PRINCIPIO DE PROPORCIONALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL[1]

María Elena Laro González
Departamento de Derecho Procesal (Universidad de Sevilla)

Sumario: I. INTRODUCCIÓN. II. PRINCIPIO DE PROPORCIONALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL AL AMPARO DE LA DIRECTIVA (UE) 2016/680. III. EL PRINCIPIO DE PROPORCIONALIDAD A LA LUZ DE LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA.

I. INTRODUCCIÓN

Desde hace ya algún tiempo las políticas europeas se han centrado en la protección de datos personales y en el intercambio de dichos datos en aras a la prevención y persecución penal. En la construcción del Espacio Europeo de Libertad, Seguridad y Justicia (en adelante, ELSJ), se puso de manifiesto en el Programa de La Haya –2005-2009– la necesidad de encontrar el equilibrio entre el intercambio de información por las fuerzas de seguridad, para la lucha contra la delincuencia transfronteriza, y la necesidad de salvaguardar la vida privada y la protección de los datos[2]. Igualmente, se reafirmó en el seno del Programa plurianual para el

[1] El presente trabajo ha sido realizado en el marco del proyecto I+D+I "Instrumentos de reconocimiento mutuo y ejecución de resoluciones penales. Incorporación al Derecho español de los avances en cooperación judicial en la Unión Europea" (MINECO, ref. DER 2015-63942-P).

[2] Comunicación de la Comisión al Consejo y al Parlamento Europeo, Programa de La Haya: Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia, (COM 2005 184 final), 10 de mayo de 2005. Concretamente, se señala entre los objetivos estratégicos la prioridad de *"Lograr el equilibrio adecuado entre el derecho a la intimidad y la seguridad cuando se comparte información entre autoridades policiales y judiciales, apoyando y fomentando un diálogo constructivo entre todos los interesados con objeto de identificar unas soluciones equilibradas respetando al mismo tiempo los derechos fundamentales a la intimidad y a la protección de datos, así como el principio de disponibilidad de la información tal como se contempla en el Programa de La Haya".*

período 2010-2014 –Programa de Estocolmo–[3], donde se contemplaba como objetivo la mejora de la protección de los datos personales. En el año 2017, se efectuó una revisión intermedia de estas orientaciones. Recientemente, en la nueva Agenda Estratégica 2019-2024[4] también se ha hecho mención a la mejora en la cooperación y en el intercambio de información para intensificar la lucha contra el terrorismo y la delincuencia transfronteriza.

La base jurídica del derecho a la protección de datos de las personas físicas podemos encontrarlo plasmado en los arts. 7 y 8 de la Carta de Derechos Fundamentales de la UE (en adelante, CDFUE) y en el art. 16, apdo. 1 del Tratado de Funcionamiento de la UE (en adelante, TFUE). Sin olvidar, que en el ordenamiento jurídico español está previsión se encuentra contemplada en el art. 18 de la Constitución Española (en adelante, CE).

Finalmente, hoy en día estas prioridades se han plasmado en la Directiva (UE) 2016/680, de 27 de abril de 2016, del Parlamento Europeo y del Consejo, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y sobre la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (en adelante, Directiva 2016/680/UE)[5].

No debemos obviar, aunque no sea objeto del presente estudio, la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave[6].

Paralelamente a lo anterior, y fuera del ámbito penal, se gestó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

---

[3] Programa de Estocolmo "Una Europa abierta y segura que sirva y proteja al ciudadano", DO C 115 de 4 de mayo de 2010. Este Programa trae su origen en la comunicación que presentó la Comisión al Parlamento, titulada "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos", (COM 2009 262 final), de 10 de junio de 2009.

[4] Vid. Comunicado de prensa del Consejo Europeo, de 20 de junio de 2019.

[5] DOUE L 119/89, de 4 de mayo de 2016.

[6] DOUE L 119/132, de 4 de mayo de 2016.

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE[7] (en adelante, RGPD), el cual resultará de aplicación al tratamiento total o parcial automatizado de datos personales, así como al tratamiento de datos no automatizados contenidos o destinados a ser incluidos en un fichero –art. 2–, constituyendo la excepción a este ámbito de aplicación el tratamiento de los datos que se efectúe por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales –será de aplicación la Directiva 2016/680/UE–.

En definitiva, la tendencia responde no solo a una actuación para investigar y perseguir el delito cometido, sino que también se prevé una actuación proactiva, con carácter de *prevención* delictiva, lo cual pone de manifiesto que se está dotando de una estructura anticipadora[8]. Este tipo de investigaciones preventivas, como veremos a continuación, pueden colisionar con el principio de especialidad.

II. PRINCIPIO DE PROPORCIONALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL AL AMPARO DE LA DIRECTIVA (UE) 2016/680

Debemos partir de la premisa que para adoptar una medida de investigación con injerencia en los derechos fundamentales de investigados y/o acusados, la

[7] DOUE L 119/88, de 4 de mayo de 2016.

[8] SÁNCHEZ RUBIO, A., "El uso de los datos personales inherentes a las pruebas electrónicas obtenidas mediante la orden europea de investigación", en VVAA (Dir. GONZÁLEZ CANO, M.I.) *Orden europea de investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, Valencia, 2019, pp. 183 y ss. En este sentido, manifiesta la autora con buen criterio que *"[ ] ya no se trata, únicamente, de reaccionar frente al delito cometido, sino antes de eso impedir su comisión, anudando al sistema de justicia criminal una función de carácter anticipativo, que hasta ahora le ha sido ajena. Se trata de una modificación de gran calado, estrechamente ligada al desarrollo tecnológico, ya que la tecnología se convierte en el medio posibilitador de la evitación. En este sentido, la acumulación y tratamiento automatizado de la información obrante en bases de datos con fines preventivos y predictivos son claros ejemplos del paralelismo existente entre el surgimiento de la evitación del delito como principal finalidad del sistema de justicia criminal y la revolución tecnológica".*

misma debe estar justificada con los fines que la legitiman, estando por tanto sometida al principio de proporcionalidad[9]. Es decir, debemos valorar que el sacrificio que suponga la medida para los derechos e intereses afectados no sea superior al beneficio que reporte para el interés público y de terceros[10].

En lo concerniente a la Directiva 2016/680/UE, tenemos que hacer referencia al contenido del art. 4.1 donde se detallan los principios rectores de la obtención, cesión y tratamiento de datos personales, considerando que los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera lícita y leal;

b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;

c) adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;

d) exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;

e) conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

---

[9] LÓPEZ-BARAJAS PEREA, I., "Garantías constitucionales en la investigación tecnológica del delito: previsión legal y calidad de la ley", *Revista de derecho Político*, nº 98, enero-abril 2017, pp. 91 y ss.

[10] *Vid.* art. 588 bis a) LECRIM. Dispone el precepto 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 ya adelantamos al principio de este epígrafe, esto pone de manifiesto la necesidad que la medida de investigación que implique el tratamiento de los datos personales esté sujeta a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida[11].

Ahora bien, esta regla general establecida en el art. 4.1 de la Directiva 2016/680/UE se excepciona con lo dispuesto en el art. 4.2 de la mencionada Directiva. Esto es, que se permite el tratamiento de los datos personales para los fines del art. 1.1 –fines de prevención, investigación, detección o enjuiciamiento– distintos de aquel para el que se recogieron, siempre que el responsable del tratamiento esté autorizado, y con sujeción a los principios de necesidad y proporcionalidad. Lo que viene a posibilitar dicha cláusula es el tratamiento de los datos para el mismo fin pero en distinta causa penal. Aquí existe una diferencia con su norma predecesora antes citada –la DM 2008/977/JAI– y es que en la norma derogada se permitía el tratamiento para otros fines distintos a los vinculados con el ámbito penal, cuestión que queda zanjada en la nueva redacción de la Directiva 2016/680/UE, pues necesariamente el tratamiento de los datos tienen que ser para fines de *prevención, investigación, detección o enjuiciamiento*[12]. Por tanto, esto se configura como la excepción al principio de especialidad.

Otra cuestión que nos parece relevante es el hecho de otorgar al responsable del tratamiento[13] la facultad de realizar el control de necesidad y proporcionalidad,

---

[11] GONZÁLEZ CANO, M.I, «Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea», en VVAA (Dir. COLOMER HERNÁNDEZ, Ignacio) *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios*, Aranzadi, Cizur Menor, 2017, pp. 41 y ss; Idem. "Reflexiones sobre libre circulación de datos personales y principio de disponibilidad en el ámbito de la cooperación judicial penal en la Unión Europea" en VVAA (coord. CACHÓN CARDENAS, M. y FRANCO ARIAS, J.) *Derecho y Proceso. Liber Amicorum del Profesor Francisco Ramos Méndez*, Atelier, Barcelona, 2018, Vol. II, pp. 1073 y ss.

[12] "Garantías del investigado y acusado en orden a la obtención, cesión y tratamiento de datos personales en el proceso penal. A propósito de la Directiva (UE) 2016/680 y su impacto en materia de prueba penal" en VVAA (Dir. GONZÁLEZ CANO, M.I.) *Orden Europea de Investigación y prueba transfronteriza en la Unión Europea*, Tirant lo Blanch, Valencia, 2019, p. 138; PILLADO GONZÁLEZ, E., "Difícil equilibrio entre seguridad y salvaguarda del derecho a la protección de datos personales en la prevención, investigación y represión de delitos en la Unión Europea", en VVAA (dir. GONZÁLEZ CANO, M.I.) *Integración europea y justicia penal*, Tirant lo Blanch, Valencia, 2018, pp. 550 y ss.

[13] Entiéndase por responsable del tratamiento la definición dada por el art. 3: *"«responsable del tratamiento» o «responsable»: la autoridad competente que sola o conjuntamente con otras determine los fines y*

supuesto que si se produce en el ordenamiento jurídico español la responsabilidad de autorizar el tratamiento de dichos datos para otra causa penal recaerá por medio de autorización judicial[14].

Por su parte, debemos traer a colación lo dispuesto en la LECRIM sobre la excepción al principio de especialidad, es decir que los datos personales recabados en la investigación de un delito concreto sean cedidos a otro proceso penal. A tal efecto, se pronuncia el art. 588 bis i de la LECRIM sobre el descubrimiento casual, el cual hace una remisión al art. 579 bis. Aunque esto queda condicionado a la legitimidad de los derechos fundamentales del investigado en el primer proceso penal. Además, debería producirse un doble control, es decir, en el segundo proceso penal, al que se van a ceder los datos, debería controlarse la concurrencia de los presupuestos del art. 588 bis a) de la LECRIM[15].

Por otro lado, en conexión con el principio de proporcionalidad debemos tener en cuenta la normativa reguladora española en lo relativo a la incorporación de los datos electrónicos de tráfico o asociados –art. 588 ter j) de la LECRIM– donde se estipula expresamente que los datos conservados por prestadores de servicios o personas que faciliten la comunicación sólo podrán ser cedidos para su incorporación al proceso con *autorización judicial*[16].

El interrogante se plantea en cuanto al juicio de proporcionalidad atendiendo a la gravedad del delito. A este respecto, nos remitimos al art. 588 ter a) de la LECRIM, relativo a los presupuestos y donde se dice que *"la autorización para la interceptación*

medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión o del Estado miembro, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o del Estado miembro".

[14] Vid. art. 588 bis b) de la LECRIM.

[15] Cfr. GONZÁLEZ CANO, M.I., "Garantías del investigado y acusado", op. cit., p. 135.

[16] También debe tenerse presente el supuesto contemplado en el art. 588 ter k) de la LECRIM "identificación mediante número IP" a los efectos de la preceptiva autorización judicial. En este caso, debemos distinguir dos supuestos: el primero, que para determinar la dirección IP se precise solicitar el dato a un prestador de servicios, supuestos en que debemos ceñirnos al contenido del art. 588 ter j) de la LECRIM, por estar vinculado a un proceso de comunicación, por tanto, resulta necesaria la preceptiva autorización judicial; y el segundo, que se pueda obtener la dirección IP por los investigadores sin necesidad de recurrir a prestadores de servicios, supuesto en el que resultaría de aplicación el art. 588 ter k) de la LECRIM, por tanto, no necesitaría autorización judicial si se puede determinar la dirección IP sin acudir al prestador de servicios. Por el contrario, sí precisará de ella si es necesario la relación de la dirección IP con un equipo o dispositivo concreto y con la persona usuaria del mismo.

de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación". Es decir, los delitos a los que hace referencia la ley presentan carácter de gravedad, tales como los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; los delitos cometidos en el seno de un grupo u organización criminal; y los delitos de terrorismo. Sin embargo, el art. 588 ter j) de la LECRIM no hace mención expresa al respecto, por tanto, surge la duda si, en relación a la incorporación al proceso de los datos, sólo es posible cuando se trate de alguno de los delitos enumerados en el art. 579.1 de la LECRIM o dicho precepto es aplicable exclusivamente a la interceptación de las comunicaciones, pero no a la incorporación de los datos asociados a dicha comunicación al proceso. La duda no tiene fácil respuesta.

Sobre ello, viene a arrojar luz la Circular de la Fiscalía General del Estado (en adelante, FGE) 2/2019[17]. Al respecto, considera la FGE que del análisis de los precedentes legislativos y del proceso de gestación de la LO 13/2015 por la que se reforma en estos aspectos la LECRIM[18], parece que se inclina por la segunda postura, es decir, que la delimitación objetiva del art. 588 ter a) de la LECRIM sólo es aplicable a la interceptación de las comunicaciones en sentido estricto. Considera la FGE que no debe desconocerse que la incorporación de los datos asociados a la comunicación al proceso supone una injerencia en los derechos fundamentales de los investigados y/o acusados, por tanto, *"exigirá siempre que se justifique su necesidad para la investigación de delitos que revistan cierta gravedad. En consecuencia, deberá incluirse siempre una especial motivación de la proporcionalidad de la medida que justifique que el sacrificio de esos derechos no va a resultar superior al beneficio que para el interés público y de terceros haya de resultar de la incorporación de los datos de tráfico al procedimiento".*

En definitiva, podemos considerar que la falta de vinculación a la gravedad del delito por el art. 588 ter j) de la LECRIM, y con base en la interpretación

[17] Circular de la Fiscalía General del Estado 2/2019, de 6 de marzo de 2019, sobre interceptación de comunicaciones telefónicas y telemáticas.

[18] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (BOE núm. 239, de 6 de octubre de 2015).

referida por la Circular de la FGE, además de la jurisprudencia del TJUE, que analizaremos en las páginas siguientes, es necesario que se ajuste al control de proporcionalidad general exigido.

Además, al margen del supuesto analizado, debemos tener presente el art. 588 ter m) de la LECRIM, que regula la medida de investigación tendente a la identificación de los titulares de un número de teléfono o de cualquier otro medio de comunicación. En este supuesto, al no afectarse el derecho fundamental al secreto de las comunicaciones, la propia Policía Judicial o el Ministerio Fiscal podrá dirigirse directamente a los prestadores de servicio.

Respecto a la duda que señalábamos anteriormente, igualmente debemos cuestionarnos si en el presente supuesto hay que hacer extensivo el alcance del requisitos de la gravedad del delito. Apunta acertadamente la Circular de la FGE citada, que en relación al principio de proporcionalidad y, particularmente, analizando la STJUE de 2 de octubre de 2018[19], sobre la que volveremos a continuación, que a pesar de tratarse de una injerencia en los derechos fundamentales de los ciudadanos, *no reviste la gravedad suficiente como para limitarla a la lucha contra la delincuencia grave, estando justificada "por el objetivo de prevenir, investigar, descubrir y perseguir delitos en general"*.

III. EL PRINCIPIO DE PROPORCIONALIDAD A LA LUZ DE LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

Las previsiones de la Directiva 2016/680/UE vinieron en gran parte precedidas de una importante jurisprudencia del TJUE, la cual ha sido decisiva en este texto normativo. Especial consideración hay que hacer a tres sentencias dictadas por este tribunal: en primer lugar, la STJUE, de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, que tiene su origen en peticiones de cuestiones prejudiciales planteadas por Irlanda y Austria[20]; en segundo lugar, la STJUE, de

[19] Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 2 de octubre de 2018, asunto C-207/16.

[20] Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 8 de abril de 2014, asunto C-293/12 y C-594/12.

21 de diciembre de 2016, en los asuntos acumulados C-203/15 y C-698/15, que tiene su origen en peticiones de cuestiones prejudiciales planteadas por Suecia y Reino Unido[21]; y, por último, la STJUE, de 2 de octubre de 2018, en el asunto C-207/16, que tiene su origen en las cuestión prejudicial planteada por la AP de Tarragona.

En la STJUE de 8 de abril de 2014, la cuestión principal que resuelve versa sobre la validez de 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[22], y su compatibilidad con los derechos a la vida privada y la protección de los datos de carácter personal, así como a la libertad de expresión (arts. 7, 8, 11 CDFUE). La cuestión trataba sobre si la conservación generalizada por los proveedores de servicios de los datos personales conllevaba una colisión con los derechos fundamentales de los arts. 7 y 8 de la CDFUE.

El TJUE establece que aunque la conservación de datos que impone la Directiva 2006/24/CE constituye una injerencia en el derecho fundamental a la protección de datos de carácter personal y en el derecho a la vida privada, no permite por sí misma la revelación del contenido de las comunicaciones.

Si bien, partiendo del presupuesto que la injerencia responde a un objetivo de interés general, considera que la intromisión en los datos personales que implica esta especie de orden de conservación de datos encuentra legitimación en la valiosa información que se puede obtener de los datos conservados para la investigación, detección y enjuiciamiento –teniendo como finalidad la seguridad y la lucha contra la delincuencia organizada–.

Partiendo de estas premisas, en primer lugar el TJUE entiende que la Directiva 2006/24/CE posee un campo de aplicación extenso, sin que se establezca limitación, pues se aplica a todos los usuarios registrados o abonados, a todos los medios de comunicación electrónica y datos; igualmente, se aplica a todas

[21] Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 21 de diciembre de 2016, asunto C-203/15 y 698/15.

[22] DOUE L/105, de 13 de abril de 2006.

las personas, incluso aquellas sobre las que no exista indicio o sospecha de la comisión de un hecho delictivo grave. Con base en ello, considera el TJUE que la Directiva 2006/24/CE constituye una injerencia en los derechos fundamentales, inicialmente legitimada por los fines generales antes expuestos, pero que no respeta el principio de proporcionalidad, siendo esto motivo suficiente por el que se declaró la invalidez de la Directiva 2006/24/CE. En especial, el TJUE estableció cinco criterios esenciales sobre el principio de proporcionalidad, que son los siguientes:

- La adopción de una medida debe estar sujeta a parámetros de necesidad y proporcionalidad, exigiendo que las excepciones a la protección de los derechos fundamentales –intimidad y protección de datos personales– no sobrepasen los límites de lo *estrictamente necesario*.

- Con base en la justificación de la necesidad de adopción de estas medidas, constituye un requisito la necesidad que existan indicios contra la persona sospechosa o acusada. Como ya hemos referido, la Directiva 2006/24/CE afecta a todas las personas sin que ni siquiera se encuentren en situación que pueda dar lugar a acciones penales. Así pues, la pretensión de contribuir a la lucha contra la delincuencia grave no exige ninguna relación entre los datos conservadas y la amenaza para la seguridad pública, el tiempo de conservación de los datos, la zona geográfica determinada y el círculo de personas concretas que puedan estar implicadas en el delito grave.

- El acceso a los datos conservados por las autoridades nacionales, previo control por un órgano jurisdiccional u organismo administrativo autónomo, en aras de limitar el acceso a los datos y su utilización a lo estrictamente necesario, previa autorización motivada, por parte de las referidas autoridades, en el marco de un procedimiento de prevención, detección o enjuiciamiento de delitos. En este sentido, la Directiva 2006/24/CE no establecía ningún criterio que limitase el número de personas autorizadas para acceder y utilizar los datos.

- Conforme a las reglas relativas a la seguridad y a la protección de los datos conservados por los proveedores de servicios de comunicaciones electrónicas de acceso público, se exige una protección eficaz de los datos conservados debido a los riesgos de abuso y acceso y utilización ilícitos

de dichos datos. En particular, la Directiva 2006/24/CE no garantiza que los proveedores apliquen un nivel elevado de protección y seguridad de los datos que eviten abusos, sino que autoriza a los proveedores a realizar una valoración económica para determinar el nivel de seguridad que apliquen.

– Por último, los datos recabados y posteriormente cedidos deben ser objeto de una causa penal concreta, con sujeción al principio de especialidad.

De otro modo, otra de las sentencias relevantes dictadas por el TJUE es la de 21 de diciembre de 2016, la cual tiene por objeto la interpretación del art. 15 apdo. 1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[23] en relación con los arts. 7, 8 y 52.1 de la CDFUE.

Sobre la primera de las cuestiones prejudiciales –asunto C-203/15– la empresa Tele2 Sverige –proveedor de servicios de telecomunicaciones– comunicó a PTS –autoridad sueca de control de los servicios de correos y telecomunicaciones– que a raíz de la invalidación de la Directiva 2006/24/CE –mediante la ST Digital Rights Ireland– no seguiría conservando los datos de comunicaciones electrónicas. Como consecuencia de ello, PTS ordenó que se volviera a conservar los datos conforme al Derecho nacional sueco. Por tanto, se plantea la presente cuestión prejudicial en aras de dilucidar la compatibilidad de los dispuesto por el Derecho sueco y el Derecho de la UE.

La siguiente cuestión prejudicial –C-698/15– trae causa de los recursos presentados por los Sres. Watson, Brice y Lewis mediante los cuales solicitaban el control de legalidad del art. 1 de la DRIPA –Data Retention and Investigatory Powers Act 2014 (Ley de 2014 sobre conservación de datos y facultades de investigación)–, el cual faculta al Ministro del Interior para adoptar un régimen general que imponga a los operadores de telecomunicaciones públicas la obligación de conservar los datos relativos a las comunicaciones durante un período máximo de doce meses, excluyendo la conservación del contenido de las comunicaciones ya que podrían vulnerar la vida privada de los usuarios de dichos servicios.

[23] DOCE nº 201, de 31 de julio de 2002.

Con base a ello, se invocó la incompatibilidad con los arts. 7 y 8 de la CDFUE y el art. 8 del CEDH. Por su parte, la Court of Appeal (England & Wales) decidió suspender el procedimiento y plantear cuestión prejudicial ante el TJUE.

En definitiva, tanto el Kammarrätten i Stockholm –Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo– como la Court of Appeal (England & Wales) –Tribunal de Apelación del Reino Unido– solicitan al TJUE que se pronuncie sobre la compatibilidad de las normas nacionales, que imponen la obligación de conservación de los datos y que prevén el acceso a dichos datos por parte de las autoridades competentes, sin sujeción a límites de la gravedad del delito ni control por parte de un órgano jurisdiccional o una autoridad administrativa independiente, con el Derecho de la Unión.

El TJUE resolvió ambas cuestiones prejudiciales concluyendo que, en consonancia con los argumentos utilizados en la Sentencia de 8 de abril de 2014, considera que la normativa nacional se opone al art. 15. apdo.1 de la Directiva 2002/58/UE, en relación con los arts. 7, 8 y 52.1 CDFUE . Y ello desde dos puntos de vista: por un lado, porque se trata de una normativa estatal *"que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica";* por otro, porque esta norma nacional *"regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, y sin exigir que los datos de que se trata se conserven en el territorio de la Unión"*.

En definitiva, considera el TJUE en la referida sentencia que, dentro del respeto al principio de proporcionalidad, podrán establecerse limitaciones al ejercicio de los derechos y libertades fundamentales cuando sean *necesarias* y respondan a objetivos de interés general. Así, en materia de protección de datos, establece la jurisprudencia del TJUE que la protección del derecho fundamental al respeto de la vida privada exige que las excepciones a la protección de los datos personales y las limitaciones de la misma no exceda de lo *estrictamente necesario*. Por tanto, una conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios, así como la obligación de conservación de los mismos de

forma sistemática y continuada, permite extraer conclusiones muy concretas sobre la vida privada de las personas cuyos datos se han conservado. Por tanto, el Derecho de la Unión se opone a esta conservación generalizada e indiferenciada, y habida cuenta de la gravedad de la injerencia en los derechos fundamentales, esta medida sólo estaría justificada cuando se trate de luchar contra la delincuencia grave, siempre que tal conservación se realice de forma selectiva de los datos de tráfico y de localización, y siempre que la conservación de los datos esté limitada a lo estrictamente necesario, en relación con las categorías de datos que deban conservarse, los medios de comunicación, las personas afectadas y el período de conservación.

Por otro lado, el acceso de las autoridades nacionales a los datos conservados debe estar sujeto a un control previo del órgano jurisdiccional o autoridad administrativa independiente y que la decisión se produzca a raíz de una solicitud motivada por parte de esas autoridades, presentada en el marco de procedimientos de prevención, descubrimiento o acciones penales. Igualmente, es necesario que dichas autoridades nacionales informen de ello a las personas afectadas, siempre que no comprometan a las investigaciones que se están llevando a cabo. Por tanto, esto pone de manifiesto la necesidad de establecer los requisitos materiales y procedimentales de acceso por parte de las autoridades a los datos conservados.

Por último, mencionamos la STJUE de 2 de octubre de 2018, que tiene por objeto la interpretación del art. 15.1 de la Directiva 2002/58/CE en relación con los arts. 7 y 8 de la CDFUE. El procedimiento principal, que, posteriormente, derivó en la presente cuestión prejudicial, traía causa en una denuncia presentada ante la Policía como consecuencia de un robo con violencia, donde se sustrajo, entre otras cosas, el teléfono móvil del denunciante. Con objeto de averiguar los sujetos responsables del hecho delictivo, la Policía solicitó que se ordenara a diversos proveedores la transmisión de datos personales en aras a la identificación de los titulares de las tarjetas SIM activadas con el teléfono móvil sustraído, resultando la diligencia denegada por el juez instructor[24].

[24] El auto se deniega en virtud de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la cual limita la cesión de los datos conservados por las operadoras de telefonía móvil a los delitos graves. Posteriormente entró en vigor la LO 13/2015, que como expone el tribunal, introduce dos criterios para determinar la gravedad del delito: por un lado, el compuesto por conductas típicas de especial relevancia; y, por otro lado, que la pena prevista para el delito en cuestión supere el umbral de tres años.

En el supuesto de hecho la cuestión se circunscribe a si la gravedad del delito cometido es suficiente para habilitar la obtención de los datos personales conservados por los proveedores de servicios, con clara injerencia en los derechos fundamentales. Al respecto considera el TJUE que la injerencia en los derechos fundamentales de los individuos no reviste el carácter de gravedad, en base a que con los datos obtenidos a través de las tarjetas SIM no se puede conocer la fecha, la hora, la duración, el lugar o los destinatarios de las comunicaciones efectuadas con esas tarjetas (es decir, los datos de tráfico o asociados a la comunicación), por tanto, no permiten extraer conclusiones precisas sobre la vida privada de los afectados. Por los motivos expuestos, concluye el TJUE que la injerencia en los derechos fundamentales está justificada con fundamento en la prevención, investigación, descubrimiento y persecución delictiva.

Por otro lado, debemos tener presente la existencia de otras medidas que sí podrían calificarse como injerencias graves en los derechos fundamentales de los arts. 7 y 8 de la CDFUE, y por ende del art. 18 de la CE, como son los datos de tráfico y geolocalización o asociados. En este supuesto, el acceso se condiciona a la previa autorización judicial y que el delito revista carácter grave, como se ha puesto de manifiesto.

Por tanto, podemos extraer dos conclusiones de la jurisprudencia del TJUE: en primer lugar, conforme al principio de proporcionalidad, con fundamento en la prevención, investigación, descubrimiento y persecución delictiva, una injerencia grave en los derechos del investigado solo puede justificarse con el objetivo de luchar contra la delincuencia grave; en segundo lugar, cuando la injerencia en los derechos del investigado no es grave, dicha injerencia puede venir justificada por el objetivo de prevenir, investigar, descubrir y perseguir los delitos en general.

A este respecto debemos referirnos a lo previsto en el art. 588. ter j) de la LECRIM, desde el prisma de la configuración del principio de proporcionalidad dada por la STJUE de 2 de octubre de 2018. Con base en ello, podemos considerar que dentro del referido precepto se pueden incluir injerencias graves para la lucha contra los delitos que revistan carácter de grave y aquellas otras injerencias que no son graves y pueden acordarse respecto a cualquier delito. Debemos recordar, que el art. 588 ter j) de la LECRIM no exige la concurrencia de ningún presupuesto de gravedad del delito, lo que no significa que no deba realizarse el control de proporcionalidad de la medida por parte de la autoridad judicial –conforme al art. 588 bis de la LECRIM–.