Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680[1]

Transfer and treatment of personal data in the criminal process. Progress and immediate challenges of the Directive (EU) 2016/680

Mª Isabel González Cano[2]

Universidad de Sevilla – España

maisabel@us.es

http://orcid.org/0000-0001-7856-8980

RESUMEN: La recogida u obtención, la cesión y el tratamiento de datos personales, en cuanto vía de investigación y obtención de material incriminatorio respecto al titular de tales datos, implican medidas que afectan a un derecho fundamental, el derecho a la protección de datos de carácter personal. Siendo ello así, la intromisión legítima de las autoridades competentes a los fines de represión, investigación y enjuiciamiento penal, deberá acomodarse a los estándares garantistas y a los principios rectores de toda medida de investigación que afecte a derechos fundamentales, tanto para legitimar tal medida como para la obtención de prueba de cargo o incriminatoria lícita. Así, la recogida, obtención y tratamiento de datos personales, a través de las medidas de investigación pertinentes, se deberá regir por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de dichas medidas, a ponderar por la autoridad judicial que las autorice, con arreglo al art. 588 bis a. de la Ley de Enjuiciamiento Criminal.

[1] Este trabajo se ha elaborado en el marco de los siguientes Proyectos de investigación: Proyecto I+D+I de Excelencia DER2015-63942P (Ministerio de Economía y Competitividad), *"Instrumentos para el reconocimiento mutuo y ejecución de resoluciones penales: incorporación al Derecho español de los avances en cooperación judicial en la Unión Europea";* Generalitat Valenciana *"Claves de la justicia civil y penal en la sociedad del miedo"* –Prometeo 2018/2011-.

[2] (1.4.1965 - 20.10.2019) Era Catedrática de Derecho Procesal en la Universidad de Sevilla, España.

PALABRAS CLAVE: Cesión datos personales; proceso penal; prueba; principio de disponibilidad.

ABSTRACT: *Collection, transfer and processing of personal data, as a means of investigation and obtaining incriminating material regarding the owner of such data, involve measures that affect a fundamental right, the right to the protection of personal data. This being the case, the legitimate interference of the competent authorities for the purposes of repression, investigation and criminal prosecution, must conform to the guarantee standards and the guiding principles of any investigation measure that affects fundamental rights, both to legitimize such measure and to Obtaining evidence of legal charge or incrimination. Thus, the collection, collection and processing of personal data, through the relevant investigation measures, shall be governed by the principles of specialty, suitability, exceptionality, necessity and proportionality of said measures, to be weighed by the judicial authority authorizing them, in accordance with art. 588 bis a. of the Law of Criminal Procedure.*

KEYWORDS: *Transfer of personal data; criminal process; evidence; principle of availability.*

1. INTRODUCCIÓN. APROXIMACIÓN AL PRINCIPIO DE DISPONIBILIDAD DE LOS DATOS PERSONALES COMO INSTRUMENTO DE LA COOPERACIÓN JUDICIAL PENAL EN LA UNIÓN EUROPEA

En el desarrollo del Derecho europeo en materia de protección de datos personales, no se trata tan solo de regular el tratamiento de los datos personales desde una perspectiva general garantista, sino también desde el punto de vista de la cooperación judicial penal, y por tanto desde la perspectiva del llamado principio de disponibilidad de los datos personales, para facilitar la persecución, investigación y enjuiciamiento de fenómenos criminales transfronterizos[3].

Ciertamente, la vía general y garantista, es la primera que se desarrolla en el ámbito del Derecho Europeo, a través de la Directiva general de protección de datos personales de 1995, que conllevó la Ley española de protección de datos personales de 1999; la Directiva de 1997, sobre el tratamiento de los datos personales y la protección de la intimidad en las comunicaciones electrónicas, y la Directiva de 2002, en materia de telecomunicaciones, sobre las que volveremos más adelante.

Todas ellas son normas cuya finalidad esencial es la protección del titular de los datos personales, consagrando el control por el mismo, en orden a la necesidad de su consentimiento para la recogida, transmisión y procesamiento, y el derecho a la información, acceso, rectificación, cancelación y oposición. Sin embargo, hay otra vertiente del Derecho europeo sobre protección de datos que resulta imprescindible, la referida a la prevención, investigación y represión del delito, la vertiente especial y excepcional, que incide en la recogida de datos y su tratamiento en orden

---

[3] GONZÁLEZ CANO, *"Nuevos paradigmas de la cooperación judicial penal en la Unión Europea"*, en VVAA (ed. por BARONA VILAR), *Justicia civil y penal en la era global*, Tirant lo Blanch, Valencia, 2017, pp. 339 y ss. Sobre los orígenes de la protección de datos en Europa, v. VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos",* en VVAA (dir. por PASCUA MATEO), *Derecho de la Unión Europea y Tratado de Lisboa,* Civitas, Madrid, 2013, pp. 561 a 565; GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* en Cuadernos digitales de formación del Consejo General del Poder Judicial, Nº 29- 2012.

a la investigación y enjuiciamiento de la delincuencia, y en la que el titular de los derechos en materia de datos personales es a su vez sospechoso, investigado o encausado en un proceso penal.

Por tanto, la recogida u obtención, la cesión y el tratamiento de datos personales, en cuanto vía de investigación y obtención de material incriminatorio respecto al titular de tales datos, implican medidas que afectan a un derecho fundamental, el derecho a la protección de datos de carácter personal. Siendo ello así, la intromisión legítima de las autoridades competentes a los fines de represión, investigación y enjuiciamiento penal, deberá acomodarse a los estándares garantistas y a los principios rectores de toda medida de investigación que afecte a derechos fundamentales, tanto para legitimar tal medida como para la obtención de prueba de cargo o incriminatoria lícita.

Así pues, tales medidas pueden limitar el derecho a la protección de datos, concebido como un derecho fundamental autónomo respecto al derecho a la intimidad del art. 18.1 de la Constitución Española (en adelante, CE), en el sentido apuntado por el Tribunal Constitucional (en adelante, TC), así, en la STC 292/2000, de 30 de noviembre.

Por tanto, la recogida, obtención y tratamiento de datos personales, a través de las medidas de investigación pertinentes, deberá regirse por los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de dichas medidas, a ponderar por la autoridad judicial que las autorice, con arreglo al art. 588 bis a. de la Ley de Enjuiciamiento Criminal (en adelante, LECRIM).

Esta vertiente o perspectiva ligada a la investigación y obtención de fuentes de prueba, está conectada ineludiblemente a la cooperación policial y judicial penal en la Unión Europea (en adelante, UE), y por tanto a la lucha contra la criminalidad transfronteriza, que cuenta con importantes instrumentos y sistemas de investigación y tratamiento de datos personales, así como para el intercambio de datos sobre personas y objetos, tales como SIS (Sistema de información de Schenguen)[4], Europol,

[4] Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schenguen de segunda generación (SIS II) (DO L 205 de 7 de agosto de 2007, p. 63).

Eurojust, OLAF (Oficina europea de lucha contra el fraude), o el Sistema de información aduanero (SID)[5].

A raíz de los trágicos acontecimientos de 2001 en Nueva York, 2004 en Madrid o 2005 en Londres, se produce un punto de inflexión en la lucha contra las formas más graves de criminalidad. A partir de estos momentos, marcados por la llamada descentralización o globalización del fenómeno terrorista, comienza un intenso e imparable proceso en aras de la priorización de esa vía especial y excepcional sobre obtención, cesión y tratamiento de los datos personales, la vía represiva, representada por ejemplo por Eurojust, o por la Directiva de 2006 sobre conservación de datos en comunicaciones electrónicas, a la que nos referiremos más adelante.

La clave de este proceso se encuentra en el nuevo paradigma en la materia, que no es otro que el llamado principio de disponibilidad[6], con arreglo al cual, las autoridades competentes de los Estados de la UE tendrían acceso y podrían disponer de las informaciones en materia de investigación y enjuiciamiento penal, en las mismas condiciones con las que cuenta el Estado en el que la información está registrada[7].

---

[5] V. DREWER-GUTIERREZ ZARZA-MORÁN MARTINEZ, *"Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF"*, en VVAA (coord.. por GUTIERREZ ZARZA*), Nuevas tecnologías, protección de datos personales y proceso penal,* La Ley, Madrid, 2012, pp. 129 y ss.

[6] Sobre la evolución de este principio en la cooperación policial y judicial, como elemento clave tanto en la inicial cooperación intergubernamental, como en los más recientes procesos de intercambio de información, FIODOROVA, *"La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015, pp. 126 a 132; IDEM, "*Cesión de datos personales en posesión de Europol",* en VVAA (dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017, pp. 145 y ss.

[7] GALÁN MUÑOZ, "*La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea"*, en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales..., op. cit,* pp. 42 y ss; IDEM, *"Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales"*, en VVAA, *Cesión de datos personales y evidencias...,* op. cit., pp. 81 y ss.

El principio de disponibilidad supone, por una parte, la obligación de tener los datos disponibles y cederlos a estos fines, es decir, para la investigación y el enjuiciamiento penal (principio de finalidad); y, por otra, la posibilidad de que esta cesión de datos no venga regida con carácter general por el principio de especialidad, es decir, la posibilidad de que la autoridad del Estado cesionario los utilice para investigar o enjuiciar un delito diferente de los alegados para solicitar y justificar la cesión.

2. EL PRINCIPIO DE DISPONIBILIDAD EN LA DECISIÓN MARCO 2008/976/JAI, DE 27 DE NOVIEMBRE DE 2008

La más reciente evolución del principio de disponibilidad, su ámbito de aplicación, principios rectores y las garantías aplicables al interesado, pasa por varios hitos normativos. La circulación de datos personales a efectos de la persecución penal, ya se contempló en el Programa de Tampere, ya que las Conclusiones del Consejo Europeo de Tampere de octubre de 1999, confirmaron la necesidad de mejorar el intercambio de información entre las autoridades policiales de los países de la UE, y el Programa de La Haya de 2004 a 2009 la corroboró en noviembre de 2004. Por su parte, el Programa de La Haya de 2005 a 2010, específicamente recoge el citado principio de disponibilidad en todo el territorio de la Unión a efectos represivos, de tal manera que se hagan compatibles la protección de los derechos fundamentales y la seguridad al compartir la información (art.2.1).

Sin remontarnos a importantes instrumentos, como el Tratado de Prüm para la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, firmado el 27 de mayo de 2005[8],

[8] Estos sistemas de acceso se incorporaron en su momento a la Propuesta de la Comisión de DM del Consejo sobre intercambio de información en virtud del principio de disponibilidad (COM (2005) 490 final). Por otra parte, hay que tener presente que las primeras iniciativas en orden a la utilización de perfiles de ADN en la investigación y el enjuiciamiento criminal se remontan a la Resolución del Consejo 97/C 193/02, sobre intercambio de resultados de análisis de ADN, de la que parte la creación de bases de datos nacionales de

dos fueron los textos en los que este paradigma de la disponibilidad está más presente. Nos referimos a la Decisión 2008/615/JAI, del Consejo, de 23 de junio de 2008, sobre cooperación transfronteriza en materia de terrorismo y delincuencia organizada (llamada Decisión Prüm); y a la DM de 2006/960, obre simplificación en el intercambio e inteligencia de los Servicios de Seguridad [9].

Sin embargo, es la DM 2008/977/JAI, de 27 de noviembre de 2008, sobre protección de datos en el marco de la cooperación judicial en materia penal[10], la que consagra el paradigma de la disponibilidad en la transmisión de datos personales en causas penales, un paradigma ya contemplado como hemos visto en el Tratado de Prüm y en las Decisiones para su implementación.

A nuestro entender, la DM 2008/977 merece ser objeto de una doble valoración, la primera referente a sus logros, y la segunda a los motivos de su escaso éxito, del cual derivan las iniciativas que han conducido a la Directiva 2016/680, de la que nos ocuparemos a continuación.

En cuanto a la primera de las valoraciones propuestas, la DM de 2008 se refiere a la necesidad de establecer el marco de la protección

---

ADN para el intercambio automatizado de datos entre los Estados miembros. Igualmente, la Resoluciones del Consejo 2001/C-187/1, y 2009/C--296/1, sobre determinación de marcadores de ADN a utilizar en las analíticas y para facilitar el intercambio de resultados de las mismas.

9 Sobre los antecedentes y la estructura de la Decisión Prüm, DE HOYOS SANCHO, *"Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos"*, en VVAA (dir. por ARANGUENA FANEGO), *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010, pp. 152 y ss. Idénticas finalidades se persiguen en la más reciente Directiva 2017/541 relativa a la lucha contra el terrorismo, y que remplaza la Decisión Marco de 2002/2008 sobre la misma, VERVAELE, *"¿La asociación organizada terrorista y sus actos anticipativos: un derecho penal y política criminal sin límites?",* en VVAA (dir. por GONZALEZ CANO), *Integración europea y justicia penal,* Tirant lo Blanch, Colección Alternativas, Valencia, 2018, pp. 207 y ss. V, también, FREIXES SANJUAN, *"Protección de datos y globalización. La Convención de Prüm",* en Revista de Derecho Constitucional europeo, nº 7, enero – junio de 2007, p. 4.

10 DM 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30 de diciembre de 2008, p. 60).

de datos en el ámbito de su cesión y tratamiento a efectos penales entre Estados, y de garantizar en cualquier caso la legalidad y la licitud en el tratamiento de dichos datos a intercambiar, y la exactitud de los datos, fundamental para su uso en una causa penal.

No debemos olvidar en este punto que, como veíamos en las páginas iniciales de este trabajo, con anterioridad a la DM 2008/977, el panorama normativo sobre esta materia, y también el plano institucional, la estructura orgánica de la cooperación judicial y el propio sistema de fuentes empleado, eran complejos y enrevesados. Por una parte, los primeros desarrollos del principio de reconocimiento mutuo, desde 2002 a 2010, no se centraron tanto en la aproximación normativa como en la armonización en cuanto a instrumentos de investigación y enjuiciamiento. Y, además, existen regulaciones que afectan a estas materias en Decisiones, Convenios o Reglamentos, sin contar con la normativa de las diversas agencias y organismos europeos que de forma más o menos directa se ocupan de la protección de datos y también de su cesión y tratamiento a efectos policiales y judiciales, como es el caso de Eurojust o Europol, o los ya citados SIS, ECRIS, SIV (Sistema de información de visados), URODAC (Sistema de comparación de huellas dactilares) o el SIA (Sistema de información aduanera)[11].

Ante tan ingente cuerpo normativo, ciertamente consideramos que la DM de 2008 procuró al menos establecer una serie de principios rectores en orden al tratamiento y protección de datos en causas criminales, siempre en la confianza de que esos mínimos facilitarían la cooperación judicial y policial transfronteriza.

Y es que el principio de disponibilidad, para la cooperación judicial y policial, necesita de una regulación por varias razones. Por un lado para poner orden en la enorme relación de normas que directa o indirectamente afectan a la materia, desde las de naturaleza aduanera hasta las que regulan el decomiso, pasando por el acceso a base de datos de ADN o de datos dactiloscópicos; evitando así regulaciones contradictorias,

---

[11] Una relación de estos instrumentos, en FIODOROVA, *"La transmisión..."*, op. cit., pp. 134 y 135. Igualmente, BAYO DELGADO – GUTIERREZ ZARZA – MICHAEL ALEXANDER, *"Intercambio de información, protección de datos y cooperación judicial penal"*, en VVAA (coord. por GUTIERREZ ZARZA), *Nuevas tecnologías...*, op. cit., pp. 195 y ss.

regímenes de autoridades competentes dispares, criterios objetivos y subjetivos diferentes a la hora de implementar medidas para recabar, almacenar y transmitir datos personales, y procedimientos de solicitud y transmisión distintos y con formularios también diferentes, lo que complica y ralentiza la labor policial y judicial.

Y, por otro lado, es precisa la regulación del principio de disponibilidad ante la necesidad de homogeneizar las garantías de las personas afectadas por estos procedimientos, como una base sólida y eficaz para la cooperación transfronteriza, como veremos más adelante.

Así, la DM de 2008 prevé la necesidad de articular normas comunes sobre el tratamiento posterior de los datos cedidos, una vez concluido su uso en la causa penal o investigación penal, así como sobre el tiempo de conservación de los datos, y su transmisión posterior a particulares.

E, igualmente, prevé la necesidad de normas comunes sobre confidencialidad y seguridad en el tratamiento de los datos cedidos, así como de normas comunes que garanticen un adecuado nivel de protección. Entre otras garantías, se menciona la información al interesado sobre la obtención de los datos, recopilación, tratamiento y cesión a otro Estado a efectos de investigación o enjuiciamiento penal, y sus consiguientes excepciones en aras de la consecución de los propios fines del intercambio, es decir, la investigación o el enjuiciamiento del delito.

Pero a pesar de todo ello, la DM de 2008 tuvo escaso éxito. Y ello, a nuestro modo de ver, por tres razones.

La primera, la naturaleza y alcance del propio instrumento normativo, la DM, que no tenía efecto directo en los ordenamientos de los Estados, lo que daba lugar a grandes diferencias en la materia a la hora de la transposición a los ordenamientos internos, y por tanto a la falta de la armonización normativa buscada.

La segunda, y como en tantas ocasiones, la limitación de la DM al ámbito transfronterizo, regulando el intercambio de datos entre Estados miembros y autoridades y sistemas de información europeos, pero sin que fuera vinculante para los asuntos internos de los Estados. Por tanto, se excluyen del ámbito de aplicación de la DM la recopilación y el tratamiento de los datos nacionales o "domésticos". Ello daría lugar a la divergencia entre los estándares de garantías establecidos en la DM respecto a la transferencia transfronteriza de datos personales, y el nivel garantista del

Derecho interno para su tratamiento dentro del propio Estado. Aunque la propia DM indica que el intercambio de datos a efectos penales se facilita cuando los Estados garantizan que el nivel de protección interno es el mismo que el de la DM para temas transfronterizos, sin embargo la misma no puede impedir que los Estados establezcan garantías mayores, aunque ello en principio no debe impedir ni obstaculizar la cooperación transfronteriza. No debe obstaculizarla, pero lo hace, ya que la DM no era un instrumento de aproximación normativa sino de establecimiento de mínimos para asuntos transfronterizos.

Y, la tercera, la circunstancia de que la DM de 2008 no estableciera el principio de especialidad. Aunque el art. 3 de la DM, como veíamos anteriormente, se refiere a un tratamiento lícito, adecuado, pertinente y no excesivo de los datos personales (principios de legalidad, finalidad y proporcionalidad), y a pesar de que se afirma que los datos sólo podrán utilizarse para el fin para el que se recabaron, tanto el art. 3.2 como el art. 11 de la DM permiten el tratamiento de dichos datos para otros fines o usos compatibles, de manera que el Estado receptor podría usar dichos datos, sin el consentimiento del sujeto afectado ni del Estado cedente, para otras finalidades diferentes de las que fundamentaron la transmisión, por ejemplo para la investigación o enjuiciamiento de otro delito, la ejecución de una pena, o en caso de graves e inmediatas amenazas a la seguridad pública. E incluso, el art. 13 prevé en el mismo sentido la transferencia a un tercer Estado, aunque en este caso se requiere el consentimiento del Estado que cedió inicialmente los datos.

A nuestro entender, esta posibilidad de que el Estado cesionario utilice los datos obtenidos para otros fines y para la investigación y enjuiciamiento de otros delitos, directamente relacionados o no con aquellos para cuya investigación y enjuiciamiento se cedieron, aunque parece responder al principio de proporcionalidad y necesariedad, sin embargo desconoce el principio de especialidad, lo que conlleva un grave déficit de garantías para el sujeto sospechoso o acusado, y, además, puede dar lugar a graves reticencias por parte del Estado cedente.

Por tanto, la DM de 2008 no sólo no establecía el principio de especialidad, sino que, como vemos, permitía la utilización de los datos transmitidos para para otros fines previstos en el Derecho interno, a diferencia incluso de instrumentos posteriores, como la antes citada DM

2009/315/JAI,[12] sobre intercambio de antecedentes penales (sistema ECRIS), cuyo art. 9, que establece las condiciones de uso de los datos de carácter personal, dispone que los datos de carácter personal comunicados para su uso en un procedimiento penal (supuestos del art. 7.1 de la DM) solo podrán ser utilizados por el Estado miembro requirente en el marco del procedimiento penal para el cual se solicitaron.

Incluso los datos de carácter personal comunicados para su uso fuera de un procedimiento penal, solo podrán ser utilizados por el Estado miembro requirente, con arreglo a su Derecho nacional, para los fines para los que los haya solicitado y dentro de los límites especificados por el Estado miembro requerido (art. 9.2 de la DM 2009/315).

Además, se prevé en el art. 9.3 de esta DM, que los Estados miembros adoptarán las medidas oportunas para garantizar que, si se transmiten a un tercer país datos de carácter personal que hayan recibido de otro Estado miembro, dichos datos estén sujetos a las mismas restricciones de utilización aplicables en un Estado miembro requirente del art. 9.2. Los Estados miembros especificarán que los datos personales que se transmitan a un tercer país a efectos de un procedimiento penal, solo podrán ser utilizados ulteriormente por dicho tercer país a efectos de un procedimiento penal[13].

Ante esta situación, el Programa de Estocolmo de 2010 a 2014, siguiendo la línea de la doble vía, la general de protección, y la excepcional y especial en materia de represión del delito, prevé la necesidad, por una parte, de un nuevo Reglamento general de protección de datos personales, que sustituyese a la Directiva de 1995 y, por otra, de una nueva Directiva sobre transmisión de datos personales en la cooperación penal, que vendría igualmente a sustituir a la citada DM de 2008.

Obviamente, al tratarse de una Directiva y no ya de una DM, el efecto armonizador sería más potente. E igualmente, se trataba de

---

[12] DM 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L93 de 7 de abril de 2009).

[13] V. BLANCO QUINTANA, "*La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales*", en BMJ, 2013, p. 23

fomentar que el instrumento no se limitase a reglamentar únicamente los intercambios transfronterizos de datos, sino que a través de la aproximación normativa también fuera aplicable al tratamiento interno de datos a efectos penales, estableciéndose el mismo nivel o estándar garantista para cualquier asunto penal, interno o transnacional.

No pasaban desapercibidas algunas cuestiones esenciales en esta proyectada aproximación normativa, como la transmisión de datos a autoridades de terceros países de la UE, y por tanto el distinto nivel garantista en los mismos. O, la posibilidad de excepcionar el principio de especialidad, es decir, establecer si el dato personal cedido a otro Estado a efectos penales, podía usarse para otros fines que, aunque legítimos, fueran ajenos al proceso penal en curso.

3 LA DOCTRINA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA SOBRE LOS PRINCIPIOS DE DISPONIBILIDAD Y PROPORCIONALIDAD EN LA OBTENCIÓN Y CESIÓN DE LOS DATOS PERSONALES

Las líneas esenciales de esa nueva proyectada Directiva sobre cesión y tratamiento de datos personales en materia de cooperación judicial penal en la UE, vienen expuestas fundamentalmente en tres Sentencias del TJUE.

La primera es la STJUE de 8 de abril de 2014, que resuelve varias cuestiones prejudiciales acumuladas (asuntos C-293/12 y C-594/12), planteadas respectivamente por la Corte Suprema de Irlanda y el TC de Austria[14]. Y la segunda, la STJUE de 21 de diciembre de 2016 (asuntos acumulados C-203/15 -Tele2 Sverige AB/Post-och telestyrelsen- y C-698/15 -Secretary of State for the Home Departament/Tom Watson y otros-). Más recientemente, la STJUE de 2 de octubre de 2018 (asunto

[14] Tribunal de Justicia de la Unión Europea, Gran Sala, Sentencia de 8 de abril de 2014, C-293/2012, Repertorio mensual de jurisprudencia, nº 6, 2014, p. 5.

Una completa exposición de las cuestiones prejudiciales irlandesa y austriaca en GONZÁLEZ PASCUAL, *"El TJUE como garante de los derechos de la UE a la luz de la Sentencia Digital Right Ireland",* en Revista de Derecho Comunitario Europeo, nº 49, 2014, pp. 943 y ss.

c 207/16), que resuelve una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona.

A) En la STJUE de 8 de abril de 2014, estas cuestiones se centraban en la adecuación 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[15], a los arts. 7, 8 y 11 de la Carta de Derechos fundamentales de la UE (en adelante, CDFUE), que establecen el derecho a la vida privada y la intimidad, a la protección de los datos personales y a la libertad de expresión.

Se trataba pues de examinar si el almacenamiento generalizado de datos de telecomunicaciones y retención de datos externos de las comunicaciones de los clientes por los proveedores de servicios, en orden a su posible tratamiento y posterior utilización en investigaciones penales[16], implicaban una intromisión ilegítima en los derechos a la intimidad y a la protección de datos personales.

El TJUE parte de que la Directiva de 2006 incide y afecta, mediante su intromisión y limitación, en tales derechos. Ahora bien, también apunta que la represión del delito, y por tanto, su investigación y enjuiciamiento, es un objetivo legítimo y de interés general, que justifica la limitación de los derechos en juego y la interferencia en su disfrute, sin que ello en principio implique una vulneración de los derechos concernidos.

El TJUE estima pues que la Directiva de 2006 afectaba a los derechos a la protección de datos y a la intimidad, aunque sin

---

[15] DO L 105, de 13 de abril de 2006. La Directiva de 2006 anulada por el TJUE, modificó en su momento la Directiva 2002/58/CE de 12 de julio de 2002 sobre tratamiento de datos personales y protección a la intimidad en el sector de comunicaciones electrónicas.

[16] Se establecía un sistema de tratamiento y almacenamiento de datos provenientes de las comunicaciones electrónicas de clientes de redes de acceso público. Este tratamiento y almacenamiento se encomendaba a las empresas encargadas de la prestación de los servicios de comunicaciones electrónicas, a efectos de que si fuera necesario se utilizaran los datos en investigaciones penales de delitos graves. El almacenamiento se establecía por un plazo de entre 6 a 24 meses.

lesionar sus contenidos esenciales, ya que las medidas de retención no implicaban el acceso al contenido de las comunicaciones (aunque si a la manera de rastrear el origen y destino de una comunicación, fecha y hora de la misma, su duración, el equipo del usuario y su localización, nombre y dirección del abonado, números de teléfono de origen y destino y en su caso dirección IP), y existían medidas en la norma para preservar ante posibles abusos en el uso de los datos por parte de las empresas.

Pero estas limitaciones o injerencias en los derechos a la intimidad y a la protección de los datos personales deben responder a unos principios rectores que son los que legitiman su uso para investigar y enjuiciar el delito. Por una parte, debe tratarse de medidas adecuadas y de previa configuración legal. Y, por otra, estas limitaciones responderán en todo caso al principio de proporcionalidad, por lo que la limitación o injerencia en el derecho debe adecuarse a la finalidad que la justifica, es decir, debe ser idónea; y, además, dicha limitación debe ser necesaria en orden a los fines de la investigación y el enjuiciamiento.

El TJUE entendió que había tres filtros que debía superar la Directiva de 2006. El primero, si afectaba, vulnerándolos, a los derechos fundamentales en cuestión; el segundo, si la Directiva pretendía la consecución de un interés general legítimo, la lucha contra la delincuencia grave; y, el tercero, si la Directiva era adecuada y necesaria para conseguir ese fin legítimo. La Directiva superó los dos primeros filtros, pero no el tercero, el juicio de proporcionalidad.

En tal sentido, la Sentencia de 2014 apuntaba como la Directiva de 2006 establecía medidas adecuadas de injerencia en los derechos fundamentales apuntados, en cuanto a su previsión legal general y en cuanto a que los fines perseguidos no implicaban en sí mismos una vulneración de tales derechos. Pero, sin embargo, estas medidas no se ajustaban a los cánones de proporcionalidad por varias razones.

El sistema de captación, recopilación y almacenamiento de datos se llevaba a cabo aún sin indicio penal alguno de comisión de un delito, y sin un catálogo preestablecido de delitos para los que podía acudirse a estas medidas, no siendo suficiente, a juicio del Tribunal, la referencia de la Directiva a delitos graves, sin ninguna otra precisión, catálogo o criterio al respecto.

En definitiva, el TJUE estableció cinco criterios esenciales sobre el principio de proporcionalidad, referido a la disponibilidad a efectos penales de los datos personales.

a) En primer lugar, el principio de disponibilidad en orden a la captación y almacenamiento de datos orientadas a la investigación y el enjuiciamiento penal, debe convivir con el respeto a los derechos fundamentales (intimidad y protección de datos personales), a través del establecimiento del principio de proporcionalidad, de manera que tales medidas respondan a los parámetros de necesidad e idoneidad.

b) En segundo lugar, es necesario preestablecer legalmente los datos objetivos y subjetivos en función de los cuales pueda justificarse la necesidad de estas medidas, es decir, la existencia de indicios contra la persona sospechosa o investigada, la discriminación en función de la persona afectada, la localización geográfica que precise el uso de la medida, el tiempo necesario para conservar los datos, etc., más allá de la genérica cláusula de la lucha contra delitos graves, que no aporta en sí misma ningún nexo de unión entre los datos que se obtengan y la finalidad perseguida.

c) En tercer lugar, es precisa también la existencia de un órgano autónomo que autorice o limite el acceso a los datos, exigencia que tampoco cumplía la Directiva.

d) En cuarto lugar, debe establecerse un marco de seguridad y protección suficiente, atendiendo a la cantidad de datos, su posible carácter sensible o los riesgos de acceso ilícito o de abusos al respecto. En tal sentido, con arreglo a la Directiva, las medidas de seguridad adecuadas de los proveedores de servicios para evitar abusos dependían de la valoración de los costes económicos para su implantación, lo cual no garantizaba la misma.

e) Y, en quinto lugar, la disponibilidad debe adecuarse al principio de especialidad, de manera que los datos recabados y cedidos lo sean en función de una causa penal concreta, en cuyo curso y sustanciación se pide la cooperación.

El principio de especialidad, que exige la relación de la investigación con un delito concreto, no impide, sin embargo, el trasvase o cesión de los datos personales recabados en una causa a otro proceso penal, con arreglo

al art. 579 bis de la LECRIM. Ello queda condicionado a la constatación de la legitimidad de la injerencia en los derechos fundamentales del investigado llevada a cabo en la primera causa. Pero dicha legitimidad para el trasvase de la información, también debería hacerse depender de otra circunstancia relevante, que no es otra que la concurrencia en la segunda causa de los presupuestos del art. 588 bis a., es decir, la procedencia (necesidad, excepcionalidad, idoneidad, etc.) en el segundo procedimiento de la medida de investigación que conduce a tales datos o informaciones[17]. Si en el segundo proceso no hubiera sido posible acordar, por ejemplo, la medida de registro remoto del equipo informático, por no tratarse de ninguno de los delitos del art. 588 septies a. de la LECRIM, ¿podría incorporarse la información obtenida con esta medida en la primera causa, sin ponderar si tal medida hubiera sido posible decidirla en el segundo proceso? A nuestro entender habría que contestar negativamente a la pregunta, de manera que sería preciso valorar la legitimidad de la adopción de la medida en el proceso de origen y en el segundo proceso. E idéntica solución en orden a la doble ponderación de la legitimidad de la medida, entendemos debe aplicarse en el ámbito de la cooperación transfronteriza.

B) Por su parte, la STJUE de 21 de diciembre de 2016, viene a resolver varias cuestiones prejudiciales acumuladas. Al día siguiente del pronunciamiento de la sentencia Digital Rights Ireland de 2014, la empresa de telecomunicación Tele2 Sverige notificó a la autoridad sueca de control de los servicios de correos y telecomunicaciones su decisión de no seguir conservando los datos y su intención de suprimir los datos ya registrados (asunto C-203/15). El Derecho sueco obliga en efecto a los proveedores de servicios de comunicaciones electrónicas a conservar de modo sistemático y continuado, sin ninguna excepción, todos los datos de tráfico y de localización de todos sus abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Por su parte, en el asunto C-698/15, los Sres. Tom Watson, Peter Brice y Geoffrey Lewis

[17] Problema que apunta COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española"*, en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales*..., op. cit., p. 838.

interpusieron recursos contra la normativa británica de conservación de datos que permite al Ministro del Interior obligar a los operadores de telecomunicaciones públicas a conservar todos los datos relativos a las comunicaciones durante un período máximo de doce meses, estando excluida la conservación del contenido de esas comunicaciones.

El Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo) y la Court of Appeal, England and Wales, Civil Division (Tribunal de Apelación del Reino Unido), solicitan al TJUE que indique si las normativas nacionales que imponen a los proveedores una obligación general de conservación de datos y que prevén el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar este acceso a los casos de lucha contra la delincuencia grave y sin supeditar el acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente, son compatibles con el Derecho de la Unión (en el presente caso, la Directiva sobre la privacidad y las comunicaciones electrónicas, interpretada a la luz de la CDFUE).

La STJUE de 21 de diciembre de 2016, viene a establecer que los Estados miembros no pueden imponer una obligación general de conservación de datos de comunicaciones y geolocalización (datos de tráfico y localización), a los proveedores de servicios de comunicaciones electrónicas.

Y ello, básicamente, porque la conservación y almacenamiento de dichos datos personales, a efectos de prevención y persecución del delito, además de por razones relativas a la seguridad pública y nacional, incide en derechos fundamentales. Por ello, hay que conceptuarlo como un instrumento excepcional, que sólo puede utilizarse en casos tasados y con arreglo al principio de proporcionalidad, sin que quepan justificaciones abstractas como la referencia a delincuencia grave, que o bien se especifica en la Ley o debe ser objeto de interpretación individualizada en el caso concreto.

a) En definitiva, en virtud del principio de especialidad, el Derecho de la UE se opone a una conservación generalizada e indiferenciada de los datos de tráfico y de localización, pero los Estados miembros podrán establecer, con carácter preventivo, una conservación selectiva de esos

datos con la única finalidad de luchar contra la delincuencia grave, siempre que tal conservación se limite a lo estrictamente necesario por lo que se refiere a las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido. El acceso de las autoridades nacionales a los datos conservados debe estar sujeto a requisitos, entre los que se encuentran en particular un control previo por una autoridad independiente, así como la conservación de los datos en el territorio de la Unión.

b) Por lo que se refiere al acceso de las autoridades nacionales competentes a los datos conservados, el TJUE confirma que la normativa nacional no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en la Directiva, ni siquiera el de la lucha contra la delincuencia grave, sino que debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados.

Esta normativa debe basarse en criterios objetivos para definir las circunstancias y los requisitos conforme a los cuales debe concederse a las autoridades nacionales competentes el acceso a los datos. En principio sólo podrá concederse un acceso, en relación con el objetivo de la lucha contra la delincuencia, a los datos de personas de las que se sospeche que planean, van a cometer o han cometido un delito grave o que puedan estar implicadas de un modo u otro en un delito grave.

No obstante, en situaciones particulares, como aquellas en las que intereses vitales de la seguridad nacional, la defensa o la seguridad pública estén amenazados por actividades terroristas, podría igualmente concederse el acceso a los datos de otras personas cuando existan elementos objetivos que permitan considerar que esos datos podrían, en un caso concreto, contribuir de modo efectivo a la lucha contra tales actividades.

c) En nuestro ordenamiento, será igualmente el Juez el que autorice la incorporación o cesión a la causa de los datos electrónicos de tráfico o asociados, conservados por los prestadores de servicios en cumplimiento de las normas de conservación, o bien por iniciativa de la Policía o del Ministerio Fiscal (art. 588 octies), o por propia iniciativa comercial (art. 588 ter de la LECRIM). Los proveedores de servicios de comunicaciones no están pues obligados a una conservación general de datos de sus usuarios.

Así, el art. 588 octies de la LECRIM, constitutivo del capítulo X (medidas de aseguramiento) del Título VIII (medidas de investigación limitativas de los derechos del art. 18 de la CE, establece la llamada "orden de conservación de datos", emitida por la Policía Judicial o por el Ministerio Fiscal a fin de requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición, hasta que se obtenga la autorización judicial correspondiente para su cesión. Los datos se conservarán durante un período máximo de 90 días, prorrogable una sola vez hasta que se obtenga la autorización judicial de la cesión o se cumplan 180 días. El requerido vendrá obligado a prestar la colaboración y asistencia, y a guardar secreto sobre esta diligencia, con arreglo al art. 588 ter e. de la LECRIM.

Por su parte, el art. 588 ter j. (datos obrantes en archivos automatizados de los prestadores de servicios), dispone que los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. Igualmente, cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

C) En tercer lugar, nos referimos a la STJUE de 2 de octubre de 2018 (asunto C 207/16), que resuelve una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona, en un proceso penal incoado por el Ministerio Fiscal. En la misma, como veremos a continuación, se analiza el criterio relativo a la gravedad del delito, en orden a la legitimidad o justificación de la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la CDFUE, y si hay que atender únicamente a la pena que pueda imponerse al delito que

se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos.

Los hechos de los que trae causa el proceso en España, parten de una denuncia presentada ante la Policía por un robo con violencia, durante el cual el denunciante resultó herido y le sustrajeron la cartera y el teléfono móvil. La Policía Judicial presentó un oficio ante el juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo móvil (en adelante, código IMEI) del teléfono móvil sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos y, en su caso, dirección.

El juez instructor denegó la diligencia solicitada por dos motivos. Por un lado, consideró que esta no era idónea para identificar a los autores del delito. Por otra parte, denegó la solicitud porque la Ley 25/2007, de 28 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves, que, con arreglo a los arts. 13.1 y 33.1 del Código Penal (en adelante, CP), son, entre otros, los sancionados con una pena de prisión superior a cinco años, siendo que los hechos investigados no parecían ser constitutivos de delito grave.

El Ministerio Fiscal interpuso recurso de apelación contra dicho auto ante la Audiencia Provincial, alegando que, dada la naturaleza de los hechos y habida cuenta de una sentencia del Tribunal Supremo, de 26 de julio de 2010, relativa a un caso similar, debería haberse acordado la cesión de los datos de que se trata. Al respecto hay que tener en cuenta que tras los hechos de los que trae causa esta cuestión prejudicial, y con posterioridad a dicho auto de la AP, la LO 13/2015, de 5 de octubre, de modificación de la LECRIM, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, supuso, atendiendo a la jurisprudencia del TC y del TS, la introducción respecto de determinadas medidas de investigación, de dos nuevos

criterios alternativos para determinar el nivel de gravedad de un delito y, por tanto, establecer dicha gravedad como presupuesto para autorizar la medida. Se trata, por un lado, de un estándar material identificado por conductas típicas de particular y grave relevancia criminógena que incorporan particulares tasas de lesividad para bienes jurídicos individuales y colectivos, tales como los delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo. Por otro, la LECRIM ha introducido un criterio normativo - formal basado en la pena prevista para el delito de que se trate, de manera que hay medidas de investigación tecnológica que sólo pueden decretarse respecto a delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión (así, con arreglo a los arts. 579.1.1º y 588 ter a. de la LECRIM respecto a la interceptación de comunicaciones telefónicas y telemáticas).

Todo ello, como alega la AP, sin perjuicio de que el interés del Estado en castigar las conductas infractoras no puede justificar injerencias desproporcionadas en los derechos fundamentales consagrados en la CDFUE. Además, al plantear la cuestión prejudicial, la AP de Tarragona afirma que la STJUE de 8 de abril de 2014 -caso Digital Rights Ireland y otros- declaró la invalidez 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, reconociendo el TJUE que la conservación y cesión de datos de tráfico constituyen injerencias especialmente graves en los derechos garantizados por los arts. 7 y 8 de la CDFUE, e identificando los criterios de apreciación del respeto del principio de proporcionalidad, entre ellos la gravedad de los delitos que justifican la conservación de estos datos y el acceso a ellos para la investigación de un delito.

Las cuestiones prejudiciales planteadas, y que son el objeto de la sentencia, son dos, y giran en torno al principio de proporcionalidad en su vertiente de gravedad del delito investigado u objeto de acusación y enjuiciamiento, como elemento determinante de la legitimidad del acceso a los datos personales derivados de comunicaciones electrónicas (datos personales de tráfico y geolocalización). De esta manera se pregunta al TJUE:

a) ¿Cómo se identifica el criterio relativo a la gravedad del delito, en orden a la legitimidad o justificación de la injerencia en los derechos

fundamentales reconocidos en los arts. 7 y 8 de la CDFUE? ¿Hay que atender únicamente a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?

b) En su caso, si se ajustara a los principios constitucionales de la UE, utilizados por la STJUE de 8 de abril de 2014 (Digital Rights Ireland y otros) como estándares de control estricto de la Directiva de 2002 antes citada, y la determinación de la gravedad del delito atendiera solo a la pena imponible, ¿cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?

Con carácter inicial, el TJUE recuerda que el acceso de las autoridades públicas a estos datos personales, constituye una injerencia en el derecho fundamental al respeto de la vida privada, consagrado en el art. 7 de la CDFUE, incluso a falta de circunstancias que permitan calificar esta injerencia de «grave», y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible, o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. Tal acceso también constituye una injerencia en el derecho fundamental a la protección de los datos personales garantizado por el art. 8 de la CDFUE, puesto que constituye un tratamiento de dichos datos.

Ahora bien, por lo que respecta a los objetivos que pueden justificar una norma nacional, como la controvertida en el litigio principal, que regula el acceso de las autoridades públicas a los datos conservados por los proveedores de servicios de comunicaciones electrónicas y, por tanto, establece una excepción al principio de confidencialidad de las comunicaciones electrónicas (Ley 25/2007, de 18 de octubre), es resaltable que la enumeración de los objetivos que figuran en el art. 15.1, primera frase, de la Directiva 2002/58, tiene carácter exhaustivo, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de ellos (en este sentido, la STJUE 21 de diciembre de 2016 (Tele2 Sverige y Watson y otros, apartados 90 y 115). Siendo el objetivo la prevención, investigación, descubrimiento y persecución de delitos, procede observar que el tenor del art. 15. 1, primera frase, de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.

A este respecto, es cierto que el TJUE ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados (STJUE de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, apartados 99 y 115). El TJUE ha motivado esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso, debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión.

Es decir, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos solo puede justificar una injerencia grave, el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave». Pero cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Por tanto, el TJUE se plantea si en el presente asunto, en función de las circunstancias del caso de autos, la injerencia en los derechos fundamentales reconocidos en los arts. 7 y 8 de la CDFUE, que entraña el acceso de la Policía Judicial a los datos de que se trata en el litigio principal, debe considerarse «grave». A este respecto, el oficio por el que la Policía Judicial solicita, a efectos de la investigación de un delito, autorización judicial para acceder a los datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, tiene por único objeto identificar a los titulares de las tarjetas SIM activadas, durante un período de doce días, con el número IMEI del teléfono móvil sustraído. De este modo, esta solicitud no tiene más objeto que el acceso a los números de teléfono correspondientes a las tarjetas SIM, así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección. En cambio, esos datos no se refieren a las comunicaciones efectuadas con el teléfono móvil sustraído ni a la localización de este.

Así, los datos a que se refiere la solicitud de acceso controvertida en el litigio principal, sólo permiten vincular, durante un período

determinado de doce días, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM. Sin un cotejo con los datos relativos a las comunicaciones realizadas con esas tarjetas SIM y de localización, estos datos no permiten conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas con las tarjetas SIM en cuestión, ni los lugares en que estas comunicaciones tuvieron lugar, ni la frecuencia de estas con determinadas personas durante un período concreto. Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados.

En tales circunstancias, el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida en el litigio principal, no puede calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se ven afectados. En consecuencia, la injerencia que supone el acceso a dichos datos puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, objetivo al que se refiere el art. 15. 1, primera frase, de la Directiva 2002/58, sin que sea necesario que dichos delitos estén calificados como «graves».

Habida cuenta de las consideraciones anteriores, con arreglo al art. 15, apartado 1, de la Directiva 2002/58, a la luz de los arts. 7 y 8 de la CDFUE, el acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

En virtud de todo lo expuesto, el TJUE (Gran Sala) declara que el art. 15.1 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), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, a la luz de los arts. 7 y 8 de la CDFUE, debe interpretarse en el sentido de que el acceso de las autoridades públicas a los datos que permiten identificar a los titulares

de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares, constituye una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

Como decíamos más arriba, hay que tener presente que con posterioridad a los hechos del litigio principal, la LECRIM ha sido modificada por la LO 13/2015, de 5 de octubre, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Dicha Ley, que entró en vigor el 6 de diciembre de 2015, reforma la intervención de comunicaciones telefónicas y telemáticas, e introduce en la LECRIM la cuestión del acceso a los datos relativos a las comunicaciones telefónicas y telemáticas conservados por los proveedores de servicios de comunicaciones electrónicas, con arreglo a lo previsto 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.

Así, el art. 588 ter a., sobre interceptación de comunicaciones telefónicas y telemáticas, en su versión resultante de la LO 13/2015, dispone, por remisión al art. 579.1.1º, que esta medida puede decretarse siempre que la investigación tenga por objeto alguno de los siguientes delitos: 1.º Delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; 2.º Delitos cometidos en el seno de un grupo u organización criminal; y, 3.º Delitos de terrorismo.

Por tanto, y salvo en casos de delitos cometidos en el seno de grupo u organización criminal o en los delitos de terrorismo, sólo cabría la interceptación de comunicaciones telefónicas y telemáticas respecto a delitos con límite máximo de al menos 3 años de prisión.

Advertimos pues que estamos ante una injerencia grave en los derechos fundamentales del investigado, que requiere venir referida a la investigación de un delito "grave", en el sentido que apunta la STJUE de 2 de octubre de 2018, tal y como lo defina la legislación estatal, e independientemente, al parecer, del concepto formal de delito grave de los arts. 13.1 y 33.1 del CP. Dicha gravedad se configura, como presupuesto de la medida de investigación, atendiendo pues a dos criterios alternativos

para determinar el nivel de gravedad de un delito y, por tanto, establecer dicha gravedad como presupuesto para autorizar la injerencia grave en los derechos fundamentales. Se trata, por un lado, de un estándar material identificado por conductas típicas de particular y grave relevancia criminógena, tales como los delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo. Por otro, la LECRIM ha introducido un criterio normativo-formal basado en la pena prevista para el delito de que se trate, de manera que hay medidas de investigación tecnológica que sólo pueden decretarse respecto a delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión (así, con arreglo a los arts. 579.1.1º y 588 ter a de la LECRIM respecto a la interceptación de comunicaciones telefónicas y telemáticas). Este límite máximo de al menos tres años de prisión, actúa como presupuesto de la medida, y entendemos que prevalece respecto al establecido en el art. 1 de la Ley 25/2007, que se refiere a delito grave.

Por su parte, el art. 588 ter j) de la LECRIM establece que los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión. El precepto no exige ningún presupuesto relativo a la gravedad de la penalidad del delito investigado, lo que no implica que no deba ajustarse a la proporcionalidad general exigida en el art. 588 bis de la LECRIM en orden a la idoneidad, necesidad y excepcionalidad de la medida de investigación.

De esta manera, y con arreglo a la doctrina fijada por la STJUE de 2 de octubre de 2018, se trata de una injerencia que implica un acceso que no es grave, por lo que puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Ahora bien, la entidad y alcance de las medidas previstas en el art. 588 ter j), incluye, no sólo las que son objeto del pleito principal del caso (acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares), que constituyen una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

También se refiere el citado precepto a otras medidas que sí podrían calificarse como injerencias graves, en orden a la afección de los derechos fundamentales de los arts. 7 y 8 de la CDFUE y 18 de la CE, como los datos de tráfico y datos de localización, respecto de los que, con arreglo al art. 1 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, el acceso se condiciona a la autorización judicial previa y, además, a que se trate de la investigación de delitos graves, requisito éste último no incluido en el art. 588 ter j).

Por delincuencia grave, consideramos que deberá entenderse en este caso, delitos cometidos en el seno de organizaciones criminales o en materia de terrorismo, así como delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, de manera que prevalece la configuración de delito grave de los arts. 579.1.1º y 588 ter de la LECRIM, respecto a la del art. 1 de la Ley 25/2007. Es decir, conforme al principio de proporcionalidad, tal y como lo configura la STJUE de 2 de octubre de 2018, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, las medidas del art. 588 ter j) incluye injerencias graves para luchar contra la delincuencia que a su vez esté también calificada de «grave», e injerencias que no son graves, y que por tanto se pueden decretar respecto a todo delito.

El TJUE ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados (así, la STJUE

de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, apartados 99 y 115). El TJUE ha motivado esa interpretación basándose en que el objetivo perseguido por una norma que regula este acceso, debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación.

Es decir, conforme al principio de proporcionalidad, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia que a su vez esté también calificada de «grave».

Pero, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general. El art. 588 ter j) de la LECRIM no exige ningún presupuesto relativo a la gravedad de la penalidad del delito investigado, lo que no implica que no deba ajustarse a la proporcionalidad general exigida en el art. 588 bis de la LECRIM.

De esta manera, y con arreglo a la doctrina fijada por la STJUE de 2 de octubre de 2018, se trata de una injerencia que implica un acceso que no es grave, por lo que puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

Ahora bien, la entidad y alcance de las medidas previstas en el art. 588 ter j), incluye, no sólo las que son objeto del pleito principal del caso (acceso de las autoridades públicas a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, como los nombres, los apellidos y, en su caso, las direcciones de dichos titulares), que constituyen una injerencia en los derechos fundamentales de estos, que no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

También se refiere el citado precepto a otras medidas que sí podrían calificarse como injerencias graves, en orden a la afección de los derechos fundamentales de los arts. 7 y 8 de la CDFUE y 18 de la CE, como los datos de tráfico y datos de localización, respecto de los que, con arreglo al art. 1 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, el acceso se condiciona a la autorización judicial previa y, además, a que se trate de la investigación de delitos graves, requisito

éste último no incluido en el art. 588 ter j), sin que pueda entenderse que el apartado 1 del precepto realice una remisión general a la legislación sobre retención de datos relativos a las comunicaciones electrónicas (Ley 25/2007).

Es decir, conforme al principio de proporcionalidad, tal y como lo configura la STJUE de 2 de octubre de 2018, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, las medidas del art. 588 ter j) incluye injerencias graves para luchar contra la delincuencia que a su vez esté también calificada de «grave», e injerencias que no son graves, y que por tanto se pueden decretar respecto a todo delito.

4. LA PROTECCIÓN DE LOS INTERESADOS EN EL TRATAMIENTO DE DATOS PERSONALES, PARA LA PREVENCIÓN, INVESTIGACIÓN, DETECCIÓN O ENJUICIAMIENTO PENAL. LA DIRECTIVA (UE) 2016/680 Y ALGUNAS REFLEXIONES SOBRE SU IMPACTO EN EL PROCESO PENAL ESPAÑOL

4.1. Ámbito de aplicación y principios rectores

La Directiva UE 2016/680, de 27 de abril de 2016[18], 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, que deroga la DM

[18] Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la 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 a la libre circulación de dichos datos y por la que se deroga la DM 2008/977/JAI del Consejo (DO L 119 de 4 de mayo de 2016, p. 89).

2008/977[19] [20], responde a una serie de principios generales que parten de las líneas de actuación del Programa de Estocolmo, así como de los criterios del TJUE antes expuestos.

Entendemos que esta nueva regulación sobre el tratamiento y análisis de datos personales en causas penales, que ya trasciende del ámbito transfronterizo y parece optar por la aproximación normativa en orden a facilitar la cooperación judicial penal, trae causa de unos primeros trabajos de la Comisión Europea que datan de 2009[21] y que defienden una política más coherente e integradora del derecho fundamental a la protección de datos personales en todos los contextos. Estos trabajos

---

[19] Hay que hacer mención igualmente de la Directiva de 27 de abril de 2016 sobre utilización de datos del PNR (Registro de nombres de pasajeros), fundamentalmente en materia de terrorismo y formas graves de delincuencia, recogidas en un catálogo expreso, y encaminada a la prevención, detección, investigación y enjuiciamiento de tales delitos.

Se prevén en este sentido, cuatro formas de intercambio de este tipo de datos: entre las UIP (Unidad de Información de Pasajeros) de los Estados, directamente en casos de urgencia; entre las autoridades competente de los Estados y la UIP de un Estado requerido; a través del acceso de Europol a dichos registros con la colaboración de la UIP de los Estados; y, mediante la transferencia a terceros países.

[20] La DM de 2008 queda derogada con efecto a partir del 6 de mayo de 2018, fecha límite establecida para la transposición de la nueva Directiva 2016/680 (arts. 59 y 63).

[21] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Internet de los objetos. Un plan de acción para Europa,* de 18 de junio de 2009, COM (2009) 278 final. V. igualmente, *Programa de Estocolmo. Una Europa abierta y segura que sirva y proteja al ciudadano,* DO C 115 de 4 de mayo de 2010, p. 1; Comunicación de la Comisión *Un enfoque global de la protección de datos personales en la Unión Europea* COM (2010) 609 final. Hay que mencionar también las iniciativas sobre construcción del mercado digital único, entre cuyas acciones se menciona la necesidad de reforma normativa, con tres grandes finalidades: superar las divergencias en la implantación de la Directiva de 1995, adaptarse a los nuevos avances tecnológicos, y afrontar la dimensión globalizada del tratamiento de datos personales en el ámbito penal y policial, *European Data Protection Supervisor, Opinion on the data protection reform package,* de 7 de marzo de 2012 (cit, por VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital…",* op. cit, p. 570).

fructifican en sendas propuestas legislativas en 2012[22], aunque habría que esperar a 2016 para ver culminados los trabajos y publicados, por una parte el Reglamento (UE) 2016/679, sobre protección de datos y, por otra, la Directiva (UE) 2016/680, sobre el tratamiento de datos personales en causas penales, a la que nos venimos refiriendo en estas páginas.

Durante estos años, no debemos olvidar que el TJUE y sus líneas maestras sobre los principios de legalidad y proporcionalidad, han influenciado decididamente la redacción de la nueva Directiva de 2016, aunque sin obviar esa orientación de política criminal centrada en el principio de disponibilidad de los datos personales a efectos penales, y el afán de compatibilizar una más eficaz persecución, investigación y enjuiciamiento del delito, aprovechando eficientemente los avances tecnológicos, con el respeto de los derechos fundamentales del titular de los datos personales, a la vez sospechoso, investigado o encausado.

En tal sentido, pasamos a continuación a exponer brevemente estos principios generales.

4.2. El principio de disponibilidad y libre circulación

La libre circulación de datos personales recogidos e intervenidos por las autoridades competentes de un Estado, debe responder a fines explícitos y legítimos de la cooperación judicial penal. Como afirma COLOMER HERNÁNDEZ[23], existe una especial vinculación entre la

---

[22] Propuesta de nuevo Reglamento sobre protección de datos -COM (2012) 11 final 2012/0011/COD-, y Propuesta de Directiva sobre tratamiento de datos personales para fines de investigación y enjuiciamiento -COM (2012) 10 final 2012/0010/COD- . V. GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* op. cit.

[23] COLOMER HERNÁNDEZ, *"La inclinación de la problemática..."*, en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales...,* op. cit., p. 831. IDEM, *"La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes"*, en VVAA (dir. por JIMÉNEZ CONDE*), Adaptación del Derecho Procesal español a la normativa europea y su interpretación por los tribunales*, Tirant lo blanch, 2018, pp. 77 y ss.; RICHARD GONZÁLEZ, *"La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE"*, en VVAA, *Adaptación...,* op. cit. pp. 475 y ss.

finalidad para la que se recaba o recoge el dato personal y el uso que después se le da en el Estado requirente o cesionario, o incluso en un tercer Estado diferente del que solicitó la transmisión.

Así, se pone de manifiesto como la rapidez de la evolución tecnológica y la globalización conllevan nuevos retos respecto a la protección de los datos personales, en cuanto derecho fundamental con arreglo a los arts. 8, apartado I de la CDFUE, y 16, apartado I, del TUE. Pero, igualmente, esa masiva recogida e intercambio de datos, sin lugar a dudas supone un activo importante en la investigación y enjuiciamiento del delito.

La libre circulación de datos entre las autoridades competentes en la investigación y enjuiciamiento del delito, debe ser facilitada en el ámbito de la cooperación penal y como instrumento para la creación y fortalecimiento del espacio europeo de libertad, seguridad y justicia, aunque siempre en un marco sólido y coherente de protección y de garantías adecuadas y efectivas de los titulares de los datos personales.

Es pues evidente que la propia eficacia de la cooperación judicial penal depende de que previamente se cree y asegure en todos los Estados miembros, un nivel uniforme y equivalente de protección de los datos personales y de su tratamiento.

Si bien es cierto que el nuevo Reglamento general 2016/679[24], de protección de datos, establece las normas generales para la protección de las personas físicas en relación con el tratamiento de sus datos personales, y para garantizar la libre circulación de datos personales en la UE, también lo es que resulta imprescindible la elaboración de una serie de normas específicas sobre protección de datos y libre circulación de los mismos en el ámbito de la cooperación penal a la que se refiere el art. 16 del TUE, es decir, en orden a la investigación y enjuiciamiento de delitos por autoridades competentes (Jueces, Fiscales, Policía), y en general por todo organismo o entidad que tenga encomendado el tratamiento de estos datos a tales fines.

---

[24] Reglamento (UE) del Parlamento Europeo y del Consejo, de 27 de abril 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119, de 4 de mayo de 2016, p. 1.).

Téngase presente que la labor normativa de la UE en materia de protección de datos comenzó con la Directiva 1995/46/CE, intentando reforzar la libre circulación de datos personales en el marco del mercado único comunitario[25], dispensando para ello un marco de protección que se extendió a datos contenidos en soporte informático o en cualquier tipo de soporte o archivo adecuado o idóneo para su tratamiento. A partir de ahí, los avances tecnológicos por una parte y, por otra, la necesidad de la obtención y tratamiento de los datos personales en el ámbito de la cooperación judicial penal, han dado lugar, como afirma GALÁN MUÑOZ, a la doble vía de protección de los datos de carácter personal, es decir, la vía garantista general, en orden a preservar ante la libre circulación de datos personales, los derechos de información, acceso, rectificación, cancelación y oposición; y, la vía excepcional o especial, la relacionada con la represión, la investigación y el enjuiciamiento del delito, que requiere un tratamiento especial[26] en cuanto se trata de medios de investigación y obtención de fuentes probatorias preconstituidas y, en definitiva, de prueba de cargo en orden a la imposición de consecuencias jurídicas sancionadoras de naturaleza penal.

Aunque ciertamente los primeros pasos normativos se dieron en el ámbito general y garantista de la protección de datos personales en un mercado único con libre circulación de servicios, bienes y personas, realmente el desarrollo legislativo más importante se ha producido en el ámbito de la utilización de datos personales como material de investigación y preconstitución probatoria de cargo, tal y como hemos visto en páginas anteriores.

Se trata pues de garantizar un mismo nivel de protección en este ámbito de la cooperación judicial penal, normas armonizadas y aproximación normativa que no deben contribuir a debilitar los estándares de protección de los Estados. Muy al contrario, los Estados, partiendo de los mínimos que se establezcan, e independientemente de la nacionalidad o residencia del titular de los datos (Considerando 17 de la Directiva

---

[25] PARIENTE DE PRADA, *El Espacio de libertad, seguridad y justicia: Schenguen y protección de datos,* Aranzadi, Cizur Menor, 2013, pp. 127 y ss.

[26] Sobre la doble vía apuntada, v. igualmente, SOLAR CLAVO, *"La doble vía europea en protección de datos",* en La Ley, nº 2832, 2012.

2016/680), de que sea persona identificada o identificable, y de que se trate de tratamiento automatizado o no de los datos (neutralidad tecnológica para evitar el riesgo de elusión del estándar de protección, con arreglo al Considerando 18), podrán lógicamente disponer mayores garantías en sus ordenamientos. Igualmente, las normas procesales penales de los Estados miembros podrán contener sus propias prescripciones sobre obtención y tratamiento de datos personales en causas penales, así como sobre identificación, datos genéticos, relativos a la salud, económicos o financieros.

Por tanto, el ámbito de aplicación de la Directiva de 2016 se amplía en relación a la DM de 2008, aunque ello convive con algunas limitaciones, ya que la Directiva no se aplica al tratamiento de datos personales en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la UE, ni por parte de instituciones, órganos u organismos de la UE (art.2.3). Igualmente, la Directiva no es aplicable a actividades en materia de recogida y tratamiento de datos personales relacionadas con la seguridad nacional (Considerando 14), aunque hay que decir que la excepción relativa a los intereses de seguridad nacional, a pesar de quedar fuera de la cobertura de ese sistema coherente y uniforme de protección del sujeto, constituye o forma parte a su vez del régimen de excepciones o limitaciones del derecho de información o del derecho de acceso del interesado a los datos personales (arts. 13 y 15), sobre el que volveremos más adelante.

Sin embargo, consideramos positiva la previsión a la que se refiere el Considerando (25) de la Directiva 2016/680, que dispone la aplicabilidad de la Directiva a las transmisiones de datos desde los Estados de la UE a Interpol y a países donde la organización tiene destinados miembros. Así, la obtención, almacenamiento y distribución de datos personales para combatir la delincuencia internacional a través de intercambio de datos con Interpol, debe garantizar el respeto a los derechos y libertades fundamentales, básicamente en orden al tratamiento automatizado de los datos.

Igualmente, los principios de libre circulación y disponibilidad incluyen las transferencias de datos personales a terceros países u organizaciones internacionales. Así, el art. 35 establece los principios generales de estas transferencias de datos personales, que quedan condicionadas por cinco presupuestos.

a) Que la transferencia sea necesaria a los fines de la cesión y el tratamiento que con carácter general establece el art. 1.1, y sobre los que trataremos a continuación.

b) Que los datos personales se transfieran a un responsable del tratamiento de un tercer país u organización internacional que sea una autoridad pública competente a los fines mencionados en el art. 1.1.

c) Que, en caso de que los datos personales se transmitan o procedan de otro Estado miembro, dicho Estado miembro haya dado su autorización previa para la transferencia de conformidad con el Derecho nacional.

d) Que la Comisión haya adoptado una decisión de adecuación o de evaluación del nivel de protección en el Estado cesionario o, a falta de la misma, la transferencia se condicione a la aportación por dicho Estado de las garantías apropiadas (arts. 36 y 37). Y,

e) que se valore especialmente la proporcionalidad de la cesión en orden a todos los factores pertinentes, entre estos la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales, y el nivel de protección de los datos personales existente en el tercer país u organización internacional a los que se transfieran ulteriormente los datos personales.

¿Se ajusta nuestra jurisprudencia a las previsiones sobre el principio de disponibilidad de la Directiva de 2016? La STS de 23 de febrero de 2017 (STS 116/2017), ha avalado la condena por fraude fiscal, fundada en una prueba de cargo derivada directamente de la ilícita obtención de archivos informáticos por un particular (el Sr. Falciani), en los que se contenían datos de las cuentas bancarias del acusado.

La información sustraída por el Sr. Falciani (datos bancarios incluidos en listados del banco suizo HSBC), fue intervenida por la autoridad francesa en un registro judicial en su domicilio, previa petición de cooperación internacional por la autoridad de Suiza en la investigación de delitos contra el secreto bancario. Posteriormente estos datos (material incriminatorio inicialmente incautado para la causa penal en Suiza), fue remitida a la AEAT española mediante un DVD creado a partir de los referidos archivos informáticos aprehendidos en poder de Falciani, que contenían datos de los contribuyentes posteriormente acusados en España.

Se trata pues de dar validez como prueba de cargo a la información y datos personales obtenidos ilegitimamente por un particular en Suiza, posteriormente intervenida por un juez francés en la investigación de los delitos cometidos por dicho particular, previa petición de cooperación internacional por Suiza en la investigación de delitos contra el secreto bancario, y remitida a la autoridad española (la Agencia española de administración tributaria) que los pidió a la autoridad administrativa francesa en virtud del Convenio de 1995 para evitar la doble imposición y prevenir el fraude fiscal.

El Tribunal Supremo concluyó que la *lista Falciani* es prueba de cargo válida *por tener la convicción* de que, aunque los datos se obtuvieron de manera ilícita, la finalidad directa o indirecta no era de utilizarlos en un proceso, ni medió acuerdo o connivencia con las autoridades de ningún país.

Además de otras relevantes cuestiones dignas de ser analizadas en esta STS, tales como el alcance del principio de no indagación, la validación de la cadena de custodia, la aplicación de la regla de exclusión por la vulneración del derecho a la protección de datos en la obtención de la información, etc.[27], hay que convenir que la cesión de datos personales por parte de la autoridad francesa a la española, y su preconstitución como prueba de cargo, plantea algunas cuestiones relevantes a efectos de la persecución criminal.

a) En primer lugar, estamos ante un caso de cooperación judicial penal, para obtener de otro Estado datos personales para la investigación y el enjuiciamiento de un delito. Una cesión de datos (que el TS llega a calificar como mera denuncia ya que los datos provienen de un particular), que debe solicitarse atendiendo al principio de especialidad, en el curso de una causa abierta, y por los cauces oportunos de obtención de material

[27] La defensa del condenado había formulado recurso de casación alegando la doctrina según la cual las pruebas derivadas de una actuación ilegítima quedan contaminadas de dicha ilicitud y por tanto no son válidas como prueba de cargo para desvirtuar la presunción de inocencia del acusado. Sin embargo el TS ha entendido que puede constituir prueba de cargo válida y suficiente para fundar la condena, un elemento de convicción derivado de una actividad ilícita llevada a cabo por un particular, siempre que dicho elemento no se haya obtenido con la finalidad de utilizarlo en un proceso; y la persona que lo obtiene que no sea un agente encubierto o conectado con la policía o aparatos del Estado.

incriminatorio en un Estado distinto al del proceso (exhorto europeo o bien Orden Europa de investigación (en adelante, OEI).

El TS apunta que la utilización de estas pruebas para desvirtuar la presunción de inocencia requiere, por una parte, la convicción de que no hay intencionalidad procesal ni conexión policial alguna en la obtención de los datos, es decir que el particular no los sustrajo para sustentar una causa penal; y, por otra, que deberá ponderarse en cada caso, por un lado la gravedad de la lesión al derecho fundamental (en este caso intimidad y protección de datos) y la gravedad del delito descubierto (fraude fiscal).

Sin embargo, la desconfianza sobre los datos "traspasados", no se debe a quien los obtiene (un particular por motivos económicos o mediáticos, o la policía en el curso de una investigación), sino por la ilicitud de la obtención de los indicios y los datos, ya que la obtención y cesión no se fundamenta en los principios de disponibilidad, especialidad y proporcionalidad.

Dejamos pues planteadas nuestras dudas sobre la observancia en este caso de los contenidos mínimos del principio de especialidad, ya que la incautación de los archivos informáticos en Francia, trae causa de una petición de cooperación judicial de Suiza, país en el que se sigue la causa por los delitos contra el secreto bancario. La cesión de los datos a Suiza se realiza con un fin explícito y determinado, que no es otro que el enjuiciamiento del Sr. Falciani, y no el uso de tales datos en la causa posterior en España.

Aprovechar ese cauce de cooperación bilateral, por un delito concreto y con un imputado individualizado, para que la información acabe siendo prueba de cargo en un proceso posterior que se abre en un tercer Estado, España, supone una vulneración del principio de especialidad. La transferencia a España, y por tanto el uso de los datos para el mismo fin pero en otra causa penal por otros delitos y contra otros sujetos, está contemplada en el art. 4.2 de la Directiva 2016/680, al modo de una manifestación ampliada del principio de disponibilidad, pero siempre contando con la autorización previa de Suiza, país que inicia la primera investigación penal.

b) En segundo lugar, el principio de especialidad, que exige la relación de la investigación con un delito concreto, no impide, sin

embargo, el trasvase o cesión de los datos personales recabados en una causa a otro proceso penal, con arreglo al art. 579 bis i. de la LECRIM. Ello queda condicionado a la constatación de la legitimidad de la injerencia en los derechos fundamentales del investigado llevada a cabo en la primera causa, que en este caso es la tramitada en Suiza con la cooperación de la autoridad francesa.

Pero dicha legitimidad para el trasvase de la información, también debería hacerse depender de otra circunstancia relevante, que no es otra que la concurrencia en la segunda causa, es decir, la tramitada en España, de los presupuestos del art. 588 bis a., es decir, la procedencia (necesidad, excepcionalidad, idoneidad, etc.) en el segundo procedimiento de la medida de investigación que conduce a tales datos o informaciones[28]. Si en el segundo proceso, seguido en España, no hubiera sido posible acordar, por ejemplo, la medida de registro remoto del equipo informático para obtener los datos bancarios del acusado, por no tratarse de ninguno de los delitos del art. 588 septies a. de la LECRIM, que no incluye los delitos contra la Hacienda Pública, ¿podría incorporarse la información obtenida con esta medida en la primera causa, sin ponderar si tal medida hubiera sido posible decidirla en el segundo proceso en España? A nuestro entender habría que contestar negativamente a la pregunta, de manera que sería preciso valorar la legitimidad de la adopción de la medida en el proceso de origen y en el segundo proceso. La doble ponderación de la legitimidad de la medida, entendemos debe aplicarse igualmente en el ámbito de la cooperación transfronteriza.

4.3. El principio de proporcionalidad. Las garantías básicas de la cesión y el tratamiento de datos personales en la cooperación judicial penal

A) El at. 4.1 de la Directiva 2016/680, establece los principios relativos al tratamiento de datos personales, de manera que "*..los Estados miembros dispondrán que los datos personales sean:*

---

[28] Problema que apunta COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española",* en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales*...,, op. cit., p. 838.

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"

La Directiva 2016/680 se refiere pues a un tratamiento de datos personales exactos y actualizados, conservados adecuadamente y tratados de manera segura, en el ámbito de la investigación y enjuiciamiento penal. Un tratamiento lícito, leal y transparente, adecuado y no excesivo, y llevado a cabo únicamente en función de los fines legales preestablecidos (art. 4.1). Ello implica que la medida que conlleve el tratamiento de datos personales debe responder a los siguientes presupuestos.

a) Estar prevista en la ley, resultar necesaria, adecuada, útil, pertinente y proporcionada a los fines de la investigación o del enjuiciamiento de un concreto delito. Así, debe justificarse su pertinencia en cuanto a los fines que se persiguen, y garantizarse que los datos en cuestión no son excesivos para lo que se investiga, ni que se conservarán más tiempo del necesario para los fines que se persiguen, es decir para culminar una investigación o el enjuiciamiento de un delito concreto contra una persona determinada, investigada o encausada.

b) Ser objeto de información al sujeto, especialmente en lo relativo a sus derechos y a los cauces para su defensa, o para hacerlos valer con relación al caso concreto.

c) Y, contar con fines específicos y legítimos, a determinar en el momento de la recopilación u obtención de los datos.

En tal sentido, el art. 8 establece los presupuestos de la licitud del tratamiento de los datos, que son la necesidad en función de los fines de investigación o enjuiciamiento, y la fundamentación de su objetivo, de manera que los Estados deberán prever en sus ordenamientos al menos los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Ahora bien, si esta es la regla general, la Directiva también dispone diversos regímenes de excepciones al elenco de derechos que consagra, y que, no lo olvidemos, vienen referidos a un sospechoso, investigado o encausado en un proceso penal.

Así, el principio rector es que los datos personales se recogen con fines determinados, explícitos y legítimos (art. 4.1), y que fuera del caso concreto debe primar la confidencialidad, impidiendo accesos no autorizados a los datos. Sin embargo, ello no obsta para que estos datos puedan ser usados para otros fines, siempre que no sean incompatibles con los relativos a la investigación y el enjuiciamiento.

En este sentido, el art. 4.2 de la Directiva 2016/680, permite el tratamiento de los datos personales, para fines del art. 1.1 (investigación y enjuiciamiento) distintos de aquel para el que se recogieron, es decir para la investigación o enjuiciamiento de otros hechos delictivos atribuibles a la misma persona o a otra hasta el momento no investigada.

Es decir, un tratamiento de los datos con el mismo fin pero en distinta causa penal. Y ello será posible si el responsable del tratamiento está autorizado, y si es necesario y proporcional con ese otro fin o causa penal. Este es pues el régimen excepcional del principio de especialidad, o régimen de disponibilidad ampliada de la Directiva.

Al respecto, sólo dos apreciaciones. La primera, es relativa a la autoridad que puede utilizar, ceder o transmitir esos datos personales para la investigación o enjuiciamiento de otra causa, que no es aunque debiera serlo, el Juez o el Fiscal, sino el responsable del tratamiento. Dicho responsable deberá valorar la necesidad y proporcionalidad del trasvase de datos al otro proceso, a ese otro "fin no incompatible", así

como la legitimidad de la cesión inicial (el doble control de legitimidad al que nos referíamos en páginas previas).

La segunda, reconocer que la disponibilidad ampliada de la Directiva 2016/680 tiene un ámbito más reducido que el previsto en el art 3.2 de la DM 2008/977. La Directiva de 2008 se refería al uso para otro fin, con el único condicionante de la compatibilidad con el fin para el que se recogieron los datos, mientras el art. 4.2 de la Directiva de 2016, al menos requiere que ese fin debe ser el genérico y único, es decir, la investigación o enjuiciamiento de un delito, aunque en otra causa por hechos o contra personas diferentes. Con ello entendemos que al menos se cierra la puerta a la posibilidad del uso de datos recabados y cedidos en función de una concreta causa criminal a otras vías sancionadoras administrativas o particulares, posibilidad que la redacción del art. 3.2 de la DM de 2008 parecía permitir. En este sentido, se especifica en el Considerando (34) que el tratamiento de datos personales, recopilados para los fines penales previstos en la Directiva, para otros fines diferentes, se regirá en cualquier caso por la Reglamento general 2016/679.

En cualquier caso, la Directiva plantea la necesidad de que los ordenamientos internos cuenten con una base jurídica clara y precisa sobre los objetivos y finalidades del tratamiento de los datos personales, los procedimientos para el mantenimiento de su integridad y confidencialidad, así como los necesarios en orden a su destrucción, con las garantías suficientes en orden a evitar abusos y arbitrariedades.

El tratamiento de los datos personales, en orden a los fines de prevención, detección, investigación y enjuiciamiento, y en su caso ejecución de resoluciones penales, abarca toda operación con datos o conjuntos de datos personales, de forma automatizada o no, entre las que se encuentran la recopilación, registro, organización, estructuración, almacenamiento, adaptación o modificación, recuperación, consulta, utilización, cotejo o combinación, limitación de tratamiento, destrucción y supresión (Considerando 34).

El objeto de la cesión deben ser datos exactos, completos y actualizados, a fin de una eficaz cooperación con datos fiables, actuales, íntegros y exactos, así como de la protección del interesado. Estos principios, recogidos en el art. 4.1, d), e) y f), además se completan en el art. 5, sobre las reglas mínimas en materia de plazos de conservación de

los datos, disponiendo que los Estados miembros fijarán plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Las normas de procedimiento garantizarán el cumplimiento de dichos plazos.

En este punto, el art. 588 bis k. de la LECRIM establece las reglas aplicables sobre destrucción y conservación de registros electrónicos e informáticos utilizados en la medida de investigación. En tal sentido, se prevé el borrado y la eliminación de los registros originales y de las copias conservadas cuando transcurran cinco años desde la ejecución de la pena, su prescripción, el sobreseimiento libre o la sentencia absolutoria firme, siempre que no se estime necesaria la conservación a juicio del tribunal.

Igualmente, el art. 6,2, establece que los Estados miembros dispondrán que las autoridades competentes verifiquen la calidad de los datos, y por tanto adopten todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o que no estén actualizados no se transmitan ni se pongan a disposición de terceros. Para ello, dicha autoridad competente, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.

B) Obviamente, la transmisión y cesión de datos, a efectos de la cooperación judicial penal, tiene su repercusión fundamental en materia de prueba, en este caso transnacional.

Conviene recordar que el art. 8 de la CDFUE, dispone que el tratamiento de datos personales se realizará de modo leal, para fines concretos, sobre la base del consentimiento del sujeto o, en su caso, en virtud de otro fundamento legal y legítimo como o es la represión, investigación y enjuiciamiento del delito..

Estos principios rectores de finalidad, especialidad y proporcionalidad, ya vistos en páginas anteriores, condicionan la obtención de datos personales y su consiguiente cesión y tratamiento a efectos penales, constituyendo pues los presupuestos habilitantes de las medidas de investigación que inciden o limitan el derecho fundamental a la protección de datos personales.

Partíamos en este punto de un casi vacío normativo en la materia, ante la inaplicación práctica del instrumento que regulaba el exhorto

europeo de obtención de prueba (DM 008/978)[29]. El exhorto no era sino una manifestación del auxilio judicial a través de la transferencia a la autoridad judicial de otro Estado de elementos probatorios que ya se tienen en un causa penal[30].

El estrecho ámbito de aplicación de la DM 2008/978[31], sobre el exhorto europeo de obtención de prueba, destinado a recabar objetos, documentos y datos, pero no a llevar a cabo pruebas transfronterizas, dio lugar a que el instrumento gozase de escaso éxito. Por ello, se vino reclamando un único instrumento sobre cooperación judicial que incluyera la mayor parte de medidas de investigación transfronteriza. Las iniciativas a este respecto dieron lugar a la Directiva 2014/41/CE, del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre la OEI[32], que establece la prueba transnacional, en definitiva un auténtico sistema de equivalencia y confianza recíproca para la ejecución de la orden emitida por la autoridad judicial de un Estado, a fin de la obtención de fuentes de prueba a practicar por el Juez de otro Estado.

Evidentemente, como afirma MARTINEZ GARCÍA[33], hay una diferencia esencial entre ambos sistemas de cooperación judicial. El exhorto europeo parte de una prueba, de datos o de una fuente de prueba ya obtenidas por el Estado requerido, y cuya transferencia se pide por el Estado emisor, lo que implica poco más que la asistencia judicial en su concepción más clásica. Sin embargo, la OEI puede suponer una mayor profundización en el principio de reconocimiento mutuo, ya que se pide al Estado requerido la práctica de una medida de investigación y la

---

29 DM 2008/978/JAI, del Consejo, de 18 de diciembre de 2008, relativa al exhorto europeo de obtención de prueba (DO L 350 de 30 de diciembre de 2008).

30 GONZÁLEZ CANO, *"La propuesta de DM relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos",* en VVAA, *La prueba en el espacio de libertad, seguridad y justicia*, Cizur Menor, 2006, pp. 95 a 116.

31 Entre otros, v. AGUILERA MORALES, "*El exhorto europeo de investigación. A las búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas",* en BIMJ, nº 2145, agosto de 2012.

32 DO L 130, de 1 de mayo de 2014.

33 MARTINEZ GARCIA, *La orden europea de investigación. Actos de investigación, ilicitud de prueba y cooperación judicial transfronteriza,* Tirant Lo Blanch, Valencia, 2016, pp. 52 y 53.

obtención de una fuente de prueba a utilizar como material incriminatorio en el Estado emisor.[34]

El mandato de transposición de la Directiva 2014/41, sobre la OEI, se cumple con la modificación de la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE, operada por la Ley 3/2018, de 11 de junio, que regula la OEI.

Una inicial aproximación a las referencias sobre cesión y protección de datos personales, tanto en la Directiva 2014/41, como en la Ley 23/2018 para su transposición, nos conducen a varias reflexiones.

a) Por una parte, de esencial importancia serán las previsiones sobre la prueba transfronteriza obtenida mediante la emisión y posterior reconocimiento y ejecución de una OEI, sobre todo en lo que hace referencia a la posible denegación de ejecución por ser un medio probatorio de imposible realización en el Estado receptor, o por no venir referido a una causa concreta (principio de especialidad).

Igualmente, serán de máxima importancia las garantías para su obtención, en definitiva la licitud de la misma, en orden a su utilización en el Estado receptor como prueba de cargo suficiente para desvirtuar la presunción de inocencia.

En tal sentido, el art. 14 de la Directiva de 2014 sobre la OEI, prevé el derecho al recurso, al igual que, como veíamos, la Directiva 2016/680 se refiere a los derechos de acceso, rectificación o supresión (arts. 13 a 18).

El art. 189.3 de la Ley 23/2014, disponía respecto al exhorto europeo para obtención de pruebas penales, que la prueba obtenida mediante exhorto producía efectos plenos, sin posibilidad de recurso para controlar las garantías en su obtención. Esta previsión del art. 189.3 de la Ley 23/2014, no atendía a los parámetros de proporcionalidad y defensa que deben regir en esta materia[35] . Téngase presente, como

---

[34] Realmente el art. 1 de la Directiva 2014/41, establece un ámbito de cooperación más amplio, ya que incluye la petición de práctica de actividad probatoria, la obtención de pruebas que ya obren en poder del Estado requerido, e incluso la realización de medidas de aseguramiento de fuentes de prueba.

[35] MARTINEZ GARCÍA, *La orden europea de investigación...,* op. cit., pp. 43 y 44.

apunta BACHMAIER[36], que la norma estaba disponiendo la extensión del reconocimiento mutuo a la admisión de la prueba obtenida en otro Estado, opción del Legislador español que no venía impuesta por la DM y que podía resultar discutible, ya que para establecer una norma de reconocimiento mutuo, no sólo en cuanto a la obtención de la prueba, sino también en materia de admisión de la prueba y valoración de la misma como prueba de cargo, sería imprescindible llevar a cabo la armonización o incluso aproximación normativa necesaria, como diremos más adelante.

b) Por otra parte, y en segundo lugar, la utilización de la OEI, para la obtención de datos personales que obren en Registros de otros Estados miembros, plantea relevantes cuestiones desde el punto de vista del derecho de defensa, y en cuanto a los principios rectores de una medida tal, es decir, la proporcionalidad, la ponderación entre los efectos de la medida y la trascendencia del delito a investigar o enjuiciar, el posible catálogo de delitos en los que utilizar esta medida, así como la idoneidad y la necesidad de la misma.

El Estado emisor de una OEI debe realizar en la propia solicitud y en la resolución que la respalda, un juicio de ponderación sobre la proporcionalidad de la medida que pide, relativo a la especialidad, finalidad, necesidad e idoneidad, en definitiva al cumplimiento de los principios rectores para llevar a cabo toda medida de investigación limitativa de los derechos del art. 18 de la CE (tal y como dispone el art. 588 bis a. de la LECRIM), entre ellas las que impliquen limitación del derecho a la protección de datos.

Así, el art. 6 de la Directiva 2014/41 dispone como condición para la emisión y transmisión de la OEI, la necesidad y proporcionalidad de la misma respecto al procedimiento en el que se va a incorporar la fuente de prueba que se obtenga a partir de la medida de investigación que se solicita, y en relación a los contenidos especificados en el art. 5 (datos

---

[36] BACHAMAIER WINTER, *"El exhorto europeo de obtención de pruebas: análisis normativo"*, en VVAA (dir. y coord. por ARANGUENA FANEGO, DE HOYOS SANCHO y RODRÍGUEZ-MEDEL NIETO), *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Aranzadi, Navarra, 2015, pp. 516 a 519. Igualmente, MARTINEZ GARCIA, *La orden europea..,* op. cit., pp. 43 y 44.

de la causa, objeto y motivos de la OEI, delitos y hechos enjuiciados y concreta medida pedida).

En el mismo sentido, el art. 20 de la Directiva 2014/41 sobre la OEI, prevé expresamente la protección de los sujetos investigados en orden al tratamiento de datos de carácter personal, en cuanto derecho fundamental del art. 8 de la CDFUE y del art. 16.I del TFUE. En concreto, se dispone que los datos personales obtenidos en virtud de una OEI se procesarán y tratarán de forma leal y transparente, cuando sea necesario y proporcionado para fines compatibles con la prevención, detección, investigación y enjuiciamiento de delitos, la aplicación de sanciones penales y el ejercicio de los derechos de defensa. Igualmente, el art. 20 se remite en orden a los derechos y a la protección del investigado, a la DM 2008/977, ahora entendemos que a la Directiva 2016/680 y por tanto a los principios rectores de la misma que veíamos en páginas previas, y que condicionarán la validez de la recogida, tratamiento y transferencia a efectos probatorios penales de los datos personales.

Estas previsiones deberán aplicarse no sólo en relación con la OEI, por lo que la Ley española de transposición (Ley 3/2018), ha recogido estos principios generales en materia de protección de datos personales de investigados o encausados, no en el articulado referido a la OEI, sino en la DA 5ª de la Ley de reconocimiento mutuo, que dispone que *„los datos de carácter personales obtenidos como consecuencia de la emisión o ejecución de un instrumento de reconocimiento mutuo estarán protegidos de conformidad con lo dispuesto en la normativa europea y española de protección de datos de carácter personal"*.

Más específicamente, el art. 193 de la Ley 23/2014, sobre la utilización en España de los datos personales obtenidos en la ejecución de la orden europea de investigación en otro Estado miembro, dispone que los datos personales obtenidos de la ejecución de una orden europea de investigación sólo podrán ser empleados en los procesos en los que se hubiera acordado esa resolución, en aquellos otros relacionados de manera directa con aquél o excepcionalmente para prevenir una amenaza inmediata y grave para la seguridad pública. Se trata pues de una suerte de transposición del principio de disponibilidad ampliada recogido en la Directiva 2016/680, que tratábamos en páginas anteriores.

Además, el precepto establece que para utilizar con otros fines los datos personales obtenidos, la autoridad española competente deberá recabar el consentimiento de la autoridad del Estado de ejecución o del titular de los datos.

Ello se completa con la previsión de que cuando en un caso concreto así lo requiera la autoridad competente del Estado de ejecución, la autoridad española competente le informará del uso que haga de los datos personales que se hubieran remitido a través de una orden europea de investigación, con excepción de aquéllos obtenidos durante su ejecución en España.

En este sentido es importante resaltar que con arreglo al ordenamiento procesal penal español, las medidas de investigación que impliquen limitaciones de los derechos fundamentales del art. 18 de la CE deben contar con autorización judicial previa a instancia de la Policía Judicial o del MF (arts. 588 bis a. b. y c.). Será el Juez el que realice la ponderación sobre la adecuación de la medida a los principios rectores mencionados (art. 588 bis c.), independientemente de las facultades que en determinados casos ostenta el MF y la Policía Judicial para la obtención de datos previos para elaborar la solicitud de tales medidas (así, el acceso a datos de identificación de usuarios, terminales y dispositivos de conectividad de los arts. 588 ter l. y m.).

c) En tercer lugar, bien es cierto que se ha avanzado considerablemente en el ya citado programa de aproximación normativa en materia de garantías procesales penales de sospechosos e investigados, y fundamentalmente en materia de presunción de inocencia. Sin embargo, la reciente Directiva en esta materia 2016/343, de 9 de marzo de 2016[37], es parca y limitada, con algunas referencias muy genéricas a la carga de la prueba, al derecho al silencio, al derecho a estar presente en el juicio, al recurso, y a la presunción de inocencia. Y desde luego no llega en ningún caso a superar las diferencias entre modelos de investigación y enjuiciamiento en materia de prueba y de obtención de fuentes de prueba, sobre todo si el medio de investigación implica injerencia en los derechos fundamentales.

[37] DO L65, de 11 de marzo de 2016.

En tal sentido, dejamos apuntadas una serie de cuestiones, a nuestro entender muy relevantes, y cuyo tratamiento merece una más amplia investigación.

La primera de estas cuestiones se refiere a si la actividad probatoria objeto de la ejecución de una OEI, y la preconstitución probatoria resultado de la misma, en este caso en orden a datos personales cedidos y tratados, se va a regir por los stándares del TJUE, que deberá determinar si la Directiva 2016/680 se adecúa o no al CEDH y a la CDFUE, y siendo probable que se cuestione de nuevo la preeminencia de estos estándares independientemente de los estándares probatorios de los TC de los Estados.

Y, la segunda cuestión, directamente relacionada con la primera. En caso de prueba transfronteriza relativa a datos personales del investigado o acusado, ¿será necesaria la aproximación normativa en orden al establecimiento de la regla de exclusión como prueba de cargo válida y suficiente? ¿Se reproducirán situaciones como la del Caso *Melloni* o como la del caso *Pupino*, y por tanto la imposiblidad de denegar el reconocimiento mutuo por motivos diferentes a los que derivan de la Directiva en cuestión, como normas mínimas que vinculan a los Estados, aunque sus estándares propios de protección sean superiores? En estos casos ¿prevalecerá la regla de exclusión probatoria que determine el TJUE en materia de prueba ilícita?[38]

La obtención, cesión y tratamiento de datos personales mediante la OEI, y de acuerdo a los principios rectores de la nueva Directiva 2016/680, nos conduce ineludiblemente a reflexionar sobre estas cuestiones de la licitud y la valoración de esta prueba transnacional.

El art. 3 de la Directiva 2014/41, establece que la OEI comprende todas las medidas de investigación que pueden adoptarse en un proceso penal; de manera que la OEI tiene un carácter general y horizontal, tal y como se recoge en el Considerando (8) de la Directiva.

Evidentemente, si bien es verdad que la falta de definición de un concepto de medida de investigación, contribuye a entender que caben todas aquellas que sean necesarias en el Estado de ejecución, también

[38] MARTINEZ GARCIA, "*La orden de investigación europea: las futuras complejidades previsibles en la implementación de la Directiva en España (I)*", en La Ley, nº 106, enero – febrero de 2014.

es cierto que puede ocasionar graves problemas respecto a su valor probatorio, tema fundamental en el proceso penal.

Y es que tanto en este punto, como en materia de reglas de control de legalidad y proporcionalidad, no existe armonización normativa, estableciéndose en cambio un sistema de doble control de estas garantías, tanto en el Estado de emisión de la OEI, imprescindible para después contar con la admisibilidad probatoria, como en el Estado de ejecución, que no supervisa el control en origen, pero atendiendo a su Derecho interno sí que determina la aceptación de la OEI, o bien la sustitución por otra más idónea o menos onerosa, o la denegación (art. 206.5 de la Ley de reconocimiento mutuo).

Este sistema de doble control nos hace pensar que la OEI, más que un mandato de actividad para llevar a la practica una medida de investigación concreta, es un mandato de resultado, con lo cual puede dudarse de su naturaleza como auténtico instrumento de reconocimiento mutuo.

La admisibilidad de la prueba transfronteriza eludiendo este sistema, sólo resultaría posible consiguiendo stándares comunes de proporcionalidad, homogeneización de garantías en las medidas de investigación limitativas de derechos fundamentales, y armonización de reglas de exclusión probatoria.

Mientras ello no sea posible o viable, es imprescindible, por una parte, acudir a un sistema de doble control de admisbilidad en los Estados de emisión y ejecución y, por otra, frente al reconocimiento incondicional del exhorto europeo que se establecía en el anterior art. 189.3 de la Ley de reconocimiento mutuo, aplicar el paradigma de los nuevos arts. 186.1 y 207.1, que condiciona la validez en España de actos de investigación realizados por el Estado de ejecución, al respeto a los principios fundamentales del ordenamiento español así como a las garantías procesales.

5. BIBLIOGRAFÍA

AGUILERA MORALES, *"El exhorto europeo de investigación. A las búsqueda de la eficacia y la protección de los derechos fundamentales en las investigaciones penales transfronterizas",* en BIMJ, nº 2145, agosto de 2012.

BACHAMAIER WINTER, *"El exhorto europeo de obtención de pruebas: análisis normativo",* en VVAA (dir. y coord. por ARANGUENA FANEGO, DE HOYOS

SANCHO y RODRÍGUEZ-MEDEL NIETO), *Reconocimiento mutuo de resoluciones penales en la Unión Europea,* Aranzadi, Navarra, 2015.

BAYO DELGADO – GUTIERREZ ZARZA – MICHAEL ALEXANDER, *"Intercambio de información, protección de datos y cooperación judicial penal"*, en VVAA (coord. por GUTIERREZ ZARZA), *Nuevas tecnologías, protección de datos personales y proceso penal,* La Ley, Madrid, 2012.

BLANCO QUINTANA, *"La comunicación de antecedentes penales entre los Estados. El Sistema europeo de información de antecedentes penales"*, en BMJ, 2013.

DE HOYOS SANCHO, *"Profundización en la cooperación transfronteriza en la Unión Europea: obtención, registro e intercambio de perfiles de ADN de sospechosos"*, en VVAA (dir. por ARANGUENA FANEGO), *Espacio europeo de libertad, seguridad y justicia: últimos avances en cooperación judicial penal,* Lex Nova, Valladolid, 2010.

COLOMER HERNÁNDEZ, *"La inclinación de la problemática provocada por la transmisión y cesión de datos personales obtenidos en un proceso penal desde el marco normativo comunitaria a la regulación y praxis española",* en VVAA, (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

DREWER - GUTIERREZ ZARZA - MORÁN MARTINEZ, *"Intercambio de información y protección de datos personales en el ámbito de Eurojust, Europol y OLAF",* en VVAA (coord.. por GUTIERREZ ZARZA), *Nuevas tecnologías, protección de datos personales y proceso penal*, La Ley, Madrid, 2012.

ETXEBERRIA GURIDI, *"La protección de datos de ADN en la Unión Europea",* en VVAA (dir. por CABEZUDO BAJO*), Las bases de datos policiales de ADN ¿son una herramienta realmente eficaz en la lucha contra la criminalidad grave nacional y transfronteriza?,* Dykinson, Madrid, 2013.

FIODOROVA, *"La transmisión de información personal y datos personales en la Unión Europea para fines de investigación de delitos",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

FIODOROVA*, "Cesión de datos personales en posesión de Europol",* en VVAA (dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017.

FREIXES SANJUAN, *"Protección de datos y globalización. La Convención de Prüm",* en Revista de Derecho Constitucional europeo, nº 7, enero – junio de 2007.

GALÁN MUÑOZ, *"La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea",* en VVAA (dir. por COLOMER HERNÁNDEZ), *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Aranzadi, Pamplona, 2015.

GALÁN MUÑOZ, *"Los nuevos instrumentos de prevención y lucha contra el nuevo terrorismo: malas noticias para la intimidad y otros derechos fundamentales",* en VVAA, *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* Aranzadi, Pamplona, 2017.

GÓMEZ COLOMER, *La prueba de ADN en el proceso penal,* Tirant lo Blanch, Valencia, 2014.

GONZÁLEZ CANO, "*Nuevos paradigmas de la cooperación judicial penal en la Unión Europea",* en VVAA (ed. por BARONA VILAR), *Justicia civil y penal en la era global*, Tirant lo Blanch, Valencia, 2017.

GONZÁLEZ CANO, *"Algunas reflexiones sobre protección de datos personales, proceso penal y cooperación judicial penal en la Unión Europea",* en Cuadernos digitales de formación del Consejo General del Poder Judicial, Nº 29- 2012.

GONZÁLEZ CANO, *"Cesión y tratamiento de datos personales, principio de disponibilidad y cooperación judicial penal en la Unión Europea",* en VVAA Dir. por COLOMER HERNÁNDEZ), *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios*, Aranzadi, Pamplona, 2017.

GONZÁLEZ CANO, *"La propuesta de DM relativa al exhorto europeo de obtención de pruebas para recabar objetos, documentos y datos",* en VVAA, La prueba en el espacio de libertad, seguridad y justicia, Cizur Menor, 2006.

GONZÁLEZ CANO *"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. por GONZÁLEZ CANO), Orden europea de investigación y prueba transfronteriza en la Unión Europea, Tirant lo Blanch, Valencia, 2019.

GONZÁLEZ PASCUAL, *"El TJUE como garante de los derechos de la UE a la luz de la Sentencia Digital Right Ireland",* en Revista de Derecho Comunitario Europeo, nº 49, 2014.

MARTINEZ GARCIA, *La orden europea de investigación. Actos de investigación, ilicitud de prueba y cooperación judicial transfronteriza,* Tirant Lo Blanch, Valencia, 2016.

MARTINEZ GARCIA, "*La orden de investigación europea: las futuras complejidades previsibles en la implementación de la Directiva en España (I)*", en La Ley, nº 106, enero – febrero de 2014.

PARIENTE DE PRADA, *El Espacio de libertad, seguridad y justicia: Schenguen y protección de datos,* Aranzadi, Cizur Menor, 2013.

RICHARD GONZÁLEZ, *"La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE"*, en VVAA (dir. por JIMÉNEZ CONDE*), Adaptación del Derecho Procesal español a la normativa europea y su interpretación por los tribunales*, Tirant lo Blanch, 2018,

SOLAR CLAVO, *"La doble vía europea en protección de datos",* en La Ley, nº 2832, 2012.

VERVAELE, *"¿La asociación organizada terrorista y sus actos anticipativos: un derecho penal y política criminal sin límites?",* en VVAA (dir. por GONZALEZ CANO), *Integración europea y justicia penal,* Tirant lo Blanch, Colección Alternativas, Valencia, 2018.

VILLARINO MARZO, *"La Unión Europea ante los retos de la era digital. La reforma de la política europea de protección de datos",* en VVAA (dir. por PASCUA MATEO), *Derecho de la Unión Europea y Tratado de Lisboa,* Civitas, Madrid, 2013.

Informações adicionais e declarações dos autores (*integridade científica*)

Declaração de conflito de interesses (conflict of interest declaration): a autora confirma que não há conflitos de interesse na realização das pesquisas expostas e na redação deste artigo.

Declaração de autoria e especificação das contribuições (declaration of authorship): todas e somente as pessoas que atendem os requisitos de autoria deste artigo estão listadas como autores; todos os coautores se responsabilizam integralmente por este trabalho em sua totalidade.

Declaração de ineditismo e originalidade (declaration of originality): a autora assegura que o texto aqui publicado não foi divulgado anteriormente em outro meio e que futura republicação somente se realizará com a indicação expressa da referência desta publicação original; também atesta que não há plágio de terceiros ou autoplágio.

Dados do processo editorial
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 10/09/2019
- Retorno rodada de correções: 21/09/2019
- *Autores convidados*

http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies - custom-1

Equipe editorial envolvida

- Editor-chefe: 1 (VGV)
- Editoras-associadas: 2 (CC e BC)

COMO CITAR ESTE ARTIGO:

GONZÁLEZ CANO, Mª Isabel. Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, p. 1331-1384, set./dez. 2019. https://doi.org/10.22197/rbdpp.v5i3.279