Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución

Julio Pérez Gil*

1. Una reforma necesaria, pero insuficiente

El ordenamiento procesal español adolecía de graves carencias en relación con las actuales formas de recopilación y análisis de información. En la práctica éstas se iban colmando mediante actuaciones de los cuerpos policiales sin claro sustento legal, las cuales posteriormente, eran acogidas (¡o no!) por los jueces. Ello producía serios problemas derivados de la muy defectuosa calidad de las normas habilitantes de injerencias en derechos fundamentales y, como consecuencia, un panorama de auténtica inseguridad jurídica. Era habitual encontrarnos ejemplos de admisión en los tribunales de lo que por vía de los hechos ya se había producido, de manera que en ocasiones asistíamos a una especie de irreflexiva convalidación normativa de lo fáctico. Por poner un par de sencillos ejemplos, no estaba muy claro en las normas procesales si requería autorización judicial acceder a la agenda o los mensajes de Whatsapp archivados en un teléfono móvil o al contenido de un dispositivo de almacenamiento de datos.

Desde diciembre de 2015 está en vigor la importante 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*

* Catedrático de Derecho Procesal. Universidad de Burgos. España

garantías procesales y la regulación de las medidas de investigación tecnológica. Esta norma, que era absolutamente necesaria, solo es comprensible como solución provisional y parcial para una necesidad acuciante del proceso penal español: una anhelada reforma integral de la LECrim (¡que data de 1882!) para la que, sin embargo, no hay consenso político suficiente.

Solo sobre esa premisa puede entenderse la particular sistemática con la que se ha abordado la modificación legal a la que nos referiremos. Ésta ha tomado por base una regulación obsoleta, pero muy depurada por la jurisprudencia (Tribunal Europeo de Derechos Humanos, Tribunal Constitucional, Tribunal Supremo y Audiencias Provinciales), dentro de la que se ha incrustado como cuerpo extraño un conjunto de novedosas diligencias de obtención y procesado de información relevante agrupadas bajo el título "medidas de investigación tecnológica".

El conjunto de la regulación abordada se sustenta sobre unos "Principios rectores" que, si bien parecen circunscribirse a este ámbito, deberían entenderse aplicables a todas las formas de investigación (de hecho, en la actualidad la investigación o es tecnológica o no es investigación). La ley se refiere así a:

- Principio de especialidad: la actuación de que se trate deberá tener por objeto el esclarecimiento de un hecho punible concreto, prohibiéndose las medidas de índole meramente prospectiva o de naturaleza predelictual. Es por ello que se exige "*que la medida esté relacionada con la investigación de un delito concreto*", sin que sean admisibles aquellas "*que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva*" (art. 588 bis a.2)]

- Principio de proporcionalidad, que a su vez se manifiesta en los siguientes subprincipios: a) idoneidad, de modo que será útil a fin de definir tanto los ámbitos objetivo y subjetivo de la medida aplicada cuanto la duración que abarque ésta (art. 588 bis a.3 y bis j); b) excepcionalidad y necesidad, que determinan que la medida adoptada deberá ser la menos gravosa o lesiva entre las posibles (art. 588 bis a.4); y c) proporcionalidad en sentido estricto, que obliga a la toma en consideración de todas las circunstancias del caso para apreciar que "*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*" (art. 588 bis a.5).

Otro aspecto que la reforma aborda con un ánimo generalizador (no siempre idóneo o posible) es lo relativo a la reserva jurisdiccional, tanto en lo referido al control *ex ante* (autorización del juez instructor para la adopción de una de tales medidas), como el control *ex post* (revisión de lo actuado y constatación de su ajuste a lo autorizado). En muchos de los casos se ha adaptado al conjunto de tales medidas la jurisprudencia consolidada particularmente en materia de intervención de comunicaciones.

La ley aborda así, por ejemplo: el contenido de la solicitud por el fiscal o la policía de la autorización judicial (art. 588 bis b); la resolución judicial autorizante (art. 588 bis c); el secreto de las actuaciones sin necesidad de que se acuerde expresamente (art. 588 bis d); el plazo de duración y sus prórrogas (art. 588 bis e y f); la forma y periodicidad del control judicial de la medida (art. 588 bis g); el tratamiento en caso de afección a terceros (art. 588 bis h); el uso de las informaciones obtenidas en un proceso distinto a aquel que motivó la adopción de una medida tecnológica de investigación, debiéndose acreditar la legitimidad de la injerencia (art. 579 bis 1 y 2); los descubrimientos casuales, esto es, hallazgos o descubrimientos no contemplados en la resolución habilitadora inicial cuya investigación deberá ser expresamente autorizada por el juez (art. 579 bis.3; 588 bis i); la finalización de las medidas por desaparición de las circunstancias que justificaron su adopción (art. 588 bis j); la destrucción de los registros originales y conservación de copia (art. 588 bis k). Se regula además en el art. 588.ter.e un aspecto llamado a alcanzar una importancia crucial en la materia: la obligación de contribuir a la investigación que se impone a "*Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual…*".

2. Un catálogo inacabado de medidas

2.1. *Aspectos generales*

Descendiendo ahora a lo concreto, las medidas se han insertado en los diversos capítulos que integran el Título VIII del Libro II de la Ley

de Enjuiciamiento Criminal, varios de ellos completamente nuevos. Con el ánimo de ofrecer una visión general y a modo de esquema, cabe destacar que las diligencias de investigación a las que nos referimos agrupan sistemáticamente de la siguiente manera:

Artículos LECrim.	**Contenido**
573-578	Del Registro de Libros y Papeles
579-588	De la detención y apertura de la correspondencia escrita y telegráfica
588 bis.a)-588 bis.k)	Disposiciones comunes
588 ter.a)-588 ter.m)	Interceptación de las comunicaciones telefónicas y telemáticas
588 quater.a)-588 quater.e)	Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos
588 quinquies.a)-588 quinquies.c)	Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización
588 sexies.a)-588 sexies.c)	Registro de dispositivos de almacenamiento masivo de información
588 septies.a)-588 septies.c)	Registros remotos sobre equipos informáticos (hacking policial)
588 octies	Medidas de aseguramiento (Orden de conservación de datos)
282 bis.) 6 y 7	Agente encubierto informático

En presencia de este catálogo tan amplio y complejo debemos detenernos en este momento solo en algunas de las diligencias que puedan servir para dar idea del conjunto de la regulación.

2.2. *Intervención de comunicaciones electrónicas (teléfono, correo electrónico, redes sociales, etc.)*

La captación en tiempo real del contenido de cualquier modalidad de comunicación electrónica, así como de los datos de tráfico asociados a ellas es, por así decirlo, la medida estrella de cuantas diligencias de investigación tecnológica se regulan en la ley. Las evidentes insufi-

ciencias e imprevisiones del régimen normativo anterior (contemplado fragmentariamente en el art. 579 LECrim) se suplen mediante un régimen general abierto a matizaciones en función de las particularidades de cada tipo de comunicación, que ahora se ha denominado "*interceptación de las comunicaciones telefónicas y telemáticas*" (Capítulo V, Título VIII, Libro II LECrim).

El ámbito material de aplicación de esta diligencia se hace de forma llamativa por remisión a lo que queda del art. 579 LECrim, referido ahora a la intervención de comunicaciones postales o telegráficas. Tal previsión sirve además de pauta general para el resto de medidas de investigación tecnológica. Para que pueda ser de aplicación en una instrucción concreta se exige la concurrencia de cualquiera de los tres requisitos que se definen en el apartado 1 del 579: a) delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; 2º delitos cometidos en el seno de un grupo u organización criminal; y 3º delitos de terrorismo. No obstante, se da acogida también a una larga reivindicación de la Fiscalía y de los cuerpos policiales para hacer posible el uso de esta diligencia también para la investigación de 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), sin vetar específicamente su uso en atención a la gravedad del delito.

Sobre esta medida opera una reserva jurisdiccional expresa, que encuentra una única excepción cuando se trate de actuaciones urgentes en materia de terrorismo (art. 588 ter d.3).

La limitación del plazo máximo de duración de la medida reproduce lo referido a la intervención de la correspondencia escrita (art. 588 ter g): 3 meses desde la fecha de la autorización, prorrogables por iguales o inferiores períodos hasta 18 meses (art. 579.2).

La reforma no desconoce las muy diversas formas de comunicación que existen en la actualidad y, sin entrar en excesivo detalle para designarlas, les otorga carta de naturaleza en el texto legal. La mención genérica a las comunicaciones incluye por ello cualquier tipo de comunicación que se realice a través del teléfono (fijo o móvil) o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual.

La resolución judicial habilitante habrá de fijar la extensión de la injerencia (la petición del Ministerio Fiscal o la Policía servirá aquí de guía), debiéndose motivar expresamente su necesidad. La ley pretende

que se exprese "*la forma o tipos de comunicaciones a que afecta*" (contenido), así como a informaciones tales como el origen o destino de la comunicación, la ubicación geográfica u otros datos de tráfico asociados o no a la comunicación. El art. 588 ter b. 2. III establece que "*se entenderá por datos electrónicos de tráfico o asociados 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.*"

Llegados a este punto, no podemos pasar por alto una de las cuestiones que más polémicas acarrea, puesto que la utilización de datos de tráfico de las comunicaciones se fundamenta en su previa conservación. En España esa obligación deriva de lo dispuesto en la *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* (a la que se remite el artículo 588 ter j LECrim). Tal norma tomaba por base la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, *sobre la 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 y por la que se modifica la Directiva 2002/58/CE*. Pero, como es bien conocido, ese marco regulador está en proceso de transformación, pues la citada Directiva fue invalidada por la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, caso *Digital Rights Ireland*. Con posterioridad el Tribunal de Luxemburgo ha venido a ratificar su posición en otros pronunciamientos la STJUE de 21 de diciembre de 2016 *Tele2 Sverige AB c Postoch telestyrelsen* (asunto C‑203/15) y *Secretary of State for the Home Department* c. *Tom Watson, Peter Brice, Geoffrey Lewis* (asunto C‑698/15), con intervención de Open Rights Group, Privacy International, Law Society of England and Wales (asuntos acumulados C‑203/15 y C‑698/15). [1]

En su interpretación de la Carta de Derechos Fundamentales de la UE el Tribunal ciertamente admite la posibilidad de que los Estados cuenten con medidas de conservación de datos de las comunicaciones,

1 También el TEDH, en su sentencia de 12 de enero de 2016, Szabó y Vissy c. Hungría, ha subrayado la importancia de las garantías enunciadas en las citadas STJUE (vid. § 68)

pero acotándolos a supuestos concretos, estableciendo límites objetivos y temporales en función del tipo de dato o la persona afectada, etc. La enorme incidencia que ello puede tener sobre las normas procesales españolas no está, a mi juicio, siendo suficientemente valorada. Cabe advertir entonces que los principios rectores más arriba aludidos desempeñan un papel esencial, pues solo será válida aquella injerencia cuando, además de ser idónea y útil, comporte el menor de los sacrificios posibles para los derechos fundamentales.

Los parámetros con los que se determine esa validez no pueden dejar de desconocer la jurisprudencia comunitaria. Se hace pues imprescindible reivindicar una reforma del régimen de conservación de datos de las comunicaciones, en las que se recoja al menos la obligación de archivo de los datos en la UE, la distinción del régimen jurídico entre diferentes tipos de datos y el acortamiento de los plazos de conservación.

Por último a este respecto debemos referirnos a determinados datos vinculados a comunicaciones cuya obtención se autoriza a la Policía, sin que sea precisa la autorización judicial. Es lo que ocurre, por ejemplo, con datos que aporten información que singularice máquinas, pero no identifique a sujetos concretos (barridos de códigos IMSI o IMEI). Asimismo, cuando la información se extraiga de entornos en los que no pueda predicarse la existencia de una expectativa de intimidad (direcciones IP públicas, información proporcionada por la víctima, etc.) (arts. 588 ter k, 588 ter l LECrim).

2.3. *Registro de dispositivos y sistemas (físicos y a distancia)*

La Ley establece una doble regulación del registro de dispositivos de almacenamiento masivo de información: a) cuando ésta requiere incautación física (o copia de la información en ellos contenida) o b) cuando se produce el registro remoto de equipos, que se autoriza únicamente para determinadas categorías delictivas graves o cuya efectiva persecución exige acudir a esta clase de medida[2].

2 La severidad de la injerencia en el ámbito de la intimidad y dignidad de la persona ha llevado al legislador a acotar mediante numerus clausus el listado de los delitos que justificarían su utilización: delitos de organizaciones criminales, terrorismo, contra menores o personas con capacidad modificada judicialmente, contra la Constitución, de traición y relativos a la seguridad o delitos cometidos a través de instrumentos informáticos o de

Una diligencia de esta naturaleza requiere de autorización judicial explícita, aun cuando la aprehensión de los dispositivos tenga lugar en el marco de un registro domiciliario (art. 588 sexies a-b). Si el acceso es remoto, la ley toma en consideración que deberá haber existido una previa investigación que permita identificar los dispositivos o sistemas que hayan de ser objeto de la medida, permita singularizarlos (art. 588 septies a.2, a) - e). Esta es la vía que permite a los investigadores policiales la instalación de software espía, cuestión que ha suscitado problemas técnicos y jurídicos diversos. En estos casos se pueden adoptar también medidas para suprimir o hacer inaccesibles los datos intervenidos (art. 588 septies a.2, letra e). El plazo máximo de duración es de un mes, prorrogable por iguales períodos hasta los 3 meses (art. 588 septies c).

La resolución judicial deberá también expresar el alcance del registro, debiendo por tanto especificar en la medida de lo posible la clase de información que se está buscando con el fin de ajustar la investigación a los parámetros propios del principio de proporcionalidad. Como es lógico, se contempla la posibilidad de que el registro se amplíe a redes a las que esté conectada (incluida "la nube" –*cloud computing*-) (arts. 588 sexies c.3 y 588 septies a.3). Para ello puede ser imprescindible la cooperación de sujetos privados (operadores y responsables de sistemas), a quienes se impone no solo la obligación de colaborar, sino también de mantener esas actuaciones en secreto (arts. 588 sexies c.5 y 588 septies b). Asimismo deberá autorizarse la realización de copias y las garantías de fiabilidad en la obtención y preservación de que se rodearán éstas (arts. 588 sexies c y 588 septies a.2 b), d) y e).

Merece la pena llamar la atención sobre lo que supone una excepción a la general necesidad de autorización jurisdiccional, prevista únicamente para los registros físicos (no así para los realizados de forma remota, en los que la previa planificación permite solicitar la autorización judicial). En tales casos, los cuerpos de Policía pueden acceder directamente "*en caso de urgencia*" a datos contenidos en un dispositivo incautado (o a sistemas accesibles desde el del investigado). Para ello deberá apreciarse "*un interés constitucionalmente legítimo que haga imprescindible la medida*" (art. 588 sexies c.3 y 4). Parece pensarse en supuestos en los que la adopción de la medida sea

cualquiera otra tecnología de la información o la telecomunicación o servicio de comunicación (art. 388 septies a.1 apartados a) - e)

inaplazable sin que pudiera alcanzarse el fin que se pretende con medidas de mera conservación en tanto se obtuviera la resolución judicial. En todo caso la medida está sometida a la ulterior convalidación judicial, a fin de que los resultados obtenidos puedan ser considerados válidos (art. 588 sexies c.3 y 4).

2.4. *Agente encubierto informático*

La reforma procesal ha abordado la figura del agente encubierto desde una doble perspectiva: a) la facultad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; y b) la figura del agente encubierto informático, en la que nos centraremos ahora.

La necesaria vigilancia policial de las redes, cuando se desarrolla en canales cerrados de comunicación y por ende conlleva una afección a la esfera privada, se confronta con aspectos problemáticos que comprometen la utilidad probatoria de las informaciones obtenidas. Con el fin de abordar la cuestión, la ley incluye una traslación al mundo digital del agente encubierto ya regulado. No obstante, no se regula la actividad de particulares infiltrados en redes criminales ni tampoco la posibilidad de usar "sistema trampa", señuelos o "cebos virtuales" (*honeypots*).

El juez deberá autorizar el uso de identidades supuestas en comunicaciones mantenidas en canales cerrados de comunicación, tarea que solo podrán desempeñar funcionarios de la Policía. Determinadas actuaciones tales como el intercambio o envío de archivos ilícitos por razón de su contenido requerirá de una nueva autorización expresa (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) (art. 282 bis 6). Naturalmente el agente encubierto no podrá incurrir en conductas que "*constituyan provocación del delito*" (art. 282 bis.5).

3. Una omisión relevante: protección de datos y proceso penal

Las garantías procesales clásicas en materia de obtención de información se vienen centrando en la forma en que ésta tiene lugar: acceder a domicilios, a comunicaciones, a sistemas de archivo, etc.

Las nuevas realidades tecnológicas nos hacen ver, sin embargo, que no debemos descuidar un aspecto esencial: el tipo y la cantidad de información que accede al proceso, así su potencialidad para afectar a la vida privada y familiar tanto del sujeto investigado como de otros.

Si ya Carnelutti se refiriera al proceso penal como la Cenicienta del Derecho Procesal, perdida entre el Derecho Penal material y el Derecho Procesal Civil, hoy podemos ver al Derecho a la Protección de Datos de Carácter Personal como una nueva Cenicienta que, obviada en las normas procesales penales por su aparente insignificancia, se viste con los ropajes de su hermana mayor, el derecho al secreto de las comunicaciones. Y creo que al final, como en el cuento, se acabará reivindicando como una verdadera protagonista cuando alguien encuentre el zapato de su horma.

A este respecto la Carta de los Derechos Fundamentales de la Unión Europea, en la interpretación que está realizando el TJUE, juega un papel absolutamente determinante. En ella se destaca la importancia tanto del derecho fundamental al respeto de la vida privada (artículo 7 de la Carta) como del derecho fundamental a la protección de los datos personales (artículo 8).[3] También el Tribunal de Estrasburgo parece reivindicar un papel activo al respecto, como demuestra su última jurisprudencia en torno al derecho a la vida privada y familiar del art. 8 del Convenio.[4]

En todas las llamadas "medidas de investigación tecnológica" se emplean instrumentos o se produce una injerencia en dispositivos que llevan aparejado un tratamiento cualificado de información de carácter personal. De ahí que todas estas medidas sean susceptibles de enmarcarse en el ámbito de cobertura del derecho fundamental a la protección de los datos de carácter personal.

Sin embargo, la proyección de este derecho en la regulación, de existir, no es clara ni mucho menos coherente. Ello se debe por un lado a la influencia directa de la regulación de la interceptación de las comunicaciones en el conjunto de medidas que se disciplinan en la Ley, pero también, y ese es el punto que aquí queremos destacar, es

3 Vid. SSTJUE Rijkeboer, C 553/07, EU:C:2009:293, apartado 47; Digital Rights Ireland y otros, C 293/12 y C 594/12, EU:C:2014:238, apartado 53, y Google Spain y Google, C 131/12, EU:C:2014:317, apartados 53, 66 y 74 y la jurisprudencia citada)

4 Entre los últimos pronunciamientos cabe reseñar, por ejemplo, las SSTEDH Sommer c. Alemania, de 27 de abril de 2017 y Trabajo Rueda c. España, de 30 de mayo de 2017.

consecuencia de la ausencia de un análisis integral de sus implicaciones en la investigación penal. Ello nos permite apreciar en relación con el derecho a la protección de datos que en algunos casos la atención debida a éste queda difuminada en la correspondiente a otros derechos fundamentales (derecho al secreto de las comunicaciones en el caso de la interceptación de las comunicaciones telefónicas y telemáticas; intimidad, en el de la captación y grabación de comunicaciones orales directas y utilización de dispositivos o medios técnicos de seguimiento y localización). Tampoco en el caso del resto de medidas, resulta claro que la nueva regulación haya tomado en consideración suficientemente el contenido esencial del derecho a la protección de datos.

Esta omisión produce desajustes, pues siendo claro que no todos los datos utilizados en el proceso penal deban estar protegidos con la misma intensidad, no encontramos previsiones legales nítidas a este respecto. Estimamos por ello que en el futuro se abandone una sistemática que induce a errores. Se ha de poner el acento en el carácter digital de las fuentes de conocimiento que llegarán a ser medios de prueba, pero no por su vinculación con las comunicaciones, sino por su propia naturaleza y características.

La valoración de las eventuales injerencias en el ámbito jurídico fundamental deberá asumir como parámetro de medición la potencialidad para generar conocimiento cuando legítimamente se desee mantener éste reservado. Así, por ejemplo, no es lo mismo que los órganos de investigación soliciten información de una operación bancaria puntual, que pedir un listado de todos los movimientos y apuntes practicados en una cuenta a lo largo de años. O no puede tener el mismo efecto solicitar esta última información cuando con ellos, por ejemplo, se pongan de manifiesto aspectos amparados por el secreto profesional del abogado que cuando se trate de datos que ni siquiera permitan identificar a una persona.[5]

Respecto de los terceros distintos del encausado que son titulares de datos de carácter personal susceptibles de verse afectados por la cesión en algunos casos (datos bancarios, correspondientes a comunicaciones electrónicas), es criticable la falta de cualquier

5 Es el supuesto de la STEDH Sommer c. Alemania, de 27 de abril de 2017

previsión destinada a su puesta en conocimiento de los eventuales afectados a fin de abrirles la posibilidad de ejercitar en sede judicial de los derechos aparejados a la protección de datos de carácter personal (acceso, rectificación y cancelación).

Por otro lado, las actividades de vigilancia vinculadas a la prevención del delito son esenciales, aun teniendo en cuenta su potencial lesividad para la esfera jurídico fundamental. Pues bien, no encontramos un marco general que nos permita por ejemplo delimitar el volumen de información (¿hasta dónde puede llegar una vigilancia?) ni tampoco la forma para hacer entrar en el proceso la información recabada con anterioridad a la comisión del delito obtenida para otras finalidades. De ahí que esta tarea deba ser propia del control judicial, que habrá de implicar la calidad, cantidad y tipo de información que formará en su momento el acervo probatorio. Más allá del control y la autorización *ex ante* sobre la forma en que se va a adquirir la información (registro, intervención de comunicaciones), es necesario, pues, considerar esenciales los controles *ex post*.

4. Referencias bibliográficas

La novedada y la enorme amplitud del tema abordado aconsejan refirse únicamente a obras muy recientes y solo a algunas de carácter general. Cabe destacar entre ellas:

CEDEÑO HERNÁN, M. (COORD.), *Nuevas tecnologías y derechos fundamentales en el proceso*, Aranzadi, 2017

DELGADO MARTÍN, J., *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley 2016

GONZÁLEZ LÓPEZ, J. J.; PÉREZ GIL, J., *The New Technology-Related Investigation Measures in Spanish Criminal Proceedings: An Analysis in the Light of the Right to Data Protection* en *European Data Protection Law Review* 2016 - 2, 242-246

PÉREZ GIL, J. (Coord.), *El proceso penal en la sociedad de la información*, La Ley 2011

RICHARD GONZÁLEZ, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y garabación de imagen y sonido*, La Ley 2017

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

SANTOS MARTÍNEZ, A. M., *Medidas de investigación tecnológica en la instrucción penal*, Bosch 2017

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