es investigación" [4], la anomia legislativa sobre el particular se mantuvo hasta que a finales del año 2015 se regularon algunos actos de esta naturaleza, corrigiendo la necesidad de cobertura normativa sobre el particular[5].

La incorporación de estas diligencias merece una valoración positiva por reconocer prácticas forenses que se llevaban a cabo sobre la única base de lo previsto para la interceptación de las comunicaciones telefónicas[6].

Así, la norma del 2015 creó un marco general a modo de disposiciones comunes y contempló diversas diligencias investigación tecnológica, algunas de las cuales se practican de forma directa sobre la evidencia y otras de forma remota, lo que, evidentemente, es más intrusivo para los derechos

2 El trámite parlamentario de esta norma puede verse en https://www.congreso.es/web/guest/busqueda-de-iniciativas?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_iniciativas_mode=mostrarDetalle&_iniciativas_legislatura=X&_iniciativas_id=121/000139.

3 Véase artículo 299 LECrim. En ese sentido, afirma Armenta Deu que "los actos de investigación no están encaminados a fundar una sentencia penal. Sólo los actos de prueba practicados en el juicio oral servirán de fundamento a la sentencia", en ARMENTA DEU, T.: *Lecciones de Derecho Procesal Penal* (quinta edición). Marcial Pons, Madrid, 2010. p. 138.

4 PÉREZ GIL, J.: "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución". En: *Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli*. Ed. Aracne, Roma, 2018.

5 La regulación de estas diligencias de investigación se ha llevado a cabo con la LO 13/2015, que las define expresamente como "tecnológicas" en su Preámbulo. Ello, no obstante, Richard González pone de manifiesto que el adjetivo "tecnológico" se refiere a la utilización de instrumentos o procedimientos técnicos que también se puede predicar de diligencias tales como la dactiloscopia o la balística, en RICHARD GONZÁLEZ, M.: "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización". En: *Diario La Ley*, nº 8808, 21 de julio de 2016. p. 4.

6 Así lo habían puesto de manifiesto también los Tribunales, vid. En ese sentido las SSTS 155/2007, de 28 de febrero; 735/2013, de 10 de octubre; 495/2014, de 17 de junio.

fundamentales de los afectados (en muchas ocasiones, desconocedores de su ejecución)[7].

1. Disposiciones comunes a las diligencias de investigación tecnológica.

Para la regulación de las diligencias de investigación tecnológica, la Ley de Enjuiciamiento Criminal ha elaborado un régimen común general a todas ellas en los artículos 588 bis a) a 588 bis k), subsidiario respecto a las regulaciones específicas.

Las citadas disposiciones de la norma adjetiva prevén que el Ministerio Fiscal o la Policía Judicial puedan solicitar al juez de instrucción[8] la adopción de alguno de estos actos de instrucción tecnológico por medio de una petición que haga referencia expresa a los siguientes extremos: la descripción del hecho objeto de investigación; la identidad del investigado o de cualquier otro afectado (cuando sea conocida); las razones que justifican la medida de acuerdo a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad; los indicios de criminalidad manifestados durante la investigación previa a la solicitud de autorización del acto de que se trate[9]; los datos de identificación del sujeto pasivo y los medios de

7 BACHMAIER WINTER, L.: "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015". En: *Boletín del Ministerio de Justicia*, Año 71, nº 2195, 2017. pp. 24-25 sostiene que, si es posible la obtención directa de la prueba, no debiesen autorizarse actos de instrucción remotos.

8 En relación con la solicitud de autorización judicial a instancia de la Policía Judicial, hay que tener presente que el Juez es el director de la investigación y que la Policía Judicial no es parte en el proceso, de modo que este tipo de resoluciones no se dictan, en realidad, a instancia de la Policía, sino, más bien, de oficio por parte del Juez, que decide a partir de lo que le informen los agentes, tal y como advierte VEGAS TORRES, J.: "Las medidas de investigación tecnológica". En: *Nuevas tecnologías y derechos fundamentales en el proceso.* Coord. Cedeño Hernán. Aranzadi, Cizur Menor, 2017. p. 32. Sobre la cuestión Cavero Forradellas asegura que la adopción de oficio de medidas de investigación es poco común en la práctica, vid. su ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", el día 27 de abril de 2016 en el curso *La interceptación de las comunicaciones telefónicas y telemáticas*. p. 33. Disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Cavero%20Forradellas,%20Gerardo.pdf?idFile=38380825-2079-4304-af21-40d9010e0ae9, pp. 27-28. En todo caso, Zoco Zabala advierte que la legitimación del Ministerio Fiscal o la Policía judicial para solicitar la intervención de las comunicaciones supone una novedad, al margen de los casos de personas intervenidas sospechosas de actuación con bandas armadas o elementos terroristas, en ZOCO ZABALA, C.: *Nuevas tecnologías y control de las comunicaciones*. Aranzadi, Cizur Menor, 2015. p. 204.

9 Sobre los indicios exigidos en el artículo 588 bis b), la STS 681/2017, de 10 de octubre afirma que deben ser "algo más que simples sospechas, pero también algo menos que

comunicación empleados; la extensión de la medida y la especificación de su contenido; la unidad investigadora de la Policía Judicial que se hará cargo de la intervención; la forma de ejecución de la medida; su duración; y, finalmente, el sujeto obligado que la llevará a cabo (si se sabe).

Aunque se tratan de reglas comunes, algunas de las diligencias tecnológicas a las que afectan tienen una regulación específica incongruente con este marco general, como es el caso, por ejemplo, de la utilización de dispositivos técnicos de captación de la imagen en lugares públicos, que no necesita de autorización judicial.

Ante tal petición, el órgano judicial, oído el Ministerio Fiscal, autorizará o denegará la diligencia a través de un Auto motivado en el (breve)[10] espacio de tiempo de, como máximo, veinticuatro horas desde que se hubiese presentado la solicitud[11]. Además, está previsto que, cuando resulte necesario para resolver sobre el cumplimiento de alguno de los requisitos, el juez pueda requerir, con interrupción del citado plazo, una ampliación o aclaración de los términos de la solicitud, lo que puede servir para evitar la nulidad de las pruebas obtenidas por medio de Autos con deficiencias en su motivación.

La decisión judicial, en el caso de permitir la medida tecnológica de investigación solicitada, deberá dictarse con plena sujeción a los principios establecidos en el artículo 588 bis a) LECrim y concretar los elementos

los indicios racionales que se exigen para el procesamiento y que desde luego deben ser evaluados en la forma en que se presentan en el momento de adoptarse la decisión judicial, sin que pueda efectuarse la evaluación de la pertinencia de la decisión desde un juicio "ex post", de acuerdo con la doctrina reiterada del Tribunal Constitucional en las SSTC 49/1999, de 5 de abril; 166/1999, de 27 de septiembre; 171/1999, de 27 de septiembre; 299/2000, de 11 de diciembre, FJ 4 ; 14/2001, de 29 de enero, FJ 5; 138/2001, de 18 de junio; 202/2001, de 15 de octubre; 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 261/2005, de 24 de octubre; 220/2006, de 3 de julio; 195/2009 de 28 de septiembre o 5/2010 de 7 de abril. En el mismo sentido, el auto del TS 298/2017, de 26 de enero y las SSTS 1007/2016, de 24 de enero; 689/2016, de 27 de julio.

10 Este plazo es ciertamente breve, dada la organización interna de las oficinas judiciales y la sobrecarga de trabajo que hay en los juzgados españoles (como puede verse en las estadísticas publicadas por el Consejo General del Poder Judicial en http://www.poderjudicial.es/cgpj/es/Temas/Estadistica-Judicial/Estadistica-por-temas/Actividad-de-los-organos-judiciales/Juzgados-y-Tribunales/Indicadores-clave/). En cualquier caso, la falta de medios materiales y personales no debe servir como pretexto para ampliar este límite previsto, si no, más bien al contrario, la exigencia de este plazo debe instar a una mayor provisión de plazas judiciales en aquellos partidos judiciales especialmente saturados.

11 De acuerdo con lo previsto en el artículo 588 bis c) LECrim.

señalados en el artículo 588 bis c) LECrim, muy similares a los exigidos por la solicitud[12], a saber: la referencia al hecho punible objeto de investigación y su calificación jurídica -con expresión de los indicios racionales en los que funde-; la identidad de los investigados y de cualquier otro afectado -de ser conocido[13]-; la extensión de la injerencia en cuanto a su alcance y motivación; la unidad investigadora de Policía Judicial que se hará cargo de la intervención; su duración; la forma y la periodicidad con la que el solicitante informará al juez sobre los resultados; la finalidad perseguida y el sujeto obligado que la llevará a cabo, si se conoce (en cuyo caso se debe mencionar, cuando proceda, el deber de colaboración y de guardar secreto, bajo apercibimiento de incurrir en un delito de desobediencia)[14].

En este sentido, la LECrim obliga a que la previa autorización judicial que acuerde alguna medida de investigación tecnológica deba respetar los clásicos principios de necesidad, idoneidad y proporcionalidad en

12 Un examen de los requisitos exigidos para la solicitud de autorización judicial frente a aquellos requeridos para que consten en la resolución judicial, ofrece una copia casi idéntica, lo que lleva a CAVERO FORRADELLAS a afirmar que se trata de una motivación por remisión en el que el juez instructor poco más tendrá que añadir a la solicitud, vid. la ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit. Ello no obstante y aunque la jurisprudencia constitucional admite que la resolución judicial integre la solicitud policial, el TS ha señalado que la motivación por remisión "se trata de una técnica jurisdiccional no modélica" (véase, a modo de ejemplo, la STS 636/2012, de 13 de julio.

13 El artículo 588 bis h) permite que se acuerden medidas de investigación aun cuando afecten a terceras personas y remite a las disposiciones específicas de cada diligencia para determinar los casos y las condiciones.

14 Este precepto recoge las exigencias de la Circular 1/2013 de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas, que dispone que "con carácter general y sin perjuicio de las modulaciones derivadas de las concretas circunstancias del caso, la resolución judicial motivada debe extenderse a los siguientes extremos: 1) los hechos investigados, o al menos, la parte de ellos respecto de los que es precisa la medida judicial; 2) la calificación jurídica de dichos hechos, esto es, el delito de que se trata 3) la imputación de dichos hechos y delito a la persona a quien se refiere la escucha; 4) la exteriorización de los indicios que el Juez ha de tener tanto sobre la persona como sobre el acaecimiento de los hechos constitutivos de delito; 5) el teléfono (o teléfonos) respecto del que se acuerda someter a escucha; 6) la relación entre el teléfono (o teléfonos) y la persona a quien se imputa el delito 7) el tiempo que habrá de durar la escucha, esto es, el plazo máximo de la intervención; 8) el período (o períodos) en los que se le debe dar cuenta al Juez del desarrollo de la escucha y de los resultados que se vayan obteniendo; 9) la persona o autoridad que solicita la medida o si se acuerda de oficio; 10) la persona o autoridad que llevará a cabo la intervención telefónica (SSTS nº 864/2005, de 22 de junio, 167/2002, de 18 de septiembre, 184/2003, de 23 de octubre)".

sentido estricto que venía exigiendo la jurisprudencia[15], a los que añade los de especialidad y excepcionalidad como elementos rectores que deben inspirar su adopción[16]. Es loable que el legislador, además de enumerarlos, haya explicado el significado y alcance de cada una de estas garantías. Tal es así, que la medida cumple con el principio de especialidad cuando está relacionada con la investigación de un delito concreto y no tiene carácter prospectivo[17]; con el de idoneidad cuando define el ámbito objetivo y subjetivo y la duración en virtud de su utilidad; con los de excepcionalidad y necesidad cuando no haya a disposición de la investigación otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida[18]. Y, finalmente, las diligencias de investigación reguladas solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio para el interés público y de terceros que resulte de su adopción[19].

15 Sobre los principios rectores exigidos jurisprudencialmente para la adopción de una medida de investigación véanse las SSTS 453/2010, de 1 de mayo; 561/2010, de 14 de junio; 796/2010, de 17 de septiembre; 1432/2011, de 16 de diciembre y la STC 123/2002, de 20 de mayo.

16 Vid. Artículo 588 bis a) LECrim.

17 La prohibición de las causas generales se ha sostenido también por la jurisprudencia en las SSTC 184/2003, de 23 de octubre, 261/2005, de 24 de octubre y las SSTS 695/2013, de 22 de julio; 689/2014, de 21 de octubre y, posteriormente a la reforma se ha reafirmado en la STS 675/2015, de 10 de noviembre.

18 Vid. artículo 588 bis a 3. González-Montes Sánchez indica que la justificación de la necesidad de la medida necesita de indicios que puedan atribuirse al sujeto pasivo de la medida y, en ese sentido, cierto grado de investigación previa, en 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 tecnológica". En: *Revista Electrónica de Ciencia Penal y Criminología*, nº 17-06, 2015. p. 28.

19 En este sentido, 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. Sobre la proporcionalidad de las medidas de investigación existe una extensa y asentada jurisprudencia que identifica tres juicios, el de idoneidad, el de necesidad y el de proporcionalidad en sentido estricto (véase, sin ánimo exhaustivo, las SSTC 173/2011, de 7 de noviembre; 199/2013, de 5 de diciembre; 16/2014, de 30 de enero; 23/2014, de 13 de febrero; 43/2014, de 27 de

Entre las normas que regulan las disposiciones comunes de estos actos de investigación, el artículo 588 bis d) dispone que, una vez acordada alguno de estos, el Juez decrete una pieza secreta y separada para su desarrollo. Esto parece adecuado porque impide que se pueda entorpecer la instrucción, pero no resulta claro si se aperturan tantas piezas como medidas instructoras se adopten –así parece desprenderse de la lectura del precepto- o si se sustanciarán todas en una sola. La segunda opción facilitaría el control judicial en el caso de la adopción de varias diligencias complementarias para un examen completo de las circunstancias que puedan arrojar información útil.

El instructor que habilitó la medida de investigación tecnológica quedará encargado del control del desarrollo y de los resultados obtenidos de la misma, en la forma y con la periodicidad que este determine[20].

En el examen de estas disposiciones comunes también resulta sorprendente la existencia de un precepto que señala que "tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos"[21] destinado al tratamiento común de la duración temporal de las medidas que, en realidad, reconduce a las normas concretas de cada diligencia[22]. Y

---

marzo) y Vegas Torres indica que el criterio de proporcionalidad en sentido estricto es el equivalente a la exigencia prevista en el artículo 588 bis a 5 LECrim, en VEGAS TORRES, cit., p. 37. El TEDH también explica que el principio de proporcionalidad se cumple cuando la medida impugnada es "necesaria en una sociedad democrática", de acuerdo con la relación entre el objetivo buscado y los medios empleados, tomando en consideración la existencia de una orden judicial basada en una sospecha razonable; el alcance limitado de la orden y garantías en su ejecución (véase las SSTDH Sher y otros c. el Reino Unido, de 20 de octubre de 2015 –disponible en http://hudoc.echr.coe.int/eng?i=001-158032- y Robathin c. Austria, de 3 de julio de 2012 -disponible en http://hudoc.echr.coe.int/eng?i=001-111890-).

20 Vid. artículo 588 bis g) LECrim.

21 Vid. Artículo 588 bis e) LECrim.

22 VILLAGÓMEZ MUÑOZ atribuye estas discordancias a que esta reforma proviene de los Anteproyectos de Código Procesal Penal de 2011 y 2014, que no tenían estas disposiciones comunes, en la ponencia "Otras medidas de investigación limitativas de derechos reconocidos por el art. 18 CE. Referencia concreta a los dispositivos de seguimiento y localización", realizada el 27 abril 2016 en el curso *La interceptación de las comunicaciones telefónicas y telemáticas*, p. 19, disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Villag%C3%B3mez%20Mu%C3%B1oz,%20Ana.pdf?idFile=1367353b-0fd9-4bab-8f57-36aad20dd137 (última consulta: 30/01/2018). Rodríguez Lainz también pone de manifiesto que la deficiente redacción de los preceptos referidos al deber de colaboración de terceros en las diligencias de registro de dispositivos de almacenamiento masivo de información y del registro

ello cuando, nótese 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. Parece razonable que esta previsión existiese únicamente en cada una de las medidas.

En todo caso, sobre la duración de estas diligencias, pese a que la LECrim no se pronuncia sobre el momento a partir del cual se computa, cabe aplicar lo que venía entendiéndose por la jurisprudencia respecto de la interceptación de comunicaciones telefónicas y telemáticas, esto es, que el *dies a quo* vendrá constituido por la fecha de la autorización judicial[23].

Ello sin perjuicio de que el Ministerio Fiscal o la Policía Judicial puedan solicitar al órgano judicial competente una prórroga de la medida de investigación con antelación a su expiración, aportando un informe detallado de los resultados hallados y de las razones que justifican su continuación. El juez, mediante Auto motivado, resolverá en un máximo de dos días sobre esta cuestión, para lo que podrá solicitar aclaraciones o información adicional[24]

La autoridad judicial también puede, de oficio, prorrogarla si subsisten las causas que motivaron su adopción. En estos supuestos en los que se

remoto sobre equipos informáticos tiene su origen en la desacertada trasposición del Borrador de Anteproyecto de Código Procesal Penal de diciembre de 2012 a la reforma operada por la LO 13/2015, en RODRÍGUEZ LAINZ, J.L.: "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?". En: *Diario La Ley*, nº 8729, 28 de marzo de 2016. pp. 11-12.

23 Vid. las SSTS 956/2011, de 29 de julio; 1078/2011, de 24 de octubre; 1161/201, de 31 de octubre; 1396/2011, de 28 de diciembre; 156/2012, de 29 de febrero; 144/2012, de 22 de marzo; 278/2012, de 3 de abril; 410/2012, de 17 de mayo; 521/2012, de 21 de junio; 621/2012, de 26 de junio; 88/2013, de 17 de enero; 33/2013, de 24 de enero; 165/2013, de 26 de marzo; 427/2013, de 10 de mayo; 506/2013, de 22 de mayo; 514/2013, de 12 de junio; 717/2013, de 1 de octubre; 746/2014, de 13 de noviembre; 841/2014, de 9 de diciembre; 34/2015; de 4 de febrero; 168/2015, de 25 de marzo; 504/2015, de 24 de julio; 85/2017, de 15 de febrero y las SSTC 205/2005, de 18 de julio; 26/2006, de 30 de enero y 68/2010, de 18 de octubre.

24 CAVERO FORRADELLAS se refiere al plazo improrrogable de dos días dado al instructor para pronunciarse sobre la prórroga de una medida de investigación y alerta que la solicitud deberá contemplarse con antelación suficiente para evitar que, traspasadas las cuarenta y ocho horas sin resolución judicial, haya que solicitar *ex novo* el acto de investigación porque ya haya cesado porque haya finalizado el periodo por la que se aprobó, vid. su ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit, pp. 31-32. El autor, además, deduce que este plazo se traduce en silencio negativo.

acuerde una prórroga, ésta comienza en la fecha de expiración del plazo acordado inicialmente[25].

Transcurrido el plazo -inicial o prorrogado- concedido para la ejecución de la diligencia de investigación, desaparecidas las circunstancias que justificaron su adopción o no obtenidos los resultados esperados con la misma, esta cesará a todos los efectos[26].

El legislador, consciente de que en muchas ocasiones se involucra a otros sujetos, señala de manera expresa que estas medidas se adoptarán aun cuando afecten a terceras personas en los casos y con las condiciones que se regulan en las disposiciones específicas de cada una de ellas[27]. Además, la LECrim también prevé un deber de colaboración[28] que, de incumplirse, puede comportar un delito de desobediencia[29].

Especial mención merece también la regulación de los denominados hallazgos casuales, que recoge -por fin- la prolija jurisprudencia existente sobre la misma[30]. Sin embargo, inexplicablemente y de forma mejorable en cuanto a técnica legislativa se refiere, se realiza remitiendo a lo previsto para el descubrimiento de información sobre un hecho distinto al investigado en los actos de detención y apertura de correspondencia escrita y telegráfica[31].

Finalmente, la Ley de Enjuiciamiento Criminal dispone como norma común a las diligencias tecnológicas, en consonancia con la jurisprudencia europea que, una vez finalizado el procedimiento por resolución firme, los tribunales dictarán las órdenes oportunas a la Policía Judicial para el borrado y eliminación de los registros originales que queden en los

25 Vid. artículo 588 bis f), 3 LECrim.

26 Vid. artículo 588 bis j) LECrim. También hace referencia al cese de la medida el artículo 588 bis e, destinado a regular la duración de la misma, que indica que "transcurrido el plazo por el que resultó concedida la medida, sin haberse acordado su prórroga, o, en su caso, finalizada ésta, cesará a todos los efectos".

27 Vid. artículo 588 bis h) LECrim.

28 Este deber se reconoce tanto en las disposiciones comunes -artículo 588 bis c), 2, h) LECrim-, como en la regulación específica de alguna diligencia tecnológica (vid. artículo 588 ter e) LECrim con respecto al deber de colaboración en la interceptación de comunicaciones telefónicas y telemáticas; o artículo 588 septies b) LECrim para el registro remoto sobre equipos informáticos).

29 Vid. artículo 588 bis c), 2, h) LECrim.

30 De especial interés resulta la lectura de la Circular 1/2019, de 6 de marzo, de la Fiscal General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica s en la Ley de Enjuiciamiento Criminal sobre los hallazgos casuales.

31 Vid. Artículo 588 bis i) que remite al 579 bis LECrim.

sistemas electrónicos e informáticos utilizados en la ejecución de la medida. Ello no obstante, el Letrado de la Administración de Justicia conservará una copia bajo su custodia, que será también destruida por la Policía Judicial cuando hayan transcurrido cinco años desde que la pena haya sido ejecutada, cuando el delito o la pena hayan prescrito o cuando el juez decrete el sobreseimiento libre o dicte sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal[32]. Nada se dice, sin embargo, aunque sería deseable, respecto de la destrucción de las copias entregadas a las partes[33].

2. La interceptación de las comunicaciones telefónicas y telemáticas.

La reforma operada por la LO 13/2015 que incorpora las medidas de investigación tecnológica modificó el artículo 579 LECrim pero que venía referido a la interceptación de las comunicaciones postales, telegráficas y telefónicas, pero que se utilizaba como "comodín" para este tipo de diligencias por la insuficiente normativa[34].

32 Artículo 588 bis k LECrim. Adviértase que la norma parece referirse únicamente a los casos de sobreseimiento libre, pese a que RODRÍGUEZ LAINZ considera que esta la destrucción de estos soportes se refiere a los supuestos de sobreseimiento libre y provisional, en la ponencia "Sobre la Ley Orgánica de modificación de la LECrim para el fortalecimiento…", cit., El principio de destrucción de los registros obedece a una instaurada jurisprudencia europea apreciable en las SSTEDH de 14 de noviembre de 2012 (parágrafos 118 y ss.); caso Vinci Construction et GTM Genie Civil et Services c. Francia, de 2 de abril de 2015 y caso Sérvulo & Associados. Sociedade de Advogados c. Portugal, de 3 de septiembre de 2015. Como acertadamente apunta Gimeno Beviá, "no es de recibo que las comunicaciones privadas permanezcan *per secula seculorum* al alcance de los miembros de la oficina judicial", en GIMENO BEVIÁ, J.: "Análisis crítico de la reforma de LECrim 2015". En: *Revista Derecho y Proceso Penal*, Aranzadi, nº 40, octubre-diciembre 2015. p. 203, afirmación que se puede hacer extensiva a toda la información obtenida por estas medidas de investigación y no sólo a las comunicaciones.

33 Esta acertada crítica expone VEGAS TORRES, J., cit., p. 47.

34 La redacción anterior del artículo 579 LECrim, aprobado por la Ley Orgánica 4/1988, de 25 de mayo, de Reforma de la Ley de Enjuiciamiento Criminal, disponía que "1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. 2. 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. 3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas

En la actualidad hay una separación entre las diligencias de intervención de las comunicaciones postales y telegráficas - previstas en el capítulo III del título VIII del Libro II (artículos 579 a 588)- y las telefónicas, a las que se adicionan las telemáticas -y que se han ubicado en el capítulo V del título VIII del Libro II (artículos 588 ter a-588 ter m)-. La adopción de estas últimas requiere de autorización judicial, cuya solicitud contendrá los requisitos que se venían exigiendo jurisprudencialmente y que ahora contempla el artículo 588 ter d) con referencia al citado 588 bis b) LECrim de las disposiciones comunes[35].

sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación". La limitada redacción del precepto que regulaba la interceptación de las comunicaciones en España hasta la reforma de la LO 13/2015 había necesitado de un vasto aporte jurisprudencial, como reconoce, incluso el Preámbulo de la reforma del año 2015: "Surge así la necesidad de encontrar un delicado equilibrio entre la capacidad del Estado para hacer frente a una fenomenología criminal de nuevo cuño y el espacio de exclusión que nuestro sistema constitucional garantiza a cada ciudadano frente a terceros. Por muy meritorio que haya sido el esfuerzo de jueces y tribunales para definir los límites del Estado en la investigación del delito, el abandono a la creación jurisprudencial de lo que ha de ser objeto de regulación legislativa ha propiciado un déficit en la calidad democrática de nuestro sistema procesal, carencia que tanto la dogmática como instancias supranacionales han recordado. Recientemente, el Tribunal Constitucional ha apuntado el carácter inaplazable de una regulación que aborde las intromisiones en la privacidad del investigado en un proceso penal. Hoy por hoy, carecen de cobertura y su subsanación no puede obtenerse acudiendo a un voluntarista expediente de integración analógica que desborda los límites de lo constitucionalmente aceptable".

35 La solicitud de autorización judicial debe contener: la descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida -si se conoce-; las razones que justifiquen la necesidad de su adopción -que han de respetar los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad-; los indicios de criminalidad existentes; los datos de identificación del investigado o encausado y de los medios de comunicación empleados; la extensión de la medida con especificación de su contenido; la unidad investigadora de la Policía Judicial que se hará cargo de la intervención y la forma de su ejecución; su duración; el sujeto obligado que la llevará a cabo -de conocerse-; 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 la identificación del medio de telecomunicación que se trate; la finalidad del acto de investigación; el conocimiento de su origen o destino, en el momento en el que la comunicación se realiza; la localización geográfica del origen o destino de

Esta habilitación solo podrá concederse para la investigación de los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación[36]; los dolosos castigados con pena con límite máximo de, al menos, tres años de prisión[37]; o los cometidos en el seno de un grupo u organización criminal o delitos de terrorismo[38]. Para estos últimos la norma contempla el salvoconducto del Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad, en los supuestos en los que concurra urgencia en la investigación que haga dificultosa la solicitud de la autorización judicial[39]. Esta licencia -que exige expresa mención de las razones que justifiquen la adopción de la medida sin el previo control judicial, la descripción de

la comunicación y el conocimiento de otros datos de tráfico asociados o no asociados concretos que han de ser obtenidos de valor añadido a la comunicación. Un interesante aporte doctrinal es el realizado por FUENTES SORIANO, O.: "La intervención de las comunicaciones tecnológicas tras la reforma de 2015". En: *El nuevo proceso penal tras las reformas de 2015*. Dir. Alonso-Cuevillas Sayrol. Atelier, Barcelona, 2016. pp. 261-286.

36 RODRÍGUEZ LAINZ advierte que la sola pertenencia a la lista de infracciones que pueden ser objeto de investigación por esta modalidad de tecnovigilancia no es aval suficiente para la superación del juicio de proporcionalidad, vid. su ponencia "Sobre la Ley orgánica de modificación de las LECrim para el fortalecimiento de las garantías procesales: la regulación de las medidas de investigación tecnológica", cit., p. 16. Además, la referencia a los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación parece provenir de la conclusión número 22.3 de la *Circular de la Fiscalía General del Estado 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas* (p. 137) referida a la proporcionalidad (texto disponible en https://www.fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/cir_inst_cons/circular_1_2013.pdf).

37 Sobre este peculiar grupo de delitos de, al menos, tres años de prisión que pueden ser objeto de la interceptación de comunicaciones, Rodríguez Lainz justifica que engloba a un gran número de las categorías de delitos que normalmente hacen uso de esta medida de investigación, si bien reconoce que contribuye a que determinados delitos con penas superiores que tampoco concurren con el resto de supuestos, no puedan hacer uso de esta diligencia, en RODRÍGUEZ LAINZ, J.L.: *El secreto de las telecomunicaciones y su interceptación legal*. Sepín, Madrid, 2016. pp. 90-91.

38 El artículo 588 ter a) restringe la autorización para la interceptación de comunicaciones telefónicas o telemáticas a los delitos del artículo 579.1 LECrim (delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal o delitos de terrorismo) y a los cometidos a través de cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación.

39 Artículo 588 ter d), apartado tercero LECrim que encuentra su respaldo constitucional en el artículo 55.2 CE. En la regulación anterior esta excepción al principio de judicialidad previa remitía la autorización al Ministro de Interior y, en su defecto, al Director de la Seguridad del Estado.

la actuación realizada, la forma en que se ha efectuado y su resultado-, ha de ponerse en conocimiento del juez competente lo más pronto posible (y siempre antes de veinticuatro horas) para que revoque o confirme motivadamente la actuación en las siguientes setenta y dos horas desde que fue ordenada[40].

La interceptación puede realizarse por un plazo de tres meses, prorrogables por períodos iguales sucesivos hasta un plazo máximo de dieciocho[41]. Adviértase que la duración total de la intervención se computará desde la fecha de la autorización y no desde la fecha de conexión real, como en ocasiones pasadas se ha entendido. Para la prórroga de la medida de investigación, el artículo 588 ter h) LECrim exhorta a la Policía Judicial a que aporte la transcripción de aquellos pasajes de las conversaciones de las que se deduzca información relevante, si bien el juez puede solicitar aclaraciones u otros datos, incluido el contenido íntegro de las conversaciones intervenidas para decidir sobre su mantenimiento.

Del estudio de las previsiones legales parece desprenderse que es necesaria autorización judicial para que los prestadores de servicios o personas que facilitan la comunicación cedan a los agentes facultados los datos electrónicos asociados vinculados a procesos de comunicación que resulten indispensables para la investigación, incluidos aquellos derivados de una búsqueda entrecruzada o inteligente de los mismos[42].

Ello, no obstante, esta regulación encuentra algunas contradicciones con la vigente Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Esta norma española traspone la Directiva europea 2006/24/CE que fue posteriormente anulada por la STJUE del 8 de abril de 2014, si bien es cierto que la nacional se entiende todavía operativa, pese a que su literalidad parece contrariar lo previsto en la LECrim en relación con la obtención de los datos de tráfico[43]. Esta cuestión fue planteada en una cuestión prejudicial por el Juzgado de instrucción nº 3 de Tarragona al

40 Así lo expresa el apartado tercero del artículo 588 ter d) LECrim. El artículo 579.4 derogado no preveía ningún plazo para la comunicación al juez competente, sino que debía realizarse "inmediatamente".

41 Artículo 588 ter g) LECrim.

42 Artículo 588 ter j) LECrim.

43 Me ocupo de esta incongruencia en ARRABAL PLATERO, P.: "Algunas cuestiones controvertidas sobre la obtención de datos de tráfico". En: *La justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro.* Dirs. Conde Fuentes, Serrano Hoyo. Coords. Arrabal Platero, García Molina. Atelier, Madrid, 2019. pp. 217-326.

Tribunal de Justicia de la Unión Europea, que resuelve parcialmente en su sentencia C-207/2016, de 2 de octubre[44].

Para el control de la medida, la Policía Judicial pondrá a disposición del Juez, con la periodicidad que éste determine, dos soportes digitales distintos: uno con la transcripción de los pasajes que considere de interés y otro con una copia de las grabaciones íntegras realizadas, con indicación en ambos del origen y destino de las comunicaciones y con la garantía de la integridad y autenticidad de las mismas a través de un procedimiento de sellado -*time stamping*-, firma electrónica o un sistema de adveración suficientemente fiable[45].

También destaca de estas reglas la inclusión del deber de colaboración con el juez, el Ministerio Fiscal o los agentes de la Policía Judicial designados en la práctica de la medida de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información y para toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual[46]. Del mismo modo, la norma prevé la obligación de guardar secreto acerca de las actividades requeridas por las autoridades y la condena por desobediencia a la conducta contraria[47].

Como dictan las disposiciones comunes, la adopción de esta medida conlleva la apertura de una pieza separada y secreta, pero, una vez expirada su vigencia -y alzado, con ello, el secreto-, las partes pueden examinar las grabaciones y, en su caso, solicitar al juez de instrucción la inclusión en las copias de aquellos fragmentos de las comunicaciones que entiendan

44 Sentencia disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=608670.
Profundizo sobre esta sentencia en ARRABAL PLATERO, P.: "El acceso policial a los datos almacenados por los prestadores de servicios a la luz de la STJUE de 2 de octubre de 2018 (ASUNTO C-207/16)". En prensa.

45 Artículo 588 ter f) LECrim. CAVERO FORRADELLAS identifica tres carencias de esta regla, la primera es que no encomienda la labor transcribir las conversaciones a la oficina judicial, sino a la Policía judicial; la segunda, directamente relacionada con la anterior es que no se dice nada sobre cómo deben plasmar estas conversaciones (de forma literal o resumidamente); y, finalmente, la norma guarda silencia sobre el cotejo entre la transcripción y la grabaciones, en la ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit., p. 44.

46 Medida que introduce el artículo 588 ter e) LECrim.

47 Artículo 588 ter e) LECrim, apartado tercero.

relevantes y que hayan sido excluidas[48]. Con un propósito garantista de los derechos individuales, se ha determinado la posibilidad de eliminar de estas grabaciones los datos referidos a aspectos de la vida íntima de las personas –con expresa mención de este extremo en la entrega a las partes-[49] y la necesaria notificación del juez de instrucción a las personas intervinientes en las comunicaciones interceptadas de la existencia de tal injerencia en su intimidad, salvo que esta información sea imposible, exija un esfuerzo desproporcionado o pueda perjudicar futuras investigaciones, excepciones que parece que se convertirán en la regla general[50].

Finalmente, cabe señalar que la LECrim adopta el Convenio sobre la Ciberdelincuencia de Budapest, del 23 de noviembre de 2001[51] al reconocer que en la interceptación de comunicaciones se accede a tres tipos de datos: el contenido de la comunicación, los datos de tráfico y los datos de abonado

48 Apartado segundo del artículo 588 ter i) LECrim.

49 En esta excepción tiene cabida la previsión del artículo 118.4 de la LECrim, que prohíbe el registro de las conversaciones entre el investigado y su abogado.

50 La persona que haya participado en una conversación intervenida a la que se le notifique tal injerencia puede solicitar la entrega de una copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia. Sobre las excepciones a la regla general de notificación de la intervención de las comunicaciones a personas ajenas a la investigación, Vegas Torres anticipa que estas se van convertir en la regla general que permita eludir la obligación de informar, lo que comportará la paradójica situación en la que los acusados de cometer un delito sean informados de la medida limitadora de derechos fundamentales y no así los terceros ajenos a esta responsabilidad penal investigada, en VEGAS TORRES, cit., pp. 46-47.

51 El apartado d del artículo 1 del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 define los datos sobre el tráfico como "cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente" y el artículo 18.3 del citado Convenio identifica como datos relativos a los abonados "toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar: a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".

o conexión[52]. Los primeros están protegidos por el derecho al secreto constitucional de las comunicaciones del artículo 18.3 CE y requiere para su acceso, de autorización judicial o debida urgencia, acreditada y valorada judicialmente con posterioridad; los datos de tráfico son aquellos vinculados a un determinado proceso de comunicación, como la fecha o la duración de una llamada[53]; y los datos de abonado o conexión existen con independencia del establecimiento o no de una comunicación, como puede ser el número de teléfono o los datos de identificación de su titular[54].

3. La identificación de usuarios, terminales y dispositivos de conectividad.

La LECrim reconoce determinadas actuaciones policiales para la identificación de usuarios, terminales y dispositivos de conectividad en tres preceptos -los artículos 588 ter k) a 588 ter m)- ubicados en la sección tercera del capítulo V del título VIII del Libro II. Se trata, como señala la Fiscalía General del Estado, de la incorporación al proceso de datos de

52 Artículo 588 ter b) LECrim, que también prevé la interceptación de los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad. Tanto CAVERO FORRADELLAS en la ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit., p. 26, cuanto RODRÍGUEZ LAINZ, en su obra "Intervención judicial de comunicaciones vs. Registro remoto sobre equipos informáticos: los puntos de fricción", ya citada, p. 13, sostienen que esta previsión se puede destinar a localizar dispositivos tecnológicos sustraídos. Sobre la precisión de "habitual u ocasionalmente" referida a los terminales o medios de comunicación utilizados por el investigado, CAVERO FORRADELLAS expone que no tiene, en realidad, gran trascendencia, porque comprende, incluso, un único uso por parte del encausado, en la ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit., p. 25.

53 La LECrim define los datos electrónicos de tráfico o asociados en el artículo 588 ter b 2 como "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".

54 Es posible identificar un cuarto elemento: aquellas comunicaciones interceptadas con esta medida de investigación que no están asociadas a un proceso de investigación, como son las conversaciones "en off" que se refiere a aquel diálogo que pueda captarse de quien realiza la llamada antes de que el receptor descuelgue y que, normalmente, será con individuos que se encuentren físicamente cercanos, vid. La ponencia de Cavero Forradellas "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit., pp. 40-41.

tráfico independientes del contenido de una comunicación, bien porque ésta ya hubiere concluido, bien porque no hubiere llegado a existir[55].

El artículo 588 ter k) está específicamente referido a la identificación de usuarios, terminales y dispositivos de conectividad a partir de una dirección IP (*Internet Protocol*), esto es, un número identificativo de cuatro grupos de tres números (xxx.xxx.xxx.xxx) que la red asigna a los *routers* y estos, a cada uno de los terminales[56]. Este precepto dispone que la Policía Judicial, cuando en el ejercicio de sus funciones de prevención y descubrimiento de los delitos, conozca una dirección IP que estuviera siendo utilizada para la comisión algún delito en Internet, puede solicitar al juez de instrucción que requiera a los sujetos el deber de colaboración del artículo 588 ter e) LECrim[57], para la cesión de los datos que permitan la identificación y localización del dispositivo de conectividad y del sospechoso[58].

Un segundo precepto, el 588 ter l) LECrim, prevé la identificación de los terminales por parte de la Policía Judicial en el marco de una investigación sin autorización judicial mediante captación de los códigos o las etiquetas técnicas del aparato de telecomunicación o de sus componentes, tales como la numeración IMSI[59] o IMEI, por medio de cualquier medio apto para

55 Circular 2/2019, de 6 de marzo, de la Fiscal General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas.

56 Esta cifra identifica a los dispositivos conectados a Internet, si bien puede variar en función de las necesidades del entorno de red. A mayor abundamiento, puede consultarse https://computerhoy.com/paso-a-paso/internet/como-saber-cual-es-direccion-ip-mi-ordenador-24347**.**

57 Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

58 CAVERO FORRADELLAS advierte que la alusión al "ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet" en el que la policía haya tenido acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito, parece hacer referencia a una actuación prospectiva, vid. su ponencia "La nueva regulación de las intervenciones telefónicas en la Ley de Enjuiciamiento Criminal", cit., pp. 13-14.

59 El IMSI -acrónimo de *International Mobile Suscriber Identity*- es un código de identificación único para cada dispositivo móvil, integrado en la tarjeta chip SIM que se inserta en el teléfono móvil para asignarle el número de abonado o MSISDN -*Mobile Station Integrated Services Digital Network*-, que permite su identificación a través de las redes GSM. Este número de abonado está compuesto por el MCC o código del País (tres dígitos), por ejemplo, *214,* que correspondería a España; por el MNC o Código de la red móvil (dos o tres dígitos), por ejemplo, *07,* que correspondería a la operadora MOVISTAR; y finalmente por el MSIN (número de diez dígitos) que contiene la identificación de la estación móvil.

identificar el equipo de comunicación o tarjeta utilizada para acceder a la red de telecomunicaciones[60]. Este artículo prevé que, conocidos estos códigos, los agentes de la Policía Judicial pueden solicitar del juez competente la intervención de las comunicaciones, indicando, eso sí, los artificios técnicos utilizados para su reconocimiento[61]. El Tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo común establecido en el artículo 588 bis c) LECrim de las disposiciones comunes. Como ha señalado GIMENO SENDRA, "este precepto no contempla el ámbito de aplicación delictual que permite el conocimiento de los datos de tráfico, (…), por lo que cabría sostener que incluso la comisión de delitos leves legitimaría esta intervención (aunque) la aplicación (…) del art. 588 bis a abogaría por la solución contraria, pues no parece que se cohoneste con los principios de proporcionalidad y de necesidad la intervención de datos de tráfico para la investigación de delitos leves"[62].

Por último, el artículo 588 ter m) LECrim, permite que el Ministerio Fiscal o la Policía Judicial puedan dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información para conocer la titularidad o el número de teléfono o de cualquier otro medio de comunicación, a partir de la identificación de su titular. Su colaboración es obligatoria, bajo apercibimiento de incurrir en un delito de desobediencia[63].

Es posible obtener el número *IMSI* de un teléfono móvil mediante un dispositivo que debe aproximarse al teléfono que se desea investigar y que simula el comportamiento de la red GSM, de forma tal que interactúa de manera equivalente a cómo lo hace una infraestructura de red de un operador móvil con un teléfono móvil que se enciende o que cambia de célula de cobertura, vid. la STS 1154/2009, de 11 de noviembre.

60 La STS 492/2016, de 8 de junio y el Auto del TS 1190/2017, de 20 de julio han señalado que, de acuerdo con artículo 588 ter l) de la Ley de Enjuiciamiento Criminal la obtención del número IMSI por el Departamento de Aduanas mediante monitorización, no puede ser considerado como un dato de carácter personal ni afecta al derecho al secreto de las comunicaciones.

61 El artículo 588 ter l) refiere que "la solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios", pero no parece que tenga que identificar qué artificio se ha utilizado, sino, únicamente su uso.

62 GIMENO SENDRA, V.: *Derecho procesal penal*, tercera edición. Thomson Reuters, Navarra, 2019. p. 564.

63 Esta previsión ya sirvió a finales del año 2015 para desestimar un recurso en el que se alegaba la obtención de los teléfonos del recurrente sin título habilitante ni resolución judicial en la STS 709/2015, de 16 de octubre.

4. La captación y grabación de las comunicaciones orales mediante la utilización de dispositivos técnicos.

Esta nueva diligencia tecnológica consiste en la colocación y utilización de dispositivos electrónicos para la captación y grabación de las comunicaciones orales que el investigado mantenga con otras personas en la vía pública, en otro espacio abierto, en el domicilio del investigado o en cualesquiera otro lugar cerrado en uno o varios encuentros concretos predecibles[64].

Para la adopción de tal acto de investigación generalmente conocido como "escucha ambiental" es necesario el cumplimento de tres requisitos: previa autorización judicial; que los hechos cuestionados sean constitutivos de unos delitos concretos -delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal o delitos de terrorismo-; y que concurran sospechas fundadas de que la información recabada aportará datos de interés para el esclarecimiento de los hechos y la identificación de su autor[65].

64 Véanse los artículos 588 quarter, letras a) y b) LECrim. Como señala la Circular 3/2019, de 6 de marzo, de la Fiscal General del Estado, sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos "quedan fuera de la regulación de la LECrim las grabaciones clandestinas realizadas por particulares, así como la aportación a juicio de lo escuchado directamente por agentes policiales sin recurrir a dispositivos electrónicos para su captación".

65 Para Conde-Pumpido la experiencia demuestra que las conversaciones que pueden ser objeto de esta diligencia se llevan a cabo de manera general en el mismo sitio sin previo aviso y que estos encuentros "concretos" se conocen con poca antelación temporal, lo que impide la instalación de los dispositivos necesarios y limita la adopción de la medida a supuestos previsibles por los investigadores, lo que conllevará su no solicitud. En este sentido, la Fiscal propone la posibilidad de la instalación de los dispositivos de grabación –con la preceptiva autorización judicial- que se activen remotamente para encuentros concretos posteriores, haciendo referencia al momento inicial y final de la grabación para un correcto control judicial de la medida, en CONDE-PUMPIDO, P.: "Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos", ponencia dictada en el seminario "La interceptación de las comunicaciones telefónicas y telemáticas" celebrado por el Ministerio Fiscal el 27 abril 2016. pp. 4-5, disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Comunicaci%C3%B3n%20Conde-Pumpido%20Garc%C3%ADa,%20Paloma.pdf?idFile=b243d8eb-4156-4d93-82b0-ccffc6992aa4 (fecha de consulta: 29/01/2018). Sobre el último requisito –la previsión de que la adopción de esta diligencia aportará información para el esclarecimiento de los hechos y la identificación de su autor-, Cabezudo Bajo refiere que se trata de una exigencia del principio de proporcionalidad, pese a que no lo recoge el artículo 588 bis a) 5, común a todas las diligencias de investigación tecnológica s del Título VIII del Libro II de la LECrim, en CABEZUDO BAJO, M.J.: "El uso de las tecnologías en la entrada y el registro domiciliario: cambio en

De la lectura de la regulación concreta de esta diligencia de investigación y de las disposiciones comunes, se extrae que el Auto judicial que acuerde la medida debe contener los siguientes elementos: el hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que se funde; la identidad de los investigados y de cualquier otro afectado, de ser conocido; su extensión temporal, con expresa mención de su alcance y la motivación de acuerdo con los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad; la unidad investigadora de la Policía Judicial que se hará cargo de la intervención; la duración; la forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la injerencia; la finalidad perseguida con ella; el sujeto obligado que la llevará a cabo, en caso de conocerse (y, cuando proceda, referencia expresa al deber de colaboración y de guardar secreto, so apercibimiento de incurrir en un delito de desobediencia); y el lugar o dependencias sometidos a vigilancia, así como los concretos encuentros del investigado que vayan a producirse y sobre los que se llevará a cabo la medida[66].

El uso de las tecnologías en la entrada y el registro domiciliario: cambio en su concepción tradicional y nuevos retos en la protección de los derechos fundamentales afectados. Revista de Derecho Penal y Criminología, 3ª época, 15.

Además, es posible que es esta resolución también se autorice expresamente la obtención de imágenes como complemento a la captación de las conversaciones[67], si bien esta previsión colisiona, en cierta manera, con la diligencia para la captación policial de imágenes en lugares públicos. que no requiere de autorización judicial[68]. Así, la Policía judicial necesita

su concepción tradicional y nuevos retos en la protección de los derechos fundamentales afectados". En: *Revista de Derecho Penal y Criminología*, 3ª época, 15. p. 87.

66 Vid. el artículo 588 quarter, letra c, LECrim que referencia las exigencias comunes para la resolución judicial del artículo 588 bis, letra c) LECrim.

67 El apartado tercero del artículo 588 quarter, letra a), LECrim legitima la grabación de imágenes siempre que la autorización judicial lo habilite. La configuración de adicional que se le otorga a la obtención de imágenes ha conllevado que el precepto orientado a los presupuestos de esta diligencia solo se refiera a las captación y grabación de comunicaciones, tal y como advierte CABEZUDO BAJO, cit., p. 83.

68 Vid. el artículo 588 quinquies a) LECrim. Sobre el particular, Conde-Pumpido subraya que la limitación del secreto de las comunicaciones con la grabación de las mismas solo puede venir dada por medio de autorización judicial, pero la ampliación de esta exigencia a la grabación de imágenes se contrapone a la práctica habitual hasta el momento, que se amparaba en el artículo 282 de la LECrim para legitimar la grabación de imágenes en

previa habilitación judicial expresa para la grabación de imagen y sonido, pero no para la captación exclusivamente de imágenes -sin sonido- en lugares públicos[69].

Si la diligencia para la captación y grabación de comunicaciones orales se adopta en el interior de un domicilio, afecta, obviamente, al derecho fundamental previsto en el artículo 18.2 de la Constitución Española, por lo que se exige resolución habilitante adicional que motive la procedencia del acceso a este espacio de intimidad protegido. Esto será así tanto si la Policía accede al domicilio para colocar los aparatos de escucha y grabación[70], cuanto si se lleva a cabo desde el exterior con aparatos técnicos (por ejemplo, con aparatos que captan y amplifican el sonido) que otorgan acceso a lo que tiene lugar en su interior en lo que se conoce como "intromisión virtual"[71].

Al respecto, la reciente STS 718/2020, de 28 de diciembre sostiene que "la utilización de dispositivos electrónicos para la captación y grabación de las comunicaciones orales y, en su caso, para la obtención de imágenes en el domicilio del investigado no es una prueba más. No puede ser contemplada por el Juez instructor como una medida de injerencia susceptible de ser acordada con los mismos presupuestos de legitimidad con los que se adoptan otras medidas de investigación tecnológica en el proceso penal. El grado de injerencia que esa medida representa en el espacio que cada

espacios públicos sin necesidad de previa resolución judicial, en CONDE-PUMPIDO, cit., p. 6.

69 Así lo interpreta también CONDE-PUMPIDO, cit, pp.13-14. Pongo de manifiesto esta contradicción en ARRABAL PLATERO, P., "Validez de la grabación policial al conductor a efectos de prueba en el delito de conducción bajo la influencia de las drogas del artículo 379.2 CP", *La Ley Privacidad*, Wolters Kluwer, nº 4, 2020.

70 Así, el artículo 588 quarter a) LECrim exige que la entrada a un domicilio u otro espacio destinado al ejercicio de la privacidad venga provista de la necesaria resolución habilitante que extienda su motivación a la procedencia del acceso a estos lugares.

71 Tanto el Tribunal Constitucional, cuanto el Tribunal Supremo, han entendido que sí se vulnera el derecho a la inviolabilidad del domicilio cuando, con el uso de instrumentos técnicos, se accede a lo que acaece dentro del domicilio sin autorización judicial, vid. SSTC 22/1984, de 17 de febrero; 22/2003, de 10 de febrero y STS 329/2016 de 20 de abril. En la fecha de la redacción de este trabajo se conoce un resumen publicado por el Ministerio de justicia del Anteproyecto de Ley de Enjuiciamiento Criminal elaborado por un comité de expertos que ha concluido el texto en 2020, en el que se señala que "se incluye en la nueva regulación la intromisión en el domicilio a través de medios electrónicas que permiten conocer desde el exterior la situación o el movimiento de personas y cosas en un espacio", vid. https://www.lamoncloa.gob.es/consejodeministros/paginas/enlaces/220711-enlacecriminal.aspx

ciudadano define para excluir a los poderes públicos y a terceros de su propia privacidad, no puede ser ponderado con el mismo ángulo valorativo con el que se aceptan otras medidas de investigación".

El control de estas diligencias lo llevará a cabo la Policía con la puesta a disposición a la autoridad judicial del soporte original o de la copia electrónica auténtica de las grabaciones de las conversaciones (e imágenes, en su caso), la transcripción de aquellas que se consideren de interés y con expresa identificación de todos los agentes que participaron en la ejecución y el seguimiento[72].

Este acto de investigación cesará cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que no es útil para la obtención los resultados pretendidos, y, en todo caso, cuando haya transcurrido el plazo para el que hubiera sido autorizado[73].

5. La captación de la imagen en lugares y espacios públicos mediante la utilización de dispositivos técnicos.

El artículo 588 quinquies LECrim, letra a), permite a la Policía Judicial la obtención y grabación de imágenes de la persona investigada en lugares o espacios públicos, por cualquier medio técnico que facilite su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes que sirvan al esclarecimiento de los hechos. Llama la atención que la captación de la imagen por medio de dispositivos técnicos está prevista conjuntamente en el capítulo VII del Título VIII del Libro II con la utilización de dispositivos o medios técnicos de seguimiento y localización, cuando son diligencias que poco tienen en común[74].

72 Conde-Pumpido señala que el requisito que exige indicar qué agentes han participado en la ejecución y seguimiento de la medida, además de que únicamente se ha previsto para esta medida, resulta innecesario, no aporta ninguna garantía adicional para los derechos fundamentales en juego y significa un incremento del trabajo burocrático que desvela un desconocimiento del funcionamiento instructor por parte del legislador, en CONDE-PUMPIDO, cit., p. 12.

73 Vid. artículo 588 bis j) LECrim, común a todas las diligencias de investigación tecnológica s.

74 Resulta curiosa la ordenación de estas dos diligencias, que poco tienen en común, en un mismo capítulo, cuando las diferencias entre ambas son notorias, ya que, por ejemplo, la captación de la imagen en espacios públicos no requiere de habilitación judicial y la utilización de dispositivos técnicos de seguimiento y de localización, sí. VILLAGÓMEZ MUÑOZ atribuye al tratamiento conjunto de la captación de la imagen en espacios públicos y de la utilización de dispositivos técnicos de seguimiento y de localización a su afectación al derecho a la intimidad, cit., p. 10.

Aunque que la mayor parte de las medidas de investigación tecnológica necesitan de autorización judicial habilitante por su afectación a derechos fundamentales de los investigados (e, incluso, de terceros), se ha articulado su dispensa respecto de la captación de la imagen mediante la utilización de dispositivos técnicos cuando se lleva a cabo en lugares públicos[75]. Tal es así, que esta medida es legítima incluso aunque afecte a personas diferentes del investigado cuando no exista otro modo útil de vigilancia o cuando existan indicios fundados de la relación de dichas personas con el investigado y con los hechos objeto de la investigación[76].

Ello, no obstante, nada se dice con respecto a su duración, por lo que habrá que estar a las disposiciones comunes de las diligencias de investigación tecnológica que, como se ha visto, limitan su práctica al al tiempo imprescindible para el esclarecimiento de los hechos, un plazo jurídico indeterminado que habrá que concretarse en cada caso.

Esta norma es fruto de la extensa jurisprudencia que ya admitía la grabación en lugares públicos sin necesidad de autorización judicial[77]. Si bien, es preciso conocer que la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos exige la obtención de una autorización judicial para la grabación con una finalidad preventiva dirigida a una pluralidad de destinatarios[78]. En este sentido, las FFCCSS necesitan de previa autorización judicial para la grabación indiscriminada de imágenes en lugares públicos, pero no es preceptiva cuando la captación de imágenes en la vía pública u otro espacio abierto se dirija a la vigilancia, el registro o el seguimiento de sospechosos de cometer actividades delictivas.

75 DURÁN SILVA, C.M., "Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado". En: *La Ley penal: revista de derecho penal, procesal y penitenciario*, nº 126, 2017.

76 Vid. artículo 588 quinquies a), apartado segundo LECrim.

77 SSTS 6 de mayo de 1991; 6 de mayo de 1993; 7 de febrero de 1994; 6 de abril de 1994; 21 de mayo de 1994; 18 de diciembre de 1995; 27 de febrero de 1996; 913/1996, de 25 de noviembre; 5 de mayo de 1997; 968/1998, de 17 de julio; 188/1999, de 15 de febrero; 14 de octubre de 2002; 354/2003, de 13 de marzo.

78 Un estudio pormenorizado de la cuestión en DURÁN SILVA, C.M.: *La videovigilancia en el proceso penal: tratamiento procesal y eficacia probatoria*. Tirant Lo Blanch, Valencia, 2017.

6. El control remoto de seguimiento y localización.

Los artículos 588 quinquies b) y c) LECrim regulan la utilización policial de dispositivos o medios técnicos de seguimiento y localización (comúnmente denominados balizas o *beepers*) con el propósito de controlar la posición geográfica de un sujeto investigado en el curso de una instrucción[79].

Cabe reparar, no obstante, que esta diligencia mostrará el posicionamiento del objeto sobre el que se ha instalado el dispositivo, pero no necesariamente de una persona en particular, que puede no estar portándolo, a bordo de la embarcación o conduciendo el vehículo balizado[80].

Si bien es cierto que la geolocalización es una medida más segura y eficaz que un seguimiento vigilado convencional y que, además, necesita de menos agentes para su puesta en práctica; no lo es menos que es más intrusiva para los derechos fundamentales de los investigados, en tanto en cuanto permite el control de los movimientos del sujeto pasivo incluso en espacios privados o en aquellos en los que no sería posible mantener el control visual[81]. Por ello, la adopción de esta diligencia necesita de previa

79 El Auto del Tribunal Superior de Justicia de Cataluña de 10 de abril de 2014 define baliza como aquel "pequeño dispositivo que, recibiendo datos de posicionamiento GPS, transmite su localización a otro dispositivo manejado por los agentes investigadores; permitiendo de este modo, y con total precisión, hacer un seguimiento minucioso de todos los movimientos del objeto seleccionado, sin más limitaciones que la de la capacidad de la batería que alimente al dispositivo oculto".

80 Recientemente se ha dictado la STS 141/2020, de 13 de mayo sobre la utilización de dispositivos y medios técnicos de seguimiento y localización que señala que la ubicación espacio-temporal del sospechoso también puede posibilitar, en ocasiones, "precipitar una radiografía ideológica o religiosa del investigado a raíz del conocimiento de su asistencia a actos públicos de una determinada formación política, el seguimiento de actos de culto de una u otra confesión religiosa, la presencia en centros de ocio expresivos de la opción sexual del investigado o, en fin, la permanencia en un centro sanitario para cualquier intervención quirúrgica".

81 Vid. VELASCO NÚÑEZ, E., "Tecnovigilancia, geolocalización y datos: aspectos procesales penales*"*. En: *Diario La Ley*, nº 8338, Año XXXV, Editorial LA LEY, 23 de junio de 2014. p. 8. Sobre esta cuestión, contrariamente a lo expuesto, Reyes López opina que la determinación espacial que realizan los dispositivos técnicos no es tan exacta como la efectúan visualmente los agentes y que, por tanto, el sacrificio del derecho es menor, en REYES LÓPEZ, J.I.: "Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la L.O. 13/2015". En: *Revista Aranzadi Doctrinal*, nº 4, Editorial Aranzadi, Cizur Menor, 2016. Resulta curiosa la sentencia 216/2016 de la Audiencia Provincial de Navarra, de 29 de julio en la que la policía afirma que "dispositivo de control" es un término técnico-policial para referirse a la ubicación estratégica y discreta de efectivos policiales sobre una persona, objeto, vehículo o lugar para proceder a su vigilancia y

autorización del juez competente[82], que, recuérdese, deberá sujetarse a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en sentido estricto, de acuerdo con las bases comunes que el artículo 588 bis a) dicta para las medidas tecnológicas[83].

---

control y no a un dispositivo de control instalado en un vehículo del investigado, para el que no se había solicitado la preceptiva autorización judicial (vulnerando el art. 588 quinquies b) y por el que el apelante instaba la nulidad de actuaciones porque entiende que la localización del domicilio en el que se había realizado una entrada y registro se conocía por la instalación de una baliza de seguimiento en el vehículo del investigado.

82 Conforme a los artículos 588 bis b y c, aplicables a los capítulos V a IX del Título VIII del Libro II de la LECrim y, por tanto, a la utilización de dispositivos técnicos de seguimiento y localización, esta habilitación judicial se puede acordar de oficio o a instancia del Ministerio Fiscal o de la Policía Judicial. Si se solicita, la petición debe contener: 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. En todo caso, la autorización deberá dictarse –en forma de auto motivado- en el plazo máximo de veinticuatro horas desde la solicitud (de ser el caso) conteniendo, al menos, los siguientes extremos: a) El hecho punible objeto de investigación y su calificación jurídica, con expresión de los indicios racionales en los que funde la medida, b) La identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido, c) La extensión de la medida de injerencia, especificando su alcance así como la motivación relativa al cumplimiento de los principios rectores establecidos en el artículo 588 bis a, d) La unidad investigadora de Policía Judicial que se hará cargo de la intervención, 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.

83 Cabría preguntarse si no es una reiteración que el mismo artículo 588 quinquies b se refiera a que se aprobará judicialmente la utilización de estos dispositivos de investigación si concurren "razones de necesidad y la medida result[a] proporcionada", cuando son de aplicación a la autorización que habilita la adopción de esta medida los citados principios rectores del artículo 588 bis a, que ya recoge los principios de necesidad y proporcionalidad. Esta mención expresa puede tener su origen en la STEDH Uzun c/ Alemania, de 2 de diciembre que disponía que el uso de los dispositivos GPS es una injerencia en la vida privada porque recopila información sistemática de una persona y su utilización sólo es legítima si es acorde a los principios de proporcionalidad y necesidad.

Para el supuesto en el que concurran razones de urgencia tales que, de no adoptarse la medida, se frustraría la investigación, la Policía Judicial está legitimada para la colocación de estos dispositivos, informando y solicitando inmediatamente su confirmación o rechazo a la autoridad judicial (siempre en un plazo no superior a veinticuatro horas) para que este (también en un máximo de veinticuatro horas) permita la continuación de la medida u ordene su cese inmediato[84]. Si el juez no ratifica el control remoto puesto en práctica por los agentes, lo obtenido hasta el momento no podrá utilizarse posteriormente en un proceso[85].

Nada dice la ley, sin embargo, sobre si, para la instalación de estos dispositivos, es posible el acceso a espacios protegidos por el 18.2 CE, como puede ser en un domicilio, en el interior de una embarcación que sirva de vivienda o una autocaravana, si bien, cabe entender que es necesaria motivación judicial adicional.

Por lo que a la duración hace referencia, el Juez autorizará la utilización de estos dispositivos técnicos de seguimiento y localización por el tiempo imprescindible para el esclarecimiento de los hechos[86] y, en todo caso, por un máximo de tres meses, prorrogables judicialmente –de oficio o previa petición razonada del Ministerio Fiscal o la Policía Judicial[87]- si existen

84 La autorización judicial para la instalación de balizas de seguimiento no venía exigiéndose jurisprudencialmente de manera general, vid. las SSTS 942/2004, de 22 de julio; 562/2007, de 22 de junio; 523/2008, de 11 de julio; 906/2008, de 19 de diciembre; 798/2013, de 5 de noviembre, casi todas referidas a balizas usadas sobre embarcaciones. El Preámbulo de la LO 13/2015 justifica la necesaria autorización judicial para la utilización de dispositivos técnicos de seguimiento y localización en la incidencia sobre la intimidad que produce que los poderes públicos puedan conocer la ubicación espacial de una persona.

85 La información obtenida por dispositivos de seguimiento y localización sin autorización judicial *ex ante* o *ex post* carece de efectos en el proceso porque así lo dispone explícitamente el artículo 588 quinquies b 4, si bien es más discutible que se haya obteniendo vulnerando derechos fundamentales porque la jurisprudencia previa a la aprobación de este precepto entendía que no, vid. las SSTS 942/2004, de 22 de julio; 562/2007, de 22 de junio; 523/2008, de 11 de julio; 906/2008, de 19 de diciembre; 798/2013, de 5 de noviembre.

86 El artículo 588 bis e) LECrim determina que las medidas reguladas en los capítulos V a IX del Título III del Libro II LECrim no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.

87 Así se desprende de la lectura conjunta de los artículos 588 bis e) y f) LECrim, aplicables a esta medida de investigación. De acuerdo con estos preceptos, también hay que tener en cuenta que si la solicitud de prórroga proviene del Ministerio Fiscal o la Policía Judicial, deberá incluir en todo caso un informe detallado del resultado de la medida y las razones que justifiquen la continuación de la misma. En el plazo de los dos días

motivos justificados tras el análisis de los resultados obtenidos, por un periodo igual o inferior, hasta un total de dieciocho meses[88]. En atención a la limitación temporal es posible que, transcurrido el plazo, los agentes policiales no tengan acceso a la baliza para recuperarla y desactivarla. En el caso de que la medida continuase más allá del periodo autorizado, la información así conocida no podrá incorporarse al acervo probatorio por ausencia de habilitación judicial.

El control se realiza cuando el Juez lo solicite y, en todo caso, cuando terminen las investigaciones, entregándole la información en los soportes originales o en copias electrónicas auténticas[89]. Como no podía ser de otro modo, la LECrim indica expresamente que la información obtenida a través de esta diligencia deberá ser debidamente custodiada para evitar su utilización indebida[90].

Finalmente, igual que sucede con la diligencia de interceptación de las comunicaciones telefónicas y telemáticas, el artículo 588 quinquies b) también establece a los prestadores, agentes y personas que nombra el artículo 588 ter e) un deber de asistencia y colaboración para con el juez, el Ministerio Fiscal y la Policía Judicial designados para la práctica de la medida[91]. El incumplimiento de este deber podría considerarse como un delito de desobediencia.

7. El registro de dispositivos de almacenamiento masivo de información.

El acceso a la información contenida en ordenadores, instrumentos de comunicación telefónica o telemática, dispositivos de almacenamiento

siguientes a la presentación de la solicitud, el juez resolverá sobre el fin de la medida o su prórroga mediante Auto motivado, si bien podrá solicitar aclaraciones o mayor información antes de dictar la resolución. Concedida la prórroga, su cómputo se iniciará desde la fecha de expiración del plazo de la medida acordada.

88 Se entiende, por tanto, que, si la policía judicial ha adoptado la medida sin la previa autorización judicial por concurrir razones de urgencia, el plazo de tres meses se inicia a partir de la fecha de la ejecución de la medida y no de la posterior autorización, en caso de confirmarse la legalidad de la misma.

89 Vid. Artículo 588 quiquies c) LECrim.

90 Artículo 588 quinquies c 3.

91 Resulta algo extraña la alusión al artículo 588 ter e, cuando podría reproducir en el artículo los sujetos a los que se refiere el citado precepto, sin necesidad de remitir a la interceptación de comunicaciones telefónicas y telemáticas.

masivo de información digital[92] o a repositorios telemáticos de datos aprehendidos necesita de previa autorización motivada del juez de instrucción[93]. Tal resolución fijará los términos y el alcance del registro, así como las condiciones y garantías de su preservación que posibiliten la práctica de un posterior dictamen policial[94]. En este sentido, no es admisible un registro ilimitado[95], si bien es cierto que la delimitación de la injerencia *ex ante* se torna, en la práctica, algo complicada, porque aunque en ocasiones es posible conocer qué elementos se quieren examinar, únicamente una valoración posterior permite determinar la relación de

92 Sobre la conceptualización de los dispositivos de almacenamiento masivo de información véase el acertado estudio pormenorizado realizado en BUENO DE MATA, F.: *Las diligencias de investigación penal en la cuarta revolución industrial*, Aranzadi, 2019. pp. 164 y ss.

93 Que, como señala FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.Á.: "Registro de dispositivos de almacenamiento masivo". En: *Dereito*, vol. 25, nº2, 2016. p. 37, deberá tomar en consideración los principios rectores establecidos en el artículo 588 bis a) LECrim.

94 A estos requisitos previstos en el artículo 588 sexies c) LECrim habrá que añadir las exigencias comunes a todas las diligencias de investigación reguladas en el capítulo IV del título VIII del Libro II de la LECrim, que contempla que la autorización judicial se sujete a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en la medida y que concrete, al menos, el hecho punible objeto de investigación y su calificación jurídica, la identidad de los investigados y de cualquier otro afectado por la medida, de ser conocido, la extensión de la medida de injerencia, especificando su alcance, la unidad investigadora de Policía Judicial que se hará cargo de la intervención, la duración de la medida, la forma y la periodicidad con la que el solicitante informará al juez sobre los resultados de la medida, la finalidad perseguida y 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. En atención al cumplimiento del principio de proporcionalidad, Cabezudo Bajo critica que las disposiciones específicas de esta medida de investigación no definan unos delitos concretos ni exijan que la resolución judicial se motive en atención a la probabilidad de éxito del fin perseguido, en CABEZUDO BAJO, cit., p. 91. Así, el Auto de la Audiencia Provincial de Tarragona, sección 2, 27/2020, de 17 de enero decreta la nulidad de la autorización judicial del volcado para su posterior estudio de toda la información obrante en unos móviles incautados a unos detenidos, por no hacer referencia a los delitos por los que se incoan las Diligencias Previas, ni realizar la necesaria ponderación con los derechos del investigado.

95 Recuérdese que "la investigación delictiva, la actuación estatal en la represión penal, está sujeta a los límites y condiciones impuestos por las normas constitucionales y procesales que salvaguardan la eficacia, intangible más allá de las restricciones admisibles, de los derechos y libertades fundamentales", como señala ASENCIO MELLADO, J. M.: "El proceso penal con todas las garantías". En: *IUS ET VERITAS: Revista de la Asociación IUS ET VERITAS*, nº 33, 2006. p. 236.

los archivos con el objeto de la investigación[96]. En todo caso, se evitará la incautación de los soportes físicos 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, salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen[97].

Así, la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos y el acceso a los mismos puede realizarse durante el transcurso de una diligencia de registro domiciliario o con independencia de ella[98]. En ambos supuestos es necesaria previa autorización expresa y razonada del juez instructor[99]. Si es previsible el hallazgo de tales dispositivos durante

96 Como acertadamente apunta Rodríguez Lainz, "sería pecar de una ingenuidad extrema pensar que un terrorista va a abrir una carpeta con el nombre "organigrama de la célula" y, en ese sentido, aboga por examinar todos los archivos, en RODRÍGUEZ LAINZ, cit., p. 9. Esta cuestión se plantea en la STEDH Robathin c. Austria, de 3 de julio de 2012 -disponible en http://hudoc.echr.coe.int/eng?i=001-111890-, que no considera desproporcionado el examen de todos los archivos electrónicos del investigado porque se había realizado a nivel superficial, servía a un objetivo legítimo y los derechos del encausado habían sido interferidos en la menor medida posible. Resulta de interés la STS 311/2020, de 15 de junio, que analiza un supuesto en el que, para superar este escollo, los agentes, en el contexto de una entrada y registro autorizada judicialmente, solicitan al investigado las claves de acceso a los equipos informáticos para realizar una inspección superficial de los mismos para determinar los que debían ser objeto de incautación, "dado que el auto judicial habilitante sólo permitía la intervención de los elementos (ordenadores, soportes informáticos, terminales de telefonía móvil, etc.) que tuvieran relación directa o indirecta con las actividades investigadas, lo que exigía ese previo examen superficial".

97 Así se desprende del artículo 588 sexies c) 2 LECrim.

98 En este sentido, Gimeno Beviá alega que no tiene sentido un tratamiento separado en función de que el dispositivo se encuentre en un domicilio o fuera de él porque las garantías son las mismas, en GIMENO BEVIÁ, J., cit., p. 208.

99 Vid. artículo 588 sexies, letra a) LECrim. Este precepto exige justificación motivada en la autorización judicial con respecto a la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital, o el acceso a repositorios telemáticos de datos, a fin de individualizar la ponderación judicial de la limitación de los diversos derechos fundamentales afectados. Con anterioridad a la inclusión de esta medida operada por el artículo diecisiete de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, la jurisprudencia entendía que la autorización judicial para la entrada en el domicilio del investigado amparaba cualquier otro acto de injerencia como la aprehensión de todos aquellos soportes de información

el registro domiciliario (y se entiende preciso su examen), podrá incluirse, en una misma resolución judicial, ambas autorizaciones con motivación individualizada[100]. Si, por el contrario, este registro no se prevé en el auto de entrada en el domicilio, el órgano judicial podrá dictar una segunda resolución que contenga la necesaria habilitación prevista en el artículo 588 sexies c[101].

En casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida, la Policía Judicial podrá acceder a la información contenida en el dispositivo incautado, poniendo inmediatamente (y en todo caso dentro del plazo máximo de veinticuatro horas) en conocimiento del juez tal circunstancia, junto con las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas a contar desde que esta fue ordenada.

Además, las autoridades y agentes encargados de la investigación podrán pedir a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo (salvo al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco o a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional) que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para

que pueda encontrarse en el interior de la vivienda al entender que el registro de libro y papeles y recogida de otros efectos e instrumentos del delito incluía también el registro de estos instrumentos -véanse las SSTS 4745/2002, de 27 de junio; 2809/2008, de 14 de mayo; 691/2009, de 5 de junio-. El TS ha comenzado ya a adoptar esta exigencia, diversa al criterio histórico, vid. STS 786/2015, de 4 de diciembre.

100 Así puede verse el Auto del Tribunal Supremo 691/2020, de 10 de septiembre que inadmite la petición del recurrente que alega nulidad de la información obtenida de un teléfono móvil porque se obtiene de un teléfono móvil al que se accede en el curso de un registro domiciliario que no cuenta con la correspondiente orden judicial. Al respecto, el Alto Tribunal sostiene que no hay vulneración del 18.2 porque el investigado autoriza en presencial de su Abogado la entrada en la vivienda y el registro del móvil cuenta con la preceptiva resolución judicial.

101 Vid. artículo 588 sexies, letra c) LECrim. La necesidad de motivar judicialmente el acceso al contenido de los dispositivos tecnológicos de manera diferenciada a la justificación que habilite el registro del domicilio ha sido puesto de manifiesto, antes y después de la reforma, por las SSTS 985/2009, de 13 de diciembre; 342/2013, de 17 de abril; 587/2014, de 18 de julio y 97/2015, de 24 de febrero.

el afectado, bajo apercibimiento de incurrir en delito de desobediencia[102]. Ello, no obstante, existen dudas acerca de la materialización de este deber de colaboración.

El estado de la técnica permite, también, el acceso remoto a datos que, aunque no se encuentren contenidos en el dispositivo sobre el que se realice la exploración, sean accesibles a través del mismo por medio de lo que se conoce como registro ampliado o *extended search of computers*[103]. Esta información disponible desde un primer dispositivo intervenido físicamente para el que se ha autorizado su registro se refiere, en la mayoría de las ocasiones, a aquella contenida en la nube o *cloud computing*[104], si bien, también puede estar en una red local (*computer network*).

La ampliación lícita del registro de un sistema a aquellos datos accesibles exige autorización judicial, que puede venir contenida en la habilitación inicial de registro o concederse posteriormente[105]. Si concurren razones de urgencia y se aprecia un interés constitucional legítimo que haga imprescindible la medida, la LECrim habilita a la Policía Judicial o al Ministerio Fiscal para que lleve a cabo la ampliación del registro, siempre que informe al juez competente sobre la forma en

102 Es necesario contraponer el deber de colaboración previsto en el artículo 588 sexies c 5 LECrim para el registro de dispositivos de almacenamiento masivo de información con el exigido para el registro remoto sobre equipos informáticos que contempla el artículo 588 septies b LECrim. Este análisis muestra que el primero de los preceptos citados es el mismo que el segundo apartado del artículo 588 septies b, si bien tienen una parte distinta (el deber de colaboración del registro de dispositivos de almacenamiento masivo de información se exceptúa cuando de ello derive una carga desproporcionada para el afectado y, para el registro remoto sobre equipos informáticos se dice que esta obligación se refiere a la información que resulte necesaria "para el buen fin de la diligencia"). Del enfrentamiento de estas dos reglas, Rodríguez Lainz destaca que la primera se refiere a la facilitación de conocimientos y, la segunda, va más allá y se refiere a que los sujetos mencionados están obligados a facilitar la colaboración y asistencia, en RODRÍGUEZ LAINZ, cit., pp. 10-11. En ese sentido, continúa el autor, se da la paradoja de que la colaboración a la Policía judicial es más amplia en el registro remoto de un dispositivo que en el registro físico del mismo.

103 BACHMAIER WINTER, cit., p. 5.

104 Las organizaciones que prestan servicios de *cloud computing* almacenan la información de sus usuarios de manera permanente en servidores alojados en cualquier parte del mundo y la envían a través de Internet a cachés temporales del equipo informático del usuario que asocie a esa "nube" o con el que acceda a él (equipo portátil, equipo de sobremesa, tableta, Smartphone…). Drive o Dropbox son ejemplos de servicios de *cloud computing.*

105 Art. 588 sexies c) LECrim que recoge lo ya dispuesto en el artículo 19.2 del Convenio de Budapest.

que se ha efectuado y su resultado en el momento más inmediato y, en todo caso, siempre en el plazo máximo de veinticuatro horas desde la actuación[106]. El juez, también de forma motivada, revocará o confirmará tal actuación en un máximo de setenta y dos horas desde que fue ordenada la interceptación[107].

Pese a que nada dice la Ley al respecto, parece acertado aplicar el artículo 588 bis k) LECrim para que se acuerde su destrucción de la información obtenida en los supuestos en los que no venga ratificada *a posteriori.*

8. El registro remoto o *hacking judicial.*

El registro remoto, registro *online, remote search* o *hacking judicial* es una técnica de investigación que consiste en el acceso y exploración a distancia de un sistema informático o dispositivo electrónico del sujeto investigado, sin su conocimiento[108]. Por lo general, esta diligencia exige que los equipos estén en funcionamiento y en línea, lo que complica su ejercicio[109].

La regulación de esta práctica en los artículos 588 septies, letras a)-c) LECrim supone un avance importante, porque venía utilizándose, por aplicación analógica, la tradicional recogida de los efectos del delito como

106 Art. 588 sexies c) LECrim, apartado cuatro.

107 Adviértase que el apartado tercero del art. 588 sexies c) LECrim habilita a la Policía Judicial y al Ministerio Fiscal a ampliar en registro sin previa autorización judicial cuando concurra urgencia y, el apartado cuarto de este mismo precepto, faculta a la Policía judicial a llevar a cabo las medidas previstas en los apartados anteriores sin previa autorización judicial cuando concurra urgencia e interés constitucional legítimo, comunicándolo al juez competente en las mismas condiciones que lo referido para la ampliación del registro que regula el apartado tercero. Esta doble previsión, que no coincide en su totalidad, recogidas en dos preceptos consecutivos de un mismo artículo demuestra una técnica legislativa deficiente que debiese corregirse.

108 PRADILLO, J.C.: *Problemas procesales de la ciberdelincuencia*. Colex Editorial Constitución y Leyes, Madrid, 2013. p. 177; AGUSTINA SANLLEHÍ, J. R.: "*Algunas consideraciones sobre el denominado hacking judicial"*. En: *Iuris*, nº 199, Sección Tribuna, Quincena del 1 al 14 octubre. Editorial La Ley, 2013. Rodríguez Lainz apunta que el registro remoto, a diferencia con la intervención de las comunicaciones, se obtiene del dispositivo, esto es, de la misma fuente de origen, en RODRÍGUEZ LAINZ, J.L.: "Intervención judicial de comunicaciones vs. Registro remoto sobre equipos informáticos: los puntos de fricción". En: *Diario La Ley*, nº 8896, 9 de enero de 2017. p. 8.

109 RICHARD GONZÁLEZ, cit*.,* p. 18.

diligencia habilitante para examinar los dispositivos electrónicos hallados en una entrada y registro en lugar cerrado[110].

En la actualidad hay tres formas distintas de llevar a cabo el registro remoto, en primer lugar, con la instalación de un software, conocido como "troyano" o *spyware*[111], que accede al contenido del dispositivo que se pretende analizar; en segundo lugar, con el uso de códigos o datos de identificación que permiten el ingreso a los contenidos del dispositivo y, en tercer lugar, con la instalación de un *keylogger*, esto es, un instrumento que, a través de un hardware o un software, almacena las pulsaciones que se realizan en el teclado de un dispositivo[112].

Este tipo de registros puede resultar útil cuando el dispositivo electrónico investigado se encuentra en constante movimiento (como ocurre, por ejemplo, con los *smartphones*); cuando el acceso al lugar donde este se halle suponga un peligro para la vida o integridad física de los agentes, de la información o del propio equipo informático; o cuando sea necesario acceder al equipo informático en tiempo real para capturar las claves utilizadas para descifrar el uso de criptografía en la información almacenada[113].

Esta medida de investigación, como puede advertirse, es harto invasiva y afecta a derechos fundamentales tales como el del secreto de las comunicaciones[114], a la protección de datos, a la inviolabilidad del domicilio

110 AGUSTINA SANLLEHÍ, cit., p. 4; ORTIZ PRADILLO, cit., pp. 178 y ss.

111 "Troyano" y *spyware* son programas espías que acceden al contenido del dispositivo en el que se instalan. El primero, como puede deducirse, debe su nombre al mitológico caballo de Troya.

112 DELGADO MARTÍN, J.: "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015". En: *Diario La Ley*, nº 8693, Sección Doctrina, 2 de febrero. Editorial La Ley, 2016. p. 14. Rodríguez Lainz indica que la utilización de códigos o datos de identificación comporta de la colaboración de terceros o de operadores que presenten servicio de la sociedad de la información y de un acceso para activar las claves que se torna complejo y, con respecto a la utilización de troyanos, expone que pueden acceder al dispositivo aprovechando su conexión a una red pública o a canales de compartición de información o por medio de un envío adjunto en un correo o mensaje, si bien, en ocasiones, se necesitará desactivar niveles o protocolos de seguridad de forma manual, en RODRÍGUEZ LAINZ, cit., p. 7.

113 DELGADO MARTÍN, J.: "La prueba electrónica en el proceso penal". En: *Diario La Ley,* Sección doctrina, La Ley, nº 8167, 2013.

114 Así, el acceso al contenido de un dispositivo electrónico implica en numerosas ocasiones también el registro de las telecomunicaciones escritas almacenadas en el dispositivo. Bachmaier Winter compara los requisitos necesarios para el registro remoto y para la interceptación telefónica y concluye que la interceptación telefónica se autoriza

(si el dispositivo capta lo que sucede en el interior de una vivienda) y, especialmente, al propio entorno virtual, una nueva garantía de creación jurisprudencial[115].

Por ello, esta diligencia únicamente está prevista para los delitos contra menores o personas con capacidad modificada judicialmente, contra la Constitución, de terrorismo, de traición y relativos a la defensa nacional, perpetrados en el seno de organizaciones criminales y cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación[116]. Un representativo sector doctrinal ha criticado, con acierto, que se permita un grado de injerencia tan grave por el único hecho de que el delito se haya consumado en el ámbito digital, sin atender a su gravedad[117].

---

para la investigación de los delitos cuya pena no llegue a los tres años de privación de libertad (salvo que se trate de los delitos de delincuencia organizada, terrorismo o delitos cometidos a través de sistemas informáticos) y el registro remoto para delitos concretos, independientemente de la pena prevista para los mismos; por lo que deduce que la intención del legislador no ha sido cubrir la interceptación en tiempo real de las telecomunicaciones con el registro remoto, aunque el acceso a esas comunicaciones en poco o nada se diferencia en la mayoría de los casos de su interceptación en tiempo real, vid. BACHMAIER WINTER, cit., p. 14.

115 RICHARD GONZÁLEZ, M., cit., p. 18. Me ocupo de este nuevo derecho fundamental en ARRABAL PLATERO, P.: "El derecho fundamental al propio entorno virtual y su incidencia en el proceso". En: *Era Digital, Sociedad y Derecho*. Dir. Fuentes Soriano; Coords. Arrabal Platero, Doig Díaz, Ortega Giménez, Turégano Mansilla. Tirant Lo Blanch, Valencia, 2020. pp. 431-441 y en ARRABAL PLATERO, P.: *La prueba tecnológica: aportación, práctica y valoración*.Tirant Lo Blanch, Valencia, 2020.

116 Vid. artículo 588 septies a) LECrim.

117 En este sentido, González Navarro afirma que "parece que con ello se equipara el hecho de que para la comisión del hecho delictivo se hayan utilizado las nuevas tecnologías con que para la investigación de los hechos (que perfectamente pueden ser de escasa relevancia, pues nada especifica el precepto en sentido contrario) se utilice una medida tan gravosa como la que aquí se estudia. Sin embargo, entiendo que la sola existencia de un ilícito penal que haya sido cometido por medio de instrumentos informáticos o de cualquier otra tecnología de la información no puede ser suficiente para legitimar, por sí misma y de forma automática, la utilización de esta medida", en GONZÁLEZ NAVARRO, A.: "Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana". En: *El proceso penal. Cuestiones fundamentales.* Coord. Fuentes Soriano. Tirant lo Blanch, 2017. p. 404. En la misma línea, entre otros, BUENO DE MATA, F.: "Drones, virus espía y agentes encubiertos en la Red". Ponencia presentada al XIX CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA MEDELLÍN, del 26 al 28 de agosto de 2015. p. 19. Bachmaier Winter justifica este supuesto en una recomendación del Convenio de Budapest que se puede leer en el Informe Explicativo del Convenio, en BACHMAIER WINTER, cit., pp. 13-14.

La adopción de esta diligencia necesita de previa aprobación en forma de Auto motivado por el juez que instruya la causa en un plazo de veinticuatro horas desde que se formule la solicitud. Esta resolución judicial debe cumplir con las disposiciones comunes previstas en los artículos 588 bis a)-c) LECrim[118] y ha de detallar numerosos datos, véase: qué dispositivos o sistemas informáticos son objeto de la medida; el alcance y forma de la misma; el software mediante el que se ejecutará el control de la información[119]; los agentes autorizados que accederán y aprehenderán los datos o archivos informáticos relevantes para la causa[120]; las medidas precisas para la preservación de la integridad de los datos almacenados y para la inaccesibilidad o supresión de los mismos del sistema informático al que se ha tenido acceso; y, en su caso, la autorización para la realización y conservación de copias de los datos informáticos -estos extremos se podrán ampliar judicialmente cuando los policías que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo-[121]. La exigencia de autorización judicial se extiende, incluso, al registro ampliado de datos que puedan estar almacenados en otro sistema informático o parte del mismo[122].

118 Bachmaier Winter sostiene que la justificación de la aplicación del principio de proporcionalidad para la adopción del auto judicial motivado se cierne compleja cuando no se trata de delitos graves, especialmente cuando estamos ante delitos cometidos a través de sistemas informáticos cuya pena prevista no es elevada, porque el perjuicio que esos delitos causan a la sociedad no siempre es tan evidente, en BACHMAIER WINTER, cit., pp. 22-23.

119 BACHMAIER WINTER, cit., p. 28 afirma que "los jueces de instrucción no tienen conocimientos de informática suficientes para decidir cuál es el software que debe utilizarse para el registro remoto o cómo debe realizarse la copia y conservación de los datos que se aprehendan. Al respecto, y en tanto los jueces de instrucción no reciban formación especializada en estas materias y se elabore un protocolo de ejecución de estas medidas, habrán de confiar en las indicaciones que reciban de los propios agentes especializados en delitos telemáticos o en peritos informáticos".

120 Richard González prevé la posibilidad de que esta medida se conceda asociada a la figura del agente encubierto informático, previsto *ex novo* por la *Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica* en el artículo 282 bis LECrim, en RICHARD GONZÁLEZ, cit., p. 19.

121 Artículo 588 septies a) y las disposiciones comunes a todas las diligencias tecnológicas previstas en el artículo 588 bis, letra c, apartado tercero LECrim.

122 La previsión de ampliar el registro a información contenida en otro sistema informático o parte de él también se regula con respecto al registro de dispositivos de almacenamiento masivo de información en el que, además y a diferencia de lo que establece el artículo 588 septies a 3 para el registro remoto, podrá llevarse a cabo de urgencia por el Ministerio Fiscal o la Policía judicial informando al juez en el plazo máximo de veinticuatro horas para que pueda refrendar o censurar la actuación.

Con respecto a su limitación temporal, la medida se ceñirá al tiempo estrictamente imprescindible para el esclarecimiento de los hechos[123], si bien tendrá una duración máxima de un mes, prorrogable por iguales periodos hasta un máximo de tres, siempre que la diligencia siga siendo adecuada, necesaria y proporcional[124]. Para el cómputo del plazo parece acertado tomar como *dies a quo* el momento en que se ha instalado y está operativo el software en el equipo en cuestión y este resulte accesible y, como *dies a quem* o momento que debiese cesar la medida, el que finaliza la efectiva clonación del contenido del dispositivo[125]. Por tanto, no se trata de una injerencia puntual, sino que, más bien, se trata de una intrusión continua del poder público[126], lo que, sumado a la clandestinidad que conlleva su carácter remoto se traduce en una importante limitación en los citados derechos fundamentales[127].

También se prevé la obligada colaboración de los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como de toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual y los titulares o responsables del sistema informático o base de datos objeto del registro para facilitar a los investigadores la práctica de

123 Tal y como establecen las disposiciones comunes del artículo 588 bis e LECrim para los actos de investigación regulados en los capítulo V a IX del título VIII del Libro II de la citada ley procesal.

124 Artículo 588 septies c. Véase que, al contrario de lo que sucede con los plazos previstos para la intervención de las comunicaciones, éstos plazos sí son acordes con los previstos para la declaración del secreto del sumario, aunque no coinciden con la prevista para las otras medidas de investigación telemática. Ello no obstante, el artículo 588 bis d LECrim declara expresamente el secreto de la causa automático para las diligencias tecnológicas.

125 Vid. BACHMAIER WINTER, cit., p. 18.

126 DELGADO MARTÍN, cit., p. 13. Sobre el particular, CONDE-PUMPIDO TOURÓN alega que si el objeto de la medida es "el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos", ésta debería estar limitada temporalmente a obtener una copia de los archivos en un momento concreto, pero que la duración de la medida de hasta tres meses no parece avalar esta interpretación, en "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)", ponencia dictada en las Jornadas de Especialistas en Criminalidad Informática celebradas por el Ministerio Fiscal el 10 marzo 2016, p. 13, disponible en https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Conde-Pumpido%20Tour%C3%B3n.pdf?idFile=4d9fe168-e9ee-4cd9-a783-68eab6158e47 (fecha de consulta: 17/01/2018).

127 BACHMAIER WINTER, cit., p. 7.

la medida, el acceso al sistema y la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización[128]. Del mismo modo, las autoridades y los agentes encargados de la investigación podrán ordenar a cualquiera que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo -salvo excepciones[129]- que facilite la información que resulte necesaria para el buen fin de la diligencia. Los sujetos citados tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades y podrán incurrir en delito de desobediencia[130].

III. CONCLUSIONES

Primera. Es reseñable y digno de elogio el esfuerzo del legislador por regular estos nuevos actos de investigación para dotarles de legalidad, así como la labor didáctica que realiza en la descripción de cada uno de los principios que deben regir la concesión de una autorización judicial (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad en sentido estricto).

Segunda. Todavía quedan cuestiones que necesitan ser matizadas, como la idoneidad de que se adopten todas las diligencias tecnológicas en una misma pieza separada que mejore su control judicial; que se prevea también la eliminación de los registros que están en posesión de las partes; la efectiva notificación a los terceros afectados en la intervención de las comunicaciones; o la eliminación de los delitos cometidos en Internet como supuesto para la adopción del *hacking* judicial. Quizás, como suele ocurrir, será la jurisprudencia la que nos ofrezca soluciones[131].

128 Artículo 588 septies b) LECrim.

129 No estarán obligados a colaborar el investigado o encausado, las personas que están dispensadas de la obligación de declarar por razón de parentesco, o aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

130 Vid. artículos 588 septies b) y 588 ter e) LECrim.

131 Una jurisprudencia como la que señala Molina Navarrete cuando señala que "la jurisprudencia "originariamente procede de la suma de dos vocablos tenidos siempre por solidos: *iuris* (Derecho) y *prudentia* (sabiduría). En la hermosa novela histórica «Memorias de Adriano», el insigne emperador –español, por cierto– ya utilizaba esa identificación entre «sabiduría», «prudencia» y «robustez» del conocimiento –lo aplicaba a su médico, que había ejercido con éxito la medicina más de 3 décadas–. Y eso pareció identificar durante tiempo la «jurisprudencia», esa sabiduría fraguada por el sucederse de las decisiones de los más altos tribunales de forma reiterada, reflexiva, seria, sólida, en definitiva", en MOLINA NAVARRETE, C.: "Ahora que el TC recela de la «cámara oculta», el TEDH la respalda en las empresas: La insoportable «liquidez» de la jurisprudencia". En: *Revista de Trabajo y Seguridad Social. CEF*, 2019.

Tercera. Sería deseable en pro de una buena técnica legislativa, que las disposiciones comunes regulen aspectos que afecten a todas las diligencias para las que están previstas y que no redunden en aspectos que ya prevén las normas específicas. Igualmente, también es importante que las disposiciones no se conviertan en remisiones, como ocurre con los hallazgos casuales.

BIBLIOGRAFÍA

AGUSTINA SANLLEHÍ, J.R.: "Algunas consideraciones sobre el denominado hacking judicial". En: *Iuris*, nº 199, Sección Tribuna, Quincena del 1 al 14 octubre, Editorial La Ley, 2013

ARMENTA DEU, T.: *Lecciones de Derecho Procesal Penal* (quinta edición), Marcial Pons, Madrid, 2010

ARRABAL PLATERO, P.: "Algunas cuestiones controvertidas sobre la obtención de datos de tráfico". En: *La justicia digital en España y la Unión Europea: situación actual y perspectivas de futuro*. Dirs. Conde Fuentes, Serrano Hoyo; Coords. Arrabal Platero, García Molina. Atelier, Barcelona, 2019.

ARRABAL PLATERO, P.: "El derecho fundamental al propio entorno virtual y su incidencia en el proceso". En *Era Digital, Sociedad y Derecho*. Dir. Fuentes Soriano; Coords. Arrabal Platero, Doig Díaz, Ortega Giménez, Turégano Mansilla. Tirant Lo Blanch, Valencia, 2020.

ARRABAL PLATERO, P.: "Validez de la grabación policial al conductor a efectos de prueba en el delito de conducción bajo la influencia de las drogas del artículo 379.2 CP". En: *La Ley Privacidad*, Wolters Kluwer, nº 4, 2020.

ARRABAL PLATERO, P.: *La prueba tecnológica: aportación, práctica y valoración*. Tirant Lo Blanch, Valencia, 2020.

ARRABAL PLATERO, P.: "El acceso policial a los datos almacenados por los prestadores de servicios a la luz de la STJUE de 2 de octubre de 2018 (ASUNTO C-207/16)". En prensa

ASENCIO MELLADO, J.M.: "El proceso penal con todas las garantías". En: *IUS ET VERITAS: Revista de la Asociación IUS ET VERITAS*, nº 33, 2006.

BACHMAIER WINTER, L.: "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015". En: *Boletín del Ministerio de Justicia*, Año 71, nº 2195, 2017.

BUENO DE MATA, F.: *Las diligencias de investigación penal en la cuarta revolución industrial*, Aranzadi, Navarra, 2019.

CABEZUDO BAJO, M.L.: "El uso de las tecnologías en la entrada y el registro domiciliario: cambio en su concepción tradicional y nuevos retos en la protección de los derechos fundamentales afectados". En: *Revista de Derecho Penal y Criminología*, 3ª época. 15.

DELGADO MARTÍN, J.: "Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015". En: *Diario La Ley*, nº 8693, Sección Doctrina, 2 de febrero, Editorial La Ley, 2016.

DURÁN SILVA, C.M.: "Aspectos procesales de la videovigilancia practicada por las Fuerzas y Cuerpos de Seguridad del Estado". En: *La Ley penal: revista de derecho penal, procesal y penitenciario*, nº 126, 2017.

DURÁN SILVA, C.M.: *La videovigilancia en el proceso penal: tratamiento procesal y eficacia probatoria*. Tirant Lo Blanch, Valencia, 2017

FERNÁNDEZ-GALLARDO FERNÁNDEZ-GALLARDO, J.Á.: "Registro de dispositivos de almacenamiento masivo". En: *Dereito*, vol. 25, nº2, 2016.

FUENTES SORIANO, O.: "La intervención de las comunicaciones tecnológicas tras la reforma de 2015". En: *El nuevo proceso penal tras las reformas de 2015.* Dir. Alonso-Cuevillas Sayrol, Atelier, Barcelona, 2016.

GIMENO BEVIÁ, J.: "Análisis crítico de la reforma de LECrim 2015". En: *Revista Derecho y Proceso Pena*l, Aranzadi, nº 40, octubre-diciembre 2015.

GIMENO SENDRA, V.: *Derecho procesal penal*, tercera edición. Thomson Reuters, Navarra, 2019.

GONZÁLEZ NAVARRO, A.: "Nuevas tecnologías aplicadas a la investigación criminal: las regulaciones española y alemana". En: *El proceso penal. Cuestiones fundamentales*. Coord. Fuentes Soriano, Tirant lo Blanch, Madrid, 2017.

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 tecnológica ". En: *Revista Electrónica de Ciencia Penal y Criminología*, nº 17-06, 2015.

MARTÍN, J.: "La prueba electrónica en el proceso penal". En: *Diario La Ley*, Sección doctrina, La Ley, nº 8167, 2013

MOLINA NAVARRETE, C.: "Ahora que el TC recela de la «cámara oculta», el TEDH la respalda en las empresas: La insoportable «liquidez» de la jurisprudencia". En: *Revista de Trabajo y Seguridad Social. CEF*, 2019.

ORTIZ PRADILLO, J.C.: *Problemas procesales de la ciberdelincuencia*. Colex Editorial Constitución y Leyes, Madrid, 2013.

PÉREZ GIL, J.: "Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución". En *Informatica giuridica e informatica forense al servizio della società della conoscenza. Scritti in onore di Cesare Maioli*. Ed. Aracne, Roma, 2018.

REYES LÓPEZ, J.I.: "Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la L.O. 13/2015". En: *Revista Aranzadi Doctrinal*, nº 4, Editorial Aranzadi, Cizur Menor, 2016.

RICHARD GONZÁLEZ, M.: "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización". En: *Diario La Ley*, nº 8808, 21 de julio de 2016.

RODRÍGUEZ LAINZ, J.L.: "¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?". En: *Diario La Ley*, nº 8729, 28 de marzo de 2016.

RODRÍGUEZ LAINZ, J.L.: "Intervención judicial de comunicaciones vs. Registro remoto sobre equipos informáticos: los puntos de fricción". En: *Diario La Ley*, nº 8896, 9 de enero de 2017.

RODRÍGUEZ LAINZ, J.L.: *El secreto de las telecomunicaciones y su interceptación legal*. Sepín, Madrid, 2016

VEGAS TORRES, J.: "Las medidas de investigación tecnológica". En: *Nuevas tecnologías y derechos fundamentales en el proceso.* Coord. Cedeño Hernán, Aranzadi, Cizur Menor, 2017.

VELASCO NÚÑEZ, E.: "Tecnovigilancia, geolocalización y datos: aspectos procesales penales". En: *Diario La Ley*, nº 8338, Año XXXV, Editorial LA LEY, 23 de junio de 2014.

ZOCO ZABALA, C.: *Nuevas tecnologías y control de las comunicaciones*. Aranzadi, Cizur Menor, 2015.