

PRINCIPIOS RECTORES EN LA ADOPCIÓN DE DILIGENCIAS
LIMITATIVAS DE LOS DERECHOS RECONOCIDOS EN EL
ART. 18 CE

*GUIDING PRINCIPLES ON THE ADOPTION OF INVESTIGATION
PROCEEDINGS THAT LIMIT THE RIGHTS RECOGNIZED BY ART. 18
SPANISH CONSTITUTION*

Rev. Boliv. de Derecho N° 31, enero 2021, ISSN: 2070-8157, pp. 236-263



Carolina
SANCHIS
CRESPO

ARTÍCULO RECIBIDO: 1 de septiembre de 2020

ARTÍCULO APROBADO: 13 de noviembre de 2020

RESUMEN: La reforma de la LECrim llevada a cabo en 2015 exige, para la adopción de las diligencias limitativas de los derechos reconocidos en el art. 18 CE, el respeto a los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Este artículo pretende, partiendo del texto legal y acudiendo a la jurisprudencia, desentrañar el verdadero significado de estos principios.

PALABRAS CLAVE: Diligencias de investigación; especialidad; idoneidad; excepcionalidad; necesidad; proporcionalidad.

ABSTRACT: *Criminal Procedure Law reform carried out in 2015 requires, in order to adopt the investigation proceedings that limit the rights recognized by art. 18 Spanish Constitution, to respect the guiding principles of speciality, suitability, exceptionality, necessity and proportionality. This article aims, departing from the legal text and considering existing jurisprudence, to unveil the true meaning of these principles.*

KEY WORDS: *Criminal investigations; speciality; suitability; exceptionality; necessity; proportionality.*

SUMARIO.- I. LA ERA DIGITAL.- II. RÉGIMEN JURÍDICO DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA. LOS PRINCIPIOS RECTORES COMO EJE AXIAL.- I. Especialidad.- 2. Idoneidad.- 3. Excepcionalidad y necesidad.- 4. Proporcionalidad.- III. A MODO DE EPÍLOGO.

I. LA ERA DIGITAL.

El modo de investigar en el proceso penal que se abre paso con el transcurrir de este nuevo siglo, es marcadamente distinto al que consagró inicialmente nuestra LECrim. A finales del siglo XIX, España todavía era una sociedad rural escasamente industrializada, donde la mayor revolución tecnológica venía de la mano de la fotografía. Casi ciento cuarenta años más tarde, el papel de la tecnología en la configuración de la inmensa mayoría de relaciones humanas es capital y ello forzosamente debía reflejarse en el modo de delinquir y en el de investigar esa delincuencia.

Actualmente nos encontramos inmersos en una verdadera revolución que ha sido ya denominada Cuarta Revolución Industrial. No se trata de una nueva etapa más, sino del advenimiento de una nueva era: la era digital. Tiene, como una de sus principales características, propiciar la transformación digital de la sociedad. De este modo, todas las realidades que hasta ahora conocíamos tienen una traducción digital lo que las dota de infinitas posibilidades de tratamiento.

Todo ello ha sucedido -está sucediendo- mientras tiene lugar el fenómeno de la universalización de la informática por el continuo desarrollo, la miniaturización y la reducción de costes en la fabricación y venta de todo tipo de dispositivos¹ y ha conllevado, además, la aparición de un nuevo contexto en el que emergen nuevas realidades. Algunas de las más significativas, son la gestión de la información que da lugar al nacimiento del *Big Data* y toda una serie de cuestiones asociadas a la

¹ PRADILLO, J. C.: "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en PÉREZ GIL, J. (coord.): *El proceso penal en la sociedad de la información*, Madrid, 2012, p. 269.

• Carolina Sanchis Crespo

Catedrática de Derecho Procesal de la Universitat de València. Docente en Universidades de Irlanda, Finlandia, Cuba, Bolivia, Argentina, México y Costa Rica. Estancias investigadoras en Universidades de Italia, Alemania, Irlanda y Estados Unidos. Autora de 7 libros siendo el último de los mismos: *Delincuencia informática. Tipos delictivos e investigación*. Con jurisprudencia tras la reforma procesal y penal de 2015, Ed. Tirant lo Blanch, 2019, 823 pp. Libro en coautoría con Eloy Velasco Núñez. Directora y coautora de 3 libros colectivos sobre fraude electrónico. Autora de más de 40 artículos científicos especializados en Derecho Procesal publicados en Revistas españolas y extranjeras. Autora de más de 15 capítulos en libros colectivos. Conferenciante en congresos internacionales y nacionales en los últimos 25 años. Directora de 2 Proyectos de investigación y participante como equipo en otros 12. Correo electrónico: carolina.sanchis@uv.es

seguridad, por la vulnerabilidad de las infraestructuras críticas y la puesta en riesgo del orden jurídico mediante la cibercriminalidad.

La mayoría de las definiciones se refieren a *Big Data* como un término aplicado a conjuntos de grandes datos caracterizados por las famosas 3V del analista Doug LANEY, de la consultora Gartner: volumen, velocidad y variedad, que superan la capacidad del *software* habitual para ser capturados, gestionados y procesados. Desde que LANEY la acuñó hace más de una década, otras V han ido añadiéndose, como la validez, la veracidad, el valor y la visibilidad. Todo un desafío para la gestión de datos. Si la información es poder, entonces el *Big Data* debe entenderse como una gran linterna que ilumina la información escondida detrás de los datos, facilitando su análisis que antes limitaba la tecnología. En palabras de Rick SMOLAN, autor de *El Rostro Humano del Big Data*, se trata de una extraordinaria revolución del conocimiento que opera casi de modo invisible, a través de los negocios, la academia, el gobierno, la salud y la vida cotidiana. Si antes los investigadores se servían de los datos para apoyar o rechazar teorías, ahora recurren a ellos para inspirarlas². El *Big Data* transforma meros datos en información valiosa para la toma de decisiones de todo tipo: económicas, políticas, humanitarias, etc.

La ingente cantidad de información que producimos procede de una gran variedad de dispositivos que forman parte de nuestra vida cotidiana. Con ellos emitimos un sinfín de datos que van conformando nuestros avatares digitales. Cada vez que clicamos en Amazon, cuando pagamos con la tarjeta en los comercios, en el supermercado, cuando opinamos en la Red, colgamos imágenes o utilizamos una nueva *app*, el *Big Data* sabe un poco más de nuestros gustos, de nosotros y nos va conociendo mejor. ¿Podemos imaginar los ajustadísimos retratos que se pueden extraer de cada uno de nosotros optimizando el análisis de todos estos datos?³

Las grandes posibilidades que pone al alcance de la mano el *Big Data* junto con el creciente desarrollo tecnológico, tienen también su lado oscuro. Y es en ese lado oscuro donde se cobijan dos grandes enemigos para la sociedad civil que adelantábamos. Se trata, de un lado, de la puesta en riesgo de las infraestructuras críticas y de otro, de las infracciones al orden jurídico por parte de la cibercriminalidad.

En cuanto a las infraestructuras críticas, se intenta protegerlas, para conjurar los riegos y convertir en lo más invulnerables posible los servicios esenciales de

2 POWERDATA información accesible en <https://www.powerdata.es/nuestra-mision> (consultada el 7 de julio de 2020).

3 VAN DEN BERG, E.: “¿Qué es eso del *Big Data*?”, *El País*, 31 de marzo de 2015.

Estado. Entendemos por tales aquellos que de no prestarse pondrían en peligro la existencia misma de la nación, como policía, educación, sanidad, suministros de energía, seguridad del tráfico, etc. A este respecto, hay que decir que desde hace más de 10 años existe en nuestro país un centro estatal que trata de convertirse en el escudo protector perfecto frente a estos ataques. Se trata del Centro Nacional de Protección de Infraestructuras y Seguridad (CNPIC). En el año 2014 fueron 63 los incidentes registrados contra centros críticos, mientras que en el año 2016 el número de incidentes se elevó a 479 y el año 2017, desde enero a julio, se habían producido ya 489 incidentes⁴. Las cifras siguen incrementándose. En los dos primeros meses de 2018 ha habido más incidentes de ciberseguridad en infraestructuras críticas que en todo 2014 (125 frente a las 63 de hace cuatro años), y la mayoría han sido intentos de escaneo de red o ataques con programas maliciosos para dañar equipos informáticos⁵.

Desde INCIBE-CERT⁶ se ha trabajado todo el año 2019 en los servicios de alerta temprana. Se publicaron 207 avisos relacionados con el sector industrial, una mínima reducción frente a los 228 de 2018⁷.

Ataques pertenecientes a este ámbito fueron los producidos por el virus *Wannacry* en mayo de 2017. Fue un ataque masivo de *ransomware* (código dañino). Tuvo lugar entre el 12 y el 16 de mayo. Produjo daños a más de 360.000 dispositivos electrónicos de más de 180 países. Las empresas afectadas conocidas fueron en España, fundamentalmente, Telefónica, Iberdrola, Gas Natural y el periódico El Mundo. También afectó a los hospitales del sistema público sanitario de Reino Unido, infectó numerosos equipos en la compañía estadounidense de transporte FedEx y causó problemas en varias cadenas de montaje de los fabricantes de vehículos Nissan y Renault. China y Rusia fueron los países a los que el ciberataque golpeó más fuerte⁸.

4 Los datos están extraídos de OLMO CALVO: “Buscando el escudo contra el Cibercrimen”, *El Mundo*, 14 de agosto de 2017.

5 “España registra en dos meses más incidentes de ciberseguridad que en todo 2014”, Agencia EFE, 31 de marzo de 2018.

6 INCIBE-INCERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. En el caso de la gestión de incidentes que afecten a operadores críticos del sector privado, INCIBE-CERT está operado conjuntamente por INCIBE y CNPIC. INCIBE-CERT es uno de los equipos de respuesta de referencia ante incidentes que se coordina con el resto de los equipos nacionales e internacionales para mejorar la eficacia en la lucha contra los delitos que involucran a las redes y sistemas de información, reduciendo sus efectos en la seguridad pública. Información accesible en <https://www.incibe-cert.es/sobre-incibe-cert/que-es-incibe-cert>, consultada el 8 de julio de 2020.

7 Información accesible en <https://www.incibe-cert.es/blog/seguridad-industrial-2019-cifras>, consultada el 8 de julio de 2020.

8 Los datos están extraídos de varios artículos publicados en prensa durante esos días como TOLEDANO, B.: “Hackean a la red interna de Telefónica y de otras grandes empresas españolas”, 12 de mayo de 2017, *El Mundo* y PALAZUELOS, F.: “Así fue el impacto del ciberataque en España”, *El País*, 18 de mayo de 2017.

Un poco más tarde, a finales de julio de 2017, un hacker accedió a un servidor de Justicia y obligó a parar Lexnet. El fallo de seguridad permitió el acceso sin control a un cierto número de casos judiciales en España. En el momento de escribirse estas líneas ya ha concluido la investigación abierta por el CGPJ sobre el suceso con su archivo⁹. La Agencia Española de Protección de Datos también ha finalizado su expediente, pero con distinto signo. Su resolución de 15 de marzo de 2018 concluye que se produjo infracción grave del artículo 44.3.d de la Ley Orgánica de Protección de Datos (LOPD) por parte del Ministerio de Justicia, durante el incidente de seguridad de 28 de julio de 2017 del sistema LexNet donde unos usuarios pudieron acceder a la información de otros usuarios.

La declaración pública de que se ha producido dicha infracción grave es la sanción que ha recibido el Ministerio. De acuerdo con la LOPD, las Administraciones Públicas no pueden ser sancionadas económicamente¹⁰. De haber sido una empresa privada, el Ministerio podría haber sido sancionado con una multa de 40.001 a 300.000 euros¹¹. Lo que todos estos incidentes ponen de manifiesto es la vulnerabilidad de los datos que afectan a infraestructuras críticas de los Estados y la imperiosa necesidad de protegerlos.

Por otro lado, en el ámbito de la lucha contra la cibercriminalidad -al que propiamente se dirige este trabajo-, la tecnología proporciona mejoras fundamentales en la investigación penal. Algunas de ellas son el análisis del

9 El Consejo General del Poder Judicial decidió archivar la investigación abierta el 27 de julio de 2017 por un fallo de seguridad en la plataforma digital de intercambio de información que usan los órganos judiciales y los abogados, conocida con el nombre de LexNet. El pleno de esta institución considera que no afectó a ficheros jurisdiccionales, sino sólo a las cuentas correspondientes a abogados, procuradores y graduados sociales. Es por ello que el CGPJ alega que no es competente para seguir investigando, porque sólo son los documentos jurisdiccionales sobre los que el órgano de gobierno de los jueces tiene competencia en materia de protección de datos.

Atendiendo a la investigación realizada hasta la fecha por el Centro de Documentación Judicial (Cendoj) en coordinación con la Agencia Española de Protección de Datos, el CGPJ justifica su decisión advirtiendo de que “no todos los tipos de cuentas quedaron afectados” por el fallo de seguridad que obligó a parar LexNet durante más de una hora. Dicho esto, argumenta que el sistema LexNet es utilizado por abogados, procuradores, graduados sociales, centros penitenciarios, funcionarios de la Oficina Judicial, Policía Nacional, policías locales, Guardia Civil y hospitales, pero no es usado por los jueces y sólo mínimamente por los fiscales.

Es más, tomando como referencia los hechos investigados en estos cinco meses, el CGPJ asegura que el fallo de seguridad que se produjo no permitió acceder a expedientes completos de casos, ni a notificaciones no comunicadas a los procuradores, así como tampoco a borrar y modificar datos del sistema o presentar escritos en nombre de terceros. Es por ello que el órgano en cuestión se retira de la investigación y la deja en manos de la Agencia Española de Protección de Datos, por ser el órgano competente para determinar si se produjeron vulneraciones en materia de protección de datos de carácter personal en ficheros no jurisdiccionales. RECUEJO, M.: “El CGPJ archiva la investigación de la avería de LexNet por no afectar a jueces y fiscales, solo a abogados”, El Mundo, 28 de diciembre de 2017.

10 Así lo establece su artículo 46.1: “Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera”.

11 La información relativa a la resolución del expediente de la Agencia Española de Protección de Datos es de RODRIGUEZ, Y.: *La AEPD declara que el Ministerio de Justicia cometió una infracción grave por el fallo de seguridad de LexNet*, Conlegal, 10 de abril de 2018.

con Zaida Devito, *Dispositivos de Arquivos Prácticos de Masivos de Telefonía Móvil y la Captación y Grabación de Conversaciones y Práct.*, 1987, utilización de balizas para el seguimiento de vehículos, la interceptación de comunicaciones, los registros remotos de equipos informáticos, la videovigilancia, el reconocimiento biométrico de los rostros de las personas, etc. Todas ellas pueden ser tremendamente útiles en las pesquisas penales, pero, al mismo tiempo, ponen en serio peligro, cuando no violentan directamente, los derechos fundamentales de las personas investigadas. Por ello era fundamental que tales herramientas tecnológicas recibieran un respaldo legislativo y, a finales del año 2015, ello por fin tuvo lugar. Hasta entonces, y ante la inacción del legislador que en pleno siglo XXI continuaba sin regular las herramientas de investigación tecnológica, se había venido practicando una suerte de tolerancia jurisprudencial con ciertas prácticas instructoras invasivas. En este sentido la STC 145/2014, 22 de septiembre, resultó paradigmática. Representa algo así como un golpe en la mesa del Alto Tribunal llamando la atención del legislador e impeliéndole a cumplir la función que le es propia.

En aquel caso se anuló una sentencia del Tribunal Supremo en la que se había avalado prueba consistente en la grabación de conversaciones que dos sospechosos de asesinato habían realizado en los calabozos policiales. Las grabaciones habían sido autorizadas por un auto judicial profusamente motivado y apoyado en el art. 579 LECrim, pero carecían de habilitación legal. En esa sentencia podemos leer¹²: “Es doctrina constante de este Tribunal (...) que aunque la literalidad de dicho precepto (art. 18.3 CE) (“se garantiza el secreto de las comunicaciones y, en especial, las postales, telegráficas y telefónicas, salvo resolución judicial”) puede inducir a pensar que la única garantía que establece inmediatamente la Constitución es la exigencia de autorización judicial, un análisis más detenido de la cuestión pone de manifiesto lo contrario, ya que, por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, que incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa, además, una habilitación legal. Esa misma jurisprudencia dispone que la reserva de ley constituye “el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas”, lo que “implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate”, pero que en todo caso determinan que “el legislador ha de hacer el ‘máximo esfuerzo posible’ para garantizar la seguridad jurídica”, esto es, “la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho” (...). Profundizando en esa exigencia, en la STC 169/2001, 16 de julio, FJ 6, sostuvimos, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las

12 STC 145/2014, 22 septiembre, (RTC 2014,145), FJ 7.

características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias, que “la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad (...). Cabe concluir afirmando que ni el art. 579.2 de la Ley de enjuiciamiento criminal (LECrim), que citan las resoluciones judiciales impugnadas (fundamento de Derecho quinto de la Sentencia de la Sala de lo Penal del Tribunal Supremo, de 2 de junio de 2010; fundamento de Derecho segundo de la Sentencia de 10 de julio de 2009 de la Sección Primera de la Audiencia Provincial de Zaragoza -sin cita expresa del precepto-, y fundamento de Derecho primero del Auto de 14 de marzo de 2007 del Juzgado de Instrucción núm. 5 de Zaragoza), ni tampoco la normativa penitenciaria a la que igualmente aluden (fundamento de Derecho cuarto de la mencionada Sentencia del Tribunal Supremo), habilitan la intervención de las comunicaciones verbales directas entre los detenidos en dependencias policiales”.

Así pues, finalmente el legislador abandonó la idea de esperar a promulgar una nueva Ley de Enjuiciamiento Criminal para incluir la investigación tecnológica e implementó esas medidas largamente esperadas, mediante 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.

II. RÉGIMEN JURÍDICO DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA. LOS PRINCIPIOS RECTORES COMO EJE AXIAL.

El régimen jurídico de las medidas de investigación tecnológica se configura mediante un marco normativo doblemente acotado: las disposiciones comunes y las específicas.

En primer lugar, aparece en la LECrim el desarrollo de las disposiciones comunes a todas las medidas, desde el art. 588 bis a hasta el bis k, ambos inclusive. Este tratamiento común consta, a su vez, de dos componentes. Uno que incluye una descripción de los principios rectores que deben respetarse en la adopción de las medidas. Se trata de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Y a continuación, como segundo elemento de este tratamiento común, se articulan toda una serie de disposiciones generales relativas al procedimiento de adopción y ejecución de todas las medidas como son: la necesidad de autorización judicial, los requisitos de la resolución, el secreto de las actuaciones, la duración, las posibilidades de prórroga, el control judicial, la posible afectación de terceras personas, etc. Seguidamente prosigue la ley con el desarrollo en concreto de cada una de las cinco medidas de investigación tecnológica.

En este trabajo nos centraremos en el primer componente, examinando el contenido de los principios, que actúan como verdadero eje axial vertebrador del régimen de adopción de las medidas de investigación tecnológica. Lo haremos entreverando referencias a las resoluciones judiciales más destacadas.

Como decíamos *supra* los principios rectores son cinco: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Suponen la plasmación positiva de una jurisprudencia largamente desarrollada por los Tribunales Supremo y Constitucional. Parafraseando a MARCHENA GÓMEZ y GONZÁLEZ-CUÉLLAR SERRANO, puede decirse que el enunciado de estos principios, actúa como recordatorio de que más allá del estricto cumplimiento de las exigencias formales a las que ha de ajustarse el órgano jurisdiccional, la garantía constitucional asociada al sacrificio de los derechos fundamentales del art. 18 CE, opera como fuente legitimante¹³.

La ley enumera expresamente estos cinco principios, sin embargo, existe uno previo a todos ellos y plenamente habilitador de la medida a adoptar. Se trata del principio de legalidad. La posibilidad de emitir un mandamiento judicial para llevar a cabo una concreta investigación tecnológica, ha de estar prevista en la ley y debe dictarse cumpliendo con los requisitos del principio de legalidad. Por su carácter precursor y evidente es lógico que la ley no lo incluya de modo expreso. No obstante, no conviene olvidar que, en un pasado no muy lejano, y acuciados por la desidia legislativa, nuestros tribunales comprometieron este principio. Esto sucedió cuando se aplicaron medidas de investigación tecnológica, como por ejemplo, el registro de dispositivos de almacenamiento masivo de información, sin sujeción a una legalidad que, por otro lado, era inexistente a pesar de ser muy necesaria. Se daba así por bueno el acto de investigación sobre uno de estos dispositivos cuando se encontraban en una entrada y registro que sí estaba autorizada, pero que no los mencionaba como posibles hallazgos. Así, en la que se calificaba como "línea jurisprudencial muy discutible sostenían que la ocupación y análisis de equipos informáticos hallados en el curso de una entrada y registro domiciliario no exigía que el mandamiento judicial contemplara expresamente tal eventualidad"¹⁴.

Además, ha de tenerse en cuenta que el principio de legalidad no se cumplirá por la mera existencia de una ley que permita el acto de investigación tecnológica, sino que es preciso que esa ley delimite con suficiente precisión en qué situaciones puede tener lugar ese acto y hasta dónde se pueden violentar los derechos afectados. De este modo se preservará la seguridad jurídica de los justiciables

13 MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N.: *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, 2015, p. 212.

14 CABEZUDO RODRÍGUEZ, N.: "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", en *Las reformas del proceso penal*, I Jornada del Boletín del Ministerio de Justicia, año LXX, Núm. 2186, febrero de 2016, p. 42, quien cita como referentes de la posición previa y la actual, respectivamente, la STS 256/2008, de 14 de mayo, FJ 2 y la STS 342/2013, de 17 de abril, FJ 8.

como eventuales destinatarios de la medida. En este sentido VELASCO NÚÑEZ, señala que “la medida tecnológica que el juez autorice debe estar prevista por una norma que la habilite, que ha de ser de calidad tal que, por un lado, permita a todo ciudadano saber antes de acordarla en qué circunstancia se puede restringir su derecho y, por otro, evitar situaciones de abuso o arbitrariedad en los agentes del Estado al hacerlo”. Concluye este autor diciendo que “el juez no podrá autorizar el uso de una medida tecnológica de investigación que no esté prevista en la ley, ni en circunstancias que vayan más allá de lo pretendido y permitido por la norma¹⁵.”

Para terminar, conviene recordar que el art. 14.1 del Convenio sobre la Ciberdelincuencia instaba a las Partes a adoptar las medidas legislativas que resultasen necesarias a los efectos de investigación o de procedimientos penales específicos de los delitos que allí se señalan. El Estado español, al cumplir las exigencias del principio de legalidad en el asunto que venimos tratando, también ha observado uno de los principales compromisos emanados de la ratificación de este Convenio¹⁶.

I. Especialidad.

El art. 588 bis a núm. 2 LECrim establece que el principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. Añadiendo a continuación, que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

De la dicción literal del precepto se desprenden dos rasgos configuradores del contenido del principio. El primero, desde un punto de vista positivo, se concreta en la exigencia de relación de la medida con la investigación de un delito determinado. El segundo, desde un punto de vista negativo, plantea tres posibles escenarios en los que la especialidad no se cumpliría: cuando la medida tenga por objeto prevenir delitos, cuando pretenda descubrirlos o cuando se dirija a despejar sospechas sin base objetiva. Y, efectivamente, en cualquiera de esos tres supuestos no existiría conexión alguna con un delito concreto.

Conviene detenernos en la afirmación positiva de la especialidad, es decir, en la relación de la medida de investigación con un delito concreto, porque cabe preguntarse hasta qué punto ha de estar identificado ese delito para que el principio de especialidad pueda estimarse cumplido.

15 VELASCO NÚÑEZ, E.: *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Madrid, 2016, p. 68.

16 El Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2011, fue ratificado por España el 3 de junio de 2010 y entró en vigor para nuestro país el 1 de octubre de ese mismo año.

La STC 26/2010, de 27 de abril¹⁷, nos proporciona en su Fundamento Jurídico segundo una certera respuesta al describir cuál ha de ser la calidad de los indicios del delito que la sentencia comienza calificando como datos objetivos. Estos indicios, dice el Tribunal: “(...) son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento, en este sentido, hemos reiterado que la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan solo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas, hallarse apoyadas en datos objetivos que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros sin lo que no serían susceptibles de control y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona”.

Retomando la pregunta que nos hacíamos antes, habrá que contestar que el delito se considerará suficientemente identificado siempre que los indicios delictuales cumplan las dos condiciones que la sentencia exige: primero, accesibilidad y control por terceros y segundo, base real desconectada de valoraciones personales.

Concretado el primer rasgo definidor del contenido del principio, pasemos ahora a considerar una parte del segundo que se formula como una prohibición. El hecho de que art. 588 bis a núm. 2 LECrim no permita medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos, no significa que estas actuaciones no pueda llevarlas a cabo la policía en cumplimiento legítimo de sus funciones siempre que no afecten a derechos fundamentales. La prohibición se ciñe al supuesto de las medidas de investigación tecnológica vulneradoras de tales derechos y a ese ámbito debe restringirse. La posible duda quedó claramente despejada por la SAN 20/2016, 18 de julio¹⁸. En ella, el Alto Tribunal refirió que la defensa, en el caso de autos, cuestionó la investigación llevada a cabo. Lo hizo pretendiendo que, al tratarse de una investigación prospectiva, era ilegal y no podía admitirse que la policía hiciese vigilancias en las redes sociales a la búsqueda de actividades delictivas, como efectivamente sucedió.

La Audiencia Nacional, sin embargo, no compartió esta alegación y fundamentó su negativa como sigue: “Las fuerzas y cuerpos de Seguridad del Estado tienen como misión entre otras funciones (...) prevenir la comisión de actos delictivos, así como investigar los delitos para descubrir y detener a los presuntos culpables (...). En el ejercicio de estas funciones nada les impide realizar servicios de vigilancia

¹⁷ STC 26/2010, de 27 de abril (RTC 2010, 26).

¹⁸ SAN 20/2016, 18 de julio, ARP 2016/781, FD Primero.

y observación por las calles y por cualquier tipo de lugares públicos, incluidas las redes sociales públicas. Es más, estas actuaciones han resultado esenciales para descubrir delitos en los que las víctimas son las personas más vulnerables, los menores. No es necesaria una denuncia previa para que la policía actúe contra los comportamientos delictivos que observa en un lugar público, sea real o virtual. Lo que no puede hacer cuando actúan de esta forma, que efectivamente puede calificarse de prospectiva, es entrar en un domicilio o intervenir una comunicación privada sea telefónica o telemática, porque lo impiden los derechos fundamentales de inviolabilidad del domicilio, de intimidad o del secreto de las comunicaciones, recogidos en la propia Constitución (...) a modo de ejemplo basta señalar que en el art. 588 quinquies a) (LECrím) permite a la policía judicial obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, sin otros requisitos”.

De este modo queda claro que el principio de especialidad solo exige la emisión de mandamientos judiciales para la ejecución de medidas de investigación tecnológica siempre y cuando se proceda para un delito concreto. Los indicios del mismo deben cumplir las dos características señaladas por el Tribunal Constitucional: accesibilidad y control por terceros y base real desconectada de valoraciones personales. Mientras que la prevención, el descubrimiento de delitos o descartar sospechas sin base objetiva, no podrán motivar esta clase de diligencias de investigación limitadoras de los derechos fundamentales del art. 18 CE, por más que la primera y la segunda de esas actividades sí puedan ser llevadas a cabo por los Cuerpos y Fuerzas del Estado en cumplimiento de sus funciones. En esos casos el espacio será público y los entornos virtuales de acceso libre.

2. Idoneidad.

El art. 588 bis a núm. 3 LECrím proclama el principio de idoneidad. Según el texto legal servirá este principio para definir el ámbito objetivo, subjetivo y la duración de la medida en virtud de su utilidad.

Una vez determinado que la medida de investigación tecnológica está relacionada con la investigación de un delito concreto, surgen inmediatamente tres interrogantes cuando se trata de aterrizar la concreta medida a aplicar: ¿qué medida va a utilizarse del elenco proporcionado por la reforma de 2015?, ¿quiénes van a ser los sujetos afectados por la misma? y ¿durante cuánto tiempo?. Todo ello, en función de lo que sea más útil para la investigación penal pero, obviamente, sin perder de vista la proporcionalidad que, como luego veremos, es el principio origen de todos los demás y verdadera *alma mater* que transversalmente los informa a todos.

En palabras de OTAMENDI ZOZAYA¹⁹ “únicamente podrán adoptarse las medidas restrictivas de derechos fundamentales que presumiblemente vayan a ofrecer una utilidad para la investigación del concreto hecho delictivo que constituye el objeto del proceso, debiendo descartarse aquellas otras que se revelan como inútiles para obtener pruebas o indicios de la comisión del hecho delictivo que se está investigando y de quienes participan en él”. Entendemos que la idoneidad, vista de este modo, se acercaría, *mutatis mutandi*, al criterio de utilidad de la actividad probatoria acuñado, *a sensu contrario*, por la LEC cuando en su art. 283 dice que no deben admitirse, por inútiles, aquellas pruebas que, según reglas y criterios razonables y seguros, en ningún caso puedan contribuir a esclarecer los hechos controvertidos.

La STC 145/2014, 22 de septiembre²⁰, es ilustrativa de los extremos que deben cubrirse para que la idoneidad se entienda satisfecha. Refiriéndose a la motivación del auto judicial que autoriza la intervención de comunicaciones telefónicas, argumenta el Alto Tribunal que debe explicitarse, en el momento de adopción de la medida: “(...) todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Por ello, el órgano judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo; indicios que han de ser algo más que simples sospechas (...). Tiene además que determinar con precisión el número o números de teléfono y personas cuyas conversaciones han de ser intervenidas, el tiempo de duración de la intervención, quiénes han de llevarla a cabo y cómo, y los periodos en los que deba darse cuenta al Juez (...). Tales exigencias de motivación se reproducen en las prórrogas y en las nuevas escuchas acordadas a partir de datos obtenidos en una primera intervención, debiendo el Juez conocer los resultados de ésta con carácter previo al acuerdo de prórroga, explicitando las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión *tácita o presunta a la inicial*”.

Nótese cómo la exigencia de motivación de las causas reclama la fijación del tiempo inicialmente y no decae esta demanda tratándose de las prórrogas. La remisión a las causas iniciales, si éstas persisten, es posible, pero ha de ser expresa.

La idoneidad se resolverá, en cada medida en particular, de una forma particularmente adaptada al caso concreto. El respeto al principio de idoneidad será controlable mediante la exteriorización, en la motivación del auto, de los

19 OTAMENDI ZOZAYA, F.: *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*, Madrid, 2017, p. 107.

20 STC 145/2014, 22 de septiembre, (RTC 2014, 145), FJ 2.

tres elementos a los que se refiere el art. 588 bis a núm. 3 LECrim. Esto es ámbito objetivo, subjetivo y duración de la medida. Y siempre deberá tenerse presente que el juicio de adecuación a la idoneidad de la medida solicitada debe hacerse ex ante, en el momento de la petición inicial policial como nos recuerda la STS 60/2020, 20 de febrero²¹ según la cual: “(...) el juicio de validez del oficio policial y auto no puede hacerse ex post si se aprehende droga, sino ex ante, a fin de proceder a valorar si se cumplen los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Y, en consecuencia, no procede validar el auto por la circunstancia de que los agentes policiales luego encuentren droga a los investigados, ya que, como efectúa el Tribunal, el juicio de idoneidad y suficiencia debe hacerse ex ante al momento de la petición inicial y valoración de los indicios existentes en la investigación, no siendo suficientes las meras sospechas y/o conjeturas que se explicitan en la sentencia (...) no siendo los argumentos expuestos en el oficio, como antes se ha expuesto con el argumento del Tribunal negando suficiencia a la motivación del auto”.

3. Excepcionalidad y necesidad.

De la excepcionalidad y la necesidad nos habla el art. 588 bis a en su número 4: “En aplicación de los principios de excepcionalidad y necesidad solo podrá acordarse la medida:

a) 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,

b) 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.”

Parece desprenderse del modo de formulación de la norma que la excepcionalidad está descrita en el apartado a) mientras que la necesidad lo está en el apartado b). En cualquier caso, ambos principios son las dos caras de una misma moneda, de modo que uno se sustenta en el otro y viceversa²² por lo que a veces se hace difícil distinguir sus exactos contornos.

La excepcionalidad permite escoger una medida más gravosa frente a otras que lo son menos, por ser la primera más adecuada debido a las concretas

21 STS 60/2020, 20 de febrero, RJ/2020/585, FD Segundo.

22 Nótese que el propio legislador los agrupa en el mismo número reconociendo de alguna manera su carácter complementario.

circunstancias de la investigación. Esa elección, la de la medida más dañosa, deviene necesaria para que la instrucción avance. Al mismo tiempo, si se acredita como necesario el recurso a una medida más lesiva para que la investigación prospere ello se hace de modo excepcional.

La conclusión práctica de lo dicho es que “el juez debe descartar autorizar medidas restrictivas de investigación tecnológica cuando le consten otras vías menos lesivas para los derechos del investigado, que, con la misma eficacia y similar o incluso menos dificultad, lleven a dar parecida información sobre el extremo o los extremos que se pretendan averiguar²³.”

De la excepcionalidad nos hablan multitud de sentencias, de entre ellas destacamos la STS 982/2016, 11 de enero de 2017²⁴, en la que se examina la observancia de este principio en la autorización de una intervención de comunicaciones telefónicas: “De la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Ciertamente en la mayoría de los supuestos de petición se estará en los umbrales de la investigación judicial -normalmente tal petición será la cabeza de las correspondientes diligencias previas-, pero en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención telefónica, por ello la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional, riesgo sobre el que esta Sala ha llamado la atención varias veces. (...)”. Idoneidad porque este medio aparezca adecuado para los fines de la instrucción, necesidad porque no existe otro medio de investigación menos invasivo, y subsidiariedad porque ya se han agotado otros medios de investigación. Son garantías y cautelas para impedir que las intervenciones se conviertan en fuente de abusos de poder de la mano de estas modernas técnicas que, si es claro que permiten avanzar investigatorias, también suponen nuevos riesgos para los derechos de las personas (...)”.

Como vemos, según el Tribunal Supremo, son incompatibles con la excepcionalidad, por su carácter extraordinario, las peticiones sistemáticas, las concesiones rutinarias y la solicitud de esta clase de medidas invasivas sin una previa y suficiente investigación policial. El Tribunal pone asimismo de manifiesto la estrecha relación entre los principios rectores que estamos analizando.

23 VELASCO NÚÑEZ, E., *Delitos tecnológicos...*, cit., p. 69.

24 STS 982/2016, 11 de enero de 2017, RJ 2017/225, FJ Segundo.

Entendemos que la doctrina también se ha referido a este principio, años antes de su formulación expresa en la LECrim, cuando hablaba de la subsidiariedad como un subprincipio del principio constitucional de prohibición de exceso que tiende a la optimización del grado de eficacia de los derechos individuales frente a las limitaciones que pudieran imponer en su ejercicio los poderes públicos. Obliga a los órganos del Estado a comparar las medidas restrictivas aplicables que sean suficientemente aptas para la satisfacción del fin perseguido y a elegir, finalmente, aquella que sea menos lesiva para los derechos de los ciudadanos²⁵.

El principio de necesidad aparece también en multitud de sentencias. De ellas seleccionamos dos.

En la primera, la STS 391/2016, 6 de mayo²⁶, nos situamos ante un supuesto en el que el principio de necesidad no se cumplió. El recurrente cuestiona la nulidad de las intervenciones telefónicas que la Audiencia decretó apoyada en dos argumentos: el hecho de considerar que no se cumplió en la autorización judicial de la diligencia el principio de necesidad, toda vez que la solicitud policial se formuló sin haber agotado previamente la práctica de otros medios de investigación que evidenciasen lo imprescindible de la realización de las “escuchas”, así como que tampoco la resolución autorizante motivaba con suficiencia las razones por las que se produjo el cambio de líneas telefónicas, objeto de investigación, correspondientes a otros titulares distintos del sospechoso inicial. El Tribunal Supremo argumenta: “Si bien le asiste plenamente la razón al Fiscal en cuanto a la existencia de constatada necesidad de la injerencia en el derecho fundamental al secreto de las comunicaciones de la autorización inicial, subsiste, sin embargo, el segundo de los argumentos utilizados por la Audiencia pues, en efecto, cuando se interesa que se extienda la intervención a otras líneas telefónicas correspondientes a distintas personas, no se explica en ningún momento, ni por la Policía al interesarlo ni por el Instructor al acceder a esa solicitud, las razones por las cuales las sospechas se extendían a estos nuevos titulares. Y es que no nos hallamos ante el supuesto, al que al parecer nos quiere remitir el Fiscal, de aquellas otras ocasiones en las que resulta indiferente la titularidad de los equipos participantes en las comunicaciones objeto de intervención que, en efecto, es circunstancia irrelevante en orden a la protección del derecho invadido, sino que, en este caso, de lo que se trata realmente, como el resultado de la investigación a la postre evidenció, era extender a otros sujetos la investigación misma, lo que, obviamente, no puede hacerse sin la suficiente justificación para ello”.

25 GONZÁLEZ-CUÉLLAR SERRANO, N.: “El principio de proporcionalidad en el Derecho procesal español”, *Cuadernos de Derecho Público*, núm. 5 (septiembre-diciembre 1998), p. 206. El autor hacía equivaler este principio al de necesidad.

26 STS 391/2016, 6 de mayo, RJ 2016/1969, FD Primero.

Observemos como, en primer lugar, aparecen nuevamente amalgamados excepcionalidad y necesidad en el primero de los argumentos de la Audiencia que se cifraba en que la solicitud policial se formuló sin haber agotado previamente la práctica de otros medios de investigación que evidenciasen lo imprescindible de la realización de las intervenciones telefónicas.

El segundo de ellos, el referido a que el auto no motivaba con suficiencia las razones por las que se produjo un cambio en las líneas telefónicas investigadas, sí nos parece encuadrable en el diseño legal del principio de necesidad. Este cambio no era solo de líneas, sino también de personas titulares de las mismas, por lo que requería una adecuada motivación. De no haberse ampliado el objeto de la investigación a esas otras líneas, la investigación se vería gravemente dificultada, como expresa el art. 588 bis a núm. 4 b LECrim. Lamentablemente, al no observarse el principio de necesidad y constatarlo así el Tribunal Supremo, las pruebas de este modo obtenidas no son valorables y se frustra el trabajo policial.

En la segunda de las sentencias seleccionadas, la STS 646/2012, 13 de julio²⁷, sí se estimó satisfecho el principio de necesidad. “La parte recurrente hace especial hincapié en la falta del requisito de la necesidad de la medida, y alega que había profundizar previamente en la investigación sobre los bienes patrimoniales de Fermín. Sin embargo, tal como se razona en la sentencia impugnada, una vez que los encargados de la pesquisa habían detectado que Marco Antonio, ahora recurrente, residía temporadas fuera de España (en Holanda) y que Fermín era, en principio, su representante permanente en el territorio español, pues vivía de forma estable en la costa malagueña, la progresión de la investigación se hacía muy difícil sin acceder a lo que hablaban entre ellos”.

Nuevamente aquí se vincula el principio de necesidad con la medida de investigación más adecuada para hacer progresar la investigación, con la diferencia, respecto al caso tratado en la sentencia anterior, de que aquí sí se motivó suficientemente y por tanto se respetó el principio rector.

4. Proporcionalidad.

A la proporcionalidad dedica el art. 588 bis a LECrim el quinto y último punto. Según este precepto, las medidas de investigación tecnológica²⁸ 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

²⁷ STS 646/2012, 13 de julio, RJ 2012/11347, FJ Segundo.

²⁸ Nótese que el artículo habla literalmente de las “las medidas de investigación reguladas en este capítulo”. Está claro que no se limita a este capítulo, sino que alcanza hasta el capítulo IX. Y, en cualquier caso, la referencia quedaría corta porque estos principios rectores habrán de regir la aplicación no solo de las medidas de investigación tecnológica, sino también la de todas aquellas medidas que supongan una limitación de los derechos fundamentales del investigado.

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 primera vista este número del artículo parece el más extenso, tanto en su formulación como en el alcance de su significado. Es lógico que así sea. Como hemos adelantado *supra*, este principio de proporcionalidad es el *alma mater* del resto de principios. Es el principio marco en el que todos los demás encuentran cabida²⁹.

La STC 207/1996, 16 de diciembre³⁰ -muy distante en el tiempo de la reforma de la LECrim de 2015-, ya vislumbró esta idiosincrasia del principio de proporcionalidad. Lo hizo permitiendo distinguir entre la proporcionalidad en sentido amplio y la proporcionalidad en sentido estricto. La primera de ellas daría cobijo al resto de principios rectores, mientras que la segunda añadiría una nota específica configuradora de la esencia de la proporcionalidad.

Recordando la doctrina sobre este principio, resumía así el Tribunal los requisitos que debía cumplir la medida de investigación para ajustarse a la proporcionalidad: "(...) que la medida limitativa del derecho fundamental esté prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo". Líneas después identificaba este fin como "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal (...)".

El Tribunal reconoce como exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, la estricta observancia del principio de proporcionalidad. Y describe con más detalle los requisitos anteriormente mencionados condensándolos en tres: "(...) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por

29 Sobre el principio de proporcionalidad existen variadas aportaciones doctrinales. Destacamos dos que la abordan monográficamente. GONZÁLEZ-CUÉLLAR SERRANO, N.: "El principio de proporcionalidad en el Derecho procesal español", cit. y PEDRAZ PENALVA, E. y ORTEGA BENITO, V.: "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas", *Revista del Poder Judicial*, núm. 17, marzo 1990, pp. 1-27.

30 STC 207/1996, 16 de diciembre, (RTC 1996, 207). Las citas de esta sentencia son todas al FJ 4.

derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

De la doctrina que se establece en esta sentencia podemos colegir, como adelantábamos, una proporcionalidad en sentido amplio y otra en sentido estricto. En la primera se englobarían los principios examinados hasta ahora: la legalidad, la especialidad, la idoneidad, la excepcionalidad y la necesidad. Esto es así porque todos contemplan transversalmente una dosis de proporcionalidad adaptada a las concretas exigencias de cada uno. Sin embargo, la esencia misma de la proporcionalidad es la denominada por el Tribunal "proporcionalidad en sentido estricto" y consiste en analizar si de la adopción de la medida se derivan "más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto". El interés general será aquí el de la investigación penal y los bienes o valores en conflicto, los intereses y derechos fundamentales del investigado.

La cuestión que surge a continuación es cómo saber cuándo el fiel de la balanza se inclina a favor del interés general de la investigación penal o en defensa de los intereses y derechos fundamentales particulares del investigado. Será esa, sin duda, una pregunta que tendrá que resolver el juez de instrucción atendiendo a las peculiaridades de cada caso concreto y sobre la que no pueden aventurarse juicios previos. Sí pueden, sin embargo, plantearse algunos parámetros que sirvan de guía. Es esto precisamente lo que hace el art. 588 bis a núm. 5 LECrim *in fine* cuando dice que "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".

Como vemos, se enumeran hasta cuatro parámetros. A saber: a) la gravedad del hecho; b) su trascendencia social o el ámbito tecnológico de producción; c) la intensidad de los indicios existentes y d) la relevancia del resultado perseguido con la restricción del derecho.

El primero de ellos parece el más evidente de todos y el más fácilmente constatable. No obstante, esta característica de la gravedad exige ser matizada. El delito grave no es solo el que a efectos penológicos tenga esa cualidad, sino también el que, por su trascendencia social, pueda ser así considerado. En este sentido la SAP de Toledo 137/2015, 5 de noviembre³¹, se refiere a ello conectando la gravedad del hecho con el segundo de los parámetros de la proporcionalidad en sentido estricto, esto es, la trascendencia social. Así, razona la Audiencia que: "La proporcionalidad tiene como consecuencia que este medio excepcional de

31 SAP de Toledo 137/2015, 5 de noviembre, JUR 2015/302509, FD Quinto.

investigación requiere una gravedad acorde y proporcionada a los delitos a investigar. Señala la Jurisprudencia que el interés del Estado y la sociedad en la persecución y descubrimiento de los hechos delictivos es directamente proporcional a la gravedad de estos, por ello solo en relación a la investigación de delitos graves será adecuado el sacrificio de los derechos fundamentales para facilitar su descubrimiento pues el juicio de proporcionalidad de los intereses en conflicto desaparecería si por delitos menores se generalizase este medio excepcional de investigación con generalizado quebranto de derechos fundamentales. Frente a otras legislaciones que establecen el catálogo de delitos para cuya investigación está previsto este medio excepcional, la legislación española vigente en el momento de iniciarse esta causa y en este momento actual guarda silencio que se interpreta por la Jurisprudencia como exigencia de que se esté en la investigación de hechos delictivos graves (...) También es Jurisprudencia reiterada la que determina que la gravedad del delito no se valora solo atendiendo a la previsión legal para el mismo de una pena privativa de libertad grave, sino también apreciar la trascendencia social del delito que se trata de investigar (...). La trascendencia social tiene relación con la alarma social (...) y se valora la misma sobre la base de que sea un delito que se venga cometiendo habitualmente (...). Es más, la alarma social hace referencia al sentimiento social de inseguridad en lo más básico dada la reiteración de estos delitos y esto es socialmente trascendental”.

Respecto al concepto de delito grave, en relación a la proporcionalidad, parecía que la resolución de la cuestión prejudicial C-207/2016, planteada por la Audiencia Provincial de Tarragona, iba a resolver las dudas acerca de lo que debía entenderse por tal, a la luz del derecho europeo³².

El procedimiento principal que dio lugar al planteamiento de la citada cuestión prejudicial, se inició con una denuncia ante la Policía por un robo con violencia cometido el 16 de febrero de 2015. El 27 de febrero del mismo año la Policía Judicial presentó un oficio ante el Juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfonos activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo

32 Respecto a la interposición de esta Cuestión prejudicial véase BAHAMONDE BLANCO, M., “Medidas de investigación tecnológica a la luz de los derechos fundamentales, una cuestión pendiente”, *Diario La Ley*, nº 9160, Sección Tribuna, 16 de marzo de 2018, pp. 1-6.

El pasado 3 de mayo de 2018 el Abogado General presentó sus Conclusiones a la petición de decisión prejudicial. En su opinión, formulada en el punto 105, “aunque la pena tiene una importancia considerable, otros factores objetivos deben asimismo tenerse en cuenta (...). Concretamente se trata, por un lado, del contexto en el que se inscribe el delito cuya comisión se imputa –si la conducta delictiva es de carácter doloso, concurren circunstancias agravantes o el autor es reincidente–, por otro lado, de la importancia de los bienes jurídicos de la sociedad que han podido resultar lesionados por el autor del delito y la naturaleza o la magnitud de los daños sufridos por la víctima y, por último de la gradación de las penas en general en el Estado miembro de que se trate. A mi juicio procede calificar en su caso un delito de “grave”, en el sentido de la jurisprudencia del Tribunal de Justicia, a partir de este conjunto de criterios de apreciación, alternativos y no exhaustivos”.

móvil (IMEI) del teléfono móvil sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos, y en su caso, dirección.

El juez instructor denegó la diligencia solicitada pues entendió que la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves y con arreglo al Código Penal español el delito en cuestión -robo con violencia- no pertenecía a esa categoría. El Ministerio Fiscal interpuso recurso de apelación contra dicho auto y posteriormente el juez planteó la cuestión prejudicial expuesta en dos fundamentales preguntas:

1) La suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea ¿puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?

2) En su caso, la determinación de la gravedad del delito atendiendo a la pena imponible ¿sería compatible con una previsión general de límite de tres años de prisión? ¿Cuál debería ser ese umbral mínimo?

Parecía, viendo el planteamiento de las cuestiones prejudiciales, que el Tribunal aclararía cuál era el estándar de gravedad del delito que permitiría una injerencia en los derechos a la intimidad y a la vida privada. Y, caso de identificarse estrictamente con un criterio de gravedad penológica, se determinaría si los tres años eran un umbral mínimo aceptable o, en su caso, dónde situarlo.

Sin embargo, el Tribunal, aunque dio en su sentencia de 2 de octubre de 2018 una solución al caso planteado, no contestó estrictamente las cuestiones formuladas.

En efecto, el Tribunal parte de una distinción ente injerencias leves e injerencias graves en los derechos fundamentales consagrados en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea³³. Considera que los datos

33 Artículo 7. Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8. Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

referidos únicamente al número de teléfono correspondiente a la tarjeta SIM, así como los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre apellidos y, en su caso, dirección, no pueden calificarse de injerencia grave. Son datos estos que no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados y por tanto no presentan una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

En cambio, los datos relativos a las comunicaciones efectuadas en el teléfono, a su localización, fecha, hora y duración de las llamadas, destinatarios de las comunicaciones efectuadas con la tarjeta SIM en cuestión o la frecuencia de estas con determinadas personas cotejados con los anteriores datos, sí permitirían extraer esas conclusiones a las que nos referíamos. Parece desprenderse de la sentencia que, en caso de delincuencia no grave, tales injerencias no serían soportables.

Con la resolución de esta cuestión prejudicial el Tribunal ha determinado la compatibilidad de nuestro ordenamiento con el derecho de la Unión, en el caso de estas injerencias leves, pero queda por saber de una manera precisa si esas otras injerencias graves -que la normativa actual sobre investigación tecnológica española permite- se ajustan al derecho de la Unión.

En cualquier caso, junto a la interpretación de la gravedad del delito bajo un criterio no penológico, siempre estará la anudada a delitos graves. Así lo indica la STS 626/2019, 18 diciembre³⁴: "(...) resulta evidente que dada la gravedad de los hechos y la amplitud de personas que estaban interviniendo, conforme se detectó resultaba clara la proporcionalidad de la injerencia y su prórroga, a fin de poder detectar y comprobar el alcance de los hechos de tanta gravedad que se estaban produciendo y detectar quiénes lo estaban llevando a cabo, a fin de cerrar el círculo de los que estaban llevando a cabo estos actos ilícitos en lugar de velar por el cumplimiento de la Ley. Resulta evidentemente proporcional adoptar las medidas judiciales de injerencia cuando se trata de delitos de corrupción en donde las autoridades públicas y los funcionarios públicos en lugar de velar por cumplir su función de protección y tutela de los intereses públicos se aprovechan de su condición de la que se prevalecen para cometer estos hechos delictivos amparados en su poder, lo que les permite una facilitación del delito, y en algunos casos la dificultad de su descubrimiento, salvo que en los delitos de cohecho, los que son sobornados pongan en conocimiento de la autoridad lo ocurrido para depurar las

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

34 STS 626/2019, 18 diciembre, RJ/2019/5423, FD Séptimo.

responsabilidades penales por los mismos. En esta tesitura la proporcionalidad de la medida de injerencia y de las prórrogas resulta evidente”.

El segundo de los parámetros para evaluar la proporcionalidad es la trascendencia social del delito investigado que se hace equivaler en el precepto al denominado ámbito tecnológico de producción. Esta asimilación llevada a cabo por el legislador constata la tendencia de transformación digital a la que nos referíamos en apartados precedentes. Actualmente la trascendencia social del delito se hace notar tanto en el mundo físico como en el mundo virtual. Por eso ha hecho bien el legislador en equiparlos, puesto que si el ámbito de producción del delito es de carácter tecnológico la trascendencia del mismo está prácticamente asegurada.

En tercer lugar, la intensidad de los indicios existentes se revela también como un buen cuantificador del principio de proporcionalidad. Cuanta más fuerza incriminatoria posean, más se fortalecerá la línea de investigación que se dirija a adoptar una herramienta tecnológica en concreto.

En la jurisprudencia consultada hallamos supuestos en los que se vincula la intensidad de los indicios, con la gravedad de los hechos investigados para justificar así la proporcionalidad de la medida adoptada. Por ejemplo, en la STS 689/2016, 27 de julio³⁵, en la que se recurría la intervención de las comunicaciones telefónicas por estimarse no proporcionadas al fin pretendido. Allí el Tribunal justifica la proporcionalidad de la medida adoptada como sigue: “El auto de intervención telefónica que se impugna, se fundamenta en la aportación policial de unos datos objetivos de investigación que fueron evaluados por el Juez instructor, quien extrajo de ellos la inferencia fundada de poder existir un delito contra la salud pública y en el que podía estar involucrado el recurrente. Concretamente, el Juez instructor destaca que el recurrente había sido detenido con anterioridad por su participación en una importante operación de narcotráfico y lo pone en relación con el seguimiento policial que se abordó en las fechas inmediatamente anteriores a la petición de intervención telefónica, en la que se había observado que el recurrente se relacionaba con múltiples personas también vinculadas policialmente (con expresión de las causas) con el tráfico de drogas e incluso con un individuo llamado Eloy, que el Juez instructor destaca que estaba siendo objeto de investigación por delitos de esa naturaleza y respecto del que tenía previsto dictar una orden de entrada y registro en su domicilio. Destaca también el Juez de instrucción que la solidez de las sospechas se refuerza por comportamientos del recurrente expresamente orientados a lograr la clandestinidad de su actuación, no sólo observando precauciones para no ser seguido o no ser vigilado (que se detallan en el oficio policial), sino buscando que cada encuentro se culminara en puntos concretos que dificultaran la observación por terceros; todo ello, unido

35 STS 626/2019, 18 diciembre, RJ 2019/5423, FD Primero.

a un modo de vida que sugería unas fuentes de riqueza que no encontraban entonces justificación.

Las sospechas fundadas de participación delictiva y de la naturaleza del ilícito que podía estar perpetrándose, unidas a los frecuentes contactos sospechosos, los notables ingresos que podía estar generando y la precaución del recurrente por que nada de su eventual comportamiento delictivo pudiera resultar visible, muestra la necesidad y proporcionalidad de la medida, sin que el Juez dejara de exteriorizar estos elementos a lo largo del Auto, ni eludiera expresar -en el fundamento tercero de la resolución- que precisamente la gravedad del delito justificaba su decisión en términos de proporcionalidad de la medida”.

Otra sentencia que merece reseñarse es la STS 811/2015, 9 de diciembre³⁶, que remarca una idea fundamental acerca de la calidad de los indicios que se aportan: “(...) no debe confundirse esa necesidad de datos justificativos de la alta probabilidad acerca de la real existencia de la comisión del delito investigado con la presentación de verdaderas pruebas acreditativas del mismo que, con su existencia, harían ya innecesaria la propia diligencia cuya autorización se interesa”.

Finalmente, queda por examinar el último de los parámetros al que alude el precepto que estudiamos. Se trata de la relevancia del resultado perseguido con la restricción del derecho.

Es evidente que el resultado perseguido con la restricción del derecho está ligado al éxito de la investigación en curso. Hasta qué punto ese éxito sea relevante -que sería el criterio a considerar-, entendemos que dependerá, o bien del vigor con el que se manifiesten los otros tres cuantificadores o bien, de razones externas, como quizá pudiera ser la conexión entre el delito investigado y los criterios de política criminal vigentes. Tales criterios focalizan el interés público en la persecución de determinados delitos, de tal modo que el éxito de esas investigaciones se muestra especialmente relevante.

Hasta aquí los parámetros para determinar la proporcionalidad en sentido estricto. En cuanto a la exteriorización del juicio de proporcionalidad, se permite que esté implícito al darse por buena la llamada motivación por remisión. La STS 55/2020, 18 febrero³⁷, explica claramente este modo de proceder y su validez: “Si bien es cierto que la motivación por remisión no es una técnica jurisdiccional modélica, pues la autorización judicial debería ser autosuficiente (...), es el caso que la doctrina constitucional admite que la resolución judicial pueda considerarse suficientemente motivada si, integrada con la solicitud policial a la que se remite, o

36 STS 811/2015, 9 de diciembre, RJ 2015/5420, FD Primero.

37 STS 55/2020, 18 febrero, RJ/2020/371, FD Tercero.

con el informe o dictamen del Ministerio Fiscal en el que se solicita la intervención (...), contiene todos los elementos necesarios para llevar a cabo el juicio de proporcionalidad (...). Resultando en ocasiones redundante que el Juzgado se dedique a copiar y reproducir literalmente la totalidad de lo narrado extensamente en el oficio o dictamen policial (sic) que obra unido a las mismas actuaciones, siendo más coherente que extraiga del mismo los indicios especialmente relevantes (...)"

III. A MODO DE EPÍLOGO.

Como epílogo a todo lo desarrollado ofrecemos estas cinco conclusiones:

1ª) Los principios rectores de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, son de aplicación no solo en las medidas de investigación tecnológica limitativas de los derechos reconocidos en el art. 18 CE, sino que operan con relación a las medidas de investigación no tecnológicas que violenten dicho artículo

2ª) Merece destacarse la encomiable labor del legislador llevando al texto legal el contenido de estos principios rectores largamente analizados por la jurisprudencia por lo que supone de acercar el texto legal a la práctica de nuestros tribunales

3ª) Estos principios tienen un contenido preciso delimitado por la normativa que los regula no quedando su observancia preterida como podía suceder antes de su plasmación legal

4ª) Aunque en las específicas regulaciones de adopción de las medidas de investigación no consten referencias expresas a los principios rectores, todos ellos actúan, como disposiciones comunes que son, al modo de presupuestos de una legitimidad que debe exteriorizarse en el auto judicial

5ª) La inclusión de estos principios como parte de la normativa reguladora de las medidas de investigación, garantiza el respeto a unos límites que no deben ser sobrepasados por una buena investigación penal, con el pretexto de alcanzar mayor eficiencia.

BIBLIOGRAFÍA

AGENCIA EFE: "España registra en dos meses más incidentes de ciberseguridad que en todo 2014", 31 de marzo de 2018.

BAHAMONDE BLANCO, M.: "Medidas de investigación tecnológica a la luz de los derechos fundamentales, una cuestión pendiente", *Diario La Ley*, nº 9160, Sección Tribuna, 16 de marzo de 2018.

CABEZUDO RODRÍGUEZ, N.: "Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal", en *Las reformas del proceso penal*, I Jornada del Boletín del Ministerio de Justicia, año LXX, Núm. 2186, febrero de 2016.

GONZÁLEZ-CUÉLLAR SERRANO, N.: "El principio de proporcionalidad en el Derecho procesal español", *Cuadernos de Derecho Público*, núm. 5 (septiembre-diciembre 1998).

MARCHENA GÓMEZ, M. y GONZÁLEZ-CUÉLLAR SERRANO, N.: *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Madrid, 2015.

OLMO CALVO: "Buscando el escudo contra el Cibercrimen", *El Mundo*, 14 de agosto de 2017.

OTAMENDI ZOZAYA, F.: *Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia*, Madrid, 2017.

PALAZUELOS, F.: "Así fue el impacto del ciberataque en España", *El País*, 18 de mayo de 2017.

PEDRAZ PENALVA, E. y ORTEGA BENITO, V.: "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas", *Revista del Poder Judicial*, núm. 17, marzo 1990.

POWERDATA información accesible en <https://www.powerdata.es/nuestra-mision> (consultada el 7 de julio de 2020).

PRADILLO, J. C.: "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en PÉREZ GIL, J. (coord.): *El proceso penal en la sociedad de la información*, Madrid, 2012.

RECUERO, M.: "El CGPJ archiva la investigación de la avería de LexNet por no afectar a jueces y fiscales, solo a abogados", *El Mundo*, 28 de diciembre de 2017.

RODRÍGUEZ, Y.: "La AEPD declara que el Ministerio de Justicia cometió una infracción grave por el fallo de seguridad de LexNet", *Confilegal*, 10 de abril de 2018.

TOLEDANO, B.: "Hackean a la red interna de Telefónica y de otras grandes empresas españolas", *El Mundo*, 12 de mayo de 2017.

VAN DEN BERG, E.: "¿Qué es eso del Big Data?", *El País*, 31 de marzo de 2015.

VELASCO NÚÑEZ, E. y SANCHIS CRESPO, C.: *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, 2019.

VELASCO NÚÑEZ, E.: *Delitos tecnológicos: definición, investigación y prueba en el proceso penal*, Madrid, 2016.

