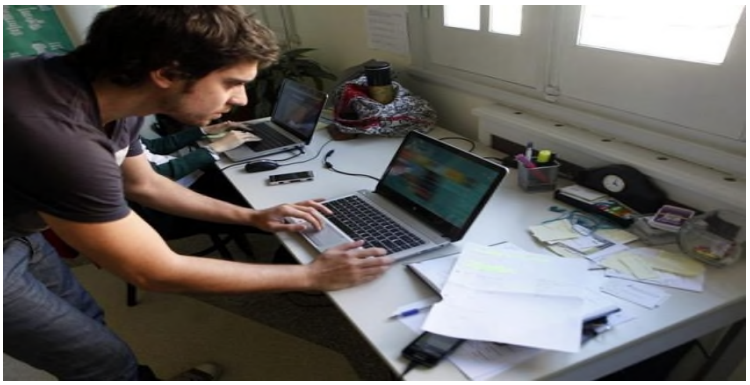

# ¿ES JUSTO EXCLUIR DELITOS DE LA INVESTIGACIÓN CRIMINAL TECNOLOGICA?

Por Francisco Javier Pérez-olleros Sánchez-Bordona

Junio 2015

**“NO OBTIENE JUSTICIA HUMANA QUIEN POSEE LA VERDAD SINO AQUEL QUE MEJOR LA EVIDENCIA”**

El artículo 24.2 de la Constitución Española consagra como derecho fundamental de todos los ciudadanos el derecho a utilizar los medios de prueba pertinentes, ejercitable en cualquier tipo de proceso (STC 173/2000, de 26 de junio, FJ 3).

Es decir, es el derecho de quien está inmerso en un conflicto que se dilucida jurisdiccionalmente, a impulsar una actividad probatoria acorde con sus intereses, siempre que la misma esté autorizada por el ordenamiento (STC 131/1995, de 11 de septiembre, FJ 2).

Este derecho lo ostenta no sólo el acusado, sino también el Ministerio Fiscal, y en su caso el resto de las acusaciones.

Pero el derecho a la prueba previsto en el art. 24.2 CE es un derecho de configuración legal, correspondiendo al legislador establecer las normas reguladoras de su ejercicio en cada orden jurisdiccional (por todas, STC 126/2011, de 18 de julio, FJ 13).

En este sentido se ha pronunciado el Tribunal Europeo de Derechos Humanos, interpretando el art. 6.1 del Convenio europeo de derechos humanos y de las libertades fundamentales (en adelante, CEDH), al indicar que "*la admisibilidad de pruebas depende, en primer lugar, de las reglas de derecho interno*" (STEDH de 14 diciembre 1999, caso A.M. contra Italia, ap. 24).

El derecho a obtener los datos del tráfico de llamadas y de navegación en internet se viene limitando en las investigaciones por delito en España, para conjugar este derecho a la prueba, con el respeto a la vida privada y al secreto en las comunicaciones, y sobre ello trata este artículo, dado los diferentes criterios jurisdiccionales al respecto que se vienen produciendo en los Juzgados y Tribunales respecto de la limitaciones en la investigación de los delitos cometidos a través de la denominada sociedad de la información, que nace al abrigo de las tecnologías –no sólo de carácter telemático, sino también de otro tipo, como el cable o la televisión digital– y que ha transformado las relaciones sociales y jurídicas.

## I.- NECESIDAD DE AUTORIZACIÓN JUDICIAL PARA LA INVESTIGACIÓN

**La Ley 9/2014, de 9 de mayo (BOE 10 de mayo), General de Telecomunicaciones,** en su **artículo 42** relativo a la conservación y cesión de datos de las comunicaciones electrónicas y redes públicas de comunicaciones, señala que:

*"La conservación y cesión de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación a los agentes facultados a través de la correspondiente autorización judicial con fines de detección,*

*investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en leyes especiales se rige por lo establecido en la Ley 25/2007, de 18 de octubre*".

La Ley 25/2007, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y Redes Públicas de Comunicaciones, por primera vez obligó legalmente y por razones de seguridad a los prestadores de servicios de la sociedad de la información a la conservación de los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, estableciendo en su artículo 1 que debían ceder dichos datos a los agentes facultados (Policía Judicial, Vigilancia Aduanera y CNI) siempre que les fuesen requeridos, a través de la correspondiente autorización judicial, y con fines de detección, investigación y enjuiciamiento de **delitos graves contemplados en el Código Penal o en las leyes penales especiales**.

De la conservación de estos datos del tráfico externos al contenido de la comunicación, se excluye el contenido de la comunicación, y por eso no afecta al núcleo del secreto de las comunicaciones, sino que a lo que fundamentalmente afecta es al derecho fundamental a la privacidad y a la limitación del uso de la informática, es decir, al artículo 18, en su apartados 1 y 4 de la Constitución Española –CE-, aunque en muchas resoluciones se cite también como injerencia el artículo 18.3 de la CE.

Por eso, la Sentencia del TJUE de 8 de abril de 2014, declaró la invalidez de la Directiva 2006/24/CE, de 15 de

marzo, sobre la conservación de datos generados o tratados en las comunicaciones electrónicas de acceso público o redes públicas, que se transpuso por la Ley 25/2007, y determinó por primera vez la monitorización de los datos de tráfico generados como consecuencia de una comunicación o de un servicio de comunicación, no del contenido de esa comunicación, invalida la Directiva 2006, no porque no sea posible guardar esos datos en ficheros, sino que entiende que conforme al contenido de la Directiva no queda suficientemente garantizados los derechos fundamentales de los artículos 7 (derecho a la vida privada y de las comunicaciones) y 8 (protección de los datos de carácter personal) de la Carta de los Derechos de la Unión.

De hecho el artículo 1.3 de la Ley 25/2007 establece:

"*Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas*."

El legislador español entiende que la Ley española 25/2007 ha ido más allá que la Directiva invalidada 2006/24/CE en la protección y control de los derechos a la privacidad y al secreto de las comunicaciones, y por ello mantiene su eficacia, si bien la reforma en ciertos aspectos que no afectan a la cuestión que analiza este artículo, en la nueva Ley General de Telecomunicaciones 9/2014.

Esta Ley 25/2007 regula por tanto, sólo la conservación y cesión de los datos de tráfico externos al

contenido de esas comunicaciones, necesarios para rastrear e identificar el origen y destino de una comunicación de telefonía de red fija y móvil, y respecto al acceso a internet, al correo electrónico y la telefonía por Internet, según relación detallada de los datos que deben conservar efectuada en el artículo 3 de la Ley 25/2007.

Datos como origen y destino de la comunicación, y hora, fecha y duración, no su contenido.

Para solicitar la cesión de estos datos de los proveedores de servicios de telecomunicaciones e internet que están obligados a conservar, se requiere autorización judicial, conforme al **Acuerdo de la Sala del Tribunal Supremo de 23 de Febrero de 2010**.

La Fiscalía también precisa de tal autorización.

La operadora no sólo conoce quién y desde dónde hace la llamada (SIM), sino también desde qué terminal telefónico se realizó.

Normalmente esos datos los conservará la operadora durante un año (artículo 5 Ley 25/2007), y aunque se cancelen se conservarán hasta la prescripción del delito a disposición de los Tribunales, y deberá cederlos en un plazo máximo de 7 días, salvo que establezca otro plazo la resolución judicial.

Lo dispuesto anteriormente, sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,

que señala que **la cancelación de los datos no supone su eliminación automática, sino su bloqueo** tal y como dispone el **artículo 16.3 de la Ley Orgánica 15/1999,** al establecer que:

"*La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión*."

Es decir, la cancelación de los datos no supone su eliminación automática para los Jueces y Policía, sino sólo su bloqueo, conservándose a su disposición y por tanto, son de posible investigación criminal, para determinar y depurar las posibles **responsabilidades nacidas del tratamiento**, durante el plazo de prescripción de éstas.

Pero si se aportara el dato habiéndose conseguido sin la autorización judicial o el consentimiento investigado, la prueba sería nula por haber sido obtenida con violación del derecho a la intimidad personal del encausado según dispone el art. 18.1 de la Constitución Española (artículo 11.1 de la LOPJ).

Y además, la ilicitud se extendería también a las pruebas derivadas o reflejas, si entre ellas y las anuladas, existe una conexión natural o causal (que constituye el presupuesto para poder hablar de prueba derivada de otra ilícitamente obtenida). En estos casos, la regla general es

que todo elemento probatorio que pretenda deducirse a partir de un hecho vulnerador del derecho fundamental, se haya también incurso en la prohibición de valoración, siempre que se establezca un nexo entre unas y otras, que permita afirmar que la ilegitimidad constitucional de las primeras se extiende también a las segundas (conexión de antijuridicidad a la que se refieren entre otras SSTC 22/2003 y 66/2009).

## II.- PROCEDIMIENTO DE CESIÓN DE DATOS

Se regula en los **artículos 6 y 7 de la Ley 25/2007**, que si fueron modificados por la disposición final 4.1 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

El artículo 6 de la citada Ley establece las normas generales sobre cesión de datos, estableciendo en su punto 1 que sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial, y que la cesión se efectuará en formato electrónico y únicamente a los agentes facultados. Y tendrán la consideración de agentes facultados la Policía judicial, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en

la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

En el **artículo 7 de la Ley 25/2007, establece**:

*"1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.*

*2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los* ***principios de necesidad y proporcionalidad****, los datos conservados que han de ser cedidos a los agentes facultados.*

*3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.*

***Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro del plazo de 7 días naturales contados a partir de las 8:00 horas del día natural siguiente a aquél en que el sujeto obligado reciba la orden****".*

Será responsable en sede judicial de recoger los datos y documentarlos el Secretario del Juzgado (334 LECR), testimoniando el soporte digital -CD o DVD, PEN-DRIVE-, pudiendo transcribirlos en papel, y al juicio oral se incorporaran a través de la lectura (730 LECR), o el examen directo por el Juez (726 LECR).


## III.- QUE SE ENTIENDE POR DELITO GRAVE A LOS EFECTOS DE LA INVESTIGACIÓN CRIMINAL DEL CIBERDELITO

Como indicamos previamente, la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, exigió un estricto control en la cesión de los datos, y en la legislación regulatoria, y consideró que esta exigencia en el control no se cumplía con la Directiva 2006/24/CE, de ahí que la invalidara.

Teniendo en cuenta la anterior exigencia, y la falta de definición en la Ley 25/2007, sobre que se entiende por delito grave a los efectos de la cesión de los datos monitorizados por las operadoras, muchos órganos unipersonales y Tribunales españoles interpretan que la gravedad del delito viene determinada por el propio Código Penal, que actualmente define como delito grave el que lleva aparejada pena privativa de libertad superior a 5 años (13 y 33 CP).

Pero también parte de la doctrina, de los Tribunales, y la propia Fiscalía General del Estado, entienden que es posible una interpretación no penológica sobre la gravedad del delito cometido con el uso de instrumentos informáticos y telemáticos, y en tal sentido se ha pronunciado:

-La Circular 1/2013 de la Fiscalía General del Estado, la gravedad debe valorarse en atención a las circunstancias del hecho, el bien jurídico protegido, la relevación social, y la jurisprudencia al caso:

- La jurisprudencia que se desprende de las SSTS 740/12 de 10 de octubre, y 497/98, de 3 de Abril.

**-** La doctrina del Tribunal Constitucional que se desprende entre otras de la STC, Pleno, 167/2002, de 18 de septiembre, y STC 104/2006, de 3 de abril, según las cuales cabe entender que la gravedad puede referirse a otros factores no penológicos, como son:

1. El bien jurídico protegido

2. La relevancia social de los hechos;

3. La potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito. Este último criterio se basa en la posibilidad de expansión de determinados delitos por las redes de comunicaciones, y la grave dificultad de su persecución por los medios tradicionales de investigación.

Por ejemplo, en una interpretación penológica estricta quedarían impunes la mayoría de los delitos de acoso u hostigamiento del **artículo 172 ter del Código Penal**, introducido a partir del 1 de julio de 2015 por la Ley Orgánica 1/2015, de 30 de marzo, cuando fueren cometidos a través de las redes sociales, o por acoso telefónico.

Comparto con esta doctrina, no en términos de “lege data”, sino de “lege ferenda”, que en todo caso es absurda por aberrante e injusta, especialmente para la víctima, e incluso podría ser inconstitucional, una interpretación que lleve a la impunidad, y por tanto a la falta de tutela judicial efectiva, que como derecho fundamental se reconoce en el artículo 24.1 de la Constitución Española, porque el juez instructor no puede investigar determinados delitos porque están castigados con pena leve o menos grave.

Y además, en los supuestos de delitos con pena leve o menos graves, se imposibilita por el ordenamiento jurídico que la propia víctima pueda aportar el flujo de llamadas emitidas y recibidas por ella misma, aportando por ejemplo su facturación detallada del servicio telefónico, pues para obtenerla ella misma también requiere autorización judicial conforme a la Agencia Española de Protección de Datos.

La anterior cuestión ha sido tratada en diversas consultas de la Agencia Española de Protección de Datos ( en adelante AEPD), como en el Informe de la AEPD 0176/2012, en el que se señala que la comunicación al abonado de los datos de las llamadas por él recibidas, no

sólo contienen datos referidos al propio abonado sino también de los terceros con los que ha mantenido las comunicaciones, por lo que su cesión requiere autorización de esos terceros o judicial, toda vez que el **artículo 3 i) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal,** define la cesión o comunicación de datos como "t*oda revelación de datos realizada a una persona distinta del interesado*", y el **artículo 11.1 de la LO 15/1999 establece como criterio general** que:

"*Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado*".

Pero los datos podrían ser facilitados por el operador, no al abonado, pero si a las Fuerzas y Cuerpos de Seguridad, previa autorización judicial, pues esta cesión si se encontraría amparada en la existencia de una norma con rango de Ley habilitante, cual es el **artículo 22.2 de la propia Ley Orgánica 15/1999**, a tenor del cual, la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales.

## IV.- AUTO DE LA SECCIÓN CUARTA DE LA AUDIENCIA PROVINCIAL DE MADRID DE 25 DE FEBRERO DE 2015

Recientemente ha sido publicada en muchos medios jurídicos la citada resolución de la Sección 4ª de la Audiencia Provincial de Madrid, dictada en recurso de apelación, de la que fue Ponente el Ilmo. Sr. Magistrado D. José Joaquín Hervás Ortiz, que por su interés traigo a colación, pues su gran difusión puede llevar a engaño sobre el estado de la cuestión, advirtiendo desde ahora que se trata de un solo Auto, no Sentencia, y de una sola Sección de la Audiencia Provincial de Madrid, que además es contradictorio con otros Autos de otras secciones del mismo Tribunal.

Así pues, el **Auto de 8 de julio de 2011 de la sección 6ª de la misma Audiencia Provincial de Madrid** considera delito grave a estos efectos conforme a los artículos 13 y 33 del CP, a los que llevan aparejada pena de más de 5 años.

El supuesto del Auto de 25 de febrero de 2015, de la Sección cuarta de la Audiencia Provincial de Madrid, se dicta en recurso de apelación de un Auto del Juzgado de Instrucción nº 38 de Madrid, de 5 de noviembre de 2.014, en el que entendió que unos comentarios en un foro no eran constitutivos de delito de calumnia del artículo 205 del

Código Penal, ni de un delito de injuria del artículo 208 del mismo cuerpo legal, sino que, a lo sumo, podrían ser constitutivos de una falta de injurias. Y, partiendo de esa calificación, dicho Juzgado acuerda el sobreseimiento provisional de la causa por falta de autor conocido, toda vez que la identificación de dicho usuario por medio de un seudónimo impedía conocer su identidad y, además, no se podía acudir a la investigación tecnológica para averiguarla porque, a juicio del Instructor, ello venía impedido por lo dispuesto en la Ley 25/2007, de 18 de octubre de 2.007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, que sólo autorizaría tal tipo de investigación en caso de delitos graves.

Partiendo de ese planteamiento, la Sección cuarta de la Audiencia Provincial de Madrid –APM-, establece en el Auto de 25 de febrero de 2015 dictado en apelación, que la Disposición Final Primera de la Ley 25/2007 dio nueva redacción al artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en el que, bajo la rúbrica de “secreto de las comunicaciones”, se señalaba que los operadores estaban obligados a realizar las interceptaciones que se autorizasen de acuerdo con lo dispuesto en el artículo 579 de la Ley de Enjuiciamiento Criminal ; y se añadía que los sujetos obligados debían facilitar al agente facultado los datos indicados en la orden de interceptación legal, indicando que la identidad o identidades del sujeto objeto de la medida de interceptación

sería uno de esos datos a facilitar, así como la identidad o identidades de otras personas involucradas en la comunicación electrónica.

Es de notar (señala el Auto de la APM) que ese artículo 33 de la Ley 32/2003, no hacía referencia alguna a la gravedad del delito que se investiga, limitándose a remitirse a lo dispuesto en el artículo 579 de la Ley de Enjuiciamiento Criminal. Y, tras la derogación de dicha Ley por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, el contenido de ese precepto se mantiene en el artículo 39 de esta última, hoy vigente.

A la vista de este panorama normativo y de la jurisprudencia del Tribunal Constitucional acerca de la posibilidad de limitar derechos fundamentales con la finalidad de esclarecer conductas delictivas, no comparte la Sección cuarta de la Audiencia Provincial de Madrid el criterio interpretativo seguido por el Juez de Instrucción "a quo", conforme al cual los artículos 1 y 6 de la Ley 25/2007, de 18 de octubre, habrían establecido una rigurosa limitación en lo que se refiere a los delitos para cuya investigación y esclarecimiento resulta posible acudir al uso de la investigación tecnológica limitadora de la intimidad o del secreto de las comunicaciones de los usuarios de los servicios o redes de comunicaciones a que dicha Ley se refiere; limitación que se basaría exclusivamente en la gravedad de las penas que, en abstracto, llevan aparejadas dichos delitos.

Tal limitación, a la que conduce la interpretación que el Juez "a quo" realiza, y de la que discrepa el Auto de la Sección cuarta de la Audiencia Provincial de Madrid, sería la única de nuestra legislación que utiliza dicho parámetro de valoración como elemento inamovible del juicio de proporcionalidad en la limitación de derechos fundamentales. Y, en tal sentido, resalta que la propia Ley 25/2007 excluye de su ámbito el núcleo esencial del derecho al secreto de las comunicaciones, esto es, el "contenido" de las comunicaciones electrónicas, para cuya interceptación -recuerda- no se establece expresa limitación legal en función de la gravedad penológica del delito, como resulta del artículo 39 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones , y de lo dispuesto en el artículo 579 de la Ley de Enjuiciamiento Criminal.

Es cierto que la Jurisprudencia constitucional, a la hora de valorar la procedencia de adoptar medidas restrictivas del derecho fundamental al secreto de las comunicaciones, ha venido haciendo referencia a la gravedad del delito investigado como elemento integrante del juicio de proporcionalidad que ha de llevarse a cabo antes de acordar la limitación del derecho, pero nunca ha fijado como parámetro exclusivo de valoración de dicha gravedad el marco penológico abstracto o concreto del delito en cuestión, sino que ha atendido a otros criterios, tales como la importancia y relevancia social del bien jurídico protegido, la trascendencia social de los efectos que el delito genera o el hecho de que el delito a investigar sea

cometido por organizaciones criminales, añadiendo que en la ponderación de la proporcionalidad de la medida ha de tomarse en consideración otro elemento de juicio relevante, como lo es la dificultad o imposibilidad de su persecución a través de otras medidas menos gravosas para los derechos fundamentales en litigio (SSTC 54/1996, FJ 8 , y 166/1999 ; FJ 3 a).

En el mismo sentido, pueden citarse, entre otras, las Sentencias del Tribunal Constitucional de 16 de mayo de 2.000 (STC núm. 126/2000, por un delito de hurto continuado), de 11 de diciembre de 2.000 ( STC núm. 299/2000, sobre un delito contrabando), de 29 de enero de 2.001 (STC núm. 14/2001, por un delito de venta de tabaco de contrabando en bares y kioscos) y de 3 de abril de 2.006 (STC núm. 104/2006 , delito contra la propiedad industrial: página web en la que se ofrecen diversos productos informáticos, con precios inferiores a los de mercado), que consideran proporcionada la limitación del secreto de las comunicaciones para la investigación de los delitos reseñados a los que, conforme su tipificación legal, corresponde pena menos grave.

Es más, abundando en esta idea, señala el Tribunal Constitucional que la insuficiente entidad o gravedad de los hechos delictivos investigados no es, en sí misma, fundamento suficiente para tachar de desproporcionada una intervención telefónica; y ha destacado que la **proporcionalidad de la restricción de todo derecho**

**fundamental** precisa que el beneficio obtenido mediante la medida sea mayor que el coste que el sacrificio comporta, por lo que ha de realizarse una ponderación global que tome en consideración el fin perseguido, la idoneidad de la medida para alcanzarlo y que no exista otra medida menos gravosa que la adoptada y de eficacia similar, añadiendo que no cabe duda de que **la investigación de delitos constituye un fin constitucionalmente legítimo en orden a la restricción del derecho fundamental al secreto de las comunicaciones. En esta materia, el Tribunal Constitucional ha reiterado que es al legislador a quien corresponde realizar el juicio de proporcionalidad efectuando la delimitación de la naturaleza y gravedad de los hechos para cuya investigación puede acordarse la intervención de las comunicaciones telefónicas y que hasta que se produzca la necesaria regulación legislativa corresponde a dicho Tribunal suplir las insuficiencias legales, precisando los requisitos que la Constitución exige para la legitimidad de las intervenciones telefónicas** ( SSTC 49/1999 ; 184/2003, del Pleno, FJ 9 ; 26/2006 , FJ 5, cuyo criterio ha sido ratificado por el TEDH en las Decisiones de inadmisión Abdulkadir Coban contra España, de 26 septiembre 2006 , y Fernández Saavedra contra España, de 7 septiembre 2010 ).

A través de la Ley 25/2007, de 18 de octubre, el legislador sigue sin determinar, con la calidad y precisión que la seguridad jurídica exige, qué ha de entenderse, a los efectos que nos ocupan, por "delito grave", de tal manera

que en esta materia sigue incurriendo en la censurable insuficiencia que tantas veces ha sido denunciada en relación con el artículo 579 de la Ley de Enjuiciamiento Criminal. Es por ello que corresponde al aplicador del Derecho realizar tal determinación atendiendo a las pautas usuales de interpretación normativa.

Pues bien, a la vista de los criterios que ya han sido expuestos, que no son otros que la propia dicción de la ley, el resto de normas legales relativas a la eventual limitación de derechos fundamentales a los fines de la investigación penal y la jurisprudencia constitucional interpretativa de los requisitos que han de ser tomados en consideración para realizar el juicio de proporcionalidad en la afectación de los derechos fundamentales, concluye el Auto de 25 de febrero de 2015 de la Sección cuarta de la APM, que no existe base suficiente para entender, como se hace en la resolución recurrida, que la Ley 25/2007 haya fijado esa gravedad tomando como exclusivo parámetro la pena legalmente prevista para el delito que se investiga y que, en consecuencia, establezca una prohibición de utilizar la investigación tecnológica para todo delito cuya pena no supere en su previsión abstracta los cinco años de prisión -que es el límite penológico a partir del cual el delito pasa a tener la consideración de grave, de conformidad con lo dispuesto en los artículos 13 y 33 de la Ley de Enjuiciamiento Criminal.

De lo expuesto concluye la Sección cuarta de la Audiencia Provincial de Madrid en dicho Auto de 25 de febrero de 2015, que hasta que el legislador no aborde la necesaria tarea de fijar, con la exigible precisión, los requisitos y límites a los que han de sujetarse las medidas restrictivas del derecho fundamental a la intimidad y al secreto de las comunicaciones, entre ellas la investigación tecnológica a que se refiere la Ley 25/2007, los órganos judiciales tendrán que seguir operando, a la hora de adoptar sus decisiones en ese campo, con los parámetros ya fijados por el Tribunal Constitucional en cobertura de la denunciada insuficiencia legal en la regulación de tan delicada materia, en atención a lo dispuesto en el artículo 5 de la Ley Orgánica del Poder Judicial , que impone a los Jueces y Tribunales una interpretación y aplicación de las leyes según los preceptos y principios constitucionales, conforme a la interpretación de los mismos que resulte de las resoluciones dictadas por el Tribunal Constitucional en todo tipo de procesos.

**En esa interpretación y en atención a la jurisprudencia constitucional, de la que se ha hecho cita anteriormente, entiende la sección 4ª de la APM que los "delitos graves" a que se refiere la Ley 25/2007 no son exclusivamente los delitos castigados con pena superior a cinco años, sino que también han de incluirse en tal expresión aquellos otros delitos castigados con pena inferior y que, por tanto, tienen la calificación legal de "delitos menos graves", pero que**

**merezcan la consideración de graves en atención a otros parámetros, tales como la importancia del bien jurídico protegido, la trascendencia social de los efectos que el delito genera o la inexistencia de medios alternativos, menos gravosos, que permitan su investigación y esclarecimiento. En este punto no puede desconocerse que los efectos socialmente nocivos de determinados hechos delictivos pueden verse incrementados exponencialmente desde el momento en que se alcanza la convicción social de su impunidad, con el consiguiente fracaso de los fines preventivos que su tipificación penal persigue.**

Destaca por último la APM en este Auto de 25-02-2015 que una interpretación de la Ley 25/2007 como la que se propugna en la resolución cuestionada impediría la investigación tecnológica del delito de posesión, producción, venta o difusión de material pornográfico en que se hayan utilizado menores de edad, previsto en el artículo 189.1.b) del Código Penal, al estar castigado con pena menos grave, o de cualquier delito de amenazas, así como del delito de favorecimiento de la prostitución de menores de edad previsto en el artículo 187.1 del Código Penal; delitos que, frecuentemente, utilizan las redes de comunicación para su comisión.

## V.- PROYECTO DE MODIFICACIÓN DE LA LEY DE ENJUICIAMIENTO CRIMINAL

## PARA LA REGULACIÓN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

El razonamiento del anterior Auto de la Sección cuarta de la Audiencia Provincial de Madrid referente a que no se limite el calificativo de delito grave al criterio estrictamente penológico, es algo debatido en la doctrina y en la aplicación del derecho por los Tribunales.

**Como argumentos contrarios a los de dicha postura no estrictamente penológica, cabe señalar:**

**1º/** Si el legislador hubiera querido establecer la posibilidad de otro criterio distinto al ya definido en el Código Penal podía haberlo hecho en la reciente reforma de la Ley General de Telecomunicaciones, Ley 9/2014, de 9 de mayo, y no lo hizo, más bien actuó en sentido contrario, y ratificó que la cesión debía regirse por la Ley 25/2007.

**2º/** Por otra parte, la conclusión de otros parámetros para calificar como grave el delito, sin que los mismos estén determinados en la Ley, como propugna el Auto de 25-02-2015, lleva a una **inseguridad jurídica** por lo arbitrario o subjetivo de esta indefinición de gravedad del delito, como criterio de proporcionalidad para conceder la diligencia de prueba solicitada (artículo 24.2 CE), y consiguientemente autorizar la restricción a la privacidad y el derecho fundamental de secreto de las comunicaciones del investigado (artículos 18.1, 3 y 4 CE), y debería hacerse en

una interpretación contraria al principio de seguridad jurídica del artículo 9.3 CE.

Por ello, se viene produciendo casos en los que el Juzgado de Instrucción interpreta que no, y la Audiencia Provincial en apelación considera que si cabe una interpretación distinta a la definición de delito grave del CP, o simplemente autoriza la diligencia sin entrar en la polémica de la calificación del delito. Y al revés, como ocurrió en una investigación sobre la identidad del usuario de la IP dinámica respecto de un cargo bancario que constituía una estafa, el Juez de Instrucción nº 4 de Valencia la concedió, y por la cuantía condenó en Juicio de Faltas como autor a quien hizo un cargo de 2 euros, pero en apelación la **Sentencia 844/14, de 5 de diciembre, de la Audiencia Provincial de Valencia**, señaló que por la levedad de las infracciones que se investigaban, y que se alejaba del delito grave al que se refiere el reiterado art. 1.1 de la Ley 25/2007 , de 18 de octubre, **la prueba obtenida con la autorización judicial era nula**, y revocó la Sentencia del Juicio de Faltas absolviendo al denunciado y apelante, declarando que para valorar la gravedad no sólo es preciso atender a la previsión legal de una pena privativa de libertad grave, sino además debe valorarse la trascendencia social del delito que se trata de investigar.

**3º/** Por otra parte, cabe entender que el conflicto de la proporcionalidad de la medida de investigación criminal es de legalidad ordinaria.

Por tanto, si es de legalidad ordinaria, el propio Tribunal Constitucional tiene declarado que desde la perspectiva de los derechos fundamentales, no le corresponde en principio la interpretación de la legalidad ordinaria, sino fiscalizar —en defensa de los derechos fundamentales— que la interpretación de la legalidad ordinaria realizada por los Tribunales sea acorde con la Constitución" (STC 162/1992, de 26 de octubre, FJ 4).

Es decir que no le corresponde al Tribunal Constitucional resolver esta cuestión en principio, sino a los Tribunales ordinarios, y en su más alta esfera al Tribunal Supremo, sin que proceda dar relevancia constitucional a cualquier interpretación o decisión judicial que aplique una regla procesal, salvo que la misma alcance a vulnerar el contenido de algún derecho fundamental, en cuyo caso si entraría a conocer el Tribunal Constitucional vía recurso de amparo.

Así pues, si entendemos que es una cuestión de legalidad ordinaria, es muy discutible el razonamiento del Auto de 25 de febrero de 2015 de la Audiencia Provincial de Madrid de que en esta cuestión haya que operar bajo los criterios fijados por el Tribunal Constitucional, como también lo es el razonamiento de que exista una falta de cobertura legal sobre que es delito grave a los efectos de autorizar la investigación sobre las comunicaciones del investigado.

Puede parecernos desacertada la limitación dada por el legislador para tal investigación, incluso como afirmé,

calificarlo de inadmisible con el derecho a ejercer el derecho a la prueba, y que esa limitación incluso pueda vulnerar Convenios Internacionales, como el Convenio del Consejo de Europa de Budapest de 2001 sobre ciberdelincuencia, lo que podría llevar a otro tipo de recurso, como sería una cuestión de inconstitucionalidad de la Ley (artículo 161 de la CE), o a la aplicación del instrumento internacional, pero lo cierto es que el Código Penal define qué es un delito grave, y por lo tanto, mi criterio es que no cabe afirmar que no existe una falta de regulación definidora del delito grave, por lo que rige en esta materia el principio de legalidad sobre la doctrina anterior a la Ley 25/2007 del Tribunal Constitucional, como han afirmado las Audiencia Provinciales de Barcelona y de Gerona en diversas Sentencias, y no en forma de Auto.

**4º/** Y es que los fundamentos del Auto de la Sección cuarta de la APM **no son compartidos por todas las Secciones** de la Audiencia Provincial de Madrid, ni por todas Audiencias Provinciales de España.

Es contraria al criterio no penológico la Sección tercera de la Audiencia Provincial de Barcelona (SAPB de de 13 de abril de 2015, entre otras), que en su **Sentencia 363/2012 de 26 de marzo** señala que la citada doctrina del Tribunal Constitucional partía del presupuesto de que nuestro ordenamiento jurídico no tenía una regulación expresa sobre los requisitos o condiciones en las que las operadores de telefonía móvil tenían que conservar y ceder

los datos a la autoridad judicial. Pero una vez aprobada la Ley 25/2007, el principio de legalidad obliga a aplicar dicha norma con preferencia a la doctrina del Tribunal Constitucional elaborada, precisamente, en un contexto de ausencia de norma legal que regulara dicha materia, y la cesión de los datos conservados por las operadoras de telefonía móvil sólo puede producirse cuando se está investigando un delito grave contemplado en el Código Penal, o en alguna ley penal especial, y por tal sólo cabe entender, conforme a lo dispuesto en el artículo 13 del Código Penal, las infracciones que la Ley castiga con pena grave, es decir, con pena de prisión superior a cinco años (artículo 33 del CP).

En este mismo sentido se declaran las Secciones 3ª y 4ª de la Audiencia Provincial de Gerona, citando por ejemplo, el Auto de 9 de abril de 2015, dictado por la Sección 3ª, que concluye desestimando el recurso de apelación que interpuso el Ministerio Fiscal en una instrucción por robo, tras la denegación del recurso de reforma al Auto dictado en fecha 21-01-2015 dictado por el Juzgado de Instrucción nº 4 de Girona, pues en síntesis entendía, que la diligencia solicitada suponía una injerencia desproporcionada al secreto de las comunicaciones, señalando la Audiencia de Gerona que la petición de datos que otorga la Ley 25/2007 sólo procede en los casos que se investiguen delitos graves en sentido estricto.

## VI.- CONCLUSIÓN

Teniendo en cuenta los razonamientos anteriores contrarios a una interpretación no penológica sobre qué se entiende por delito grave a los efectos de la cesión de datos de la Ley 25/2007, desde la legalidad vigente y el principio de seguridad jurídica, considero que solo procede autorizar judicialmente dicha cesión teniendo en cuenta la definición de delito grave que efectúa el Código Penal vigente.

No obstante, es cierto que el razonamiento contenido en el Auto de 25-02-2015 de la APM, es el más flexible para posibilitar la tutela judicial efectiva en el ejercicio por el Ministerio Fiscal y las acusaciones del derecho a la prueba.

Y también no parece discutible que con arreglo a la redacción actual del artículo 579 de la LECR, la interpretación más flexible parece la más coherente, pues de otro modo, se daría la paradoja que para un mismo de delito, una medida más invasiva de la intimidad como es la intervención de la comunicación, podría acordarse al amparo de dicho precepto, que exige para la interceptación de las comunicaciones telefónicas del investigado que el delito sea de los que llevan aparejado pena superior a cinco años, mientras se deniega por aplicación del artículo 1 de la Ley 25/2007 otra mucho más inocua, como es que la operadora remita listado del flujo de llamadas entrantes y salientes del número de la víctima.

Pero desde el punto de vista de determinar con seguridad jurídica la estricta legalidad, que en el fondo es

determinar que han querido realmente establecer nuestros representantes parlamentarios cuando aprobaron la Ley 25/2007, es especialmente indicativo el que se encuentre en trámite parlamentario, ya en el Senado, el **Proyecto de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantía procesales y la regulación de las medidas de investigación tecnológica** (BOCG de 20 de marzo de 2015), en el que aún reconociendo su Exposición de Motivos que en la investigación de algunos hechos delictivos, la incorporación al proceso de los datos electrónicos de tráfico o asociados, puede resultar de una importancia decisiva, la reforma acoge el criterio fijado por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, **modifica el artículo 579 de la LECR, requiriendo que la autorización judicial de la cesión a los agentes facultados sólo debe otorgarse cuando hubiera indicios de obtener el descubrimiento o la comprobación de algún hecho o circunstancia relevante para la causa, siempre que la investigación fuere de un delito doloso castigado con pena con límite mínimo de tres años de prisión** (el Proyecto por error habla de "*máximo de, al menos, tres años de prisión*"), o delitos cometidos en el seno de un grupo u organización criminal, y delitos de terrorismo.

Por lo tanto, el gobierno, y nuestros representantes parlamentarios, siguen aferrados a un criterio penológico en

cuanto a la proporcionalidad de la investigación de los metadatos en las comunicaciones, salvo para los delitos de terrorismo y delincuencia organizada, y pese a los casos de impunidad que este criterio viene produciendo en la investigación criminal actual en delitos de muy diversa naturaleza (desde estafas "*on line*", a quebrantamientos de medidas judiciales de prohibición de comunicación, hostigamientos telefónicos e informáticos, injurias, amenazas, revelación de secretos, etc.), si bien **el listón de proporcionalidad que pretende el Proyecto para considerar un delito grave a los efectos de la investigación criminal tecnológica se baja a delitos castigados de forma objetiva a partir de tres años de prisión, en vez de cinco años como actualmente se desprende de la Ley 25/2007.**

Se zanjaría la polémica interpretativa, y a la vez se mejoraría la tutela judicial efectiva y la protección de las víctimas, si se enmendara el Proyecto de modificación de la Ley de Enjuiciamiento Criminal permitiendo la autorización de cesión de datos por las operadoras en la investigación de todo delito que tenga aparejada pena de más de cinco años de prisión (o tres años como recoge el Proyecto al que nos hemos referido), pero también en la investigación de cualquier otro delito cuando se aportaran indicios objetivos o evidencias de que se hubiere cometido o se estuviera cometiendo, pero cuya autoría y prueba de su comisión sólo fuera posible a través de la cesión de los datos de tráfico, que por imperativo legal vienen conservando los

proveedores de servicios de comunicaciones electrónicas de acceso público, o de redes públicas de comunicaciones.

Finalizo esta aportación amigo lector agradeciendo el tiempo que ha dedicado a su lectura, y para cualquier comentario o aportación sobre esta delicada cuestión puede remitirlo a justiciahispana@gmail.com