Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

ASPECTOS RELEVANTES DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS EN EL PROCESO PENAL ESPAÑOL

RELEVANT ASPECTS OF THE INTERCEPTING OF TELEPHONE COMMUNICATIONS IN THE SPANISH CRIMINAL PROCESS

Alberto Varona Jiménez*
a.varona@poderjudicial.es

Recibido: 14/09/2020 Aceptado: 05/10/2020

Resumen

Bajo estas líneas vamos a realizar un análisis de los aspectos más relevantes de la regulación de las intervenciones telefónicas en el sistema procesal español. La normativa actual, producto de una reforma operada en el año 2015, incorpora un copioso cuerpo jurisprudencial y responde a la necesidad de salvaguardar la calidad democrática de nuestro sistema procesal a través de un adecuado respeto del principio legalidad. La reforma, que incorporó otras medidas de investigación tecnológica, contiene aspectos relevantes como son el alcance objetivo y subjetivo de la medida, el contenido de la resolución judicial o la definición de los principios rectores para la adopción de la medida.

Palabras clave

Interceptación de las comunicaciones telefónicas. Inviolabilidad de las comunicaciones. Proceso Penal. Investigación tecnológica. España. Principio de Proporcionalidad

Abstract

Under these lines we are going to carry out an analysis of the most relevant aspects of the regulation of intercepting telephone communications in the Spanish procedural system. The current regulations, the product of a reform carried out in 2015, incorporates a copious body of jurisprudence and responds to the need to safeguard the democratic quality of our procedural system through adequate respect for the principle of legality. The reform, which incorporated other technological research measures, contains relevant aspects such as the objective and subjective scope of the measure, the content of the court decision or the definition of the guiding principles for the adoption of the measure.

Keywords

Intercepting Telephone Communications. Inviolability of communications. Criminal Process. Technological research. Spain. Principle of proporcionality

* El autor es magistrado español con más de 15 años de antigüedad en la carrera judicial y destino en la Audiencia Provincial de Barcelona, órgano colegiado de enjuiciamiento de delitos castigados con pena superior a 5 años de prisión. Profesor permanente del área penal y procesal penal de la Escuela Judicial de España desde el año 2015. Profesor del Curso de Formación Judicial Especializada dirigida a jueces, fiscales y defensores públicos iberoamericanos, años 2016-2020. Doctor en Derecho por la Universidad Autónoma de Barcelona. Licenciado en Derecho Económico por la Universidad de Deusto. Experto en Ciberdelincuencia: ha impartido conferencias sobre esta materia en países como Bolivia, Colombia, Costa Rica y Perú. Autor de diversas publicaciones en revistas especializadas. https://orcid.org/0000-0001-9467-0352

I. Introducción

La regulación del proceso penal en España se encuentra recogida fundamentalmente en una ley que data del año 1881, la llamada Ley de Enjuiciamiento Criminal (en lo sucesivo LECrim). Basada en un sistema acusatorio mixto, en el que la función de investigación judicial se residencia en un órgano judicial unipersonal (los juzgados de instrucción), ha sufrido múltiples reformas a lo largo de sus más de cien años de vigencia.

En los últimos años han sido varios los anteproyectos de reforma que han tratado de modificar el sistema procesal vigente[1]. El objetivo no ha sido otro que tratar de incorporarnos a la línea seguida por la mayoría de los países de nuestro entorno, que han atribuido la función de investigación al Ministerio Fiscal, quedando el juzgado de instrucción con una función de juez de garantías. Lo cierto es que esta reforma, que genera tanto detractores como fervientes defensores, no ha tenido éxito por la falta de consenso político, algo convulso en los últimos años en España.

A pesar de ello, existía una realidad constatable: la normativa preexistente de la intervención de las comunicaciones telefónicas se antojaba insuficiente. La regulación se circunscribía a un solo artículo cuya simple lectura evidenciaba las costuras de nuestra regulación, pensada para un tiempo muy lejano al actual. En concreto, antes de la reforma, decía el artículo 579 de la Ley de Enjuiciamiento criminal que "2. (…) *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* (…) *telefónicas de las personas 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*".

Las carencias habían traspasado fronteras y habían sido puestas de manifiesto por instancias internacionales desde la Sentencia del Tribunal Europeo de los Derechos Humanos de 30 de julio de 1998, caso Valenzuela Contreras contra España[2]. La reforma operada por el legislador en el año 1988, a través de la Ley Orgánica 4/1988, de 25 de mayo, que introdujo el precepto transcrito, no fue suficiente, y las altas instancias judiciales nacionales, la Sala de lo Penal del Tribunal Supremo y el Tribunal Constitucional, realizaron un arduo esfuerzo de interpretación, completando aquellas carencias.

Pero el avance de la ciberdelincuencia conllevó la necesidad de adoptar otro tipo de medidas como la colocación de micrófonos

1 Actualmente, se acaba de elaborar por la comisión de expertos una propuesta. Disponible en https://www.lamoncloa.gob.es/consejodeministros/paginas/enlaces/220711-enlacecriminal.aspx

2 Tienen la versión en español de esta sentencia en la siguiente dirección: http://hudoc.echr.coe.int/spa?i=001-163845

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

o la interceptación de una comunicación telemáticas. Difícilmente se podían adoptar estas medidas con un alto grado de injerencia en el derecho a la intimidad sin un adecuado presupuesto legal. El simple desarrollo constitucional, por reconocible que fuese esa labor, afectaba también la calidad democrática de nuestro Estado de Derecho.

Ello es lo que motiva que el legislador acometa una reforma inaplazable sin esperar a la reforma del modelo procesal. Se trata de la reforma operada 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. La reforma regula cinco medidas de investigación, que vienen precedidas de un conjunto de disposiciones comunes a todas ellas: interceptación de las comunicaciones telefónicas y telemáticas; captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; utilización de dispositivos técnicos de captación de la imagen, seguimiento y de localización; registro de dispositivos de almacenamiento masivo de información; y registros remotos sobre equipos informáticos.

En este trabajo nos vamos a centrar en el análisis de la interceptación de las comunicaciones telefónicas. De su importancia no cabe duda. La interceptación de las comunicaciones telefónicas afecta al derecho al secreto de las comunicaciones, en el que se protege la comunicación formal, independientemente del contenido de lo comunicado. Este derecho aparece recogido en el art. 8 del Convenio para la Protección de los Derechos Humanos y de las libertades fundamentales: "*1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*".

Pero la razón de ser de este trabajo obedece al desarrollo nacional de esta regulación. La reforma disciplina todos y cada uno de los aspectos de la medida de investigación: su ámbito subjetivo, su alcance objetivo, el contenido de la resolución, los principios rectores que deben respetarse en su adopción, la ejecución de la medida, el acceso a las grabaciones o el acceso a los datos electrónicos asociados o no a una comunicación. Algunos de estos aspectos son extrapolables a otras legislaciones, siquiera como criterios interpretativos jurisprudenciales para resolver determinadas controversias. La importancia de armonizar y modernizar nuestras legislaciones en un mundo cada vez más globalizado es otro aspecto a tener en cuenta. No son palabras gratuitas sino que aparecen como uno de los objetivos del Convenio iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, suscrito en Madrid en el año 2014 en el ámbito de la COMJIB[3].

II. Concepto de interceptación de las comunicaciones telefónicas

El legislador español no da una definición de qué se entiende por comunicación telefónica. A priori, esta carencia resulta irrelevante porque es notorio y conocido que estamos ante la escucha y grabación de la comunica-

3 Convenio disponible en https://ficp.es/wp-content/uploads/CONVENIO-CIBERDELITO-VERSION-A-LA-FIRMA.pdf

ción producida a través de un teléfono. Sin embargo, actualmente todas las comunicaciones telefónicas utilizan tecnologías digitales, manejadas por sistemas informáticos, para su transmisión y gestión técnica. Y los llamados teléfonos inteligentes han pasado a convertirse en auténticos mini computadores. La delimitación de esta forma entre las comunicaciones telefónicas y las telemáticas se difumina.

En nuestra opinión, cuando hablamos de comunicaciones telefónicas son aquellas comunicaciones que se producen a través del teléfono, que no generan datos de tráfico en nuestras facturas (conocidos como megas o gigas) y que no se producen a través de internet. Parece claro que una llamada a través de la red 4G es una llamada telefónica mientras que una llamada mediante WhatsApp es más bien telemática, por más que se produzca a través del teléfono. Lo mismo ocurre con los mensajes de texto. Los SMS han pasado a ser una reliquia del pasado debido apps de mensajería como la citada WhatsApp, Facebook o Telegram. Estos últimos tampoco serían propiamente comunicaciones telefónicas, por más que podamos operar a través del teléfono.

En cualquier caso, más allá de determinadas singularidades en el alcance de la medida, la previsión expresa en la ley de que se aplique a las comunicaciones telemáticas el mismo régimen previsto para las comunicaciones telefónicas, convierte la cuestión conceptual en meramente formal en España.

III. Presupuestos para la adopción de la medida: contenido de la resolución judicial y principios rectores

Como premisa básica es importante tener en cuenta, como hemos reseñado en la introducción, que en España la instrucción de los procedimientos judiciales corresponde a un órgano judicial unipersonal (el llamado Juez de Instrucción). El Ministerio Fiscal es una parte más del procedimiento, que interviene en defensa del interés público. Partiendo de esta premisa, la interceptación de las comunicaciones telefónicas es acordada por el Juez de Instrucción, de oficio o a instancia del Ministerio Fiscal o la autoridad policial, a través de solicitud escrita, con un plazo máximo para resolver de 24 horas[4]. La ejecución permanece en todo momento bajo el control de la autoridad judicial (arts. 588 bis b1 y c1 LECrim).

Es por todos sabido que para que una injerencia en los derechos fundamentales sea constitucionalmente legítima es preciso que se autorice mediante una resolución judicial motivada, que refleje la existencia de los presupuestos habilitantes de la medida —previa incoación de un proceso penal, indicios de delito y su conexión con la persona afectada por la medida interesada— y que satisfaga los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad.

Como apunta SANTOS[5], "*la motivación resulta fundamental. Exige un examen riguroso del contenido de la solicitud de la medida, así como la justificación exhaustiva del cumplimiento de los principios esenciales para su adopción. Constituye así elemento de garantía de constitucionalidad y validez de la medida, a la vista de los intereses en juego y de la lesión que para los derechos fundamentales del investigado implica su adopción*".

4 Como regla especial, el legislador español habilita expresamente al Gobierno para ordenar la interceptación en casos de urgencia cuando las investigaciones se realicen para la averiguación de delitos relacionados con bandas armadas o elementos terroristas, dando cuenta a la autoridad judicial en el plazo máximo de 24 horas (art. 588 ter d, apartado tercero).

5 Alberto Santos, *Medidas de investigación tecnológica en la instrucción penal* (Barcelona: Wolters Kluwer, 2017), 85.

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

La reforma acoge esta doctrina y da un paso más allá al enumerar los extremos que ha de contener la resolución judicial que acuerde la interceptación de las comunicaciones y que además es predicable de todas las medidas de investigación tecnológica (art. 588 bis c LECrim):

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 art. 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".

Conviene precisar que en España no todos los delitos legitiman la adopción de esta interceptación. El legislador exige que la investigación tenga por objeto 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; delitos de terrorismo; o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación (art. 588 ter a LECrim). Esto no quiere decir que la concurrencia de algunos de estos delitos determine automáticamente la legitimidad de la medida. Será un presupuesto necesario, pero seguido del análisis de la proporcionalidad en el caso concreto. Y en este sentido, el legislador español ha establecido una definición concreta y expresa de cada uno de estos principios en el art. 588 bis a LECrim. Por su relevancia a efectos de derecho comparado, merece especial atención el análisis pausado de estos principios rectores:

> *"2. El principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.*
>
> *"3. El principio de idoneidad servirá para definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad".*
>
> *"4. En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida: cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, 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".*

> *"5. Las medidas de investigación reguladas en este capítulo 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 que de su adopción resulte para el interés público y de terceros. 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".*

A la vista de estos cuatros principios, nos gustaría realizar dos consideraciones: por un lado, obsérvese cómo se deja constancia expresa de la imposibilidad de realizar investigaciones prospectivas, cuando el artículo dispone que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva; y por otro lado, debemos prestar una especial atención al principio de proporcionalidad.

Como señala DELGADO[6], el principio de proporcionalidad despliega sus efectos en dos ámbitos: en la actividad del legislador, obligándole a ponderar las necesidades del ius puniendi frente a las exigencias derivadas del adecuado respeto a los derechos fundamentales afectados; y frente al órgano jurisdiccional, exigiéndole una ponderación de todas las circunstancias concurrentes en cada caso concreto. Este segundo es al que se refiere el legislador en este precepto. El legislador ofrece una serie de criterios para valorar el principio de proporcionalidad en sentido estricto: a) la trascendencia social o el ámbito tecnológico de producción: esta segunda referencia resulta esencial para poder luchar contra el cibercrimen. Si el delincuente ha utilizado las nuevas tecnologías para facilitar la comisión de su ilícito penal, parece lógico que el Estado pueda luchar con esas mismas herramientas en la búsqueda del esclarecimiento del hecho y la determinación de los responsables; b) la gravedad del hecho, en el que habrá que tener en cuenta la pena asignada al tipo penal, pero también el bien jurídico protegido y la propia dinámica comisiva; c) la relevancia del resultado perseguido con la restricción del derecho; y d) la intensidad de los indicios racionales de criminalidad.

IV. Alcance subjetivo y objetivo de la medida de investigación

IV.1 Ámbito subjetivo

La norma española regula con detalle el ámbito subjetivo de la medida. Para intervenir un terminal o medio de comunicación no es necesario que el investigado[7] tenga la titularidad. Es suficiente con que lo utilice habitual u ocasionalmente (art. 588 ter b1 LECrim).

Dos cuestiones nos podemos plantear: ¿qué ocurre cuando el investigado hace uso de celulares de terceras personas?; y ¿si es posible intervenir un celular ignorando los datos concretos de la persona que vamos a investigar?

6 Joaquín Delgado, *Investigación tecnológica y prueba digital en todas las jurisdicciones* (Madrid: Wolters Kluwer, 2016), 344-345

7 Conviene aclarar que el término "investigado" ha sido introducido en nuestro proceso penal con motivo de la misma reforma operada por la Ley Orgánica 13/2015, en sustitución del antiguo y estigmatizado término de "imputado". Con arreglo al preámbulo de esta reforma, el término investigado sirve "*para identificar a la persona* (física o jurídica, añadimos nosotros) *sometida a investigación por su relación con un delito*".

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

Respecto a la primera pregunta, la ley prevé la posibilidad de intervenir los pertenecientes a una tercera persona en tres supuestos alternativos: a) que exista constancia de que el sujeto investigado se sirve del tercero para transmitir o recibir información; b) que el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad; o c) que sea utilizado maliciosamente vía telemática sin conocimiento de su titular. En los casos cada vez más habituales de desapariciones de jóvenes en los que existen sospechas de criminalidad, será posible intervenir el terminal o medio de comunicación de la propia víctima cuando sea previsible un grave riesgo para la vida (art. 588 ter b y c LECrim).

La segunda pregunta se la plantea SANTOS[8] cuando reflexiona sobre el hecho de que uno de los efectos de la prohibición de acordar medidas de investigación con carácter prospectivo es la necesidad de identificar a los investigados. No obstante, considera que esta reflexión puede plantearse en término absolutos cuando no sea posible identificar al autor u este utilice un pseudónimo, y ello porque en su opinión la norma da cobertura legal para interpretar que aquella determinación solo es exigible cuando sea conocido.

IV.2 Ámbito objetivo

El legislador español determina también el alcance de qué medidas puede comprender la interceptación de las comunicaciones telefónicas. Así el art. 588 ter d LECrim habilita para acordar:

- El registro y la grabación del contenido de la comunicación.
- El conocimiento de su origen o destino, en el momento en que se realiza la comunicación.
- La localización geográfica del origen o destino de la comunicación
- El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

Sobre la base de este precepto podemos establecer tres consideraciones:

En primer lugar, el legislador distingue entre el acceso al contenido de la comunicación telefónica y los datos electrónicos asociados o no a un proceso de comunicación. Los datos asociados a un proceso de comunicación son los conocidos como datos de tráfico[9]. Como hemos expuesto, la Ley de Enjuiciamiento Criminal cita expresamente el origen y el destino de la comunicación, o la geolocalización de los intervinientes en la misma. Cuando hablamos de datos no asociados a una comunicación concreta estamos pensando en los datos del número de cuenta bancaria donde se domicilian los recibos o los datos de las antenas BTS (sin recurrir a grandes tecnicismos podemos decir que son aquellas estaciones a las que se conectan nuestros teléfonos móviles para tener cobertura 3G, 4G o 5G, en cada momento,

8 Alberto Santos, *Medidas de investigación tecnológica en la instrucción penal* (Barcelona: Wolters Kluwer, 2017), 89.

9 (19) El art. 1 del Convenio de Budapest 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*". Por su parte la Ley de Enjuiciamiento Criminal, los define como "*todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*". (art. 588 ter b, apartado segundo, párrafo tercero).

lo que nos permite recibir o realizar llamadas, o recibir mensajes de todo tipo).

En segundo lugar, aunque no lo diga expresamente el texto legal, el legislador prevé la posibilidad de que esta interceptación se pueda producir en tiempo real ("*en el momento en que se realiza la comunicación*") o en diferido, esto es a posteriori. Comencemos por la modalidad de "a tiempo real". En España el sistema utilizado para la ejecución de la interceptación se conoce con el nombre de SITEL (sistema integrado de interceptación de telecomunicaciones.) Como señalan RUIZ Y VIDAL[10], quienes realizan una interesante reflexión sobre la constitucionalidad del sistema, "*es un avanzado sistema informático desarrollado por la multinacional Ericsson en el año 2002, depende del Ministerio del Interior y es utilizado conjuntamente por las Direcciones Generales de Policía y Guardia Civil, así como por el Centro Nacional de Inteligencia. El desarrollo de este sistema informático, como se desprende de la Sentencia del Tribunal Supremo de 13 de marzo de 2009, responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones*".

El sistema SITEL utilizado en España para ejecutar las interceptaciones, habilita para no solo escuchar y grabar el contenido de las comunicaciones telefónicas sino para acceder también en tiempo real a determinados datos como son el número de origen y destino de la comunicación, así como la ubicación en el espacio (su geolocalización) de los intervinientes en la llamada.

10 María Ruiz y Tomás Vidal, "Análisis de la constitucionalidad de SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal", *Revista Aranzadi doctrinal*, 9 (2016).

Pero también existe la posibilidad de acceder a los datos electrónicos asociados o no a un proceso de comunicación a posteriori, cuando sean datos almacenados por las compañías prestadoras del servicio de las comunicaciones bien en el cumplimiento de sus obligaciones legales de retención de datos[11] bien por motivos comerciales. Para ello será necesario también una resolución judicial, pudiendo acordarse medidas de aseguramiento para garantizar su efectividad. En concreto, el artículo 588 ter j LECrim regula el acceso de datos de tráfico existentes en archivos automatizados. Estos datos solo podrán ser incorporados con autorización judicial siempre que su conocimiento resulte indispensable para la investigación, incluida la búsqueda entrecruzada o inteligente de datos. Habrá que razonar los datos que se solicitan y las razones que justifican la cesión[12].

Pero es más, la Ley de Enjuiciamiento Criminal habilita a la Policía Judicial y al Ministerio Fiscal para que puedan ordenar a cualquier persona física o jurídica el aseguramiento y conservación de datos almacenados con el objetivo de evitar su eliminación o manipulación

11 La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Se trata de una transposición de la Directiva 2006/24/CE, del Parlamento Europeo y Consejo, de 15 de marzo, sobre conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. Tienen esta norma a su disposición en la siguiente url: https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243&p=20140510&tn=1

12 La exigencia de autorización judicial se adecúa a la doctrina sentada por las sentencias del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 y 21 de diciembre de 2016 sobre la Directiva 2006/24/CE, que abogaban por el control judicial de dicha cesión a fin de garantizar los derechos fundamentales a la intimidad y a la protección de datos. La Sentencia de 21 de diciembre de 2016 está a su disposición en http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=ES

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

y garantizar la ulterior incorporación al proceso judicial. Los datos se conservarán durante un periodo máximo de 90 días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan 180 días (art. 588 octies LECrim). Ello no es más que una consecuencia del art. 16 del Convenio de Budapest de 2001, sobre ciberdelincuencia.

Ahora bien, cabe plantearse si cualquier delito legitima y habilita para acceder a estos datos. En este punto cobra especial importancia la Sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 2 de octubre de 2018, sobre el umbral de gravedad del delito que puede legitimar el acceso[13]. El Tribunal determinó que cuando la injerencia en los derechos no sea especialmente grave, la diligencia de investigación puede estar justificada por el simple objetivo de prevenir, investigar, descubrir y perseguir infracciones no especialmente graves, delitos en general.

Siguiendo con los datos electrónicos, como excepción a la necesidad de resolución judicial para recabar datos electrónicos asociados o no a un proceso de comunicación, los arts. 588 ter k y l LECrim habilitan para que en el ejercicio de sus funciones la policía judicial pueda valerse de artificios técnicos para conocer los códigos de identificación de cualquier medio de comunicación, con referencia expresa al IMSI o el IMEI de un dispositivo. A estos artificios se refiere BARRIO[14], cuando expone que así sucede con los IMSI-catchers o stingrays, que funciona como una antena simulada a modo de puente entre la antena del operador de la red móvil y los dispositivos para posibilitar la captura de estos datos sin conocimiento del usuario investigado.

Además, el art. 588 ter m LECrim habilita tanto a la Policía Judicial como al Ministerio Fiscal para dirigirse a los prestadores de servicios para que faciliten la titularidad de estos datos no asociados a un proceso de comunicación concreto. También podrán solicitar que se les facilite el número de teléfono o los datos identificativos de cualquier medio de comunicación.

Esta misma posibilidad diferida de acceder al contenido de la comunicación sería también factible en el caso del propio contenido de la comunicación cuando se encontrase grabada en un dispositivo electrónico, pero en tal caso la norma diligencia investigación aplicable sería la del registro de dispositivos informáticos.

Finalmente, en cuanto a la duración posible de la interceptación, contamos con una duración inicial máxima de 3 meses, prorrogable hasta un máximo de 18 meses. Se prevé expresamente como *dies a quo* para realizar el cómputo la fecha en que se dictó la resolución judicial, con independencia del momento en que se hizo efectiva.

V. Aspectos prácticos de la reforma

La primera pregunta que nos tenemos que plantear es si es posible intervenir una comunicación entre el investigado y su letrado. La respuesta es negativa. Como señala BOLDO, la reforma del año 2015 recogió una doctrina jurisprudencial del Tribunal Supremo bien definida sobre el derecho a la confidencialidad entre las conversaciones de abogado y cliente en el proceso penal[15]. La reforma determina

13 Sentencia disponible en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=945817

14 Moisés Barrio, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos* (Madrid: Wolters Kluwer, 2018), 265.

15 GABRIELA BOLDO en "La reforma operada por la reforma operada por la LO 13/2015, de 5 de octubre,

que como regla general todas las conversaciones de los investigados, detenidos o no, con sus letrados tendrán carácter confidencial. Como consecuencia de ello, si estas conversaciones o comunicaciones hubieran sido captadas o intervenidas durante la ejecución de alguna de las diligencias reguladas en esta ley, el juez ordenará la eliminación de la grabación, dejando constancia de estas circunstancias en las actuaciones. Ahora bien, esta regla general tiene una excepción legalmente prevista, cual es que se constate la existencia de indicios objetivos de la participación del abogado en el hecho delictivo investigado o de su implicación junto con el investigado o encausado en la comisión de otra infracción penal (arts. 118.4 y 520.7 de la Ley de Enjuiciamiento Criminal). En el caso de que esta conversación se produzca en un centro penitenciario, la Ley Orgánica General Penitenciaria de 1979 exige que se trate de delitos de terrorismo (art. 51.2).

La segunda pregunta que nos planteamos es qué ocurre cuando en el curso de una interceptación aparecen indicios de la comisión de otro delito distinto del que justificó la adopción de la diligencia de investigación. Estamos ante los llamados hallazgos casuales (art. 588 bs i en relación con el art. 579bis LECrim). El legislador prevé el resultado podrá ser utilizado como medio de investigación o prueba en otro proceso penal. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen. Recibidas las actuaciones por el juez competente para conocer del nuevo delito, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo incluyera en su momento. Como señala CASANOVA[16], esta norma regula acertadamente las exigencias que durante los últimos años había reclamado el Tribunal Supremo en la materia al tiempo que brinda una mayor seguridad jurídica. No obstante, la autora pone de manifiesto que hubiese sido deseable que el legislador hubiese circunscrito la posibilidad de utilizar los resultados en el segundo proceso cuando el delito objeto de investigación en el segundo proceso hubiese permitido practicar una medida de intervención telefónica.

La tercera pregunta que queremos resolver es si es viable técnicamente y, en tal caso, si es válida la grabación de una conversación oral mantenida por el investigado con otra persona presente e interceptada a partir de una llamada efectuada al teléfono, que actuaría en este caso como micrófono ambiente. La respuesta es afirmativa. El teléfono pueda captar, también lícitamente, conversaciones ambientales, incluso antes de que el destinatario de la comunicación haya descolgado el teléfono. En este sentido, la STS nº 373/2016, de 3 de mayo, en un supuesto similar señala que "*en cuanto a la utilización del móvil de los investigados como micrófono de ambiente, que se afirma por los recurrentes como injerencia no autorizada y de la que también predican que conculca la inviolabilidad del domicilio, primeramente hemos de despojar lo acaecido de tal naturaleza; única-*

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 los art. 118, 52 y 520 ter LECrim. *Revista de Derecho vLex*, 137 (2015).

16 Roser Casanova, "Nueva regulación de las intervenciones telefónicas: especial atención a la utilización del resultado de esta diligencia en un proceso penal distinta". En *el Proceso Penal. Cuestiones fundamentales,* con ensayos de varios autores y Olga Fuentes Soriano (coordinadora). (Valencia: Tirant lo Blanch, 2016), 327-338.

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

mente cuando la llamada ha sido establecida y el móvil la recibe, antes de aceptarla el destinatario, el sistema comienza a grabar; es decir, la llamada, para la que existía acuerdo judicial de intervención y grabación, ya se había producido, con independencia de que si el destinatario no la acepta, no genere coste para quien la realiza. Pero el ámbito de la resolución judicial, no depende del coste o gratuidad de la llamada. De otra parte, la grabación en esos instantes, no se magnifica en su captación, sino que al igual que acontece al registrar conversaciones, los ruidos próximos o de ambiente del preciso lugar donde se encuentren los móviles conectados a través de la correspondiente llamada, también restan grabados en un segundo plano con mayor o menor precisión..." Continua diciendo la sentencia, con cita de la STS 592/2013 de 11 de junio (RJ 2013, 7084) que ... «*no era comprensible la denuncia sobre la potencialidad grabadora derivada del sistema SITEL en referencia a que el terminal telefónico capte cualquier conversación que, una vez activado, se produzca, no solamente a través de la línea telefónica sino en el ambiente en que se encuentra ubicado*".

La cuarta pregunta que nos planteamos es si la grabación clandestina por particulares de sus propias comunicaciones está sujeta a esta regulación. Y la respuesta es negativa porque no atenta contra el derecho al secreto de las comunicaciones (SSTS nº 421/2014, de 16 de mayo y 250/2017, de 5 de abril) y afectando únicamente al derecho a la intimidad cuando *la conversación tuviera un contenido que afectara al núcleo esencial del derecho a la intimidad* (STS nº 421/2014, de 16 de mayo). Por ello, la admisión como prueba de una de estas grabaciones no requiere autorización judicial pero sí *un riguroso juicio de ponderación entre los derechos a la intimidad y a la propia imagen y la posible existencia de un fin legítimo, atendiendo siempre a los principios de proporcionalidad, necesidad y racionalidad* (STS nº 793/2013, de 28 de octubre).

La quinta pregunta es qué ocurre si durante una grabación salen a luz cuestiones íntimas del investigado ajeno a la investigación. Sobre esta cuestión se ocupa también la reforma. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Sin embargo, esta regla general tiene excepciones cuando se hayan grabado conversaciones íntimas ajenas a la investigación (art. 588 ter i LECrim). En tal supuesto, si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso. La ley concreta que una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa.

El legislador también habilita a los terceros afectados el acceso a las grabaciones. Ello es posible porque el juez de instrucción habrá de notificar su existencia a las personas intervinientes en las comunicaciones interceptadas, informándoles de las concretas comunicaciones en las que haya participado. Si la persona notificada lo solicita se le entregará 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. No obstante, comoquiera que ello puede acarrear una carga desproporcionada para los órganos judicial o directamente

no ser viable, se establece la previsión de que aquella obligación de notificación órgano judicial no existe cuando sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones.

Por último, merece una mención el deber de colaboración y el control de la medida. Respecto al primero, el art. 588 ter e LECrim dispone que todos los prestadores de servicios de telecomunicaciones, así como cualquier persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono están obligados a prestar la asistencia y colaboración precisas para la ejecución de la medida y a guardar secreto, so pena de incurrir en un delito de desobediencia. Respecto a la segunda cuestión, el art. 588 ter f en relación con el art. 588 bis g LECrim establecen que la policía judicial, que es a quien corresponde la ejecución de la medida, darán cuenta al juez instructor con la periodicidad que determine (que lógicamente variará en función de la intensidad de los indicios), mediante la aportación de las grabaciones íntegras realizadas y la transcripción de los pasajes que considere de interés.

VI. Conclusiones

La reforma operada en el año 2015 en el proceso penal español ha supuesto un avance fundamental en la utilización de las medidas de investigación tecnológica, situando a España en la vanguardia en su reconocimiento y adopción. La nueva regulación establece una prolija normativa de la interceptación de las comunicaciones telefónicas, necesaria para dar respuesta al principio de legalidad y salvaguardar el derecho fundamental a la inviolabilidad de las comunicaciones. Aspectos como el contenido exhaustivo de la resolución judicial, el ámbito subjetivo de la medida o la definición de los principios rectores de la adopción de la medida son especialmente relevantes. Si queremos luchar de forma efectiva contra la delincuencia trasnacional es importante armonizar nuestras legislaciones. Este es el objetivo de los principales instrumentos en esta materia como son el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de ciberdelincuencia, hecho en Madrid el 28 de mayo de 2014, y el Convenio del Consejo de Europa sobre Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001.

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937

REFERENCIAS BIBLIOGRÁFICAS

Doctrina

Barrio, Moisés. Delitos 2.0. *Aspectos penales, procesales y de seguridad de los ciberdelitos.* Madrid: Wolters Kluwer, 2018.

Boldo, Gabriela. "La reforma operada por la LO 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica en los art. 118, 52 y 520 ter LECrim. *Revista de Derecho vLex*, 137 (2015).

Casanova, Roser. "Nueva regulación de las intervenciones telefónicas: especial atención a la utilización del resultado de esta diligencia en un proceso penal distinta". En *el Proceso Penal. Cuestiones fundamentales,* con ensayos de varios autores y Olga Fuentes Soriano (coordinadora). Valencia: Tirant lo Blanch, 2016, 327-338.

Delgado, Joaquín. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Madrid: Wolters Kluwer, 2016.

Ruiz, María, y Tomás Vidal. "Análisis de la constitucionalidad de SITEL. Breves consideraciones a partir de la Ley Orgánica 13/2015, de reforma de la Ley de Enjuiciamiento Criminal". *Revista Aranzadi doctrinal*, 9 (2016): 135-162.

Santos, Alberto. *Medidas de investigación tecnológica en la instrucción penal*. Barcelona: Wolters Kluwer, 2017.

Normativa española

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. Disponible en https://www.boe.es/buscar/doc.php?id=-BOE-A-2015-10725

Ley de Enjuiciamiento Criminal, aprobada por Real Decreto de 14 de septiembre de 1882. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria. Disponible en https://www.boe.es/buscar/act.php?id=-BOE-A-1979-23708

Normativa internacional

Convenio de Budapest sobre ciberdelincuencia de 23 de noviembre de 2011. Disponible en inglés en https://www.coe.int/en/web/cybercrime/the-budapest-convention. Versión en castellano disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Convenio iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, suscrito en Madrid en el año 2014 en el ámbito de la COMJIB. Disponible en https://ficp.es/wp-content/uploads/CONVENIO-CIBERDELITO-VERSION-A-LA-FIRMA.pdf

Jurisprudencia

Sentencia del Tribunal Europeo de los Derechos Humanos de 30 de julio de 1998, caso Valenzuela Contreras contra España. Disponible en: http://hudoc.echr.coe.int/spa?i=001-163845

Sentencia del Tribunal Supremo de 28 de octubre de 2013. Disponible en https://supremo.vlex.es/vid/475261966

Sentencia del Tribunal Supremo de 16 de mayo de 2014. Disponible en https://supremo.vlex.es/vid/derecho-funcionario-publico-definicion-514867486

Sentencia de la Sala Segunda del Tribunal Supremo de 3 de mayo de 2016. Disponible en https://supremo.vlex.es/vid/638419861

Sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 2 de octubre de 2018. Sentencia disponible en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=206332&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=945817

Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política
N° 9, 2020, pp. 159-172
ISSN 2410-5937