TRIBUNAL DE JUSTICIA
DE LA UNIÓN EUROPEA

DIRECCIÓN DE INVESTIGACIÓN Y
DOCUMENTACIÓN

Ficha temática

PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

El derecho a la protección de los datos de carácter personal es un derecho fundamental cuyo respeto constituye un objetivo importante para la Unión Europea.

Está consagrado en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») que dispone, en su artículo 8, que:

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

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

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

Este derecho fundamental se halla íntimamente ligado, además, al derecho al respeto de la vida privada y familiar, consagrado en el artículo 7 de la Carta.

El derecho a la protección de los datos de carácter personal también se recoge en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), que sustituyó a este respecto al artículo 286 CE.

Por lo que se refiere al Derecho derivado, la Comunidad Europea se ha ido dotando, a partir de mediados de los años noventa, de diversos instrumentos destinados a garantizar la protección de los datos personales. La Directiva 95/46/CE, relativa a la protección de las personas físicas en

lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, [1] adoptada sobre la base del artículo 100 A CE, constituía a este respecto el principal acto jurídico de la Unión en la materia. En ella se establecían las condiciones generales para la licitud del tratamiento de los datos y los derechos de los interesados, y se disponía la creación en los Estados miembros de autoridades independientes de control.

La Directiva 2002/58/CE [2] vino a completar posteriormente la Directiva 95/46, armonizando las disposiciones de la legislación de los Estados miembros relativas a la protección del derecho a la intimidad, en particular en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas. [3] Es de señalar que el legislador de la Unión tiene intención de reexaminar esta Directiva. A este respecto, la Comisión presentó el 10 de enero de 2017 una propuesta con el fin de sustituir dicha Directiva por un reglamento relativo a la vida privada y las comunicaciones electrónicas. [4]

Además, en el campo del espacio de libertad, seguridad y justicia (antiguos artículos 30 TUE y 31 TUE), la Decisión marco 2008/977/JAI [5] regulaba (hasta el mes de mayo de 2018), la protección de los datos personales en el ámbito de la cooperación judicial en materia penal y policial.

En 2016, la Unión Europea reformó el marco jurídico global en la materia. Para ello adoptó el Reglamento (UE) 2016/679, [6] sobre la protección de datos (en lo sucesivo, «RGPD»), que deroga la Directiva 95/46 y es aplicable desde el 25 de mayo de 2018, así como la Directiva (UE) 2016/680, [7] relativa a la protección de dichos datos en materia penal, que deroga la Decisión marco 2008/977/JAI y cuyo plazo de transposición por parte de los Estados miembros expiró el 6 de mayo de 2018.

Por último, la protección de los datos personales en lo que respecta a su tratamiento por parte de las instituciones y órganos de la UE estaba inicialmente garantizada por el Reglamento (CE)

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), versión consolidada de 20 de noviembre de 2003, derogada a partir del 25 de mayo de 2018 (véase la nota 5).

2 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) (DO 2002, L 201, p. 37), versión consolidada de 19 de diciembre de 2009.

3 La Directiva 2002/58/CE fue modificada por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54). Esta Directiva fue declarada inválida por el Tribunal de Justicia en su sentencia de 8 de abril de 2014, Digital Rights Ireland y Seitlinger y otros (C-293/12 y C-594/12, EU:C:2014:238), por vulnerar gravemente los derechos al respeto de la vida privada y a la protección de los datos de carácter personal (véase la sección I.1 de la presente ficha, titulada «Conformidad del Derecho derivado de la Unión con el derecho a la protección de los datos de carácter personal»).

4 Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM/2017/010 final — 2017/03 (COD).

5 Decisión Marco 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 2008, L 350, p. 60), derogada a partir del 6 de mayo de 2018 (véase la nota 6).

6 Reglamento (UE) 2016/679 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 datos y por el que se deroga la Directiva 95/46/CE (DO 2016, L 119, p. 1).

7 Directiva (UE) 2016/680 del Parlamento Europeo y de 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 Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

n.º 45/2001. [8] Este Reglamento posibilitó la creación, en 2004, del Supervisor Europeo de Protección de Datos. En 2018, la Unión Europea se dotó de un nuevo marco jurídico en la materia, en particular mediante la adopción del Reglamento (UE) 2018/1725, [9] por el que se derogan el Reglamento n.º 45/2001 y la Decisión n.º 1247/2002/CE [10] y que es aplicable desde el 11 de diciembre de 2018. En aras de un enfoque coherente de la protección de los datos personales en el conjunto de la Unión, este nuevo Reglamento tiene por objeto armonizar en la medida de lo posible la normativa en la materia con el régimen establecido por el RGPD.

8 Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO 2001, L 8, p. 1).

9 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

10 Decisión n.º 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio de 2002, relativa al estatuto y a las condiciones generales de ejercicio de las funciones de Supervisor Europeo de Protección de Datos (DO 2002, L 183, p. 1).

Índice

I. EL DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL RECONOCIDO POR LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA 5

1. CONFORMIDAD DEL DERECHO DERIVADO DE LA UNIÓN CON EL DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL 5

2. RESPETO DEL DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN LA APLICACIÓN DEL DERECHO DE LA UNIÓN 9

II. EL TRATAMIENTO DE DATOS PERSONALES EN EL SENTIDO DE LA NORMATIVA GENERAL EN LA MATERIA 11

1. TRATAMIENTOS DE DATOS PERSONALES EXCLUIDOS DEL ÁMBITO DE APLICACIÓN DE LA DIRECTIVA 95/46 11

2. CONCEPTO DE «DATOS PERSONALES» 13

3. CONCEPTO DE «TRATAMIENTO DE DATOS PERSONALES» 15

4. CONCEPTO DE «FICHERO DE DATOS PERSONALES» 21

5. CONCEPTO DE «RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES» 21

6. CONDICIONES DE LICITUD DE UN TRATAMIENTO DE DATOS PERSONALES 24

III. TRATAMIENTOS DE DATOS PERSONALES CON ARREGLO A LA DIRECTIVA 2002/58 34

IV. TRANSFERENCIA DE LOS DATOS PERSONALES A PAÍSES TERCEROS 40

V. LA PROTECCIÓN DE LOS DATOS PERSONALES EN INTERNET 48

1. DERECHO DE OPOSICIÓN AL TRATAMIENTO DE LOS DATOS PERSONALES («DERECHO AL OLVIDO») 48

2. TRATAMIENTO DE LOS DATOS PERSONALES Y DERECHOS DE PROPIEDAD INTELECTUAL 49

3. RETIRADA DE ENLACES A DATOS PERSONALES 54

4. CONSENTIMIENTO DEL USUARIO DE UN SITIO DE INTERNET AL ALMACENAMIENTO DE INFORMACIÓN O AL ACCESO A INFORMACIÓN MEDIANTE *COOKIES* 57

VI. AUTORIDADES NACIONALES DE CONTROL 59

1. ALCANCE DEL REQUISITO DE INDEPENDENCIA 59

2. DETERMINACIÓN DEL DERECHO APLICABLE Y DE LA AUTORIDAD DE CONTROL COMPETENTE 61

3. FACULTADES DE LAS AUTORIDADES NACIONALES DE CONTROL 63

VII. ÁMBITO DE APLICACIÓN TERRITORIAL DE LA LEGISLACIÓN EUROPEA 67

VIII. DERECHO DE ACCESO DEL PÚBLICO A LOS DOCUMENTOS DE LAS INSTITUCIONES DE LA UNIÓN EUROPEA Y PROTECCIÓN DE LOS DATOS PERSONALES 68

I. El derecho a la protección de los datos de carácter personal reconocido por la Carta de los Derechos Fundamentales de la Unión Europea

1. Conformidad del Derecho derivado de la Unión con el derecho a la protección de los datos de carácter personal

Sentencia de 9 de noviembre de 2010 (Gran Sala), Volker und Markus Schecke y Eifert (C-92/09 y C-93/09, EU:C:2010:662) [11]

En este asunto, en los litigios principales se enfrentaban unos agricultores y el Land Hessen, en relación con la publicación en el sitio de Internet de la Bundesanstalt für Landwirtschaft und Ernährung (Oficina Federal de Agricultura y Alimentación) de sus datos personales como beneficiarios de fondos procedentes del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader). Esos agricultores se oponían a dicha publicación, alegando, en particular, que no existía un interés público preponderante que la justificara. El Land Hessen consideraba, por su parte, que la publicación de los citados datos se derivaba de los Reglamentos (CE) n.º 1290/2005 [12] y 259/2008, [13] que regulan la financiación de la política agrícola común y exigen que se publique la información relativa a las personas físicas beneficiarios del FEAGA y del Feader.

En estas circunstancias, el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania) planteó al Tribunal de Justicia varias cuestiones relativas a la validez de determinadas disposiciones del Reglamento n.º 1290/2005 y a la del Reglamento n.º 259/2008, que imponen la puesta a disposición del público de dicha información, en particular a través de sitios web gestionados por los organismos nacionales.

El Tribunal de Justicia señaló, en lo que atañe a la adecuación entre el derecho a la protección de los datos de carácter personal reconocido en la Carta y la obligación de transparencia en relación con los fondos europeos, que la publicación en un sitio web de los datos nominales de los beneficiarios de los fondos y de los importes específicos percibidos por ellos constituye, a causa del libre acceso de los terceros al sitio, una lesión del derecho de los beneficiarios afectados al respeto de su vida privada, en general, y a la protección de sus datos de carácter personal, en particular (apartados 56 a 64).

---

11 Esta sentencia fue mencionada en el Informe Anual de 2010, p. 11.

12 Reglamento (CE) n.º 1290/2005 du Consejo, de 21 de junio de 2005, sobre la financiación de la política agrícola común (DO 2005, L 209, p. 1), derogado por el Reglamento (UE) n.º 1306/2013 del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, sobre la financiación, gestión y seguimiento de la Política Agrícola Común (DO 2013, L 347, p. 549).

13 Reglamento (CE) n.º 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) n.º 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de fondos procedentes del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader) (DO 2008, L 76, p. 28), derogado por el Reglamento de Ejecución (UE) n.º 908/2014 de la Comisión, de 6 de agosto de 2014, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 1306/2013 del Parlamento Europeo y del Consejo en relación con los organismos pagadores y otros organismos, la gestión financiera, la liquidación de cuentas, las normas relativas a los controles, las garantías y la transparencia (DO 2014, L 255, p. 59).

Para que una lesión de esos derechos pueda considerarse justificada, es preciso que esté establecida por la ley, respete el contenido esencial de dichos derechos y, respetando el principio de proporcionalidad, sea necesaria y responda efectivamente a objetivos de interés general reconocidos por la Unión (apartado 65). En este contexto, el Tribunal de Justicia considera que, si bien es cierto que en una sociedad democrática los contribuyentes tienen derecho a ser informados sobre la utilización de los fondos públicos, no es menos cierto que el Consejo y la Comisión estaban obligados a ponderar equilibradamente los distintos intereses en juego, lo que exigía verificar, antes de adoptar las disposiciones impugnadas, si la publicación de esos datos a través de un sitio web único en cada Estado miembro iba más allá de lo necesario para alcanzar los legítimos objetivos perseguidos (apartados 77, 79, 85 y 86).

Así pues, el Tribunal de Justicia declaró inválidas ciertas disposiciones del Reglamento n.º 1290/2005 y el Reglamento n.º 259/2008 en su totalidad, en la medida en que obligaban, por lo que respecta a las personas físicas beneficiarias de ayudas del FEAGA y del Feader, a publicar datos de carácter personal de todos los beneficiarios, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas habían percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas (apartado 92 y punto 1 del fallo). Sin embargo, el Tribunal de Justicia estimó que no podían impugnarse los efectos de las publicaciones de las listas de los beneficiarios de tales ayudas llevadas a cabo por las autoridades nacionales en el período anterior a la fecha de pronunciamiento de la sentencia (apartado 94 y punto 2 del fallo).

Sentencia de 17 de octubre de 2013, Schwarz (C-291/12, EU:C:2013:670)

El Sr. Schwarz solicitó al Ayuntamiento de la ciudad de Bochum (Alemania) la expedición de un pasaporte, pero se negó a que para ello le tomaran sus impresiones dactilares. Al rechazar el Ayuntamiento tal solicitud, el Sr. Schwarz interpuso recurso ante el Verwaltungsgericht Gelsenkirchen (Tribunal de lo Contencioso-Administrativo de Gelsenkirchen, Alemania) con objeto de que se ordenara al Ayuntamiento que le expidiese un pasaporte sin tomar sus impresiones dactilares. Ante dicho órgano jurisdiccional, el Sr. Schwarz impugnaba la validez del Reglamento (CE) n.º 2252/2004, [14] que estableció la obligación de tomar las impresiones dactilares a los solicitantes de pasaportes, alegando, entre otras cosas, que dicho Reglamento vulneraba el derecho a la protección de los datos de carácter personal y el derecho al respeto de la vida privada.

En este contexto, el Verwaltungsgericht Gelsenkirchen planteó una cuestión prejudicial al Tribunal de Justicia con el fin de saber si dicho Reglamento es válido, especialmente con arreglo a la Carta, en la medida en que obliga a los solicitantes de pasaportes a dar sus impresiones dactilares y dispone que estas se conserven en los pasaportes.

El Tribunal de Justicia respondió afirmativamente, considerando que, aunque la toma y conservación de impresiones dactilares por parte de las autoridades nacionales, reguladas por el artículo 1, apartado 2, del Reglamento n.º 2252/2004, constituyen una lesión de los derechos

[14] Reglamento (CE) n.º 2252/2004 del Consejo, de 13 de diciembre de 2004, sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros (DO 2004, L 385, p. 1), en su versión resultante del Reglamento (CE) n.º 444/2009 del Parlamento Europeo y del Consejo, de 6 de mayo de 2009 (DO 2009, L 142, p. 1).

al respeto de la vida privada y a la protección de los datos de carácter personal, tal restricción está justificada por el objetivo de proteger los pasaportes contra su uso fraudulento.

Así, en primer lugar, esta limitación, establecida por la ley, persigue un objetivo de interés general reconocido por la Unión, en la medida en que pretende impedir, en particular, la entrada ilegal de personas en el territorio de la Unión (apartados 35 a 38). A continuación, la toma y conservación de impresiones dactilares son idóneas para alcanzar este objetivo. En efecto, por una parte, aunque el método de verificación de identidad mediante impresiones dactilares no sea totalmente fiable, reduce considerablemente el riesgo de admisión de personas no autorizadas. Por otra parte, la falta de concordancia de las impresiones dactilares del poseedor del pasaporte con los datos integrados en ese documento no significa que se vaya a denegar automáticamente al interesado su entrada en el territorio de la Unión, sino que tendrá como única consecuencia un control en profundidad para acreditar de manera definitiva la identidad de esa persona (apartados 42 a 45).

Por último, en cuanto a la necesidad de ese tratamiento, no se ha puesto en conocimiento del Tribunal de Justicia la existencia de medidas distintas del método basado en las impresiones dactilares que contribuyan con la suficiente eficacia al objetivo de proteger los pasaportes contra su uso fraudulento y lesionen con menor gravedad los derechos reconocidos por los artículos 7 y 8 de la Carta (apartado 53). El artículo 1, apartado 2, del Reglamento n.º 2252/2004 no implica un tratamiento de las impresiones dactilares tomadas que vaya más allá de lo necesario para lograr ese objetivo. En efecto, dicho Reglamento dispone expresamente que las impresiones dactilares solo podrán utilizarse con el único fin de verificar la autenticidad del pasaporte y la identidad de su titular. Además, el artículo 1, apartado 2, de este Reglamento garantiza una protección contra el riesgo de lectura de los datos que contengan impresiones dactilares por parte de personas no autorizadas y dispone que las impresiones dactilares se conserven únicamente en el propio pasaporte, cuya posesión exclusiva corresponde a su titular (apartados 54 a 57, 60 y 63).

Sentencia de 8 de abril de 2014 (Gran Sala), Digital Rights Ireland y Seitlinger y otros (asuntos acumulados C-293/12 y C-594/12, EU:C:2014:238) [15]

Esta sentencia tiene su origen en una serie de cuestiones prejudiciales de apreciación de la validez de la Directiva 2006/24/CE sobre conservación de datos, considerada en relación con los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal, cuestiones que fueron planteadas al Tribunal de Justicia en sendos litigios nacionales ante un tribunal irlandés y otro austriaco. En el asunto C-293/12, la High Court (Tribunal Superior, Irlanda) conocía de un litigio entre la sociedad Digital Rights y las autoridades irlandesas referente a la legalidad de unas medidas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas. En el asunto C-594/12, el Verfassungsgerichtshof (Tribunal Constitucional, Austria) conocía de varios recursos de inconstitucionalidad en los que se solicitaba la anulación de la disposición nacional de transposición de la Directiva 2006/24 al Derecho austriaco.

[15] Esta sentencia fue mencionada en el Informe Anual de 2014, p. 60.

En sus peticiones de decisión prejudicial, el tribunal irlandés y el austriaco preguntaron al Tribunal de Justicia sobre la validez de la Directiva 2006/24 con arreglo a los artículos 7, 8 y 11 de la Carta. Más concretamente, dichos órganos jurisdiccionales preguntaron al Tribunal de Justicia si la obligación de conservar durante un determinado período ciertos datos relativos a la vida privada de las personas y a sus comunicaciones y de permitir que accedieran a ellos las autoridades nacionales competentes, obligación impuesta por dicha Directiva a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, suponía una injerencia injustificada en esos derechos fundamentales. Los datos de que se trata son, en particular, los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación y el equipo de comunicación de los usuarios y para identificar la localización del equipo de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en particular, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que esta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto.

En primer lugar, el Tribunal de Justicia declaró que, al imponer tales obligaciones a dichos proveedores, las disposiciones de la Directiva 2006/24 constituían una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, reconocidos en los artículos 7 y 8 de la Carta. En este contexto, el Tribunal de Justicia declaró que dicha injerencia podía justificarse por la persecución de un objetivo de interés general, como la lucha contra la delincuencia organizada. A este respecto, el Tribunal de Justicia señaló, en primer lugar, que la conservación de los datos impuesta por la Directiva no podía lesionar el contenido esencial de los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal, en la medida en que no permitía conocer el contenido de las comunicaciones electrónicas como tal y se establecía que los proveedores de servicios o redes debían respetar determinados principios de protección y de seguridad de los datos. En segundo lugar, el Tribunal de Justicia señaló que la conservación de los datos para su eventual transmisión a las autoridades nacionales competentes respondía efectivamente a un objetivo de interés general, a saber, la lucha contra la delincuencia grave y, en definitiva, a la seguridad pública (apartados 38 a 44).

Sin embargo, el Tribunal de Justicia consideró que, al adoptar la Directiva sobre conservación de datos, el legislador de la Unión había sobrepasado los límites que impone el respeto del principio de proporcionalidad. Por tanto, declaró la invalidez de la Directiva al considerar que la injerencia de gran magnitud y especial gravedad en los derechos fundamentales que dicha norma implicaba no estaba regulada con la precisión suficiente para garantizar que la injerencia se limitara a lo estrictamente necesario (apartado 65). En efecto, la Directiva 2006/24 se aplicaba de manera generalizada a todas las personas y a todos los medios de comunicación electrónica y datos relativos al tráfico, sin establecer diferenciación, limitación o excepción alguna en función del objetivo de lucha contra los delitos graves (apartados 57 a 59). Por otra parte, la Directiva no establecía ningún criterio objetivo que permitiera garantizar que las autoridades nacionales competentes tendrían acceso a los datos y podrían utilizarlos exclusivamente a efectos de prevenir, detectar o perseguir penalmente las infracciones que pudieran considerarse suficientemente graves para justificar tal injerencia, ni las condiciones materiales y

de procedimiento para acceder a esos datos o utilizarlos (apartados 60 a 62). En lo que respecta al período de conservación de los datos, la Directiva prescribía un período mínimo de seis meses, sin establecer distinción alguna entre las categorías de datos en función de su eventual utilidad para el objetivo perseguido o de las personas afectadas (apartados 63 y 64).

Por otra parte, por lo que se refiere a las exigencias derivadas del artículo 8, apartado 3, de la Carta, el Tribunal de Justicia afirmó que la Directiva 2006/24 no establecía garantías suficientes que permitieran proteger de manera eficaz los datos contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de los mismos, y no obligaba tampoco a conservar los datos en el territorio de la Unión.

En consecuencia, dicha Directiva no garantizaba plenamente el control del cumplimiento de las exigencias de protección y seguridad por parte de una autoridad independiente, como se exige expresamente en la Carta (apartados 66 a 68).

2. Respeto del derecho a la protección de los datos de carácter personal en la aplicación del Derecho de la Unión

Sentencia de 21 de diciembre de 2016 (Gran Sala), Tele2 Sverige (asuntos acumulados C-203/15 y C-698/15, EU:C:2016:970) [16]

A raíz de la sentencia Digital Rights Ireland y Seitlinger y otros, que declaró inválida la Directiva 2006/24 (véase *supra*), el Tribunal de Justicia conoció de dos asuntos relativos a la obligación general impuesta en Suecia y en el Reino Unido a los proveedores de servicios de comunicaciones electrónicas de conservación de los datos relativos a dichas comunicaciones, conservación que exigía la Directiva invalidada.

El día siguiente al pronunciamiento de la sentencia Digital Rights Ireland y Seitlinger y otros, la empresa de telecomunicaciones 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). En efecto, el Derecho sueco obligaba a los proveedores de servicios de comunicaciones electrónicas a conservar de manera sistemática y continuada, sin ninguna excepción, todos los datos de tráfico y de localización de todos los abonados y usuarios registrados, en relación con todos los medios de comunicación electrónica. En el asunto C-698/15, tres personas habían interpuesto recursos contra el régimen británico de conservación de datos, que permitía que el Ministro de Interior obligara a los operadores de telecomunicaciones públicas a conservar todos los datos relativos a las comunicaciones, exceptuando el contenido de dichas comunicaciones, durante un período máximo de doce meses.

En sus peticiones de decisión prejudicial, el Kammarrätten i Stockholm (Tribunal de Apelación de lo Contencioso-Administrativo de Estocolmo, Suecia) y la Court of Appeal [(England and Wales) (Civil Division) (Tribunal de Apelación de Inglaterra y País de Gales, Sala de lo Civil, Reino Unido)],

[16] Esta sentencia fue mencionada en el Informe Anual de 2016, p. 62.

solicitaban al el Tribunal de Justicia que se pronunciara sobre la interpretación del artículo 15, apartado 1, de la Directiva 2002/58, conocida como «Directiva sobre la privacidad y las comunicaciones electrónicas», que permite que los Estados miembros establezcan determinadas excepciones a la obligación, impuesta por dicha Directiva, de garantizar la confidencialidad de las comunicaciones electrónicas y de sus datos de tráfico.

En su sentencia, el Tribunal de Justicia comenzó por afirmar que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11, y del artículo 52, apartado 1, de la Carta, se opone a una normativa nacional, como la sueca, que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Según el Tribunal de Justicia, una normativa nacional de este tipo sobrepasa, por tanto, los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el mencionado artículo 15, apartado 1, interpretado en relación con los citados artículos de la Carta (apartados 99 a 105, 107 y 112 y punto 1 del fallo).

Esta misma disposición, interpretada a la luz de los mismos artículos de la Carta, se opone igualmente a una normativa nacional que regula la protección y la seguridad de los datos de tráfico y de localización, en particular el acceso de las autoridades nacionales competentes a los datos conservados, sin limitar dicho acceso, en el marco de la lucha contra la delincuencia, a los casos de delincuencia grave, sin supeditar dicho acceso a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente y sin exigir que los datos de que se trata se conserven en el territorio de la Unión (apartados 118 a 122 y 125 y punto 2 del fallo).

En cambio, el Tribunal de Justicia consideró que el artículo 15, apartado 1, de la Directiva 2002/58/CE no se opone a una normativa que permita, con carácter preventivo, la conservación selectiva de datos de esta naturaleza a efectos de la lucha contra la delincuencia grave, siempre que dicha conservación esté limitada a lo estrictamente necesario en relación con las categorías de datos y los medios de comunicación a los que haga referencia, con las personas afectadas y con el período de conservación seleccionada. Para cumplir estos requisitos, dicha normativa nacional debe establecer, en primer lugar, normas claras y precisas que permitan proteger eficazmente los datos contra los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario. En segundo lugar, en relación con los requisitos materiales que debe cumplir una normativa nacional para garantizar que se limita a lo estrictamente necesario, la conservación de los datos debe responder a criterios objetivos y debe existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr. En particular, tales requisitos deben permitir delimitar efectivamente, en la práctica, el alcance de la medida y, en consecuencia, el público afectado. Por lo que se refiere a esta delimitación, la normativa nacional debe basarse en elementos objetivos que permitan centrarse en un público cuyos datos puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave o prevenir un riesgo grave para la seguridad pública (apartados 108 a 111).

II. El tratamiento de datos personales en el sentido de la normativa general en la materia

1. Tratamientos de datos personales excluidos del ámbito de aplicación de la Directiva 95/46

Sentencia de 30 de mayo de 2006 (Gran Sala), Parlamento/Consejo (C-317/04 y C-318/04, EU:C:2006:346)

Tras los atentados terroristas del 11 de septiembre de 2001, los Estados Unidos adoptaron una normativa en virtud de la cual las compañías aéreas que operen en rutas con destino u origen en Estados Unidos o que atraviesen su territorio están obligadas a facilitar a las autoridades estadounidenses un acceso electrónico a los datos contenidos en sus sistemas de reserva y de control de salidas, denominados «Passenger Name Records» (en lo sucesivo, «PNR»).

Al considerar que estas disposiciones podían ser contrarias a la normativa de la UE y a la de los Estados miembros en materia de protección de datos, la Comisión inició negociaciones con las autoridades estadounidenses. Como resultado de dichas negociaciones, la Comisión adoptó el 14 de mayo de 2004 la Decisión 2004/535/CE, [17] en la que se hacía constar que el Servicio de aduanas y protección de fronteras de los Estados Unidos (United States Bureau of Customs and Border Protection; en lo sucesivo, «las aduanas estadounidenses») ofrecía un nivel adecuado de protección de los datos de los PNR transferidos desde la Comunidad (en lo sucesivo, «Decisión de protección adecuada»). A continuación, el 17 de mayo de 2004, el Consejo adoptó la Decisión 2004/496/CE, [18] por la que se aprobaba la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos sobre el tratamiento y la transferencia de los datos de los PNR a las aduanas estadounidenses por parte de las compañías aéreas establecidas en el territorio de los Estados miembros de la Comunidad.

El Parlamento Europeo solicitó al Tribunal de Justicia la anulación de las dos decisiones antes mencionadas, alegando, en particular, que la Decisión de protección adecuada había sido adoptada *ultra vires*, que el artículo 95 CE (actualmente artículo 114 TFUE) no constituía una base jurídica apropiada para la Decisión por la que se aprobaba la celebración del Acuerdo y, en ambos casos, que existía una violación de los derechos fundamentales.

Por lo que se refiere a la Decisión de protección adecuada, el Tribunal de Justicia examinó, en primer lugar, si la Comisión podía adoptar tal Decisión sobre la base de la Directiva 95/46. En este contexto, señaló que se deducía de la Decisión de protección adecuada que la transferencia de los datos de los PNR a las aduanas estadounidenses constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal. A juicio

[17] Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection) (DO 2004, L 235, p. 11).

[18] Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (DO 2004, L 183, p. 83, y corrección de errores en DO 2005, L 255, p. 168).

del Tribunal de Justicia, si bien es cierto que las compañías aéreas recogían inicialmente los datos de los PNR en el marco de una actividad sometida al Derecho de la Unión, a saber, la venta de un billete de avión que da derecho a una prestación de servicios, el tratamiento de datos contemplado en la Decisión de protección adecuada tenía, sin embargo, una naturaleza bien distinta. En efecto, esta Decisión no se refería a un tratamiento de datos necesario para realizar una prestación de servicios, sino a un tratamiento de datos que se consideraba necesario para salvaguardar la seguridad pública y para fines represivos (apartados 56 y 57).

A este respecto, el Tribunal de Justicia señaló que el hecho de que los datos de los PNR hubieran sido recogidos por operadores privados con fines mercantiles y de que fueran estos quienes organizaban su transferencia a un Estado tercero no impedía calificar esa transferencia de tratamiento de datos excluido del ámbito de aplicación de la Directiva. En efecto, dicha transferencia se insertaba en un marco creado por los poderes públicos y cuyo objetivo era proteger la seguridad pública. Por consiguiente, el Tribunal de Justicia concluyó que la Decisión de protección adecuada no estaba comprendida en el ámbito de aplicación de la Directiva porque se refería a un tratamiento de datos personales excluido de dicho ámbito. En consecuencia, el Tribunal de Justicia anuló la Decisión de protección adecuada (apartados 58 y 59).

En lo que respecta a la Decisión del Consejo, el Tribunal de Justicia declaró que el artículo 95 CE, puesto en relación con el artículo 25 de la Directiva 95/46, no podía constituir la base de la competencia de la Comunidad para celebrar el Acuerdo en cuestión con los Estados Unidos. En efecto, ese Acuerdo se refería a la misma transferencia de datos que la Decisión de protección adecuada y, por tanto, a tratamientos de datos que no estaban comprendidos en el ámbito de aplicación de la Directiva. Por consiguiente, el Tribunal de Justicia anuló la Decisión del Consejo por la que se aprobaba la celebración del Acuerdo (apartados 67 a 69).

Sentencia de 11 de diciembre de 2014, Ryneš (C-212/13, EU:C:2014:2428)

En respuesta a una serie de agresiones, el Sr. Ryneš había instalado en su vivienda una cámara de vigilancia. Tras un nuevo ataque contra su casa, las grabaciones de dicha cámara habían permitido identificar a dos sospechosos, que fueron procesados. Uno de los sospechosos impugnó ante la Agencia checa de protección de datos de carácter personal la legalidad del tratamiento de los datos grabados por la cámara de vigilancia, y dicha Agencia declaró que el Sr. Ryneš había infringido las normas en materia de protección de los datos de carácter personal y le impuso una multa.

El Sr. Ryneš recurrió en casación la sentencia del Městský soud v Praze (Tribunal municipal de Praga, República Checa) que había confirmado la resolución de la Agencia, y el Nejvyšší správní soud (Tribunal Supremo de lo Contencioso-Administrativo), que conocía del recurso de casación, preguntó al Tribunal de Justicia si la grabación efectuada por el Sr. Ryneš a fin de proteger su vida, su salud y sus bienes constituía un tratamiento de datos excluido del ámbito de aplicación de la Directiva 95/46 por la razón de que tal grabación había sido efectuada por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, en el sentido del artículo 3, apartado 2, segundo guion, de dicha Directiva.

El Tribunal de Justicia declaró que la utilización de un sistema de cámara de vídeo que da lugar a la obtención de imágenes de personas que luego se almacenan en un dispositivo de grabación continuada, como un disco duro, sistema de videovigilancia instalado por una persona física en su vivienda familiar con el fin de proteger los bienes, la salud y la vida de los propietarios de la vivienda y cuya vigilancia cubre también el espacio público, no constituye un tratamiento de datos efectuado en el ejercicio de actividades exclusivamente personales o domésticas (apartado 35 y fallo).

A este respecto, el Tribunal de Justicia recordó que la protección del derecho fundamental a la vida privada, garantizado por el artículo 7 de la Carta, exige que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario. Teniendo en cuenta que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que puede vulnerar las libertades fundamentales y, en particular, el derecho a la intimidad o la protección de la vida privada, deben ser interpretadas a la luz de los derechos fundamentales recogidos en la citada Carta, la excepción prevista en el artículo 3, apartado 2, segundo guion, de dicha Directiva debe ser interpretada en sentido estricto (apartados 27 a 29). Además, el propio texto de esta disposición excluye del ámbito de aplicación de la Directiva 95/46 el tratamiento de datos efectuado en el ejercicio de actividades «exclusivamente» personales o domésticas. Ahora bien, en la medida en que una vigilancia por videocámara se extienda, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente «personal o doméstica», en el sentido de dicha disposición (apartados 30, 31 y 33).

2. Concepto de «datos personales»

Sentencia de 19 de octubre de 2016, Breyer (C-582/14, EU:C:2016:779) [19]

El Sr. Breyer había presentado ante los tribunales de lo contencioso-administrativo alemanes un recurso en el que solicitaba que se prohibiera a la República Federal de Alemania conservar o permitir que terceros conservasen ciertos datos informáticos que eran transmitidos a los sitios de Internet de organismos federales alemanes al terminar cada consulta de esos sitios. En efecto, para prevenir ataques y posibilitar el ejercicio de acciones penales contra los «piratas», el proveedor de servicios de medios en línea de los organismos federales alemanes registraba unos datos consistentes en una dirección IP dinámica (dirección IP que cambia en cada conexión a Internet), y la fecha y hora de la sesión de consulta del sitio. A diferencia de las direcciones IP estáticas, las direcciones IP dinámicas no permitían, *a priori*, establecer un vínculo, mediante ficheros accesibles al público, entre un ordenador concreto y la conexión física a la red utilizada por el proveedor de acceso a Internet. Los datos registrados no permitían, por sí solos, que el proveedor de servicios de medios en línea identificara al usuario. Sin embargo, el proveedor de acceso a Internet disponía, por su parte, de información adicional que, si se combinaba con esa dirección IP, permitiría identificar a dicho usuario.

[19] Esta sentencia fue mencionada en el Informe Anual de 2016, p. 61.

En este contexto, el Bundesgerichtshof (Tribunal Supremo de lo Civil y Penal, Alemania), que conocía del recurso de casación, planteó al Tribunal de Justicia la cuestión de si una dirección IP registrada por un prestador de servicios de medios en línea con ocasión de un acceso a su sitio de Internet constituye para este un dato personal.

En primer lugar, el Tribunal de Justicia consideró que para que un dato pueda ser calificado de «dato personal» en el sentido del artículo 2, letra a), de la Directiva 95/46 no es preciso que toda la información que permita identificar al interesado se encuentre en poder de una sola persona. El hecho de que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios de medios en línea, sino del proveedor de acceso a Internet de ese usuario, no parece que pueda excluir que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea constituyan, para este, datos personales en el sentido del artículo 2, letra a), de la Directiva 95/46 (apartados 43 y 44).

Por consiguiente, el Tribunal de Justicia declaró que una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal, en el sentido del artículo 2, letra a), de la Directiva 95/46, cuando este disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona (apartado 49 y punto 1 del fallo).

Sentencia de 20 de diciembre de 2017, Nowak (C-434/16, EU:C:2017:994)

Tras suspender el examen organizado por el Institute of Chartered Accountants of Ireland (Colegio de censores jurados de cuentas de Irlanda), el Sr. Nowak, contable en prácticas, presentó, con arreglo al artículo 4 de la Ley de Protección de Datos, una solicitud de acceso a todos los datos de carácter personal que le concernían en poder del Colegio de censores jurados. Este último remitió al Sr. Nowak ciertos documentos, pero rehusó enviarle su examen, basándose en que no contenía datos personales, a efectos de lo establecido en la Ley de Protección de Datos.

Como el Comisario de Protección de Datos tampoco tramitó su reclamación de acceso a dicho documento por los mismos motivos, el Sr. Nowak se dirigió a los tribunales nacionales. La Supreme Court (Tribunal Supremo, Irlanda), que conocía de un recurso de casación interpuesto por el Sr. Nowak, preguntó al Tribunal de Justicia si el artículo 2, letra a), de la Directiva 95/46, debe interpretarse en el sentido de que, en unas circunstancias como las del litigio principal, las respuestas escritas de un aspirante en un examen profesional y las eventuales anotaciones del examinador en relación con aquellas son datos personales, a efectos de dicha disposición.

En primer lugar, el Tribunal de Justicia señaló que para que un dato pueda ser calificado de «dato personal», en el sentido del artículo 2, letra a), de la Directiva 95/46, no es preciso que toda la información que permita identificar al interesado se encuentre en poder de una sola persona. Por otra parte afirmó que, en el supuesto de que el examinador no conozca la identidad del aspirante al evaluar las respuestas dadas por este en el examen de que se trate, la entidad que organice el examen (en ese caso el Colegio de censores jurados) dispone, en cambio, de los datos necesarios para identificar al aspirante sin dificultades o dudas mediante

su número de identificación, marcado en el examen o en su cubierta delantera, y así atribuirle sus respuestas.

En segundo lugar, el Tribunal de Justicia indicó que las respuestas escritas proporcionadas por un aspirante en un examen profesional son datos relacionados con su persona. En efecto, el contenido de tales respuestas revela el nivel de conocimientos y el grado de competencia del aspirante en un área determinada, así como, en su caso, el proceso de reflexión, el discernimiento y la capacidad de análisis del propio aspirante. Además, mediante la obtención de las respuestas se pretende valorar la capacidad profesional del aspirante y su aptitud para ejercer el oficio de que se trate. Más aún, la utilización de los referidos datos, que se traduce, en particular, por el éxito o el fracaso del aspirante en el examen en cuestión, puede tener efectos sobre sus derechos e intereses, ya que, por ejemplo, puede condicionar sus oportunidades de acceder a la profesión o empleo al que aspira o influir en esas oportunidades. La constatación de que las respuestas escritas de un aspirante en un examen profesional son datos que le conciernen debido a su contenido, finalidad y efectos también es válida, por lo demás, cuando se trata de un examen en el que pueden utilizarse libros (apartados 31 y 36 a 40).

En tercer lugar, por lo que se refiere a las anotaciones del examinador sobre las respuestas del candidato, el Tribunal de Justicia consideró que, al igual que las respuestas facilitadas por el candidato durante el examen, son datos sobre el candidato, ya que expresan la opinión o valoración del examinador sobre los resultados individuales del aspirante en el examen y, en particular, sobre sus conocimientos y competencias en el área de que se trate. Tales anotaciones, por lo demás, tienen precisamente la finalidad de documentar la evaluación de los resultados del aspirante por parte del examinador, y pueden tener efectos para ese aspirante (apartados 42 y 43).

En cuarto lugar, el Tribunal de Justicia consideró que las respuestas escritas de un aspirante en un examen profesional y las eventuales anotaciones al respecto del examinador pueden ser verificadas en lo que respecta a su exactitud y a la necesidad de conservarlas, en el sentido del artículo 6, apartado 1, letras d) y e), de la Directiva 95/46, y pueden ser rectificadas o suprimidas, con arreglo a su artículo 12, letra b). El hecho de conferir al aspirante un derecho de acceso a esas respuestas y anotaciones de acuerdo con el artículo 12, letra a), de dicha Directiva sirve al objetivo de esta, consistente en garantizar la protección del derecho a la intimidad del aspirante en lo que respecta al tratamiento de sus datos, y ello con independencia de si el aspirante tiene o no también ese derecho de acceso en virtud de la normativa nacional aplicable al procedimiento de examen. Finalmente, el Tribunal de Justicia subrayó que los derechos de acceso y rectificación, con arreglo al artículo 12, letras a) y b), de la Directiva 95/46, no incluyen las preguntas del examen, que por su propia naturaleza no son datos personales del candidato (apartados 56 y 58).

Habida cuenta de estas consideraciones, el Tribunal de Justicia concluyó que, en circunstancias tales como las del litigio principal, las respuestas por escrito proporcionadas por un aspirante durante un examen profesional y las eventuales anotaciones del examinador referentes a dichas respuestas son datos personales, en el sentido del artículo 2, letra a), de la Directiva 95/46 (apartado 62 y fallo).

3. Concepto de «tratamiento de datos personales»

Sentencia de 6 de noviembre de 2003 (Gran Sala), Lindqvist (C-101/01, EU:C:2003:596)

La Sra. Lindqvist, que trabajaba como voluntaria en una parroquia de la Iglesia protestante de Suecia, había creado con su ordenador personal una serie de páginas web que contenían datos personales de varias personas que, como ella, trabajaban como voluntarios en dicha parroquia. La Sra. Lindqvist fue condenada al pago de una multa por haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datainspektion (organismo público para la protección de los datos transmitidos por vía informática), por haberlos transferido a países terceros sin autorización y por haber tratado datos personales delicados.

En el marco del recurso de apelación interpuesto por la Sra. Lindqvist contra dicha decisión ante el Göta hovrätt (Tribunal de Apelación Contencioso-Administrativo, Suecia), este último preguntó al Tribunal de Justicia con carácter prejudicial, entre otras cosas, si la Sra. Lindqvist había realizado un «tratamiento de datos de carácter personal, total o parcialmente automatizado», en el sentido de la Directiva 95/46.

El Tribunal de Justicia declaró que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales», el sentido de dicha Directiva (apartado 27 y punto 1 del fallo). En efecto, dicho tratamiento de datos personales efectuado en el ejercicio de actividades voluntarias o religiosas no está comprendido en ninguna de las excepciones al ámbito de aplicación de la Directiva, ya que no entra en las categorías de actividades que tengan por objeto la seguridad pública ni en la categoría de actividades exclusivamente personales o domésticas, que quedan fuera del ámbito de aplicación de la Directiva (apartados 38, 43 a 48 y punto 2 del fallo).

Sentencia de 13 de mayo de 2014 (Gran Sala), Google Spain y Google (C-131/12, EU:C:2014:317)

En 2010, un nacional español interpuso ante la Agencia Española de Protección de Datos (en lo sucesivo, «AEPD») una reclamación contra La Vanguardia Ediciones, S. L., editora de un diario español de gran tirada, así como contra Google Spain y Google. Esta persona se basaba en que, cuando un internauta introducía su nombre en el buscador del grupo Google, la lista de resultados contenía enlaces hacia dos páginas del diario La Vanguardia de 1998 que anunciaban una subasta inmobiliaria organizada a raíz de un embargo por deudas del interesado. En su reclamación, esta persona solicitaba, por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o bien utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o a Google que eliminaran u ocultaran sus datos personales para que desaparecieran de sus resultados de búsqueda y de los enlaces de La Vanguardia.

La AEPD desestimó la reclamación contra La Vanguardia, considerando que el editor había publicado legalmente la información en cuestión, pero la estimó en lo que respecta a Google Spain y a Google, exigiendo a estas dos sociedades que tomasen las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos. Dichas sociedades

interpusieron sendos recursos contra la mencionada resolución ante la Audiencia Nacional solicitando que se anulara la resolución de la AEPD, y la Audiencia Nacional planteó una serie de preguntas al Tribunal de Justicia.

De este modo, el Tribunal de Justicia tuvo ocasión de precisar el concepto de «tratamiento de datos personales» en Internet con arreglo a la Directiva 95/46.

El Tribunal de Justicia declaró que la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales» cuando esa información contiene datos personales (punto 1 del fallo). El Tribunal de Justicia recordó además que las operaciones a las que se refiere la Directiva deben calificarse también de «tratamiento de datos personales» en el supuesto de que se refieran únicamente a información ya publicada tal cual en los medios de comunicación. Una excepción general a la aplicación de la Directiva en tal supuesto dejaría esta última en gran medida vacía de contenido (apartados 29 y 30).

Sentencia de 10 de julio de 2018 (Gran Sala), Jehovan todistajat (C-25/17, EU:C:2018:551) [20]

La autoridad finlandesa de protección de datos había adoptado una resolución mediante la cual se prohibía a la comunidad de los Testigos de Jehová recoger o tratar datos personales en el marco de la actividad de predicación puerta a puerta llevada a cabo por sus miembros sin respetar los requisitos que impone la normativa finlandesa para el tratamiento de tales datos. En el ámbito de su actividad de predicación puerta a puerta, los miembros de dicha comunidad realizan anotaciones sobre las visitas efectuadas a personas que ni ellos mismos ni la comunidad conocen previamente. Estos datos se recogen a modo de recordatorio y con el fin de poderse recuperar para una eventual visita posterior, sin que los interesados hayan dado su consentimiento ni hayan sido informados. A este respecto, la comunidad de los Testigos de Jehová ha impartido instrucciones a sus miembros acerca de esas anotaciones, instrucciones que figuran en al menos una de sus publicaciones dedicadas a la actividad de predicación.

El Tribunal de Justicia declaró que la recogida de datos personales por miembros de una comunidad religiosa en el marco de una actividad de predicación puerta a puerta y el tratamiento posterior de esos datos no están exceptuados del ámbito de aplicación de la Directiva 95/46, puesto que no constituyen ni tratamientos de datos personales efectuados en el ejercicio de actividades contempladas en el artículo 3, apartado 2, primer guion, de dicha Directiva ni tratamientos de datos personales efectuados por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas a efectos del artículo 3, apartado 2, segundo guion, de dicha Directiva (apartado 51 y punto 1 del fallo).

[20] Esta sentencia fue mencionada en el Informe Anual de 2018, pp. 87 y 88.

Sentencia de 14 de febrero de 2019, Buivids (C-345/17, EU:C:2019:122)

En este asunto, el Tribunal de Justicia se centró en la interpretación, por una parte, del ámbito de aplicación de la Directiva 95/46 y, por otra parte, del concepto de «tratamiento de datos personales con fines exclusivamente periodísticos» contemplado en el artículo 9 de dicha Directiva.

Esta sentencia se inscribe en el contexto de una petición de decisión prejudicial remitida por el Tribunal Supremo de Letonia, que conocía de un litigio entre el Sr. Buivids (en lo sucesivo, «recurrente») y la agencia estatal de protección de datos, relativo a un recurso por el que se solicitaba que se declarase ilegal una resolución de dicha autoridad según la cual el Sr. Buivids había vulnerado la normativa nacional en materia de protección de datos personales al publicar en un sitio de Internet un vídeo grabado por él mismo de su declaración ante la policía en las dependencias de la comisaría de la policía nacional, durante la tramitación de un expediente administrativo sancionador. Tras la desestimación de sus pretensiones por dos órganos jurisdiccionales de rango inferior, el recurrente interpuso recurso de casación ante el Tribunal Supremo, ante el que invocó su derecho a la libertad de expresión, alegando que el vídeo en cuestión mostraba a funcionarios de la policía nacional, que tienen la condición de personas públicas, en un lugar accesible al público y que, en consecuencia, las disposiciones de la Ley de protección de datos no son aplicables a estas personas.

Por lo que respecta, en primer lugar, al ámbito de aplicación de la Directiva 95/46, el Tribunal de Justicia señaló, por una parte, que las imágenes de los miembros de la policía grabadas en el vídeo en cuestión son datos personales y, por otra parte, que la grabación en vídeo de esas personas almacenada en la memoria de la cámara utilizada por el recurrente constituye un tratamiento de datos personales. Así pues, el Tribunal de Justicia añadió que publicar una grabación de vídeo que contiene datos personales en un sitio de Internet de vídeos en el que los usuarios pueden enviarlos, verlos y compartirlos constituye un tratamiento total o parcialmente automatizado de esos datos. Por otra parte, el Tribunal de Justicia subrayó que dicha grabación y su publicación no están comprendidas entre las excepciones previstas al ámbito de aplicación de la Directiva 95/46, relativas en particular a los tratamientos de datos personales realizados en el marco de actividades que no están incluidas en el ámbito de aplicación de dicha Directiva y los tratamientos que se inscriben en el marco del ejercicio de las actividades exclusivamente personales o domésticas. Por lo tanto, el Tribunal de Justicia concluyó que la grabación en vídeo de policías en una comisaría, durante una toma de declaración, y la publicación del vídeo grabado en un sitio de Internet de vídeos en el que los usuarios pueden enviarlos, verlos y compartirlos están comprendidas en el ámbito de aplicación de esta Directiva (apartados 31, 32, 35, 39, 42 y 43 y punto 1 del fallo).

Por lo que respecta, en segundo lugar, al alcance del concepto de «tratamiento de datos personales con fines exclusivamente periodísticos», el Tribunal de Justicia recordó, en primer lugar, que, haciendo una interpretación amplia del concepto de «periodismo», las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 se aplican a toda persona que ejerza una actividad periodística. Así pues, el Tribunal de Justicia declaró que el hecho de que el recurrente no fuese periodista profesional no excluía que la grabación del vídeo controvertido y su transmisión pudieran calificarse como «tratamiento de datos personales con fines exclusivamente periodísticos». Además, el Tribunal de Justicia subrayó que las exenciones y excepciones previstas en el artículo 9 de la Directiva 95/46 solo deben aplicarse en la medida en

que resulten necesarias para conciliar dos derechos fundamentales, a saber, el derecho a la intimidad y el derecho a la libertad de expresión. A este respecto, el Tribunal de Justicia precisó que no se podía excluir que la grabación y la publicación del vídeo controvertido, que se efectuaron sin informar a los interesados de la realización de esa grabación y de su finalidad, constituya una injerencia en el derecho fundamental al respeto de la intimidad de estas personas. Por lo tanto, concluyó que la grabación y la publicación en un sitio de Internet de vídeos del vídeo controvertido pueden constituir un tratamiento de datos personales con fines exclusivamente periodísticos, siempre que se deduzca de dicho vídeo que las citadas grabación y publicación tienen como única finalidad la divulgación al público de información, opiniones o ideas, lo que debe comprobar el tribunal remitente (apartados 51, 52, 55, 63, 67 y punto 2 del fallo).

Sentencia de 22 de junio de 2021 (Gran Sala), Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504)

A B, persona física, se le impusieron puntos por una o varias infracciones de tráfico. Estos puntos fueron inscritos por la Ceļu satiksmes drošības direkcija (Dirección de seguridad vial, Letonia; en lo sucesivo, «CSDD») en el registro nacional de vehículos y conductores.

En virtud de la normativa letona sobre circulación vial, [21] la información relativa a los puntos impuestos a conductores inscritos en dicho registro es accesible al público y es comunicada por la CSDD a cualquier persona que lo solicite, sin que se tenga que justificar un interés específico en obtener dicha información, incluidos operadores económicos a efectos de reutilización. Al albergar dudas sobre la legalidad de esta normativa, B interpuso un recurso de inconstitucionalidad ante la Latvijas Republikas Satversmes tiesa (Tribunal Constitucional, Letonia), para que este órgano jurisdiccional examinara la conformidad de dicha normativa con el derecho al respeto de la vida privada.

El Tribunal Constitucional consideró, en el marco de su apreciación de dicho derecho constitucional, que debía tener en cuenta el RGPD. Así pues, solicitó al Tribunal de Justicia que aclarara el alcance de varias disposiciones del RGPD con el fin de determinar la compatibilidad de la normativa letona sobre circulación vial con dicho Reglamento.

Mediante su sentencia, pronunciada en Gran Sala, el Tribunal de Justicia considera que el tratamiento de datos personales relativos a los puntos constituye un «tratamiento de datos personales relativos a condenas e infracciones penales», [22] para el que el RGPD prevé una mayor protección debido al carácter especialmente sensible de los datos en cuestión (apartados 10, 46, 74 y 94 y punto 1 del fallo).

En este contexto, observa, con carácter preliminar, que los datos relativos a los puntos son datos personales y que su comunicación por parte de la CSDD a terceros constituye un tratamiento comprendido en el ámbito de aplicación material del RGPD. En efecto, dicho ámbito de aplicación es muy amplio y ese tratamiento no está comprendido en las excepciones a la aplicabilidad del Reglamento (apartados 60, 61 y 72).

---

21 Artículo 14[1], apartado 2, de la Ceļu satiksmes likums (Ley de Tráfico), de 1 de octubre de 1997 (Latvijas Vēstnesis, 1997, n.º 274/276).

22 Artículo 10 del RGPD.

Así pues, por una parte, dicho tratamiento no está cubierto por la excepción relativa a la no aplicación del RGPD a un tratamiento efectuado en el marco de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión. [23] Debe considerarse que la citada excepción tiene como único objeto excluir del ámbito de aplicación de ese Reglamento al tratamiento de datos personales efectuado por autoridades estatales en el marco de una actividad dirigida a preservar la seguridad nacional o de una actividad que pueda incluirse en la misma categoría. Estas actividades comprenden, en particular, las que tienen por objeto proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad. Ahora bien, las actividades relativas a la seguridad vial no persiguen este objetivo y, por lo tanto, no pueden incluirse en la categoría de las actividades que tienen por objeto la preservación de la seguridad nacional (apartados 62 a 66 y 68).

Por otra parte, la comunicación de datos personales relativos a los puntos tampoco es un tratamiento comprendido por la excepción que prevé que no se aplique el RGPD al tratamiento de datos personales efectuado por las autoridades competentes en materia penal. [24] El Tribunal de Justicia observa, en efecto, que no puede considerarse que, en el ejercicio de dicha comunicación, la CSDD sea una de esas «autoridades competentes» [25] (apartados 69 a 71).

Para determinar si el acceso a los datos personales relativos a infracciones de tráfico, como los puntos, constituye un tratamiento de datos personales relativos a «infracciones», [26] los cuales gozan de una mayor protección, el Tribunal de Justicia constata, basándose en particular en la génesis del RGPD, que este concepto se refiere exclusivamente a las infracciones penales. No obstante, el hecho de que, en el sistema jurídico letón, las infracciones de tráfico estén tipificadas como infracciones administrativas no es determinante para apreciar si tales infracciones están comprendidas en el concepto de «infracción penal», en la medida en que se trata de un concepto autónomo del Derecho de la Unión que exige, en toda la Unión, una interpretación autónoma y uniforme. Así pues, tras recordar los tres criterios pertinentes para apreciar el carácter penal de una infracción, a saber, la calificación jurídica de la infracción en Derecho interno, la naturaleza de la infracción y el grado de severidad de la sanción impuesta, el Tribunal de Justicia declara que las infracciones de tráfico en cuestión están comprendidas en el concepto de «infracción» en el sentido del RGPD. Por lo que respecta a los dos primeros criterios, el Tribunal de Justicia constata que, aunque las infracciones no se califiquen de «penales» en Derecho nacional, tal carácter puede derivarse de la naturaleza de la infracción y, especialmente, de la finalidad represiva que persiga la sanción que la infracción puede implicar. Pues bien, en el caso de autos, la atribución de puntos por infracciones de tráfico, al igual que las demás sanciones que la comisión de aquellas puede implicar, persiguen, entre otras cosas, tal finalidad represiva. En cuanto al tercer criterio, el Tribunal de Justicia observa que solo las infracciones de tráfico de cierta gravedad implican la imposición de puntos y que, por lo tanto, pueden dar lugar a sanciones de cierta severidad. Además, la imposición de tales puntos se suma generalmente a la sanción impuesta, y la acumulación de estos puntos conlleva

[23] Artículo 2, apartado 2, letra a), del RGPD.
[24] Artículo 2, apartado 2, letra d), del RGPD.
[25] Artículo 3, apartado 7, de la 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 Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).
[26] Artículo 10 del RGPD.

consecuencias jurídicas que pueden incluso llegar a la prohibición de conducir (apartados 77, 80, 85, 87 a 90 y 93).

4. Concepto de «fichero de datos personales»

Sentencia de 10 de julio de 2018 (Gran Sala), Jehovan todistajat (C-25/17, EU:C:2018:551)

En esta sentencia (véase asimismo la sección II.3, titulada «Concepto de tratamiento de datos personales»), el Tribunal de Justicia precisó el concepto de «fichero» a que se refiere el artículo 2, letra c), de la Directiva 95/46.

Así, tras haber recordado que dicha Directiva únicamente se aplica a los tratamientos manuales de datos personales cuando los datos tratados estén incluidos o destinados a ser incluidos en un fichero, el Tribunal de Justicia declaró que el citado concepto comprende un conjunto de datos personales recogidos en relación con una actividad de predicación puerta a puerta, consistentes en nombres, direcciones y otra información relativa a las personas contactadas, siempre que los datos estén estructurados según criterios determinados que permitan, en la práctica, recuperarlos fácilmente para su utilización posterior. Para que dicho conjunto de datos esté comprendido en ese concepto no es preciso que incluya fichas, catálogos específicos u otros sistemas de búsqueda (apartado 62 y punto 2 del fallo).

5. Concepto de «responsable del tratamiento de datos personales»

Sentencia de 10 de julio de 2018 (Gran Sala), Jehovan todistajat (C-25/17, EU:C:2018:551)

En este asunto (véanse asimismo las secciones II.3 y II.4, tituladas «Concepto de "tratamiento de datos personales"» y «Concepto de "fichero de datos personales"»), el Tribunal de Justicia se pronunció sobre la responsabilidad de una comunidad religiosa con respecto a los tratamientos de datos personales efectuados en el marco de una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad.

Así, el Tribunal de Justicia consideró que la obligación que incumbe a todas las personas de cumplir las normas del Derecho de la Unión en materia de protección de datos personales no puede considerarse una injerencia en la autonomía organizativa de las comunidades religiosas. A este respecto, concluyó que el artículo 2, letra d), de la Directiva 95/46, en relación con el artículo 10, apartado 1, de la Carta, debe interpretarse en el sentido de que permite considerar que una comunidad religiosa es responsable, junto con sus miembros predicadores, de los tratamientos de datos personales efectuados por estos últimos en relación con una actividad de predicación puerta a puerta organizada, coordinada y fomentada por dicha comunidad, sin que sea necesario que la comunidad tenga acceso a los datos ni haga falta demostrar que la comunidad ha impartido a sus miembros instrucciones por escrito o consignas respecto a esos tratamientos (apartados 74 y 75 y punto 3 del fallo).

Sentencia de 5 de junio de 2018 (Gran Sala), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388) [27]

La autoridad alemana de protección de datos, en su condición de autoridad de control, en el sentido del artículo 28 de la Directiva 95/46, había ordenado a una empresa alemana, especializada en el ámbito de la educación y que ofrecía servicios de formación mediante una página de fans alojada en el sitio de la red social Facebook, desactivar su página de fans. Según la citada autoridad, ni esa empresa ni Facebook habían informado a los visitantes de la página de fans de que esta recogía, mediante *cookies*, datos personales relativos a ellos y después dicha empresa y Facebook trataban esos datos.

En este contexto, el Tribunal de Justicia precisó el contexto de «responsable del tratamiento» de datos personales. A este respecto, consideró que el administrador de una página de fans alojada en Facebook, como la empresa de que se trata en el procedimiento principal, participa, mediante su acción de configuración (en función, en particular, de su audiencia destinataria, así como de objetivos de gestión o de promoción de sus actividades), en la determinación de los fines y los medios del tratamiento de los datos personales de los visitantes de su página de fans. De este modo, según el Tribunal de Justicia, dicho administrador debe ser calificado de responsable de ese tratamiento en la Unión, en el sentido del artículo 2, letra d), de la Directiva 95/46, conjuntamente con Facebook Ireland (filial en la Unión de la empresa americana Facebook) (apartado 39).

Sentencia de 29 de julio de 2019, Fashion ID (C-40/17, EU:C:2019:629)

En este asunto, el Tribunal de Justicia tuvo ocasión de desarrollar el concepto de «responsable del tratamiento» en relación con la integración de un *plug-in* en una página web.

En el caso de que se trataba, Fashion ID, empresa alemana de comercio electrónico que se dedica a la venta de prendas de vestir, insertó en su sitio de Internet el módulo social «me gusta» de la red social Facebook. Esta inserción parece tener como consecuencia que, cuando un visitante consulta el sitio de Internet de Fashion ID, se transmiten a Facebook Ireland datos personales de ese visitante. Al parecer la transmisión se efectúa sin que dicho visitante sea consciente de ello y con independencia de si es miembro de la red social Facebook o de si clicó en el botón «me gusta» de Facebook.

Verbraucherzentrale NRW, asociación de utilidad pública de defensa de los intereses de los consumidores, reprocha a Fashion ID haber transmitido a Facebook Ireland datos de carácter personal pertenecientes a los visitantes de su sitio de Internet, por un lado, sin el consentimiento de estos últimos y, por otro, incumpliendo las obligaciones de información establecidas en las disposiciones relativas a la protección de los datos personales. Al conocer del litigio, el Oberlandesgericht Düsseldorf (Tribunal Superior Regional de lo Civil y Penal de Düsseldorf, Alemania) solicitó al Tribunal de Justicia que interpretase diversas disposiciones de la Directiva 95/46.

[27] Esta sentencia fue mencionada en el Informe Anual de 2018, pp. 86 y 87.

En primer lugar, el Tribunal de Justicia declaró que el administrador de un sitio de Internet, como Fashion ID, puede ser considerado responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46. Sin embargo, esa responsabilidad se limita a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente, a saber, la recogida y la comunicación por transmisión de los datos en cuestión. En cambio, según el Tribunal de Justicia, cabe excluir en principio, que Fashion ID determine los fines y los medios de las operaciones ulteriores de tratamiento de datos personales, efectuadas por Facebook Ireland tras su transmisión a esta última, de modo que Fashion ID no puede ser considerada responsable de esas operaciones, en el sentido de dicho artículo 2, letra d) (apartados 76 y 85 y punto 2 del fallo).

Además, el Tribunal de Justicia subrayó que es necesario que el administrador de un sitio de Internet y el proveedor de un módulo social, como Facebook Ireland, persigan, cada uno de ellos, con esas operaciones de tratamiento, un interés legítimo, en el sentido del artículo 7, letra f), de la Directiva 95/46, para que estas queden justificadas (apartado 97 y punto 3 del fallo).

Por último, el Tribunal de Justicia precisó que el consentimiento del interesado, a que se refieren el artículo 2, letra h), y el artículo 7, letra a), de la Directiva 95/46, debe ser solicitado por el administrador de un sitio de Internet únicamente por lo que se refiere a las operaciones de tratamiento de datos personales cuyos fines y medios determina ese administrador. En tal situación, la obligación de información establecida en el artículo 10 de dicha Directiva recae también sobre dicho administrador; no obstante, la información que este último ha de comunicar al interesado debe referirse únicamente a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina (apartado 106 y punto 4 del fallo).

Sentencia de 9 de julio de 2020, Land Hessen, C-272/19, EU:C:2020:535

Un ciudadano que había presentado una petición a la Comisión de peticiones del Parlamento del Estado Federado de Hesse (Alemania) solicitó a dicha Comisión el acceso a los datos de carácter personal que le afectaban, registrados por dicha Comisión en el marco del tratamiento de su petición. Su solicitud se basaba en el RGPD, que reconoce el derecho de todo interesado a obtener del responsable del tratamiento el acceso a los datos personales que le conciernen.

El presidente del Parlamento del Estado Federado de Hesse denegó dicha solicitud alegando que el procedimiento de petición constituye una función parlamentaria y que el Parlamento no está sujeto al RGPD.

El Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania), ante quien recurrió el ciudadano, considera que el Derecho alemán no reconoce ningún derecho de acceso a los datos de carácter personal en el contexto de una petición como la controvertida. Sin embargo, por entender que tal derecho de acceso podría derivarse del RGPD, el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden) preguntó al Tribunal de Justicia sobre esta cuestión. Asimismo, al albergar dudas acerca de su propia independencia y por tanto acerca de su condición de órgano jurisdiccional, facultado para plantear cuestiones prejudiciales al Tribunal de Justicia, el Verwaltungsgericht

Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden) preguntó también al Tribunal de Justicia sobre este extremo.

Mediante su sentencia, el Tribunal de Justicia responde que, en la medida en que una comisión de peticiones del Parlamento de un estado federado de un Estado miembro determine, sola o junto con otros, los fines y los medios del tratamiento de datos personales, esa comisión debe calificarse de «responsable del tratamiento» a efectos del RGPD. [28] El tratamiento de datos personales efectuado por tal comisión está por tanto sujeto a dicho Reglamento, y concretamente a la disposición que confiere a los interesados un derecho de acceso a los datos personales que les conciernan. [29]

El Tribunal de Justicia declara en particular que a las actividades de la Comisión de peticiones del Parlamento del Estado Federado de Hesse no se les aplica ninguna excepción que esté prevista en el RGPD. Admite que tales actividades son de naturaleza pública y propias de dicho estado federado, ya que dicha Comisión contribuye indirectamente a la actividad parlamentaria, pero señala que dichas actividades son también de naturaleza tanto política como administrativa. Además, afirma que de los elementos que obran en poder del Tribunal de Justicia no se desprende en modo alguno que dichas actividades correspondan, en este asunto, a ninguna de las excepciones previstas por el RGPD (apartados 71 a 74 y fallo).

6. Condiciones de licitud de un tratamiento de datos personales

Sentencia de 16 de diciembre de 2008 (Gran Sala), Huber (C-524/06, EU:C:2008:724) [30]

La Oficina Federal de migración y refugiados (Bundesamt für Migration und Flüchtlinge, Alemania) gestionaba un Registro central de extranjeros que recogía determinados datos personales relativos a los extranjeros que residieran en territorio alemán por un período superior a tres meses. El Registro se utilizaba con fines estadísticos y en el ejercicio, por parte de los servicios de seguridad y policía y de las autoridades judiciales, de competencias en materia de diligencias penales y de investigaciones relativas a comportamientos delictivos o que pusieran en peligro la seguridad pública.

El Sr. Huber, de nacionalidad austriaca, se instaló en Alemania en 1996 para ejercer allí la profesión de agente de seguros por cuenta propia. Al considerarse discriminado en razón del tratamiento de que eran objeto los datos sobre su persona contenidos en ese Registro, pues tal base de datos no existe para los nacionales alemanes, el Sr. Huber solicitó la cancelación de esos datos.

En este contexto, el Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunal Superior de lo Contencioso-Administrativo del Land de Renania del Norte-Westfalia), al conocer del litigio, pidió al Tribunal de Justicia que se pronunciase sobre la compatibilidad con el

[28] Artículo 4, apartado 7, del RGPD.
[29] Artículo 15 del RGPD.
[30] Esta sentencia fue mencionada en el Informe Anual de 2008, p. 45.

Derecho de la Unión del tratamiento de los datos personales que lleva a cabo el mencionado Registro.

El Tribunal de Justicia comenzó por recordar que el derecho de un ciudadano de la Unión a residir en el territorio de un Estado miembro del que no es nacional no es incondicional, sino que puede estar sujeto a limitaciones. Por lo tanto, el uso de un Registro de ese tipo en apoyo de las autoridades encargadas de aplicar la normativa en materia de derecho de residencia es, en principio, legítimo, y, habida cuenta de su naturaleza, compatible con la prohibición de discriminación por razón de la nacionalidad contenida en el artículo 12 CE, apartado 1 (actualmente artículo 18 TFUE, párrafo primero). No obstante, tal Registro no podrá contener más información que la que resulte necesaria, en el sentido de la Directiva sobre la protección de los datos de carácter personal, a esos efectos (apartados 54, 58 y 59).

Por lo que se refiere al concepto de «necesidad» del tratamiento, en el sentido del artículo 7, letra e), de la Directiva 95/46, el Tribunal de Justicia recordó, en primer lugar, que se trata de un concepto autónomo del Derecho de la Unión que debe recibir una interpretación que responda plenamente al objeto de la Directiva 95/46, tal como lo define su artículo 1, apartado 1. El Tribunal de Justicia afirmó además que un sistema de tratamiento de datos personales de tales características es conforme con el Derecho de la Unión si contiene únicamente los datos necesarios para la aplicación de la mencionada normativa por parte de dichas autoridades y si su carácter centralizado permite una aplicación más eficaz de dicha normativa en lo que atañe al derecho de residencia de los ciudadanos de la Unión que no sean nacionales de ese Estado miembro.

En todo caso, no cabe considerar necesarios, en el sentido del artículo 7, letra e), de la Directiva 95/46, la conservación y el tratamiento de datos personales nominativos en el marco de un Registro de este tipo con fines estadísticos (apartados 52, 66 y 68).

Por otra parte, con respecto a la cuestión del uso de los datos contenidos en el Registro para combatir la delincuencia, el Tribunal de Justicia señaló que tal finalidad tiene necesariamente por objeto la persecución de los crímenes y delitos cometidos, con independencia de la nacionalidad de sus autores. Así pues, desde el punto de vista del objetivo de combatir la delincuencia, para un Estado miembro la situación de sus nacionales no puede ser diferente de la de los ciudadanos de la Unión que no sean nacionales suyos y residan en su territorio. Por consiguiente, la diferencia de trato, en aras de la lucha contra la delincuencia, entre aquellos nacionales y estos ciudadanos de la Unión que se deriva del tratamiento sistemático de los datos personales relativos únicamente a los ciudadanos de la Unión que no sean nacionales del Estado miembro de que se trate, constituye una discriminación prohibida por el artículo 12 CE, apartado 1 (apartados 78 a 80).

Sentencia de 24 de noviembre de 2011, ASNEF y FECEMD (C-468/10 y C-469/10, EU:C:2011:777)

La Asociación Nacional de Establecimientos Financieros de Crédito (en lo sucesivo, «ASNEF»), por un lado, y la Federación de Comercio Electrónico y Marketing Directo (en lo sucesivo, «FECEMD»), por otro lado, interpusieron ante el Tribunal Supremo español sendos recursos contencioso-administrativos contra numerosos artículos del Real Decreto 1720/2007, que desarrollaba la Ley Orgánica 15/1999, por la que se transponía la Directiva 95/46.

En particular, la ASNEF y la FECEMD consideraban que, para permitir el tratamiento de datos personales sin el consentimiento del interesado, el Derecho español añadía un requisito que no estaba presente en la Directiva 95/46 y que consistía en exigir que tales datos constaran en «fuentes accesibles al público», como las enumeradas en el artículo 3, letra j), de la Ley Orgánica 15/1999. A este respecto, alegaban que dicha Ley y el Real Decreto 1720/2007 restringían el alcance del artículo 7, letra f), de la Directiva 95/46, que somete el tratamiento de datos personales sin el consentimiento del interesado a un requisito relacionado únicamente con el interés legítimo perseguido por el responsable del tratamiento o el tercero o terceros a los que se comuniquen los datos.

A este respecto, el Tribunal de Justicia comenzó por señalar que el artículo 7 de la Directiva 95/46 establece una lista exhaustiva y taxativa de los casos en que un tratamiento de datos personales puede considerarse lícito. Por consiguiente, los Estados miembros no pueden introducir, amparándose en el artículo 5 de la Directiva, principios relativos a la legitimación de los tratamientos de datos personales que difieran de los enunciados en el artículo 7 ni modificar, mediante exigencias adicionales, el alcance de los principios establecidos en dicho artículo 7. En efecto, el artículo 5 solo autoriza a los Estados miembros a precisar, dentro de los límites del capítulo II de esa Directiva y, por ende, del artículo 7 de esta, las condiciones en que los tratamientos de datos personales son lícitos (apartados 30, 32 y 33).

En particular, los Estados miembros pueden establecer principios rectores para efectuar la ponderación de los derechos e intereses en conflicto, requerida por el artículo 7, letra f), de dicha Directiva. También pueden tomar en consideración el hecho de que la gravedad de la lesión de los derechos fundamentales de la persona afectada por dicho tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público (apartados 44 y 46).

Sin embargo, el Tribunal de Justicia estimó que, si una normativa nacional excluye la posibilidad de tratar determinadas categorías de datos personales, estableciendo con carácter definitivo el resultado de la ponderación de los derechos e intereses en conflicto respecto de tales categorías, sin permitir un resultado diferente en atención a las circunstancias particulares de cada caso concreto, no se trata ya de una precisión en el sentido del artículo 5 de la Directiva 95/46. Por consiguiente, el Tribunal de Justicia concluyó que el artículo 7, letra f), de la mencionada Directiva se opone a que un Estado miembro excluya de forma categórica y generalizada la posibilidad de someter a un tratamiento de datos determinadas categorías de datos personales, sin permitir una ponderación de los derechos e intereses en conflicto en cada caso concreto (apartados 47 y 48).

Sentencia de 19 de octubre de 2016, Breyer (C-582/14, EU:C:2016:779)

En esta sentencia (véase también la sección II.2, titulada «Concepto de "datos personales"»), el Tribunal de Justicia se pronunció igualmente sobre la cuestión de si el artículo 7, letra f), de la Directiva 95/46 se opone a una disposición nacional con arreglo a la cual, por una parte, un prestador de servicios de medios en línea solo puede recoger y utilizar los datos personales de un usuario sin su consentimiento cuando ello sea necesario para ofrecer y facturar el uso concreto del medio en línea por ese usuario y, por otra parte, el objetivo de garantizar el

funcionamiento general del medio en línea no puede justificar la utilización de esos datos tras la conclusión de cada operación de uso concreta.

El Tribunal de Justicia declaró que el artículo 7, letra f), de la Directiva 95/46 se opone a la normativa de que se trata. En efecto, según dicho artículo 7, letra f), el tratamiento de datos personales es lícito si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado. Pues bien, en ese asunto, la normativa alemana había excluido de manera categórica y generalizada la posibilidad de tratar determinadas categorías de datos personales, sin permitir una ponderación de los derechos e intereses en conflicto en cada caso concreto. Al actuar así, había reducido ilegalmente el alcance del principio establecido en el artículo 7, letra f), de la Directiva 95/46, impidiendo poner en la balanza el objetivo de garantizar la capacidad general de funcionamiento del medio en línea, por una parte, y el interés o los derechos y libertades fundamentales de los usuarios, por otra (apartados 62 a 64 y punto 2 del fallo).

Sentencia de 4 de mayo de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Ese asunto tiene su origen en un litigio entre la policía nacional letona y Rīgas satiksme, sociedad que gestiona los trolebuses municipales de Riga, en relación con la solicitud de comunicación de los datos identificativos del causante de un accidente. El accidente de tráfico se produjo tras detener un taxista su vehículo al borde de la calzada. En el momento en que un trolebús de Rīgas satiksme pasaba junto al taxi, el pasajero que ocupaba el asiento trasero del taxi había abierto la puerta, que rozó y dañó la carrocería del trolebús. A fin de interponer una demanda civil, Rīgas satiksme solicitó a la policía nacional que le comunicara los datos identificativos del causante del accidente. La policía se negó a facilitar el número de identificación y el domicilio del pasajero y los documentos relativos a las explicaciones facilitadas por las personas implicadas en el accidente, por la razón de que los documentos obrantes en procedimientos administrativos sancionadores solo pueden ser comunicados a quienes sean parte en dichos procedimientos y, en lo referente al número de identificación y a la dirección, la Ley de protección de datos de las personas físicas prohibía divulgar la información relativa a los particulares.

En estas circunstancias, el Augstākās tiesas Administratīvo lietu departaments (Sala de lo Contencioso-Administrativo del Tribunal Supremo, Letonia) decidió plantear al Tribunal de Justicia la cuestión de si el artículo 7, letra f), de la Directiva 95/46 obliga a comunicar datos personales a un tercero para que este pueda interponer una demanda indemnizatoria en vía civil por los daños que haya causado el interesado en la protección de dichos datos y si la circunstancia de que dicho interesado sea menor de edad puede tener incidencia en la interpretación de la citada disposición.

El Tribunal de Justicia declaró que el artículo 7, letra f), de la Directiva 95/46 debe interpretarse en el sentido de que no obliga a comunicar datos personales a un tercero para que este pueda interponer una demanda indemnizatoria en vía civil por los daños que haya causado el interesado en la protección de dichos datos. Sin embargo, tal disposición no se opone a dicha comunicación en el supuesto de que se efectuara al amparo del Derecho nacional y cumpliendo los requisitos fijados en esa disposición (apartados 27 y 34 y fallo).

En este contexto, el Tribunal de Justicia indicó que, sin perjuicio de las comprobaciones que deba realizar al respecto el juez nacional, en circunstancias tales como las del asunto principal no parece justificado que, por ser el causante del daño menor de edad, se deniegue a la víctima la comunicación de los datos personales necesarios para interponer una demanda indemnizatoria contra dicho causante o, en su caso, contra quien ejerza la patria potestad (apartado 33).

Sentencia de 27 de septiembre de 2017, Puškár (C-73/16, EU:C:2017:725)

En el litigio principal, el Sr. Peter Puškár había interpuesto un recurso ante el Najvyšší súd Slovenskej republiky (Tribunal Supremo de la República Eslovaca) en el que solicitaba que se ordenase a la Finančné riaditel'stvo (Dirección de Tributos), a todas las delegaciones de Hacienda dependientes de ella y al Kriminálny úrad finančnej správy (Unidad de Delitos de la Administración Tributaria) que no incluyeran su nombre en la lista de personas que la Dirección de Tributos considera testaferros, lista elaborada por dicho organismo a efectos recaudatorios y de cuya actualización se ocupan la propia Dirección y la Unidad de Delitos de la Administración Tributaria (en lo sucesivo, «la lista controvertida»). Además, había solicitado que se eliminara toda mención de su nombre en dichas listas y en el sistema informático de las autoridades financieras.

En estas circunstancias, el Najvyšší súd Slovenskej republiky (Tribunal Supremo de la República Eslovaca) planteó al Tribunal de Justicia la cuestión, entre otras, de si el derecho al respeto de la vida privada y familiar, del domicilio y las comunicaciones, consagrado en el artículo 7, y el derecho a la protección de los datos de carácter personal, consagrado en el artículo 8 de la Carta, podían interpretarse en el sentido de que no permiten que un Estado miembro elabore, sin el consentimiento de la persona interesada, listas de datos personales a efectos recaudatorios, es decir, en el sentido de que la obtención de datos personales por parte de las autoridades públicas para combatir el fraude fiscal constituye en sí misma un riesgo.

El Tribunal de Justicia declaró que el artículo 7, letra e), de la Directiva 95/46 no se opone a que, sin que medie el consentimiento de los interesados, las autoridades de los Estados miembros traten datos personales a efectos de recaudación y de lucha contra el fraude fiscal, tal como se hizo en el litigio principal mediante la elaboración de la lista controvertida, siempre que, por un lado, la normativa nacional confiera a dichas autoridades misiones de interés público en el sentido de dicha disposición, que la elaboración de la lista y la inclusión en la misma de los interesados sean efectivamente idóneas y necesarias para cumplir los objetivos perseguidos y que existan motivos suficientes para presumir que la inclusión de los interesados en la lista obedece a un motivo y siempre que, por otro lado, concurran todas las condiciones a que obliga la propia Directiva 95/46 para que ese tratamiento de datos personales sea lícito (apartado 117 y punto 3 del fallo).

A este respecto, el Tribunal de Justicia señaló que corresponde al tribunal nacional comprobar si la elaboración de la lista controvertida resulta necesaria para el cumplimiento de las misiones de interés público de que se trata en el asunto principal, teniendo en cuenta en particular la finalidad exacta de la elaboración de la lista, los efectos jurídicos a los que quedan sometidas las personas que figuran en ella y si la lista misma es o no pública. Además, con arreglo al principio de proporcionalidad, corresponde al tribunal nacional comprobar si la elaboración de la lista

controvertida y la inclusión en ella de los interesados son adecuadas para cumplir los objetivos que persiguen y si no existen medios menos gravosos para alcanzarlos (apartados 111, 112 y 113).

Además, el Tribunal de Justicia constató que el hecho de que una persona esté incluida en la lista controvertida es algo que puede lesionar algunos de sus derechos, puesto que podría dañar su buen nombre y afectar a sus relaciones con las autoridades tributarias. Podría también afectar a su presunción de inocencia (derecho plasmado en el artículo 48, apartado 1, de la Carta) y a la libertad de empresa (reflejada en el artículo 16 del mismo texto) de las personas jurídicas relacionadas con las personas físicas incluidas en la lista controvertida. Por consiguiente, esa lesión de sus derechos solo será razonable si existen motivos suficientes para sospechar que el interesado ocupa puestos directivos ficticios en las personas jurídicas con las que se le relaciona, por lo que está perjudicando la recaudación y la lucha contra el fraude fiscal (apartado 114).

Por otra parte, el Tribunal de Justicia estimó que si al amparo del artículo 13 de la Directiva 95/46 existieran motivos para limitar algunos de los derechos establecidos en los artículos 6 y 10 a 12 de dicha Directiva, como el derecho de información del interesado, tal limitación debería ser necesaria para la salvaguardia de alguno de los intereses mencionados en el apartado 1 del propio artículo 13, como por ejemplo un interés económico y financiero importante en asuntos fiscales, y además debería basarse en medidas legales (apartado 116).

Sentencia de 11 de noviembre de 2020, Orange Romania (C-61/19, EU:C:2020:901)

Orange România presta servicios de telecomunicaciones móviles en el mercado rumano. El 28 de marzo de 2018, la Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Autoridad Nacional de Supervisión del Tratamiento de Datos Personales, Rumanía) le impuso una multa por recoger y conservar copias de los documentos de identidad de sus clientes sin el consentimiento expreso de estos.

Según la ANSPDCP, durante el período comprendido entre el 1 y el 26 de marzo de 2018, Orange România celebró contratos de prestación de servicios de telecomunicaciones móviles que incluyen una cláusula en virtud de la cual los clientes han sido informados y han prestado su consentimiento para la recogida y la conservación de una copia de su documento de identidad a efectos de su identificación. El responsable del tratamiento marcó la casilla correspondiente a esta cláusula antes de la firma del contrato.

En este contexto, el Tribunalul București (Tribunal de Distrito de Bucarest, Rumanía) solicitó al Tribunal de Justicia que aclarase las condiciones en que puede considerarse válido el consentimiento de los clientes para el tratamiento de sus datos personales.

El Tribunal de Justicia recuerda, en primer lugar, que el Derecho de la Unión [31] establece una lista de los casos en que un tratamiento de datos personales puede considerarse lícito. En particular, el consentimiento del interesado ha de ser libre, específico, informado e

[31] Artículo 7 de la Directiva 95/46 y artículo 6 del RGPD.

inequívoco. [32] A este respecto, el consentimiento no se presta válidamente en caso de silencio, de casillas marcadas por defecto o de inacción (apartados 34, 36, 37 y 39).

Además, cuando el consentimiento del interesado se preste en el contexto de una declaración escrita que también se refiera a otros asuntos, dicha declaración debe presentarse de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. Para garantizar al interesado una verdadera libertad de elección, las estipulaciones contractuales no deben inducirle a error en lo que respecta a la posibilidad de celebrar el contrato pese a negarse a dar su consentimiento para el tratamiento de sus datos (apartados 34, 36, 37, 39 y 41).

El Tribunal de Justicia precisa que, al ser Orange România el responsable del tratamiento de los datos personales, debe estar en condiciones de demostrar la licitud del tratamiento de esos datos y, por lo tanto, en este caso, la existencia de un consentimiento válido de sus clientes. A este respecto, dado que no parece que los propios clientes interesados marcasen la casilla relativa a la recogida y conservación de las copias de su documento de identidad, el mero hecho de que esa casilla se marcase no demuestra que exista una manifestación afirmativa de su consentimiento. Corresponde al órgano jurisdiccional nacional efectuar las comprobaciones oportunas a tal efecto (apartados 42 y 46).

Corresponde asimismo al órgano jurisdiccional remitente, según el Tribunal de Justicia, apreciar si las estipulaciones contractuales controvertidas podían o no inducir a error al interesado en cuanto a la posibilidad de celebrar el contrato pese a no consentir en el tratamiento de sus datos, ya que no se precisa esta posibilidad. Además, en caso de que un cliente se negase a prestar su consentimiento para el tratamiento de sus datos, el Tribunal de Justicia observa que Orange România le exigía declarar por escrito que no consentía en la obtención ni en la conservación de la copia de su documento de identidad. Según el Tribunal de Justicia, tal requisito adicional puede afectar indebidamente a la libre elección de oponerse a esa obtención y esa conservación. En cualquier caso, dado que dicha sociedad está obligada a demostrar que sus clientes han manifestado su consentimiento para el tratamiento de sus datos personales mediante un comportamiento activo, no puede exigirles que manifiesten su negativa de manera activa (apartados 49 a 51).

El Tribunal de Justicia concluye por lo tanto que un contrato relativo a la prestación de servicios de telecomunicaciones que contiene una cláusula conforme a la cual el interesado ha sido informado y ha consentido en la obtención y la conservación de una copia de su documento de identidad con fines de identificación no permite demostrar que esa persona haya dado válidamente su consentimiento para dicha obtención y dicha conservación cuando la casilla referente a dicha cláusula haya sido marcada por el responsable del tratamiento de datos antes de la firma del contrato, cuando las estipulaciones contractuales de dicho contrato puedan inducir al interesado a error sobre la posibilidad de celebrar el contrato en cuestión pese a negarse a consentir en el tratamiento de sus datos, o cuando la libre elección de oponerse a dicha obtención y dicha conservación se vea indebidamente obstaculizada por ese responsable, al exigir que el interesado, para negarse a dar su consentimiento, cumplimente un formulario adicional en el que haga constar esa negativa (apartado 52 y fallo).

[32] Artículo 2, letra h), de la Directiva 95/46 y artículo 4, punto 11, del RGPD.

Sentencia de 12 de mayo de 2021 (Gran Sala), Bundesrepublik Deutschland (Notificación roja de Interpol) (C-505/19, EU:C:2021:376)

En 2012, la Organización Internacional de Policía Criminal (en lo sucesivo, «Interpol») publicó, a petición de los Estados Unidos y sobre la base de una orden de detención dictada por las autoridades de este país, una notificación roja referida a WS, de nacionalidad alemana, con miras a su eventual extradición. Cuando se localiza en un Estado afiliado a Interpol a una persona objeto de una notificación roja, ese Estado debe, en principio, proceder a su detención preventiva o a vigilarla o limitar sus desplazamientos.

No obstante, antes de que se publicase dicha notificación roja, se había incoado contra WS en Alemania un procedimiento de investigación referido, según el órgano jurisdiccional remitente, a los mismos hechos que aquellos en los que se basaba dicha notificación roja. Este procedimiento se archivó con carácter firme en 2010, una vez que WS hubo abonado una determinada cantidad dineraria, acogiéndose a un procedimiento específico de transacción previsto en el Derecho penal alemán. Posteriormente, el Bundeskriminalamt (Oficina Federal de Policía Criminal, Alemania) informó a Interpol de que consideraba que, a la vista de ese procedimiento anterior, el principio *non bis in idem* era aplicable al presente asunto. Este principio, consagrado tanto en el artículo 54 del Convenio de aplicación del Acuerdo de Schengen [33] como en el artículo 50 de la Carta, prohíbe, en particular, que una persona que ya haya sido juzgada por sentencia firme sea procesada de nuevo por el mismo delito.

En 2017, WS interpuso un recurso contra la República Federal de Alemania ante el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania) con la pretensión de que se ordenara a esta adoptar las medidas necesarias para la retirada de la notificación roja. A este respecto, WS invoca, además de la violación del principio *non bis in idem*, la violación de su derecho a la libre circulación, garantizado por el artículo 21 TFUE, dado que no puede desplazarse a los Estados parte en el Acuerdo de Schengen o a los Estados miembros sin correr el riesgo de ser detenido. Aduce asimismo que, debido a estas violaciones, el tratamiento de sus datos personales consignados en la notificación roja es contrario a la Directiva 2016/680, relativa a la protección de los datos personales en materia penal. [34]

En este contexto, el Tribunal de lo Contencioso-Administrativo de Wiesbaden decidió consultar al Tribunal de Justicia sobre la aplicación del principio *non bis in idem* y, más concretamente, sobre la posibilidad de que se proceda a la detención preventiva de una persona objeto de una notificación roja en una situación como esta. Además, en caso de que este principio sea aplicable, el órgano jurisdiccional remitente desea que se dilucide qué consecuencias se

[33] Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la Supresión Gradual de los Controles en las Fronteras Comunes (DO 2000, L 239, p. 19; en lo sucesivo, «CAAS»).

[34] 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 Decisión 2008/977/JAI (DO 2016, L 119, p. 89).

derivarían para el tratamiento por parte de los Estados miembros de los datos personales consignados en tal notificación.

En su sentencia pronunciada en Gran Sala, el Tribunal de Justicia declara, entre otros extremos, que las disposiciones de la Directiva 2016/680, a la luz del artículo 54 del CAAS y del artículo 50 de la Carta, deben interpretarse en el sentido de que no se oponen al tratamiento de los datos personales consignados en una notificación roja emitida por Interpol mientras no se haya determinado, mediante una resolución judicial firme, que el principio *non bis in idem* es aplicable a los hechos en los que dicha notificación se basa, siempre y cuando dicho tratamiento cumpla los requisitos establecidos por esta Directiva (apartado 121 y punto 2 del fallo).

En lo referente a la cuestión de los datos personales consignados en una notificación roja de Interpol, el Tribunal de Justicia indica que toda operación realizada sobre tales datos, como su registro en los ficheros de búsqueda de un Estado miembro, constituye un «tratamiento» comprendido en la Directiva 2016/680. [35] Estima además, por un lado, que ese tratamiento persigue un fin legítimo y, por otro, que no puede considerarse ilícito solamente porque el principio *non bis in idem* pudiera resultar aplicable a los hechos en que se basa la notificación roja. [36] Por añadidura, tal tratamiento por parte de las autoridades de los Estados miembros puede resultar indispensable precisamente para comprobar si dicho principio resulta aplicable (apartados 111, 114, 116, 117 y 119).

En estas circunstancias, el Tribunal de Justicia declara, asimismo, que la Directiva 2016/680, a la luz del artículo 54 del CAAS y del artículo 50 de la Carta, no se opone al tratamiento de los datos personales que figuran en una notificación roja mientras no se haya determinado en una resolución judicial firme que el principio *non bis in idem* resulta aplicable al caso. No obstante, tal tratamiento debe respetar los requisitos establecidos en dicha Directiva. Desde esta perspectiva, en particular, debe ser necesario para la realización de una tarea efectuada por una autoridad nacional competente para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales [37] (apartado 121 y punto 2 del fallo).

En cambio, cuando el principio *non bis in idem* resulta aplicable, ya no es necesario registrar en los ficheros de búsqueda de los Estados miembros datos personales consignados en una notificación roja de Interpol, puesto que tal persona ya no puede ser objeto de diligencias penales por los hechos a los que se refiere dicha notificación roja y, en consecuencia, ser detenida por esos hechos. De ello se sigue que esa persona debe poder exigir la supresión de sus datos. Si no obstante se mantiene este registro, debe acompañarse de la indicación de que esa persona no puede volver a ser perseguida en un Estado miembro o en un Estado contratante por los mismos hechos, por encontrarse protegida por el principio *non bis in idem* (apartado 120).

35 Véanse los artículos 2, apartado 1, y 3, punto 2, de la Directiva 2016/680.
36 Véanse los artículos 4, apartado 1, letra b), y 8, apartado 1, de la Directiva 2016/680.
37 Véanse el artículo 1, apartado 1, y el artículo 8, apartado 1, de la Directiva 2016/680.

Sentencia de 22 de junio de 2021 (Gran Sala), Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504)

En esta sentencia (véase asimismo la sección II.3, titulada «Concepto de "tratamiento de datos personales"»), el Tribunal de Justicia declara que el RGPD se opone a la normativa que obliga a la Ceļu satiksmes drošības direkcija (Dirección de seguridad vial, Letonia; en lo sucesivo, «CSDD») a establecer que los datos relativos a los puntos impuestos por infracciones de tráfico sean accesibles al público, sin que la persona que solicita el acceso tenga que justificar un interés específico en obtenerlos. Señala que no se ha demostrado la necesidad, en particular en relación con el objetivo de mejorar la seguridad vial invocado por el Gobierno letón, de una comunicación de datos personales relativos a puntos impuestos por infracciones de tráfico. Además, según el Tribunal de Justicia, ni el derecho del público a acceder a documentos oficiales ni el derecho a la libertad de información justifican tal normativa (apartados 113, 120 a 122 y punto 2 del fallo).

En este contexto, el Tribunal de Justicia subraya que la mejora de la seguridad vial que persigue la normativa letona es un objetivo de interés general reconocido por la Unión y que, por tanto, los Estados miembros pueden calificar la seguridad vial de «misión realizada en interés público». [38] Sin embargo, no se ha demostrado la necesidad del régimen letón de comunicación de datos personales relativos a los puntos para lograr el objetivo perseguido. En efecto, por una parte, el legislador letón dispone de numerosas vías de acción que le habrían permitido alcanzar este objetivo por otros medios menos atentatorios contra los derechos fundamentales de las personas afectadas. Por otra parte, deben tenerse en cuenta el carácter sensible de los datos relativos a los puntos y el hecho de que su comunicación al público puede constituir una injerencia grave en los derechos al respeto de la vida privada y a la protección de los datos personales, ya que puede provocar la desaprobación de la sociedad y conllevar la estigmatización de la persona afectada (apartados 109 a 113).

Además, el Tribunal de Justicia considera que, habida cuenta del carácter sensible de estos datos y de la gravedad de la injerencia en esos dos derechos fundamentales, dichos derechos prevalecen tanto sobre el interés del público en tener acceso a documentos oficiales, por ejemplo el registro nacional de vehículos y conductores, como sobre el derecho a la libertad de información (apartados 120 y 121).

Por otra parte, por idénticas razones, el Tribunal de Justicia declara que el RGPD se opone también a la normativa letona en la medida en que autoriza a la CSDD a comunicar los datos relativos a los puntos impuestos a conductores por infracciones de tráfico a operadores económicos para que estos puedan reutilizarlos y comunicarlos al público (apartado 126 y punto 3 del fallo).

Por último, el Tribunal de Justicia precisa que el principio de primacía del Derecho de la Unión se opone a que el órgano jurisdiccional remitente, que conoce del recurso interpuesto contra la normativa letona, calificada por el Tribunal de Justicia de incompatible con el Derecho de la

[38] En virtud del artículo 6, apartado 1, letra e), del RGPD, el tratamiento de datos personales será lícito cuando sea «necesario para el cumplimiento de una misión realizada en interés público [...]».

Unión, decida mantener los efectos jurídicos de dicha normativa hasta la fecha en que dicho órgano jurisdiccional remitente dicte sentencia firme (apartado 137 y punto 4 del fallo).

III. Tratamientos de datos personales con arreglo a la Directiva 2002/58

Sentencia de 2 de octubre de 2018 (Gran Sala), Ministerio Fiscal (C-207/16, EU:C:2018:788) [39]

El objeto de este asunto era la denegación por parte de un juez de instrucción español de una solicitud presentada en el contexto de una investigación sobre un robo con violencia de una cartera y un teléfono móvil. Más concretamente, la policía judicial había solicitado a dicho juez que le concediese acceso a los datos identificativos de los usuarios de los números de teléfono activados desde el teléfono robado durante un período de doce días desde la fecha del robo. La negativa se había basado en que los hechos que motivaron las diligencias penales no eran constitutivos de delito grave —esto es, según el Derecho español, un delito sancionado con pena de prisión superior a cinco años—; siendo así que el acceso a los datos identificativos únicamente es posible en este tipo de delitos.

Tras haber recordado que el acceso de autoridades públicas a los datos personales conservados por proveedores de servicios de comunicaciones electrónicas, en el marco de un procedimiento de instrucción penal está incluido en el ámbito de aplicación de la Directiva 2002/58, el Tribunal de Justicia declaró que el acceso a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, tales como los nombres y apellidos y, en su caso, direcciones de esos titulares, constituye una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, consagrados por la Carta, aun a falta de circunstancias que permitan calificar dicha 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. No obstante, el Tribunal de Justicia subrayó que esa injerencia 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 efecto, si bien la Directiva 2002/58 enumera de forma exhaustiva los objetivos que pueden justificar una norma nacional que regule el acceso de las autoridades públicas a los datos en cuestión y que, por tanto, establezca una excepción al principio de confidencialidad de las comunicaciones electrónicas, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de esos objetivos, el Tribunal de Justicia observa que, por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, el tenor 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 (apartados 38, 42, 59 a 63 y fallo).

En este contexto, el Tribunal de Justicia precisó que si bien, en su sentencia Tele2 Sverige y Watson y otros, [40] había declarado que solo la lucha contra la delincuencia grave puede

[39] Esta sentencia fue mencionada en el Informe Anual de 2018, pp. 88 y 89.

justificar un acceso de las autoridades públicas 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, tal interpretación estaba motivada 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. Por lo tanto, conforme al principio de proporcionalidad, una injerencia grave solo puede justificarse en este ámbito por el objetivo de luchar contra la delincuencia que a su vez deba calificarse de «grave». En cambio, cuando la injerencia no es grave, el referido acceso puede estar justificado por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general (apartados 54 a 57).

Por lo que respecta a este caso concreto, el Tribunal de Justicia consideró que el acceso limitado únicamente a los datos cubiertos por la solicitud controvertida no podía calificarse de injerencia «grave» en los derechos fundamentales de los individuos cuyos datos se veían afectados, puesto que esos datos no permitían extraer conclusiones precisas sobre su vida privada. El Tribunal de Justicia concluyó que la injerencia que supondría el acceso a tales datos podía estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general, sin que fuese necesario que dichos delitos estuviesen calificados como «graves» (apartados 61 y 62).

Sentencias de 6 de octubre de 2020 (Gran Sala), Privacy International (C-623/17, EU:C:2020:790) y La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791)[41]

La jurisprudencia relativa a la conservación y el acceso a los datos personales en el ámbito de las comunicaciones electrónicas, en particular la sentencia Tele2 Sverige y Watson y otros, en la que el Tribunal de Justicia consideró que los Estados miembros no podían imponer a los proveedores de servicios de comunicaciones electrónicas una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización, suscitó las preocupaciones de algunos Estados, que temieron haber sido privados de un instrumento que consideran necesario para proteger la seguridad nacional y luchar contra la delincuencia.

Con este trasfondo se sometieron al Investigatory Powers Tribunal (Tribunal de las Facultades de Investigación, Reino Unido) (Privacy International, C-623/17), al Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia) (La Quadrature du Net y otros, asuntos acumulados C-511/18 y C-512/18) y a la Cour constitutionnelle (Tribunal Constitucional, Bélgica) (Ordre des barreaux francophones et germanophone y otros, C-520/18) varios litigios relativos a la legalidad de las normativas adoptadas por algunos Estados miembros en estos ámbitos, que establecían, en particular, la obligación de que los proveedores de servicios de comunicaciones electrónicas transmitieran a una autoridad pública o conservaran de manera generalizada e indiferenciada los datos de tráfico y de localización de los usuarios.

Mediante dos sentencias dictadas en Gran Sala, el 6 de octubre de 2020, el Tribunal de Justicia declara, en primer lugar, que la Directiva 2002/58 se aplica a normativas nacionales que obligan a los proveedores de servicios de comunicaciones electrónicas a conservar datos de tráfico y

[40] Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, *Tele2 Sverige y Watson y otros* (C-203/15 y C-698/15, EU:C:2016:970).
[41] Estas sentencias fueron mencionadas en el Informe Anual de 2020, pp. 29 a 32.

localización o a transmitirlos a las autoridades nacionales de seguridad e inteligencia a efectos de la protección de la seguridad nacional y de la lucha contra la delincuencia (apartado 49 y punto 1 del fallo de la sentencia Privacy International y apartado 104 de la sentencia La Quadrature de Net y otros).

A continuación, el Tribunal de Justicia recuerda que la Directiva 2002/58 [42] no permite que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y a la prohibición de almacenar esos datos se convierta en la regla. Esto implica que dicha Directiva únicamente autoriza a los Estados miembros a adoptar, entre otros con fines de seguridad nacional, medidas legales para limitar el alcance de los derechos y obligaciones contemplados en la propia Directiva, en particular la obligación de garantizar la confidencialidad de las comunicaciones y de los datos de tráfico, [43] que sean conformes con los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y con los derechos fundamentales garantizados por la Carta [44] (apartados 59 y 60 de la sentencia Privacy International y apartados 111 y 113 de la sentencia La Quadrature du Net y otros).

En este contexto, el Tribunal de Justicia considera, por una parte, en el asunto Privacy International, que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, con el fin de proteger la seguridad nacional, la transmisión generalizada e indiferenciada a las agencias de seguridad e información de los datos de tráfico y de localización. Por otra parte, en los asuntos acumulados La Quadrature du Net y otros, así como en el asunto Ordre des barreaux francophones et germanophone y otros, el Tribunal de Justicia estima que esta misma Directiva se opone a medidas legislativas que imponen a los proveedores de servicios de comunicaciones electrónicas, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización.

En efecto, estas obligaciones de transmisión y de conservación generalizada e indiferenciada de tales datos constituyen injerencias especialmente graves en los derechos fundamentales garantizados por la Carta, sin que el comportamiento de las personas cuyos datos se ven afectados guarde relación alguna con el objetivo perseguido por la normativa controvertida. De manera análoga, el Tribunal de Justicia interpreta el artículo 23, apartado 1, del RGPD, a la luz de la Carta, en el sentido de que se opone a una normativa nacional que obliga a los proveedores de acceso a servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la conservación generalizada e indiferenciada, en particular, de los datos personales relativos a dichos servicios (apartados 71 y 82 y punto 2 del fallo de la sentencia Privacy International y apartados 146, 168, 174, 177 y 212 y puntos 1 y 3 del fallo de la sentencia La Quadrature du Net y otros).

En cambio, el Tribunal de Justicia estima que, en situaciones en las que el Estado miembro se enfrente a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a que se obligue a los

[42] Artículo 15, apartados 1 y 3, de la Directiva 2002/58.
[43] Artículo 5, apartado 1, de la Directiva 2002/58.
[44] En particular, los artículos 7, 8 y 11 así como el artículo 52, apartado 1, de la Carta.

proveedores de servicios de comunicaciones electrónicas a conservar de manera generalizada e indiferenciada datos de tráfico y de localización. En este contexto, el Tribunal de Justicia señala que la decisión que establezca dicho requerimiento, para un período temporalmente limitado a lo estrictamente necesario, debe ser objeto de un control efectivo, bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya resolución tenga efecto vinculante, con el fin de comprobar la existencia de una de esas situaciones y el cumplimiento de los requisitos y garantías previstos. En estas mismas condiciones, la Directiva tampoco se opone al análisis automatizado de los datos, en particular de los datos de tráfico y de localización, de todos los usuarios de comunicaciones electrónicas (apartados 137 a 139, 177 a 179 y puntos 1 y 2 del fallo de la sentencia La Quadrature du Net y otros).

El Tribunal de Justicia añade que la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a medidas legislativas que permitan el recurso a una conservación selectiva, temporalmente limitada a lo estrictamente necesario, de los datos de tráfico y de localización, que se delimite, sobre la base de criterios objetivos y no discriminatorios, en función de categorías de personas afectadas o mediante un criterio geográfico. Asimismo, esta Directiva no se opone a medidas de esta índole que dispongan una conservación generalizada e indiferenciada de las direcciones IP atribuidas a la fuente de una comunicación, siempre que el período de conservación se limite a lo estrictamente necesario, ni a las que dispongan esa conservación de los datos relativos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas. En este último caso, los Estados miembros no están obligados a limitar temporalmente la conservación. Por otra parte, dicha Directiva no se opone a una medida legislativa que permita el recurso a una conservación rápida de los datos de que dispongan los proveedores de servicios cuando se produzcan situaciones en las que resulte necesario conservar dichos datos más allá de los plazos legales de conservación de estos con el fin de esclarecer infracciones penales graves o atentados contra la seguridad nacional, cuando la comisión de tales infracciones o atentados ya haya quedado acreditada o cuando su existencia pueda sospecharse razonablemente (apartados 161, 163 y 168, y punto 1 del fallo de la sentencia La Quadrature du Net y otros).

Asimismo, el Tribunal de Justicia declara que la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas la obligación de recurrir a la recopilación en tiempo real, en particular, de los datos de tráfico y de localización, cuando esa recopilación se limite a las personas de las que se sospeche fundadamente que están implicadas de un modo u otro en actividades terroristas y esté sujeta a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, con el fin de garantizar que dicha recopilación en tiempo real únicamente se autoriza dentro de los límites de lo estrictamente necesario. En caso de urgencia, el control debe efectuarse en breve plazo (apartado 192 y punto 2 del fallo de la sentencia La Quadrature du Net y otros).

Por último, el Tribunal de Justicia aborda la cuestión del mantenimiento de los efectos en el tiempo de una normativa nacional declarada incompatible con el Derecho de la Unión. A este respecto, considera que un órgano jurisdiccional nacional no puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le incumbe, en relación con una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e

indiferenciada de los datos de tráfico y de localización, considerada incompatible con la Directiva 2002/58, interpretada a la luz de la Carta.

Dicho esto, para dar una respuesta útil al órgano jurisdiccional nacional, el Tribunal de Justicia recuerda que la admisibilidad y la apreciación de las pruebas obtenidas mediante una conservación de datos contraria al Derecho de la Unión, en un proceso penal incoado contra sospechosos de delitos graves, se rigen, en el estado actual del Derecho de la Unión, únicamente por el Derecho nacional. No obstante, el Tribunal de Justicia precisa que la Directiva 2002/58, interpretada a la luz del principio de efectividad, exige que el juez penal nacional excluya las pruebas obtenidas mediante una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de tal proceso penal, si las personas sospechosas de haber cometido delitos no pueden pronunciarse eficazmente sobre esas pruebas (apartados 222 y 228 y punto 4 del fallo de la sentencia La Quadrature du Net y otros).

Sentencia de 2 de marzo de 2021 (Gran Sala), Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, EU:C:2021:152)

En Estonia se incoó un proceso penal contra H. K. por los cargos de robo, utilización de la tarjeta bancaria de un tercero y violencia contra los intervinientes en un procedimiento judicial. Por estos delitos, H. K. fue condenada por un tribunal de primera instancia a una pena privativa de libertad de dos años, sentencia que fue posteriormente confirmada en apelación. Los atestados en los que se basa la apreciación de esos delitos fueron redactados, en particular, sobre la base de datos personales generados en el marco de la prestación de servicios de comunicaciones electrónicas. El Riigikohus (Tribunal Supremo, Estonia), ante el que H. K. interpuso un recurso de casación, albergaba dudas en cuanto a la compatibilidad con el Derecho de la Unión [45] de las condiciones en las que los servicios de investigación tuvieron acceso a esos datos.

Estas dudas se refieren, en primer lugar, a si la duración del período en el que los servicios de investigación tuvieron acceso a los datos constituye un criterio que permita evaluar la gravedad de la injerencia de dicho acceso en los derechos fundamentales de las personas afectadas. Así, cuando ese período es muy breve o la cantidad de datos recogidos es muy limitada, el tribunal remitente se preguntaba si el objetivo de lucha contra la delincuencia en general, y no solo de lucha contra la delincuencia grave, puede justificar tal injerencia. En segundo lugar, el tribunal remitente albergaba dudas sobre la posibilidad de considerar al Ministerio Fiscal estonio, habida cuenta de las distintas funciones que le atribuye la normativa nacional, una autoridad administrativa «independiente», en el sentido de la sentencia Tele2 Sverige y Watson y otros, [46] que pueda autorizar el acceso de la autoridad investigadora a los datos en cuestión.

Mediante su sentencia, pronunciada en Gran Sala, el Tribunal de Justicia declara que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a una normativa nacional que autoriza el acceso de las autoridades públicas a datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación

[45] Más concretamente, con el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8 y 11, así como del artículo 52, apartado 1, de la Carta.

[46] Sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970, apartado 120).

electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública. Según el Tribunal de Justicia, la duración del período para el que se solicite acceder a esos datos y la cantidad o naturaleza de los datos disponibles en ese período es irrelevante al respecto. Además, el Tribunal de Justicia considera que esa Directiva, en relación con la Carta, se opone a una normativa nacional que atribuye competencia al Ministerio Fiscal para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización con el fin de realizar la instrucción penal (apartados 45 y 59 y puntos 1 y 2 del fallo).

En lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos pretendido por la normativa controvertida, de conformidad con el principio de proporcionalidad, el Tribunal de Justicia considera que solo los objetivos de lucha contra la delincuencia grave o de prevención de las amenazas graves contra la seguridad pública pueden justificar el acceso de las autoridades públicas a un conjunto de datos de tráfico o de localización que puedan permitir extraer conclusiones precisas sobre la vida privada de las personas afectadas, sin que otros factores relativos a la proporcionalidad de la solicitud de acceso, como la duración del período para el que se solicita el acceso a tales datos, puedan conllevar que el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general justifique tal acceso (apartados 33 y 35).

Por lo que respecta a la competencia atribuida al Ministerio Fiscal para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización con el fin de dirigir la instrucción penal, el Tribunal de Justicia recuerda que corresponde al Derecho nacional determinar los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos de que disponen. No obstante, para cumplir el requisito de proporcionalidad, una normativa de este tipo debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger de manera eficaz esos datos contra los riesgos de abuso. Dicha normativa debe ser legalmente imperativa en Derecho interno e indicar en qué circunstancias y con arreglo a qué requisitos materiales y procedimentales puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario (apartado 48).

Según el Tribunal de Justicia, para garantizar en la práctica el íntegro cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados se supedite a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se dicte a raíz de una solicitud motivada de dichas autoridades presentada, en particular, en el marco de procedimientos de prevención, descubrimiento y persecución de delitos. En caso de urgencia debidamente justificada, el control debe efectuarse en breve plazo (apartado 51).

A este respecto, el Tribunal de Justicia precisa que el control previo requiere, entre otras cosas, que el órgano jurisdiccional o la entidad encargada de efectuar dicho control disponga de todas

las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses y derechos de que se trate. En el caso concreto de la investigación penal, tal control exige que ese órgano jurisdiccional o esa entidad esté en condiciones de ponderar adecuadamente, por una parte, los intereses relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso. Cuando dicho control no lo lleve a cabo un órgano jurisdiccional sino una entidad administrativa independiente, esta debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad, y, para ello, ha de estar a resguardo de toda influencia externa (apartados 52 y 53).

Según el Tribunal de Justicia, de ello resulta que el requisito de independencia que debe cumplir la autoridad que ejerce el control previo obliga a que dicha autoridad tenga la condición de tercero respecto de la que solicita el acceso a los datos, de modo que la primera pueda ejercer ese control con objetividad e imparcialidad, y a resguardo de toda influencia externa. En particular, en el ámbito penal, el requisito de independencia implica que la autoridad que ejerce ese control previo, por una parte, no esté implicada en la realización de la investigación penal de que se trate y, por otra parte, que tenga una posición neutral frente a las partes del procedimiento penal. Sin embargo, no ocurre así con un Ministerio Fiscal, como el Ministerio Fiscal estonio, que dirige el procedimiento de investigación y ejerce, en su caso, la acusación pública. De ello se deduce que el Ministerio Fiscal no puede llevar a cabo ese control previo (apartados 54, 55 y 57).

IV. Transferencia de los datos personales a países terceros

Sentencia de 6 de noviembre de 2003 (Gran Sala), Lindqvist (C-101/01, EU:C:2003:596) [47]

En este asunto (véase también la sección II.3, titulada «Concepto de "tratamiento de datos personales"»), el órgano jurisdiccional remitente deseaba saber, entre otras cosas, si la Sra. Lindqvist había realizado una transferencia de datos a un país tercero en el sentido de dicha Directiva.

El Tribunal de Justicia declaró que no existe una «transferencia de datos a un país tercero» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio de Internet en el que se puede consultar la página web y que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros (apartado 71 y punto 4 del fallo).

En efecto, teniendo en cuenta, por un lado, el estado de desarrollo de Internet en el momento de la elaboración de la Directiva 95/46 y, por otro, la inexistencia de criterios aplicables al uso de

[47] Esta sentencia fue mencionada en el Informe Anual de 2003, p. 67.

Internet en su capítulo IV —al que pertenece dicho artículo 25—, dirigido a garantizar un control, por parte de los Estados miembros, de las transferencias de datos personales hacia países terceros y a prohibirlas cuando no ofrezcan un nivel de protección adecuado, no cabe presumir que el legislador comunitario tuviera la intención, en su momento, de incluir en el concepto de «transferencia de datos a un país tercero», la citada difusión de datos en una página web, ni siquiera cuando dichos datos estén al alcance de las personas de países terceros que dispongan de los medios técnicos para acceder a ellos (apartados 63, 64 y 68).

Sentencia de 6 de octubre de 2015 (Gran Sala), Schrems (C-362/14, EU:C:2015:650) [48]

El Sr. Schrems, ciudadano austriaco y usuario de la red social Facebook, había presentado una reclamación ante el Data Protection Commissioner (Comisario para la protección de datos, Irlanda) basada en que Facebook Ireland transfería a los Estados Unidos los datos personales de sus usuarios y los conservaba en servidores situados en ese país, donde eran objeto de tratamiento. Según el Sr. Schrems, el Derecho y las prácticas de Estados Unidos no garantizaban una protección suficiente contra la vigilancia, por parte de sus autoridades públicas, de los datos transferidos a ese país. El Data Protection Commissioner desestimó esa reclamación, en particular porque en su Decisión 2000/520/CE [49] la Comisión había estimado que, en el marco del régimen llamado de «puerto seguro» (en inglés, «safe harbour»), [50] Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos.

En este contexto, la High Court (Tribunal Superior, Irlanda) remitió al Tribunal de Justicia una petición de interpretación del artículo 25, apartado 6, de la Directiva 95/46, en virtud del cual la Comisión puede dictaminar que un tercer país garantiza un nivel de protección adecuado de los datos transferidos, así como, en esencia, una solicitud destinada a determinar la validez de la Decisión 2000/520, adoptada por la Comisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46.

El Tribunal de Justicia declaró inválida la Decisión de la Comisión en su conjunto, señalando, en primer lugar, que su adopción requería la constatación, debidamente motivada por la Comisión, de que el país tercero considerado garantiza efectivamente un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión. Ahora bien, como la Comisión no lo indicó así en la Decisión 2000/520, el artículo 1 de esta vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa. En efecto, los principios de «puerto seguro» son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión, sin que se exija que las autoridades públicas estadounidenses se sometan a esos principios. Además, la Decisión 2000/520 hace posibles injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos, sin contener

[48] Esta sentencia fue mencionada en el Informe Anual de 2015, p. 53.

[49] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO 2000, L 215, p. 7).

[50] El régimen de puerto seguro incluye una serie de principios relativos a la protección de los datos de carácter personal a los que se pueden adherir voluntariamente las empresas estadounidenses.

ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en esos derechos ni poner de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza (apartados 82, 87 a 89, 96 a 98 y punto 2 del fallo).

Además, el Tribunal de Justicia declaró inválido el artículo 3 de la Decisión 2000/520, en la medida en que este priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue factores que puedan afectar a la compatibilidad con la protección de la privacidad y los derechos y libertades fundamentales de las personas de una decisión de la Comisión que haya constatado que un país tercero garantiza un nivel de protección adecuado (apartados 102 a 104). El Tribunal llegó a la conclusión de que la invalidez de los artículos 1 y 3 de la Decisión 2000/520 tenía el efecto de afectar a la validez de esa Decisión en su conjunto (apartados 105 y 106).

En cuanto a la imposibilidad de justificar tal injerencia, el Tribunal observa, en primer lugar, que una normativa de la Unión que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de estos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ellos (apartado 91).

Además, y sobre todo, la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (apartado 92). Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización (apartado 93). En particular, una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada. De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta (apartados 94 y 95).

Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017 (Gran Sala) (EU:C:2017:592)

El 26 de julio de 2017, el Tribunal de Justicia se pronunció por primera vez sobre la compatibilidad de un proyecto de acuerdo internacional con la Carta de los Derechos

Fundamentales de la Unión Europea y, en particular, con las disposiciones relativas al respeto de la vida privada y a la protección de los datos personales.

La Unión Europea y Canadá negociaron un Acuerdo sobre el tratamiento y la transferencia de datos de los registros de nombres de los pasajeros (Acuerdo sobre los PNR) que se firmó en 2014. El Consejo de la Unión Europea solicitó su aprobación al Parlamento Europeo, y este decidió solicitar el dictamen del Tribunal de Justicia sobre si el Acuerdo previsto se ajustaba al Derecho de la Unión.

El Acuerdo previsto permite la transferencia sistemática y continuada de los datos de los PNR de la totalidad de los pasajeros aéreos a una autoridad canadiense para que los utilice y conserve, y para que eventualmente los transfiera con posterioridad a otras autoridades y a otros países terceros, con el fin de luchar contra el terrorismo y otros delitos graves de carácter transnacional. A tal efecto, el Acuerdo previsto establece un período de conservación de los datos de cinco años y una serie de requisitos en materia de seguridad y de integridad de los PNR, como el enmascaramiento inmediato de los datos sensibles, y reconoce derechos de acceso a los datos, de rectificación y de borrado, así como la posibilidad de interponer recursos administrativos o judiciales.

Los datos de los PNR contemplados en el acuerdo comprenden, en particular, además del nombre y la información de contacto del pasajero o pasajeros aéreos, la información necesaria para efectuar la reserva, como las fechas de viaje previstas y el itinerario del viaje, la información sobre el billete, los grupos de personas registrados con el mismo número de reserva, datos de pago y facturación, la información relativa al equipaje y observaciones generales relativas a los pasajeros.

En su dictamen, el Tribunal de Justicia estimó que el Acuerdo sobre los PNR no puede celebrarse en su forma actual, debido a la incompatibilidad de varias de sus disposiciones con los derechos fundamentales reconocidos por la Unión.

El Tribunal de Justicia afirmó, en primer lugar, que constituyen injerencias en el derecho garantizado en el artículo 7 de la Carta tanto la transferencia de los datos de los PNR de la Unión a la autoridad canadiense competente como el marco regulador negociado por la Unión con Canadá sobre los requisitos relativos a la conservación de esos datos, su utilización y sus posibles transferencias posteriores a otras autoridades canadienses, a Europol, a Eurojust, a las autoridades judiciales o policiales de los Estados miembros o a otras autoridades de otros países terceros. Dichas operaciones son asimismo constitutivas de una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta, puesto que constituyen tratamientos de datos de carácter personal (apartados 125 y 126).

Además, puso de relieve que, aun cuando algunos de los datos de los PNR, aisladamente considerados, no parezcan poder revelar información importante sobre la vida privada de las personas afectadas, no deja de ser cierto que, considerados en conjunto, dichos datos pueden revelar, entre otros extremos, un itinerario de viaje completo, hábitos de viaje, relaciones existentes entre dos o varias personas así como información sobre la situación económica de los pasajeros aéreos, sus hábitos alimentarios o su estado de salud, y podrían incluso proporcionar datos sensibles sobre dichos pasajeros, tal como se definen en el artículo 2,

letra e), del Acuerdo previsto (datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas, etc.) (apartado 128).

A este respecto, el Tribunal de Justicia estimó que, aunque las injerencias controvertidas puedan justificarse por la búsqueda de un objetivo de interés general (como el de garantizar la seguridad pública en el contexto de la lucha contra los delitos de terrorismo y los delitos graves de carácter transnacional), son varias las disposiciones del Acuerdo que no se limitan a lo estrictamente necesario ni establecen reglas claras y precisas.

En particular, el Tribunal de Justicia señaló que, habida cuenta del riesgo de un tratamiento de los datos contrario al principio de no discriminación, la transferencia de datos sensibles a Canadá exigiría una justificación concreta y particularmente sólida, basada en motivos distintos de la protección de la seguridad pública contra el terrorismo y los delitos graves de carácter transnacional, pero que en aquel caso no existía tal justificación. El Tribunal de Justicia dedujo de ello que las disposiciones del Acuerdo sobre la transferencia de datos sensibles a Canadá y sobre el tratamiento y la conservación de esos datos eran incompatibles con los derechos fundamentales (apartados 165 y 232).

En segundo lugar, el Tribunal de Justicia consideró que el almacenamiento continuado de los datos de los PNR de la totalidad de los pasajeros aéreos después de su partida de Canadá, permitido por el Acuerdo previsto, no se limitaba a lo estrictamente necesario. En efecto, en lo que se refiere a los pasajeros aéreos respecto de los cuales no se haya identificado un riesgo en materia de terrorismo o de delincuencia grave de carácter transnacional a su llegada a Canadá ni hasta que partan de ese país, no parece que exista, después de que esos pasajeros hayan abandonado el país, relación alguna, ni siquiera indirecta, entre los datos de sus PNR y el objetivo perseguido por el Acuerdo previsto que pudiera justificar la conservación de esos datos. No obstante, en la medida en que se identifiquen, en casos particulares, elementos objetivos que permitan considerar que determinados pasajeros aéreos podrían, incluso después de su partida de Canadá, presentar un riesgo en términos de lucha contra el terrorismo y la delincuencia grave de carácter transnacional, el almacenamiento de los datos de los PNR de tales pasajeros parece admisible aun después de concluida su estancia en ese país, incluso durante un período de cinco años (apartados 205 a 207 y 209).

En tercer lugar, el Tribunal de Justicia indicó que el derecho fundamental al respeto de la vida privada, consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, conlleva que la persona de que se trate pueda cerciorarse de la exactitud y de la licitud del tratamiento de sus datos personales. Para poder efectuar las comprobaciones necesarias, esa persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento.

A este respecto subrayó que, en el Acuerdo previsto, es importante que los pasajeros sean informados de la transferencia de sus datos de los PNR al país tercero del que se trata y de la utilización de esos datos, siempre que tal comunicación no pueda perjudicar a las investigaciones llevadas a cabo por las autoridades públicas contempladas en el Acuerdo previsto. En efecto, tal información resulta, de hecho, necesaria para que los pasajeros aéreos puedan ejercer su derecho a solicitar el acceso a los datos de los PNR que les conciernan y, en su caso, su rectificación, así como a interponer, con arreglo al artículo 47, párrafo primero, de la Carta, un recurso efectivo ante un tribunal.

Así pues, en los supuestos en los que concurren circunstancias que justifican la utilización de los datos de los PNR para la lucha contra el terrorismo y los delitos graves de carácter transnacional y que requieren una autorización previa de una autoridad judicial o de una entidad administrativa independiente, la información individual de los pasajeros aéreos resulta necesaria. Lo mismo sucede en los casos en que los datos de los PNR de los pasajeros aéreos se comunican a otras autoridades públicas o a particulares. No obstante, únicamente debe proporcionarse tal información cuando no pueda perjudicar a las investigaciones llevadas a cabo por las autoridades públicas contempladas en el Acuerdo previsto (apartados 219, 220, 223 y 224).

Sentencia de 16 de julio de 2020 (Gran Sala), Facebook Ireland y Schrems (C-311/18, EU:C:2020:559) [51]

El RGPD dispone que la transferencia de tales datos hacia un país tercero únicamente puede efectuarse, en principio, cuando el país tercero de que se trate garantice un nivel de protección adecuado de los mismos. Según dicho Reglamento, la Comisión puede hacer constar que un país tercero garantiza, a la vista de su legislación interna o de sus compromisos internacionales, un nivel de protección adecuado. [52] A falta de esta decisión de adecuación, tal transferencia solo puede efectuarse si el exportador de los datos personales, establecido en la Unión, ofrece garantías adecuadas, que pueden resultar en particular de cláusulas tipo de protección de datos adoptadas por la Comisión, y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. [53] Por otra parte, el RGPD establece, de forma precisa, las condiciones en que puede efectuarse tal transferencia a falta de una decisión de adecuación o de garantías adecuadas. [54]

El Sr. Maximillian Schrems, nacional austriaco residente en Alemania, es usuario de Facebook desde 2008. Al igual que ocurre con los demás usuarios residentes en la Unión, los datos personales del Sr. Schrems se transfieren total o parcialmente a servidores pertenecientes a Facebook Inc., situados en el territorio de los Estados Unidos, donde son objeto de tratamiento. El Sr. Schrems presentó una reclamación ante la autoridad irlandesa de control con la finalidad esencial de que se prohibiesen tales transferencias. Afirmó que el Derecho y las prácticas de los Estados Unidos no ofrecían una protección suficiente contra el acceso, por parte de las autoridades públicas, a los datos trasferidos a ese país. La reclamación fue desestimada, debido, en particular, a que la Comisión había declarado, en su Decisión 2000/520, [55] que los Estados Unidos ofrecían un nivel adecuado de protección. Mediante sentencia dictada el 6 de octubre de 2015, el Tribunal de Justicia, resolviendo una cuestión prejudicial planteada por la High Court (Tribunal Superior, Irlanda), declaró inválida dicha Decisión (en lo sucesivo, «sentencia Schrems I») [56] (apartados 52 y 53).

---

51 Esta sentencia fue mencionada en el Informe Anual de 2020, pp. 26 a 29.

52 Artículo 45 del RGPD.

53 Artículo 46, apartados 1 y 2, letra c), del RGPD.

54 Artículo 49 del RGPD.

55 Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO 2000, L 215, p. 7).

56 Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650 (véase asimismo CP n.º 117/15).

Tras la sentencia Schrems I y la consiguiente anulación, por el órgano jurisdiccional irlandés, de la decisión desestimatoria de la reclamación del Sr. Schrems, la autoridad de control irlandesa invitó a este a modificar su reclamación teniendo cuenta la invalidación por el Tribunal de Justicia de la Decisión 2000/520. En su reclamación modificada, el Sr. Schrems sostiene que los Estados Unidos no ofrecen protección suficiente de los datos transferidos a dicho país. Solicita que en el futuro se suspendan o se prohíban las transferencias de sus datos personales desde la Unión a los Estados Unidos, que Facebook Ireland efectúa desde entonces basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión 2010/87/UE. [57] Al estimar que la tramitación de la reclamación del Sr. Schrems dependía, entre otros factores, de la validez de la Decisión 2010/87, la autoridad de control irlandesa inició un procedimiento ante la High Court con el fin de que esta plantease una petición de decisión prejudicial al Tribunal de Justicia. Tras la incoación de dicho procedimiento, la Comisión adoptó la Decisión (UE) 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU [58] (apartados 54, 55 y 57).

Mediante su petición de decisión prejudicial, el órgano jurisdiccional remitente pregunta al Tribunal de Justicia acerca de la aplicabilidad del RGPD a transferencias de datos personales basadas en cláusulas tipo de protección contenidas en la Decisión 2010/87, acerca del nivel de protección exigido por dicho Reglamento en relación con tales transferencias y acerca de las obligaciones que incumben a las autoridades de control en este contexto. Además, la High Court plantea la cuestión de la validez tanto de la Decisión 2010/87 como de la Decisión 2016/1250.

El Tribunal de Justicia observa que el examen de la Decisión 2010/87 a la luz de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») no pone de manifiesto elemento alguno que pueda afectar a su validez. En cambio, declara inválida la Decisión 2016/1250 (puntos 4 y 5 del fallo).

El Tribunal de Justicia considera, en primer lugar, que el Derecho de la Unión, y en particular el RGPD, se aplica a una transferencia de datos personales efectuada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, aun cuando, en el transcurso de dicha transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado. Precisa que ese tipo de tratamiento de datos efectuado por las autoridades de un país tercero no puede excluir tal transferencia del ámbito de aplicación del RGPD (apartados 86, 88, 89 y punto 1 del fallo).

Por lo que respecta al nivel de protección exigido respecto de dicha transferencia, el Tribunal de Justicia declara que las exigencias previstas en ese sentido por las disposiciones del RGPD, que se refieren a garantías adecuadas, derechos exigibles y acciones legales efectivas, deben interpretarse en el sentido de que las personas cuyos datos personales se transfieren a un país

[57] Decisión de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo (DO 2010, L 39, p. 5), en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (DO 2016, L 344, p. 100).

[58] Decisión de Ejecución de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU. (DO 2016, L 207, p. 1).

tercero sobre la base de cláusulas tipo de protección de datos deben gozar de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por dicho Reglamento, interpretado a la luz de la Carta. En este contexto, precisa que la evaluación de ese nivel de protección debe tomar en consideración tanto las estipulaciones contractuales acordadas entre el exportador de los datos establecido en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país (apartado 105 y punto 2 del fallo).

Por lo que respecta a las obligaciones que incumben a las autoridades de control en el contexto de tal transferencia, el Tribunal de Justicia declara que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, dichas autoridades están obligadas a suspender o prohibir una transferencia de datos a un país tercero cuando consideren, a la luz de todas las circunstancias específicas de la referida transferencia, que las cláusulas tipo de protección de datos no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos, exigida por el Derecho de la Unión, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos (apartado 121 y punto 3 del fallo).

El Tribunal de Justicia examina seguidamente la validez de la Decisión 2010/87. Según el Tribunal de Justicia, la validez de esta Decisión no queda desvirtuada por el mero hecho de que las cláusulas tipo de protección de datos recogidas en ella no vinculen, debido a su carácter contractual, a las autoridades del país tercero al que pueden transferirse datos personales. En cambio, aclara, esa validez depende de si tal Decisión incluye mecanismos efectivos que permitan en la práctica garantizar que el nivel de protección exigido por el Derecho de la Unión sea respetado y que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas o de que resulte imposible su cumplimiento. El Tribunal de Justicia declara que la Decisión 2010/87 establece tales mecanismos. A este respecto, subraya, en particular, que dicha Decisión instaura la obligación del exportador de los datos y del destinatario de la transferencia de comprobar previamente que ese nivel de protección se respeta en el país tercero de que se trate y que obliga al destinatario a informar al exportador de los datos de su eventual incapacidad para cumplir las cláusulas tipo de protección, incumbiendo entonces a este último suspender la transferencia de datos o rescindir el contrato celebrado con el primero (apartados 132, 136, 137, 142 y 148 y punto 4 del fallo).

El Tribunal examina, por último, la validez de la Decisión 2016/1250 atendiendo a las exigencias derivadas del RGPD, leído a la luz de las disposiciones de la Carta que garantizan el respeto de la vida privada y familiar, la protección de los datos personales y el derecho a la tutela judicial efectiva. A este respecto, el Tribunal de Justicia señala que dicha Decisión consagra, al igual que la Decisión 2000/520, la primacía de las exigencias relativas a la seguridad nacional, al interés público y al cumplimiento de la legislación americana, posibilitando de este modo las injerencias en los derechos fundamentales de las personas cuyos datos son transferidos a ese país tercero. Según el Tribunal de Justicia, las limitaciones de la protección de los datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización, por las autoridades estadounidenses, de los datos transferidos desde la Unión a dicho país tercero, y

que la Comisión evaluó en la Decisión 2016/1250, no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas, en el Derecho de la Unión, por el principio de proporcionalidad, en la medida en que los programas de vigilancia basados en esa normativa no se limitan a lo estrictamente necesario. Basándose en las constataciones expuestas en dicha Decisión, el Tribunal de Justicia pone de manifiesto que, por lo que respecta a determinados programas de vigilancia, de la citada normativa no se desprende en modo alguno la existencia de limitaciones a la habilitación que otorga para la ejecución de esos programas ni tampoco la existencia de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de los mismos. El Tribunal de Justicia añade que, si bien esta misma normativa contempla exigencias que las autoridades americanas deben respetar, al ejecutar los programas de vigilancia en cuestión, no confiere a las personas afectadas derechos exigibles frente a las autoridades estadounidenses ante los tribunales (apartados 164, 165, 180 a 182, 184 y 185).

En cuanto a la exigencia de tutela judicial, el Tribunal de Justicia declara que, contrariamente a lo que consideró la Comisión en la Decisión 2016/1250, el mecanismo del Defensor del Pueblo contemplado en dicha Decisión no proporciona a esas personas ninguna vía de recurso ante un órgano que ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión, capaz de garantizar tanto la independencia del Defensor del Pueblo previsto por dicho mecanismo como la existencia de normas que faculten a aquel para adoptar decisiones vinculantes para los servicios de inteligencia americanos. Por todos estos motivos, el Tribunal de Justicia declara inválida la Decisión 2016/1250 (apartados 195 a 197 y 201, y punto 5 del fallo).

V. La protección de los datos personales en Internet

1. Derecho de oposición al tratamiento de los datos personales («derecho al olvido»)

Sentencia de 13 de mayo de 2014 (Gran Sala), Google Spain y Google (C-131/12, EU:C:2014:317)

En dicha sentencia (véase también la sección II.3, titulada «Concepto de "tratamiento de datos personales"»), el Tribunal de Justicia precisó el alcance de los derechos de acceso y de oposición al tratamiento de los datos personales en Internet, previstos en la Directiva 95/46.

Así, al pronunciarse sobre la cuestión del alcance de la responsabilidad del gestor de un motor de búsqueda en Internet, el Tribunal de Justicia consideró, en esencia, que, para respetar los derechos de acceso y de oposición garantizados por los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46, siempre que se cumplan realmente los requisitos establecidos en ellos, dicho gestor está obligado a eliminar, de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, los vínculos a páginas web publicadas por terceros y que contengan información relativa a esa persona. El Tribunal de Justicia precisó que tal obligación puede existir igualmente en el supuesto de que ese nombre o esa información no hayan sido borrados previa o simultáneamente de esas páginas web y, en su

caso, aunque la publicación en dichas páginas sea en sí misma lícita (apartado 88 y punto 3 del fallo).

Por otra parte, con respecto a la cuestión de si la Directiva permite que el interesado solicite que los enlaces a páginas web se supriman de dicha lista de resultados por la razón de que desea que los datos sobre su persona sean «olvidados» después de un cierto tiempo, el Tribunal señala, en primer lugar, que incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando esos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron, en particular cuando tales datos son inadecuados, no pertinentes o ya no pertinentes o excesivos en relación con estos fines y con el tiempo transcurrido (apartado 93). Por consiguiente, en el supuesto en el que se aprecie, tras una solicitud del interesado, que la inclusión de esos vínculos en la lista es, en la situación actual, incompatible con la Directiva, la información y los vínculos que figuren en esa lista deben eliminarse (apartado 94) En este contexto, la constatación de que el interesado tiene derecho a que la información relativa a él deje de estar vinculada a su nombre por una lista de resultados no presupone que la inclusión de tal información en la lista de resultados cause un perjuicio al interesado (apartado 96 y punto 4 del fallo).

Por último, el Tribunal de Justicia precisó que, como el interesado puede solicitar, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, que la información de que se trate deje de ponerse a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda a partir del nombre de esa persona. Sin embargo, tal no sería el caso si por razones específicas, tales como el papel desempeñado por dicha persona en la vida pública, resultara que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate (apartado 97 y punto 4 del fallo).

2. Tratamiento de los datos personales y derechos de propiedad intelectual

Sentencia de 29 de enero de 2008 (Gran Sala), Promusicae (C-275/06, EU:C:2008:54) [59]

Promusicae, una asociación española sin ánimo de lucro que agrupa a productores y editores de grabaciones musicales y audiovisuales, había recurrido ante los tribunales españoles para que ordenase a Telefónica de España, S. A. U. (sociedad cuya actividad consiste, entre otras, en prestar servicios de acceso a Internet), que revelara la identidad y la dirección de determinadas personas a las que prestaba un servicio de acceso a Internet y de las que se conocía su dirección IP y su fecha y hora de conexión. Según Promusicae, estas personas utilizaban el programa de intercambio de archivos denominado «peer to peer» o «P2P» (medio transparente para compartir contenidos, independiente, descentralizado y dotado de funciones de búsqueda y descarga avanzadas) y permitían acceder, en una carpeta compartida de su ordenador personal, a fonogramas cuyos derechos patrimoniales de explotación pertenecían a los asociados de Promusicae. Por consiguiente, dicha asociación solicitó que se le facilitase la

[59] Esta sentencia fue mencionada en el Informe Anual de 2008, p. 46.

información referida para poder ejercitar contra los interesados las correspondientes acciones civiles.

En estas circunstancias, el Juzgado de lo Mercantil n.º 5 de Madrid planteó al Tribunal de Justicia la cuestión de si el Derecho de la Unión obliga a los Estados miembros, para garantizar una protección efectiva de los derechos de autor, a imponer el deber de comunicar datos personales en el marco de un procedimiento civil.

Según el Tribunal de Justicia, dicha petición de decisión prejudicial planteaba la cuestión de la necesaria conciliación de las exigencias relacionadas con la protección de distintos derechos fundamentales, a saber, por una parte, el derecho al respeto de la intimidad y, por otra parte, los derechos a la protección de la propiedad y a la tutela judicial efectiva.

A este respecto, el Tribunal de Justicia declaró que las Directivas 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), [60] 2001/29/CE, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, [61] 2004/48/CE, relativa al respeto de los derechos de propiedad intelectual, [62] y 2002/58 no obligan a los Estados miembros a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Sin embargo, el Derecho de la Unión exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de estas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros, no solo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de estas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad (apartado 70 y fallo).

Sentencia de 24 de noviembre de 2011, Scarlet Extended (C-70/10, EU:C:2011:771) [63]

La Société belge des auteurs, compositeurs et éditeurs SCRL (Sociedad belga de autores, compositores y editores; en lo sucesivo, «SABAM») había constatado que ciertos internautas que utilizaban los servicios de Scarlet Extended SA (en lo sucesivo, «Scarlet») como proveedor de acceso a Internet descargaban en Internet, sin autorización y sin pagar derechos, obras que figuraban en su catálogo mediante redes «peer to peer». SABAM sometió el asunto al juez

[60] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO 2000, L 178, p. 1).

[61] Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (DO 2001, L 167, p. 10).

[62] Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (DO 2004, L 157, p. 45, y corrección de errores en DO 2004, L 195, p. 16).

[63] Esta sentencia fue mencionada en el Informe Anual de 2011, p. 37.

nacional y obtuvo, en primera instancia, un requerimiento judicial dirigido a Scarlet para que pusiera fin a esas infracciones de los derechos de autor, impidiendo cualquier forma de envío o de recepción por parte de sus clientes, mediante un programa «peer-to-peer», de archivos electrónicos que reprodujeran una obra musical del repertorio de SABAM.

Scarlet recurrió en apelación ante la Cour d'appel de Bruxelles (Bélgica), que suspendió el procedimiento para preguntar al Tribunal de Justicia, con carácter prejudicial, si tal requerimiento era compatible con el Derecho de la Unión.

El Tribunal de Justicia declaró que las Directivas 95/46, 2000/31, 2001/29, 2002/58 y 2004/48, leídas conjuntamente e interpretadas a la luz de los requisitos derivados de la protección de los derechos fundamentales aplicables, deben interpretarse en el sentido de que se oponen a un requerimiento judicial por el que se ordena a un proveedor de acceso a Internet, como Scarlet, establecer un sistema de filtrado de todas las comunicaciones electrónicas que circulen a través de sus servicios, en particular mediante la utilización de programas «peer-to-peer», que se aplique indistintamente con respecto a toda su clientela, con carácter preventivo, exclusivamente a sus expensas y sin limitación en el tiempo, y que además sea capaz de identificar en la red de dicho proveedor la circulación de archivos electrónicos que contengan una obra musical, cinematográfica o audiovisual sobre la que el solicitante del requerimiento alegue ser titular de derechos de propiedad intelectual, con el fin de bloquear la transmisión de archivos cuyo intercambio vulnere los derechos de autor (apartado 54 y fallo).

En efecto, según el Tribunal de Justicia, tal requerimiento no respeta la prohibición, establecida en el artículo 15, apartado 1, de la Directiva 2000/31, de imponer a dicho proveedor una obligación general de supervisión, ni tampoco el requisito de garantizar un justo equilibrio entre, por un lado, la protección del derecho de propiedad intelectual y, por otro, la protección de la libertad de empresa, el derecho a la protección de los datos de carácter personal y la libertad de recibir o comunicar informaciones (apartados 40 y 49).

En este contexto, el Tribunal de Justicia señaló, por un lado, que el requerimiento judicial por el que se ordena establecer el sistema de filtrado litigioso implicaría un análisis sistemático de todos los contenidos y la recopilación e identificación de las direcciones IP de los usuarios que hayan originado el envío de contenidos ilícitos en la red, dándose la circunstancia de que dichas direcciones son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios (apartado 51). Por otro lado, dicho requerimiento judicial podría vulnerar la libertad de información, dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito. En efecto, no se discute que la licitud de una transmisión depende igualmente de la aplicación de las excepciones legales a los derechos de autor, que varían de un Estado miembro a otro. Además, en determinados Estados, ciertas obras pueden pertenecer al dominio público o los autores afectados pueden ponerlas gratuitamente a disposición pública en Internet (apartado 52).

Por consiguiente, el Tribunal de Justicia declaró que, si adoptara el requerimiento judicial por el que se obliga a Scarlet a establecer el sistema de filtrado litigioso, el órgano jurisdiccional nacional en cuestión no respetaría el requisito de garantizar un justo equilibrio entre, por un lado, el derecho de propiedad intelectual y, por otro, la libertad de empresa, el derecho a la

protección de los datos de carácter personal y la libertad de recibir o comunicar informaciones (apartado 53).

Sentencia de 19 de abril de 2012, Bonnier Audio y otros (C-461/10, EU:C:2012:219)

El Högsta domstolen (Tribunal Supremo, Suecia) solicitó al Tribunal de Justicia que interpretase, con carácter prejudicial, las Directivas 2002/58 y 2004/48 en el contexto de un litigio entre Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB y Storyside AB (en lo sucesivo, «Bonnier Audio y otros»), por una parte, y Perfect Communication Sweden AB (en lo sucesivo, «ePhone»), por otra, relativo a la oposición de esta última a una solicitud de requerimiento judicial de comunicación de datos presentada por Bonnier Audio y otros.

En ese asunto, Bonnier Audio y otros eran editores, titulares de los derechos exclusivos de reproducción, edición y puesta a disposición del público de 27 obras en formato de audiolibros. Bonnier Audio y otros consideraban que se habían vulnerado sus derechos exclusivos por la difusión al público de esas 27 obras, sin su consentimiento, mediante un servidor FTP («file transfer protocol» o protocolo de transferencia de archivos), que permite compartir archivos y transferir datos entre ordenadores conectados a Internet. Por consiguiente, solicitaron a los tribunales suecos un requerimiento judicial para que se les comunicara el nombre y la dirección del usuario de la dirección IP desde la que presuntamente se habían transmitido los archivos controvertidos.

En este contexto, el Högsta domstolen, ante el que se había recurrido en casación, solicitó al Tribunal de Justicia que se pronunciase sobre la cuestión de si el Derecho de la Unión se opone a la aplicación de una disposición de Derecho nacional, basada en el artículo 8 de la Directiva 2004/48, que, a efectos de identificación de un abonado, permitía que se requiriese en un procedimiento civil a un proveedor de acceso a Internet para que facilitara al titular de un derecho de autor o a su causahabiente la identidad del abonado al que se había asignado una dirección IP supuestamente utilizada para infringir dicho derecho. En la cuestión se presuponía, por una parte, que el demandante había aportado indicios reales de vulneración de un derecho de autor y, por otra parte, que la medida era proporcionada.

El Tribunal de Justicia recordó, en primer lugar, que el artículo 8, apartado 3, de la Directiva 2004/48, interpretado en relación con el artículo 15, apartado 1, de la Directiva 2002/58, no se opone a que los Estados miembros establezcan una obligación de transmitir a particulares datos personales para permitir ejercer acciones ante la jurisdicción civil contra las infracciones al Derecho de propiedad intelectual, pero tampoco les obliga a establecer tal obligación. Sin embargo, incumbe a las autoridades y a los órganos jurisdiccionales de los Estados miembros, no solo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también procurar no basarse en una interpretación de estas que entre en conflicto con los derechos fundamentales o con los demás principios generales del Derecho de la Unión, como el principio de proporcionalidad (apartados 55 y 56).

A este respecto, el Tribunal de Justicia señaló que, para que pudiera emitirse un requerimiento judicial para la comunicación de los datos en cuestión, la normativa nacional controvertida exigía que existieran indicios reales de vulneración de un derecho de propiedad intelectual sobre una obra, que los datos solicitados pudieran facilitar la investigación de la vulneración del

derecho de autor y que las razones que motivaran dicho requerimiento fueran de un interés superior a los inconvenientes o demás perjuicios que este pudiera causar a su destinatario o a otros intereses contrapuestos (apartado 58).

El Tribunal de Justicia concluyó, por tanto, que las Directivas 2002/58 y 2004/48 no se oponen a una normativa nacional, como la que es objeto del procedimiento principal, en la medida en que dicha normativa permita al órgano jurisdiccional nacional que conozca de una acción por la que se solicite un requerimiento judicial de comunicación de datos de carácter personal, ejercitada por una persona legitimada, ponderar, en función de las circunstancias de cada caso y con la debida observancia de las exigencias derivadas del principio de proporcionalidad, los intereses contrapuestos existentes (apartado 61 y fallo).

Sentencia de 17 de junio de 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

La empresa Mircom International Content Management & Consulting (M.I.C.M.) Limited (en lo sucesivo, «Mircom») presentó una demanda de información dirigida contra Telenet BVBA, un proveedor de acceso a Internet, ante el ondernemingsrechtbank Antwerpen (Tribunal de Empresas de Amberes, Bélgica; en lo sucesivo, «tribunal remitente»). Esta demanda tenía por objeto obtener una resolución que obligara a Telenet a proporcionar los datos de identificación de sus clientes basándose en las direcciones IP recopiladas, por cuenta de Mircom, por una sociedad especializada. Las conexiones a Internet de ciertos clientes de Telenet se habían utilizado para compartir, a través de una red entre pares (peer-to-peer) y por medio del protocolo BitTorrent, películas incluidas en el catálogo de Mircom. Telenet se opuso a las pretensiones de Mircom.

En este contexto, el tribunal remitente preguntó al Tribunal de Justicia, en primer lugar, si intercambiar a través de dicha red partes de un archivo multimedia que contiene una obra protegida constituye una comunicación al público con arreglo al Derecho de la Unión. Seguidamente, el tribunal remitente preguntó si el titular de derechos de propiedad intelectual, como es el caso de Mircom, que no utiliza esos derechos, sino que reclama daños y perjuicios a los supuestos infractores, puede disfrutar de las medidas, procedimientos y recursos previstos por el Derecho de la Unión para garantizar la observancia de esos derechos, por ejemplo, pidiendo información. Por último, el tribunal remitente solicitó al Tribunal de Justicia que aclarase si se ajustan a Derecho, por una parte, el modo en que Mircom obtuvo las direcciones IP de los clientes y, por otra parte, la comunicación de los datos que Mircom pidió a Telenet.

El Tribunal de Justicia declaró que el Derecho de la Unión [64] no se opone, en principio, ni al registro sistemático, por parte del titular de derechos de propiedad intelectual y por parte de un tercero que actúa por cuenta de este, de direcciones IP de usuarios de redes entre pares (peer-to-peer) cuyas conexiones de Internet supuestamente se utilizaron en actividades infractoras contra la propiedad intelectual (tratamiento de datos inicial), ni tampoco a la comunicación de los nombres y de las direcciones postales de esos usuarios al comentado titular o a un tercero para la presentación de una demanda de indemnización (tratamiento de datos efectuado en una fase posterior). No obstante, las iniciativas y las pretensiones al efecto han de ser

[64] Artículo 6, apartado 1, letra f), del RGPD y artículo 15, apartado 1, de la Directiva 2002/58.

justificadas, proporcionadas y no abusivas y fundamentarse jurídicamente en una medida legal nacional que limite el alcance de los derechos y obligaciones comprendidos en el Derecho de la Unión. El Tribunal de Justicia precisó que este último ordenamiento no impone, a una sociedad como Telenet, la obligación de comunicar a los particulares datos personales para permitir ejercer acciones ante la jurisdicción civil contra las infracciones al Derecho de propiedad intelectual. Sin embargo, el Derecho de la Unión permite a los Estados miembros imponer tal obligación (apartados 97, 125 a 127 y punto 3 del fallo).

3. Retirada de enlaces a datos personales

Sentencia de 24 de septiembre de 2019 (Gran Sala), GC y otros (Retirada de enlaces a datos sensibles) (C-136/17, EU:C:2019:773)[65]

En esta sentencia, el Tribunal de Justicia, reunido en Gran Sala, precisó las obligaciones del gestor de un motor de búsqueda en el marco de una solicitud de retirada de enlaces relativa a datos sensibles.

Google había denegado las solicitudes de cuatro personas de retirar de la lista de resultados ofrecida por el motor de búsqueda en respuesta a una búsqueda efectuada a partir de sus respectivos nombres diversos enlaces a páginas web publicadas por terceros, principalmente artículos de prensa. A raíz de las denuncias de estas personas, la Comisión Nacional de Informática y Libertades (CNIL, Francia) se negó a requerir a Google para que procediera a la retirada de los enlaces solicitada. El Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), al conocer del asunto, solicitó al Tribunal de Justicia que aclarase las obligaciones que incumbían al gestor de un motor de búsqueda en relación con la tramitación de una solicitud de retirada de enlaces en virtud de la Directiva 95/46.

En primer lugar, el Tribunal de Justicia recordó que el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad, está prohibido, [66] salvo determinadas excepciones y restricciones a esta prohibición. Por lo que respecta al tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, en principio solo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías adecuadas y específicas en el Derecho nacional [67] (apartados 39 y 40).

El Tribunal de Justicia declaró que la prohibición y las restricciones relativas al tratamiento de esas categorías especiales de datos se aplican al gestor de un motor de búsqueda, al igual que a cualquier otro responsable del tratamiento de datos personales. En efecto, la finalidad de esas

65 Esta sentencia fue mencionada en el Informe Anual de 2019, pp. 117 y 118.
66 Artículo 8, apartado 1, de la Directiva 95/46 y artículo 9, apartado 1, del Reglamento 2016/679.
67 Artículo 8, apartado 5, de la Directiva 95/46 y artículo 10 del Reglamento 2016/679.

prohibiciones y restricciones consiste en garantizar una mayor protección frente a tales tratamientos, que, en atención a la particular sensibilidad de esos datos, pueden constituir una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales (apartados 42 a 44).

No obstante, el gestor de un motor de búsqueda no es responsable de que en una página web publicada por un tercero figuren datos personales, sino de crear un enlace a esa página. En tales circunstancias, la prohibición y las restricciones relativas al tratamiento de datos sensibles únicamente se aplican a ese gestor en razón de esa tarea de enumeración de resultados y, por lo tanto, a través de la comprobación a la que cabrá proceder, bajo el control de las autoridades nacionales competentes, tras la recepción de una solicitud formulada por el interesado (apartados 46 y 47).

En segundo lugar, el Tribunal de Justicia consideró que, cuando el gestor reciba una solicitud de retirada de enlaces relativa a datos sensibles, está obligado en principio, salvo ciertas excepciones, a acceder a dicha solicitud. Por lo que respecta a esas excepciones, el gestor puede, en particular, negarse a acceder a tal solicitud cuando compruebe que los enlaces conducen a datos que han sido manifiestamente hechos públicos por el interesado, [68] siempre que la inclusión de tales enlaces cumpla los demás requisitos de legalidad de un tratamiento de datos personales y salvo que el interesado tenga derecho a oponerse a tal tratamiento por razones legítimas propias de su situación particular [69] (apartados 65 y 69).

En cualquier caso, cuando reciba una solicitud de retirada de enlaces, el gestor de un motor de búsqueda debe verificar si la inclusión en la lista de resultados del enlace a una página web en la que se han publicado datos sensibles, presentada tras una búsqueda efectuada a partir del nombre de esa persona, resulta estrictamente necesaria para proteger el derecho a la libertad de información de los internautas potencialmente interesados en acceder a esa página web mediante tal búsqueda. A este respecto, el Tribunal de Justicia subrayó que, si bien los derechos al respeto de la vida privada y a la protección de los datos personales prevalecen, con carácter general, sobre la libertad de información de los internautas, este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate, del carácter sensible de esta para la vida privada del interesado y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que el interesado desempeñe en la vida pública (apartados 66 y 68).

En tercer lugar, el Tribunal de Justicia declaró que, en el marco de una solicitud de retirada de enlaces que dirigen a páginas web en las que se publica información sobre un procedimiento judicial en materia penal incoado contra el interesado, que hace referencia a una etapa anterior de ese procedimiento y que ya no corresponde a la situación actual, incumbe al gestor de un motor de búsqueda apreciar si, a la luz del conjunto de circunstancias del caso concreto, esa persona tiene derecho a que la información en cuestión ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre. No obstante, aun cuando este no sea el caso debido a que la inclusión del enlace controvertido es estrictamente necesaria para conciliar los derechos al respeto de la vida

[68] Artículo 8, apartado 2, letra e), de la Directiva 95/46 y artículo 9, apartado 2, letra e), del Reglamento 2016/679.
[69] Artículo 14, párrafo primero, letra a), de la Directiva 95/46 y artículo 21, apartado 1, del Reglamento 2016/679.

privada y a la protección de los datos del interesado con la libertad de información de los internautas potencialmente interesados, ese gestor estará obligado, a más tardar en el momento de la solicitud de retirada de enlaces, a estructurar la lista de resultados de tal manera que la imagen global que resulte de ella para el internauta refleje la situación judicial actual, lo que requerirá, en particular, que en dicha lista se indiquen en primer lugar enlaces a páginas web que contengan información al respecto (apartados 77 y 78).

Sentencia de 24 de septiembre de 2019 (Gran Sala), Google (Alcance territorial del derecho a la retirada de enlaces) (C-507/17, EU:C:2019:772) [70]

La Comisión Nacional de Informática y Libertades (CNIL) (Francia) requirió a Google para que, cuando esta empresa acceda a una solicitud de retirada de enlaces, suprima de la lista de resultados que aparece tras una búsqueda efectuada a partir del nombre de la persona de que se trate, los enlaces que dirijan a páginas web que incluyan datos personales relativos a esta en todas las extensiones de nombre de dominio de su motor de búsqueda. A raíz de la negativa de Google a cumplir este requerimiento, la CNIL impuso a dicha empresa una sanción de 100 000 euros. El Consejo de Estado, ante el que recurrió Google, solicitó al Tribunal de Justicia que precisase el alcance territorial de la obligación del gestor de un motor de búsqueda de aplicar el derecho a la supresión de enlaces en virtud de la Directiva 95/46.

En primer lugar, el Tribunal de Justicia recordó la posibilidad que tienen las personas físicas de invocar, basándose en el Derecho de la Unión, su derecho a la supresión de enlaces contra el gestor de un motor de búsqueda que disponga de uno o varios establecimientos en el territorio de la Unión, independientemente de que el tratamiento de datos personales (en este caso, la enumeración de enlaces a páginas web en las que figuran datos personales relativos a la persona que invoca ese derecho) tenga o no lugar en la Unión. [71]

Por lo que respecta al alcance del derecho a la retirada de enlaces, el Tribunal de Justicia consideró que el gestor de un motor de búsqueda no está obligado a proceder a dicha retirada en todas las versiones de su motor de búsqueda, sino solo en las versiones de este que corresponden al conjunto de los Estados miembros. Señaló a este respecto que, si bien una retirada de enlaces universal podría, habida cuenta de las características de Internet y de los motores de búsqueda, responder plenamente al objetivo del legislador de la Unión consistente en garantizar un nivel elevado de protección de los datos personales en el conjunto de la Unión, del Derecho de la Unión [72] no se desprende sin embargo en modo alguno que, para la realización de tal objetivo, el legislador de la Unión haya optado por atribuir al derecho a la retirada de enlaces un alcance que vaya más allá del territorio de los Estados miembros. En particular, aunque el Derecho de la Unión establece mecanismos de cooperación entre autoridades de control de los Estados miembros para llegar a una decisión común, basada en un equilibrio entre el derecho a la protección de la vida privada y de los datos personales, por una parte, y el interés del público de los distintos Estados miembros en tener acceso a una información, por otra, tales mecanismos no están actualmente previstos en lo que se refiere al alcance de la retirada de enlaces fuera de la Unión (apartados 62 y 73).

---

70 Esta sentencia fue mencionada en el Informe Anual de 2019, pp. 118 y 119.

71 Artículo 4, apartado 1, letra a), de la Directiva 95/46, y artículo 3, apartado 1, del Reglamento 2016/679.

72 Artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 y artículo 17, apartado 1, del Reglamento 2016/679.

En el estado actual del Derecho de la Unión, incumbe al gestor de un motor de búsqueda proceder a la retirada de enlaces solicitada no solo de la versión del motor de búsqueda correspondiente al Estado miembro de residencia del beneficiario de esa retirada de enlaces, sino de las versiones del motor correspondientes a todos los Estados miembros, en particular con el fin de garantizar un nivel coherente y elevado de protección en el conjunto de la Unión. Por otra parte, incumbe a ese gestor adoptar, si es necesario, medidas suficientemente eficaces para impedir o, al menos, dificultar seriamente a los internautas de la Unión el acceso, en su caso a partir de una versión del motor de búsqueda correspondiente a un Estado tercero, a los enlaces objeto de la solicitud de retirada, y corresponde al órgano jurisdiccional nacional comprobar si las medidas adoptadas por el gestor cumplen ese requisito (apartado 70).

Por último, el Tribunal de Justicia subrayó que, si bien el Derecho de la Unión no obliga al gestor de un motor de búsqueda a proceder a la retirada de enlaces de la totalidad de las versiones de su motor, tampoco lo prohíbe. Por lo tanto, una autoridad de control o judicial de un Estado miembro sigue siendo competente para realizar, de conformidad con los estándares nacionales de protección de los derechos fundamentales, una ponderación entre, por un lado, los derechos del interesado al respeto de su vida privada y a la protección de sus datos personales y, por otro lado, el derecho a la libertad de información y, al término de esta ponderación, exigir, en su caso, al gestor del motor de búsqueda que proceda a retirar los enlaces de todas las versiones de dicho motor (apartados 65 y 72).

4. Consentimiento del usuario de un sitio de Internet al almacenamiento de información o al acceso a información mediante cookies

Sentencia de 1 de octubre de 2019 (Gran Sala), Planet49 (C-673/17, EU:C:2019:801) [73]

Mediante esta sentencia, el Tribunal de Justicia declaró que el consentimiento al almacenamiento de información o al acceso a información mediante *cookies* instaladas en el equipo terminal del usuario de un sitio de Internet no es válidamente prestado cuando la autorización resulta de una casilla marcada por defecto, con independencia de que esa información consista o no en datos personales. Además, el Tribunal de Justicia precisó que el proveedor de servicios debe indicar al usuario de un sitio de Internet la duración del funcionamiento de las *cookies,* así como la posibilidad o imposibilidad de que los terceros accedan a esas *cookies*.

El litigio principal versaba sobre la organización de un juego promocional por Planet49 en el sitio de Internet www.dein-macbook.de. Para participar, los internautas debían comunicar su nombre y dirección en una página web en la que figuraban una serie de casillas para marcar. La casilla que autorizaba la instalación de las *cookies* estaba marcada por defecto. Al conocer de un recurso interpuesto por la Federación alemana de asociaciones de consumidores, el Bundesgerichtshof (Tribunal Supremo de lo Civil y Penal, Alemania) albergaba dudas sobre la validez del consentimiento prestado por los usuarios mediante la casilla marcada por defecto y sobre el alcance de la obligación de información que recaía sobre el proveedor del servicio.

[73] Esta sentencia fue mencionada en el Informe Anual de 2019, pp. 120 y 121.

La petición de decisión prejudicial tenía como objeto principal la interpretación del concepto de «consentimiento» contemplado en la Directiva 2002/58, [74] puesta en relación con la Directiva 95/46 [75] y con el RGPD. [76]

En primer lugar, el Tribunal de Justicia observó que el artículo 2, letra h), de la Directiva 95/46, a la que se remite el artículo 2, letra f), de la Directiva 2002/58, define el consentimiento como «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». Señaló que la exigencia de una «manifestación» de voluntad del interesado sugiere claramente un comportamiento activo y no pasivo. Pues bien, el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de Internet. Además, la génesis del artículo 5, apartado 3, de la Directiva 2002/58, que dispone desde su modificación por la Directiva 2009/136 que el usuario debe haber «dado su consentimiento», muestra que el consentimiento del usuario ya no puede presumirse y debe resultar del comportamiento activo de este último. Por último, el consentimiento activo está expresamente previsto en la actualidad en el RGPD, [77] cuyo artículo 4, punto 11, exige una manifestación de voluntad que adopte la forma, concretamente, de una «clara acción afirmativa» y cuyo considerando 32 excluye expresamente que pueda haber consentimiento en caso de «silencio, [...] casillas ya marcadas o [...] inacción» (apartados 49, 52, 56 y 62).

El Tribunal declaró por lo tanto que el consentimiento no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento. Añadió que el hecho de que ese usuario active el botón de participación en el juego con fines promocionales de que se trata no basta para considerar que el usuario ha dado de manera válida su consentimiento para la colocación de *cookies* (apartado 63).

En segundo lugar, el Tribunal de Justicia declaró que el artículo 5, apartado 3, de la Directiva 2002/58 pretende proteger al usuario de cualquier injerencia en su esfera privada, independientemente de que dicha injerencia afecte a datos personales o de otro tipo. De ello se desprende que el concepto de «consentimiento» no debe interpretarse de manera diferente en función de que la información almacenada o consultada en el equipo terminal del usuario de un sitio de Internet sean o no datos personales (apartados 69 y 71).

En tercer lugar, el Tribunal de Justicia señaló que el artículo 5, apartado 3, de la Directiva 2002/58 exige que el usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos. Pues bien, una información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa. A este respecto, el Tribunal de Justicia consideró que la información acerca del tiempo durante el cual las *cookies* estarán

---

74 Artículos 2, letra f), y 5, apartado 3, de la Directiva 2002/58, en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11).

75 Artículo 2, letra h), de la Directiva 95/46.

76 Artículo 6, apartado 1, letra a), del Reglamento 2016/679.

77 *Ibidem*.

activas y la posibilidad de que terceros tengan acceso a ellas forma parte de la información clara y completa que el proveedor de servicios debe facilitar al usuario de un sitio de Internet (apartados 73 a 75 y 81).

VI. Autoridades nacionales de control

1. Alcance del requisito de independencia

Sentencia de 9 de marzo de 2010 (Gran Sala) Comisión/Alemania (C-518/07, EU:C:2010:125) [78]

En su recurso, la Comisión solicitó al Tribunal de Justicia que declarase que la República Federal de Alemania había incumplido las obligaciones que le incumbían en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, al someter a la tutela del Estado a las autoridades de control competentes para vigilar en los diferentes Länder (Estados federados) el tratamiento de los datos personales en el sector no público, y al haber adaptado así incorrectamente su normativa nacional al requisito de «total independencia» de las autoridades encargadas de garantizar la protección de estos datos.

La República Federal de Alemania defendía, por su parte, que el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 exige la independencia funcional de las autoridades de control, en el sentido de que estas deben ser independientes del sector no público sujeto a su control y no deben estar expuestas a influencias externas. Ahora bien, a su juicio, la tutela que el Estado ejerce en los Länder alemanes no constituía tal influencia externa, sino un mecanismo de vigilancia interna de la Administración, que llevan a cabo autoridades incardinadas en la misma estructura administrativa a la que pertenecen las autoridades de control y, como estas, obligadas a cumplir los objetivos de la Directiva 95/46.

El Tribunal de Justicia estimó que la garantía de independencia de las autoridades de control nacionales establecida en la Directiva 95/46 trata de asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y debe interpretarse a la luz de ese objetivo. Dicha garantía no se ha establecido para conceder un estatuto particular a esas autoridades mismas o a sus agentes, sino para reforzar la protección de las personas y de los organismos afectados por sus decisiones, de modo que las autoridades de control deben actuar con objetividad e imparcialidad en el ejercicio de sus funciones (apartado 25).

El Tribunal de Justicia consideró que esas autoridades de control competentes para vigilar el tratamiento de los datos personales en el sector no público han de disfrutar de una independencia que les permita ejercer sus funciones sin influencia externa. Esta independencia excluye no solo cualquier influencia que pudieran ejercer los organismos sujetos a control, sino también toda orden o influencia externa, directa o indirecta, que pudiera poner en peligro el cumplimiento de la tarea de dichas autoridades, consistente en establecer un justo equilibrio

[78] Esta sentencia fue mencionada en el Informe Anual de 2010, p. 34.

entre la protección del derecho a la intimidad y la libre circulación de datos personales. La mera posibilidad de que las autoridades de tutela puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de estas. Por un lado, podría darse en tal caso una «obediencia anticipada» de las autoridades de control a la vista de la práctica decisoria de la autoridad de tutela. Por otro, el papel de guardianas del derecho a la intimidad que asumen las autoridades de control exige que sus decisiones y, por tanto, ellas mismas, estén por encima de toda sospecha de parcialidad. Según el Tribunal de Justicia, la tutela del Estado sobre las autoridades nacionales de control no es compatible con el requisito de independencia (apartados 30, 36 y 37 y fallo).

Sentencia de 16 de octubre de 2012 (Gran Sala), Comisión/Austria (C-614/10, EU:C:2012:631)

En su recurso, la Comisión solicitó al Tribunal de Justicia que declarase que la República de Austria había incumplido las obligaciones que le incumbían en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 al no haber adoptado todas las medidas necesarias para que la normativa vigente en Austria cumpliera el requisito de independencia por lo que se refiere a la Datenschutzkommission (comisión de protección de datos), creada como autoridad de control en materia de protección de los datos personales.

El Tribunal declaró la existencia de un incumplimiento por parte de Austria, considerando, en esencia, que no cumplía el criterio de independencia de la autoridad de control, establecido por la Directiva 95/46, el Estado miembro que establece un marco normativo en virtud del cual el administrador de dicha autoridad es un funcionario del Estado sometido a supervisión jerárquica, su secretaría está integrada en la estructura orgánica del Gobierno nacional y el Jefe del Gobierno nacional tiene un derecho incondicional a informarse de todos los aspectos de la gestión de dicha autoridad (apartado 66 y fallo).

El Tribunal de Justicia recordó, en primer lugar, que los términos «con total independencia» del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 implican que las autoridades de control han de disfrutar de una independencia que les permita ejercer sus funciones sin influencia externa. A este respecto, el hecho de que una autoridad de esta índole disfrute de una independencia funcional, en la medida en que sus miembros son independientes y no están sujetos a instrucción alguna en el ejercicio de sus funciones, no basta por sí solo para preservar de toda influencia externa a la autoridad de control. En efecto, la independencia exigida en este contexto tiene por objeto excluir no solo la influencia directa, en forma de instrucciones, sino también toda forma de influencia indirecta que pueda orientar las decisiones de la autoridad de control. Por otra parte, dado el papel de guardianas del derecho a la intimidad que asumen las autoridades de control, es preciso que sus decisiones, y por tanto ellas mismas, estén por encima de toda sospecha de parcialidad (apartados 41 a 43 y 52).

El Tribunal de Justicia precisó que, para poder cumplir el requisito de independencia establecido en el citado artículo de la Directiva 95/46, no es necesario que la autoridad nacional de control disponga de una línea presupuestaria autónoma similar a la contemplada en el artículo 43, apartado 3, del Reglamento n.º 45/2001. En efecto, los Estados miembros no están obligados a reproducir en su normativa nacional disposiciones análogas a las del capítulo V del Reglamento n.º 45/2001 con el fin de garantizar la total independencia de su autoridad o autoridades de

control y, por tanto, pueden establecer que, desde el punto de vista del Derecho presupuestario, la autoridad de control dependa de un Ministerio determinado. No obstante, la atribución de los medios humanos y materiales que necesita tal autoridad de control no debe impedir que ejerza sus funciones «con total independencia», en el sentido del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 (apartado 58).

Sentencia de 8 de abril de 2014 (Gran Sala), Comisión/Hungría (C-288/12, EU:C:2014:237) [79]

En este asunto, la Comisión solicitó al Tribunal de Justicia que declarase que Hungría había incumplido las obligaciones que le incumbían en virtud de la Directiva 95/46 al poner fin antes de tiempo al mandato de la autoridad de control de la protección de los datos personales.

El Tribunal de Justicia declaró que incumple las obligaciones que le incumben en virtud de la Directiva 95/46 un Estado miembro que pone fin antes de tiempo al mandato de la autoridad de control de la protección de los datos personales (apartado 62 y punto 1 del fallo).

En efecto, según el Tribunal de Justicia, la independencia de la que han de disfrutar las autoridades de control competentes para vigilar el tratamiento de dichos datos excluye en particular toda orden o influencia externa con independencia de la forma que revista, directa o indirecta, que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea de dichas autoridades, consistente en establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de los datos personales (apartado 51).

El Tribunal de Justicia recordó, además, que la independencia funcional no basta por sí sola para preservar a las autoridades de control de toda influencia externa, pues la mera posibilidad de que las autoridades de tutela del Estado puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de estas. Pues bien, si cada Estado miembro tuviera la posibilidad de poner fin al mandato de una autoridad de control antes de que este llegue al término inicialmente previsto sin respetar las normas y las garantías establecidas previamente en tal sentido por la legislación aplicable, la amenaza de esa terminación anticipada que en tal caso planearía sobre dicha autoridad durante todo su mandato podría generar una forma de obediencia de esta al poder político incompatible con el mencionado requisito de independencia. Además, en tal situación, no cabría considerar que la autoridad de control pueda actuar, en cualquier circunstancia, por encima de toda sospecha de parcialidad (apartados 52 a 55).

2. Determinación del Derecho aplicable y de la autoridad de control competente

[79] Esta sentencia fue mencionada en el Informe Anual de 2014, p. 62.

Sentencia de 1 de octubre de 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

La Nemzeti Adatvédelmi és Információszabadság Hatóság (Autoridad nacional encargada de la protección de datos y de la libertad de información, Hungría) había impuesto una multa a la sociedad Weltimmo, cuyo domicilio social se encuentra en Eslovaquia y que gestiona un sitio de Internet de anuncios de inmuebles situados en Hungría, debido a que esta no había procedido a suprimir los datos personales de los anunciantes en dicho sitio de Internet, pese a haberlo solicitado estos, y había comunicado estos datos a empresas de cobro de impagados para obtener el pago de facturas impagadas. Según la autoridad húngara de control, la sociedad Weltimmo había infringido así la ley húngara que transpone la Directiva 95/46.

La Kúria (Tribunal Supremo, Hungría), ante la que se presentó un recurso de casación, albergaba dudas en cuanto a la determinación del Derecho aplicable y a las facultades de que dispone la autoridad húngara de control a la luz de los artículos 4, apartado 1, y 28 de la Directiva 95/46. Dicho órgano jurisdiccional planteó en consecuencia al Tribunal de Justicia varias cuestiones prejudiciales.

Por lo que respecta al Derecho nacional aplicable, el artículo 4, apartado 1, letra a), de la Directiva 95/46 permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que este ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento. Para determinar si así ocurre, el órgano jurisdiccional remitente puede tener en cuenta, por un lado, el hecho de que la actividad del responsable de dicho tratamiento, en cuyo marco este tiene lugar, consiste en la gestión de sitios de Internet de anuncios de inmuebles situados en el territorio de dicho Estado miembro y redactados en la lengua de ese Estado y que, en consecuencia, se dirige principalmente, incluso íntegramente, a dicho Estado miembro. El órgano jurisdiccional remitente puede tener en cuenta igualmente, por otro lado, el hecho de que ese responsable dispone de un representante en el referido Estado miembro que se encarga de cobrar los ingresos resultantes de dicha actividad y de representarlo en los procedimientos administrativo y judicial relativos al tratamiento de los datos en cuestión. El Tribunal de Justicia precisó que, en cambio, no es relevante la cuestión de la nacionalidad de las personas afectadas por dicho tratamiento de datos (apartado 41 y punto 1 del fallo).

Por lo que se refiere a la competencia y a las facultades de la autoridad de control que entiende de las denuncias, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, el Tribunal de Justicia consideró que dicha autoridad puede examinar tales denuncias sea cual sea el Derecho aplicable, e incluso antes de saber cuál es el Derecho nacional aplicable al tratamiento de los datos de que se trate (apartado 54). Sin embargo, si llega a la conclusión de que es aplicable el Derecho de otro Estado miembro, no puede imponer sanciones fuera del territorio de su propio Estado miembro. En tal situación, en ejecución de la obligación de cooperación que se establece en el artículo 28, apartado 6, de esa Directiva, le corresponde solicitar a la autoridad de control de ese otro Estado miembro que declare la existencia de una eventual infracción del Derecho aplicable y que imponga sanciones si este lo permite,

[80] Esta sentencia fue mencionada en el Informe Anual de 2015, p. 55.

basándose, en su caso, en la información que ella le haya remitido (apartados 57 y 60 y punto 2 del fallo).

3. Facultades de las autoridades nacionales de control

Sentencia de 6 de octubre de 2015 (Gran Sala), Schrems (C-362/14, EU:C:2015:650)

En ese asunto (véase también la sección IV, titulada «Transferencia de los datos personales a países terceros»), el Tribunal de Justicia declaró que las autoridades nacionales de control son competentes para controlar las transferencias de datos personales a terceros países.

A este respecto, el Tribunal de Justicia indicó, en primer lugar, que las autoridades nacionales de control disponen de una amplia gama de facultades, enumeradas de forma no exhaustiva por el artículo 28, apartado 3, de la Directiva 95/46, que constituyen otros tantos medios necesarios para el cumplimiento de sus funciones. Así pues, esas autoridades disponen, en particular, de facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio (apartado 43).

En lo que atañe a la facultad de controlar las transferencias de datos personales a países terceros, el Tribunal de Justicia estimó que, ciertamente, del artículo 28, apartados 1 y 6, de la Directiva 95/46 resulta que las facultades de las autoridades nacionales de control abarcan los tratamientos de datos personales realizados en el territorio del Estado miembro de esas autoridades, de modo que estas no disponen, con fundamento en ese artículo 28, de facultades respecto a los tratamientos de datos realizados en el territorio de un país tercero (apartado 44).

No obstante, la operación consistente en hacer transferir datos personales desde un Estado miembro a un país tercero constituye por sí misma un tratamiento de datos personales realizado en el territorio de un Estado miembro. Por consiguiente, dado que, con arreglo al artículo 8, apartado 3, de la Carta y al artículo 28 de la Directiva 95/46, las autoridades nacionales de control están encargadas del control del cumplimiento de las normas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales, toda autoridad nacional de control está investida de la competencia para comprobar si una transferencia de datos personales desde su Estado miembro a un país tercero respeta las exigencias establecidas por esta Directiva (apartados 45 y 47).

Sentencia de 5 de junio de 2018 (Gran Sala), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

En esta sentencia (véase asimismo la sección II.5, titulada «Concepto de "responsable del tratamiento de datos personales"») que trata, entre otros extremos, de la interpretación de los artículos 4 y 28 de la Directiva 95/46, el Tribunal de Justicia se pronunció sobre el alcance de las facultades de intervención de que disponen las autoridades nacionales de control respecto de un tratamiento de datos personales que implique la participación de varios actores.

Así, el Tribunal de Justicia declaró que cuando una empresa establecida fuera de la Unión Europea (como la empresa americana Facebook) dispone de varios establecimientos en diversos Estados miembros, la autoridad de control de un Estado miembro está facultada para ejercer los poderes que le confiere el artículo 28, apartado 3, de la mencionada Directiva respecto a un establecimiento de esa empresa situado en el territorio de ese Estado miembro (en este caso, Facebook Germany), aun cuando, en virtud del reparto de funciones dentro del grupo, por un lado, este establecimiento únicamente se encarga de la venta de espacios publicitarios y de otras actividades de marketing en el territorio de dicho Estado miembro y, por otro lado, la responsabilidad exclusiva de la recogida y del tratamiento de los datos personales incumbe, para todo el territorio de la Unión Europea, a un establecimiento situado en otro Estado miembro (en este caso, Facebook Ireland) (apartado 64 y punto 2 del fallo).

Además, el Tribunal de Justicia precisó que cuando la autoridad de control de un Estado miembro pretende ejercer frente a una entidad establecida en el territorio de ese Estado miembro los poderes de intervención contemplados en el artículo 28, apartado 3, de la Directiva 95/46 debido a infracciones de las normas relativas a la protección de datos personales cometidas por un tercero responsable del tratamiento de esos datos que tiene su domicilio en otro Estado miembro (en este caso, Facebook Ireland), dicha autoridad de control es competente para apreciar, de manera autónoma respecto de la autoridad de control de este último Estado miembro (Irlanda), la legalidad del referido tratamiento de datos y puede ejercer sus poderes de intervención frente a la entidad establecida en su territorio sin instar previamente la intervención de la autoridad de control del otro Estado miembro (apartado 74 y punto 3 del fallo).

Sentencia de 15 de junio de 2021 (Gran Sala), Facebook Ireland y otros (C-645/19, EU:C:2021:483)

El 11 de septiembre de 2015, el presidente de la Comisión belga de protección de la vida privada (en lo sucesivo, «CPVP») ejercitó ante el Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primera Instancia Neerlandófono de Bruselas, Bélgica) una acción de cesación contra Facebook Ireland, Facebook Inc. y Facebook Belgium, que tenía por objeto poner fin a infracciones de la legislación en materia de protección de datos supuestamente cometidas por Facebook. Estas infracciones consistían, en particular, en la recogida y utilización de información sobre los hábitos de navegación de los internautas belgas, poseedores o no de una cuenta Facebook, mediante diferentes tecnologías, como cookies, complementos sociales [81] o píxeles.

El 16 de febrero de 2018, dicho órgano jurisdiccional se declaró competente para conocer de esa acción y, en cuanto al fondo, declaró que la red social Facebook no había informado suficientemente a los internautas belgas de la recogida y del uso de dicha información. Por otra parte, no se consideró válido el consentimiento dado por los internautas a la recogida y al tratamiento de tal información.

El 2 de marzo de 2018, Facebook Ireland, Facebook Inc. y Facebook Belgium interpusieron recurso de apelación contra esa sentencia ante el Hof van beroep te Brussel (Tribunal de

[81] Por ejemplo, los botones «Me gusta» o «Compartir».

Apelación de Bruselas, Bélgica), que es el órgano jurisdiccional remitente en el presente asunto. Ante este órgano jurisdiccional, la Autoridad de Protección de Datos belga (en lo sucesivo, «APD») ha actuado como sucesor legal del presidente de la CPVP. El órgano jurisdiccional remitente solo se ha declarado competente para conocer del recurso de apelación interpuesto por Facebook Belgium.

El órgano jurisdiccional remitente alberga dudas acerca de los efectos de la aplicación del mecanismo de «ventanilla única» previsto por el RGPD [82] en las competencias de la APD y, más concretamente, se pregunta si, con respecto a los hechos posteriores a la entrada en vigor del RGPD, a saber, el 25 de mayo de 2018, la APD puede ejercitar acciones judiciales contra Facebook Belgium, dado que Facebook Ireland ha sido identificada como la responsable del tratamiento de los datos en cuestión. En efecto, desde esta fecha y, en particular, en aplicación del principio de «ventanilla única» establecido por el RGPD, el Comisario irlandés de protección de datos es el único competente para ejercitar una acción de cesación, bajo el control de los órganos jurisdiccionales irlandeses (apartados 36 y 37).

En su sentencia, dictada por la Gran Sala, el Tribunal de Justicia precisa los poderes de las autoridades nacionales de control en el marco del RGPD. De este modo, declara, en particular, que, en determinadas condiciones, este Reglamento autoriza a una autoridad de control de un Estado miembro a ejercer su facultad de poner en conocimiento de los órganos jurisdiccionales de ese Estado miembro cualquier supuesta infracción de RGPD y de iniciar o ejercitar acciones judiciales con respecto a un tratamiento de datos transfronterizo, [83] aunque no sea la autoridad de control principal en lo referente a ese tratamiento (punto 1 del fallo).

En primer lugar, el Tribunal de Justicia precisa las condiciones en las que una autoridad nacional de control, que no tiene la condición de autoridad principal con respecto a un tratamiento transfronterizo, debe ejercer su facultad de poner en conocimiento de los órganos jurisdiccionales de un Estado miembro cualquier supuesta infracción del RGPD y, si procede, iniciar o ejercitar acciones judiciales para garantizar la aplicación de este Reglamento. Así, por una parte, el RGPD debe conferir a dicha autoridad de control competencia para adoptar una decisión en la que se declare que dicho tratamiento incumple las normas que contiene ese Reglamento y, por otra parte, esa facultad debe ejercerse respetando los procedimientos de cooperación y de coherencia establecidos por dicho Reglamento [84] (apartado 75 y punto 1 del fallo).

En efecto, en el caso de los tratamientos transfronterizos, el RGPD establece el mecanismo de «ventanilla única», [85] basado en un reparto de competencias entre una «autoridad de control principal» y las demás autoridades de control interesadas. Este mecanismo exige una cooperación estrecha, leal y efectiva entre estas autoridades, para garantizar una protección coherente y homogénea de las normas relativas a la protección de datos personales y preservar así su efecto útil. El RGPD establece a este respecto la competencia de principio de la autoridad

---

82 A tenor del artículo 56, apartado 1, del RGPD: «Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado».

83 En el sentido del artículo 4, punto 23, del RGPD.

84 Establecidos en los artículos 56 y 60 del RGPD.

85 Artículo 56, apartado 1, del RGPD.

de control principal para adoptar una decisión en la que se declare que un tratamiento transfronterizo incumple las normas establecidas en dicho Reglamento, [86] mientras que la competencia de las demás autoridades nacionales de control para adoptar tal decisión, incluso con carácter provisional, constituye la excepción. [87] No obstante, en el ejercicio de sus competencias, la autoridad de control principal no puede prescindir de un diálogo indispensable y de una cooperación leal y efectiva con las demás autoridades de control interesadas. Por ello, en el marco de esta cooperación, la autoridad de control principal no puede pasar por alto los criterios de las demás autoridades de control interesadas, y toda objeción pertinente y motivada formulada por una de estas últimas autoridades tiene por efecto bloquear, al menos temporalmente, la adopción del proyecto de decisión de la autoridad de control principal (apartados 50 a 53, 56 a 59 y 63 a 65).

El Tribunal de Justicia precisa, además, que el hecho de que una autoridad de control de un Estado miembro que no sea la autoridad de control principal con respecto a un tratamiento de datos transfronterizo solo pueda ejercer la facultad de poner en conocimiento de los órganos jurisdiccionales de ese Estado miembro cualquier supuesta infracción del RGPD y de iniciar o ejercitar acciones judiciales respetando las reglas de reparto de las competencias decisorias entre la autoridad de control principal y las demás autoridades de control [88] es conforme con los artículos 7, 8 y 47 de la Carta, que garantizan al interesado, respectivamente, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva (apartado 67).

En segundo lugar, el Tribunal de Justicia declara que, en caso de tratamiento de datos transfronterizo, el ejercicio de la facultad de una autoridad de control de un Estado miembro, distinta de la autoridad de control principal, de iniciar o ejercitar acciones judiciales [89] no exige que el responsable o encargado del tratamiento transfronterizo de datos personales contra el que se ejercite dicha acción disponga de un establecimiento principal u otro establecimiento en el territorio de dicho Estado miembro. Sin embargo, el ejercicio de esta facultad debe estar comprendida en el ámbito de aplicación territorial del RGPD, [90] lo que supone que el responsable o el encargado del tratamiento transfronterizo disponga de un establecimiento en el territorio de la Unión (apartados 80, 83 y 84 punto 2 del fallo).

En tercer lugar, el Tribunal de Justicia declara que, en caso de tratamiento de datos transfronterizo, la facultad de una autoridad de control de un Estado miembro, distinta de la autoridad de control principal, de poner en conocimiento de los órganos jurisdiccionales de este Estado cualquier supuesta infracción de dicho Reglamento y, si procede, iniciar o ejercitar acciones judiciales puede ejercerse tanto con respecto al establecimiento principal del responsable del tratamiento que se encuentra en el Estado miembro de dicha autoridad como con respecto a otro establecimiento de ese responsable, siempre que la acción judicial tenga por objeto un tratamiento de datos efectuado en el contexto de las actividades de ese establecimiento y que dicha autoridad tenga competencia para ejercer esa facultad.

---

86 Artículo 60, apartado 7, del RGPD.

87 El artículo 56, apartado 2, y el artículo 66 del RGPD establecen las excepciones al principio de la competencia decisoria de la autoridad de control principal.

88 Establecidas en los artículos 55 y 56, ambos en relación con el artículo 60 del RGPD.

89 En virtud del artículo 58, apartado 5, del RGPD.

90 El artículo 3, apartado 1, del RGPD establece que este Reglamento se aplica al tratamiento de datos personales efectuado «en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no».

Sin embargo, el Tribunal de Justicia precisa que el ejercicio de esta facultad supone que el RGPD sea aplicable. En el presente asunto, dado que las actividades del establecimiento del grupo Facebook situado en Bélgica están indisociablemente vinculadas al tratamiento de los datos personales de que se trata en el litigio principal, de los que Facebook Ireland es el responsable en lo que se refiere al territorio de la Unión, este tratamiento se realiza «en el contexto de las actividades de un establecimiento del responsable» y, por tanto, está efectivamente comprendido en el ámbito de aplicación del RGPD (apartados 94 a 96 y punto 3 del fallo).

En cuarto lugar, el Tribunal de Justicia declara que, cuando una autoridad de control de un Estado miembro que no es la «autoridad de control principal» ejercitó, antes de la fecha de entrada en vigor del RGPD, una acción judicial cuyo objeto era un tratamiento transfronterizo de datos personales, dicha acción puede mantenerse, desde el punto de vista del Derecho de la Unión, sobre la base de las disposiciones de la Directiva 95/46, que sigue siendo aplicable en lo que se refiere a las infracciones de las normas que establece, cometidas hasta la fecha en la que dicha Directiva fue derogada. Además, dicha acción puede ser ejercitada por esa autoridad por infracciones cometidas después de la fecha de entrada en vigor del RGPD, siempre que sea en una de las situaciones en las que, excepcionalmente, dicho Reglamento confiere a esa misma autoridad competencia para adoptar una decisión por la que se declare que el tratamiento de datos de que se trata no cumple las disposiciones de dicho Reglamento y siempre que se respeten los procedimientos de cooperación y coherencia que este último establece (apartado 105 y punto 4 del fallo).

En quinto y último lugar, el Tribunal de Justicia reconoce el efecto directo de la disposición del RGPD en virtud de la cual cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones de ese Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales. Por consiguiente, tal autoridad puede invocar dicha disposición para ejercitar o retomar una acción contra particulares, aun cuando dicha disposición no se haya aplicado específicamente en la legislación del Estado miembro de que se trate (apartado 113 y punto 5 del fallo).

VII. Ámbito de aplicación territorial de la legislación europea

Sentencia de 13 de mayo de 2014 (Gran Sala), Google Spain y Google (C-131/12, EU:C:2014:317)

En esta sentencia [véanse también las secciones II.3, titulada «Concepto de "tratamiento de datos personales"», y V.1, titulada «Derecho de oposición al tratamiento de los datos personales ("derecho al olvido")»], el Tribunal de Justicia se pronunció, asimismo, sobre el ámbito geográfico de aplicación de la Directiva 95/46.

Así, el Tribunal de Justicia declaró que un tratamiento de datos personales es efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro, en el sentido de la Directiva 95/46, cuando el gestor de un motor de búsqueda, pese a estar domiciliado en un Estado tercero, crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios

propuestos por el mencionado motor de búsqueda y cuya actividad se dirige a los habitantes de este Estado miembro (apartados 55 y 60 y punto 2 del fallo).

En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en un Estado miembro, pese a estar separadas, se hallan indisociablemente ligadas dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades (apartado 56).

VIII. Derecho de acceso del público a los documentos de las instituciones de la Unión Europea y protección de los datos personales

Sentencia de 29 de junio de 2010 (Gran Sala), Comisión/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, sociedad creada para importar cerveza alemana destinada a los establecimientos de despacho de bebidas alcohólicas del Reino Unido, no lograba vender su producto, ya que gran número de titulares de establecimientos de despacho de bebidas alcohólicas del Reino Unido se encontraban vinculados por contratos de compra en exclusiva que les obligaban a adquirir la cerveza a determinadas empresas cerveceras.

En virtud de la normativa del Reino Unido sobre el suministro de cerveza (en lo sucesivo, «GBP», por «Guest Beer Provision»), las empresas cerveceras británicas estaban obligadas a permitir que los titulares de establecimientos compraran cerveza procedente de otra empresa cervecera, a condición de que de que se tratara de cerveza envasada en barril. Ahora bien, la mayoría de las cervezas fabricadas fuera del Reino Unido no podían considerarse «cerveza envasada en barril» en el sentido de la GBP y no estaban comprendidas, pues, en el ámbito de aplicación de dicha disposición. Al considerar que dicha normativa constituía una medida de efecto equivalente a una restricción cuantitativa a la importación, Bavarian Lager presentó una denuncia ante la Comisión.

En el transcurso del procedimiento por incumplimiento incoado por la Comisión contra el Reino Unido, el 11 de octubre de 1996 se celebró una reunión entre representantes de las administraciones comunitaria y británica y representantes de la Confédération des brasseurs du marché commun (Confederación de empresas cerveceras del Mercado Común; en lo sucesivo, «CBMC»). Tras haber sido advertida por las autoridades británicas de la modificación de la normativa controvertida para permitir la venta de cerveza embotellada como cerveza de distinta procedencia, al igual que la cerveza envasada en barril, la Comisión informó a Bavarian Lager de la suspensión del procedimiento por incumplimiento.

Bavarian Lager solicitó obtener el acta completa de la reunión de octubre de 1996, con indicación de los nombres de todos los participantes. Mediante decisión de 18 de marzo de

2004, la Comisión desestimó la solicitud invocando la protección de la intimidad de esas personas, garantizada por el Reglamento 45/2001.

Bavarian Lager interpuso a continuación un recurso ante el Tribunal General solicitando la anulación de esa decisión de la Comisión. En su sentencia de 8 de noviembre de 2007, el Tribunal General anuló la decisión de la Comisión, considerando que la mera inscripción del nombre de los interesados en el listado de los participantes en una reunión en nombre de la entidad que representaban no suponía un perjuicio ni una amenaza para la intimidad de esas personas. La Comisión, apoyada por el Reino Unido y el Consejo, interpuso un recurso de casación ante el Tribunal de Justicia contra esa sentencia.

El Tribunal de Justicia señaló en primer lugar que, cuando una solicitud basada en el Reglamento n.º 1049/2001, [91] relativo al acceso del público a los documentos, pretende obtener el acceso a documentos que contienen datos personales, el Reglamento n.º 45/2001 es aplicable en su totalidad, incluida la disposición que impone al destinatario de la transmisión de datos personales la obligación de demostrar que la divulgación de tales datos es necesaria y la disposición que confiere a la persona afectada la posibilidad de oponerse en cualquier momento, por razones imperiosas y legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento (apartado 63).

A continuación, el Tribunal de Justicia declaró que el listado de los participantes en una reunión celebrada en el marco de un procedimiento por incumplimiento, que figura en el acta de dicha reunión, contenía datos personales, en el sentido del artículo 2, letra a), del Reglamento n.º 45/2001, ya que era posible identificar a las personas que habían podido participar en esa reunión (apartado 70).

Por último, llegó a la conclusión de que la Comisión había respetado lo dispuesto en el artículo 8, letra b), de dicho Reglamento al exigir que se demostrara la necesidad de transmitir los datos personales concernientes a las personas que no habían otorgado su consentimiento expreso a la difusión de tales datos personales (apartado 77).

En efecto, como en el marco de la solicitud de acceso a ese acta en virtud del Reglamento n.º 1049/2001 no se había presentado ninguna justificación expresa y legítima ni ningún argumento convincente para demostrar la necesidad de transmitir dichos datos personales, la Comisión no había podido poner en la balanza los distintos intereses de las partes implicadas. Tampoco había podido verificar, como exige el artículo 8, letra b), del Reglamento n.º 45/2001, si existían razones para suponer que esa transmisión pudiera perjudicar los intereses legítimos de los interesados (apartado 78). [92]

Sentencia de 16 de julio de 2015, ClientEarth y PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

La Autoridad Europea de Seguridad Alimentaria (EFSA) había creado un grupo de trabajo para elaborar una orientación sobre la forma de aplicar el artículo 8, apartado 5, del Reglamento (CE)

[91] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO 2001, L 145, p. 43).

[92] Esta sentencia fue mencionada en el Informe Anual de 2010, p. 14.

n.º 1107/2009, [93] a tenor del cual el solicitante de una autorización de comercialización de un producto fitosanitario debe adjuntar al expediente la documentación científica accesible y validada por la comunidad científica, según lo determine la EFSA, relativa a los efectos secundarios provocados por la sustancia activa y sus metabolitos pertinentes, tanto en la salud como en el medio ambiente y en las especies no objetivo.

El proyecto de orientación se sometió a información pública, y ClientEarth y Pesticide Action Network Europe (en lo sucesivo, «PAN Europe») presentaron observaciones sobre dicho proyecto. En este contexto, presentaron conjuntamente a la EFSA una solicitud de acceso a ciertos documentos relativos a la preparación del proyecto de orientación, incluidas las observaciones de los expertos externos.

La EFSA autorizó a ClientEarth y a PAN Europe el acceso a las observaciones individuales de los expertos externos sobre el proyecto de orientación. No obstante, indicó que había ocultado el nombre de esos expertos, conforme al artículo 4, apartado 1, letra b), del Reglamento n.º 1049/2001 y a la legislación de la Unión sobre la protección de los datos personales, en especial el Reglamento n.º 45/2001, alegando al respecto que la divulgación del nombre de esos expertos constituía una transmisión de datos personales en el sentido del artículo 8 del Reglamento n.º 45/2001 y que no concurrían en ese caso los requisitos para la transmisión formulados en ese artículo.

ClientEarth y PAN Europe interpusieron por tanto un recurso ante el Tribunal General para la anulación de la decisión de la EFSA. Como el Tribunal General desestimó dicho recurso, ClientEarth y PAN Europe interpusieron ante el Tribunal de Justicia un recurso de casación contra la sentencia del Tribunal General. [94]

En primer lugar, el Tribunal de Justicia señaló que, como esa información permitiría atribuir a un determinado experto una observación específica, afectaba a personas físicas identificadas y por tanto constituía un conjunto de datos personales, en el sentido del artículo 2, letra a), del Reglamento n.º 45/2001. Dado que los conceptos de «datos personales», en el sentido del artículo 2, letra a), del Reglamento n.º 45/2001, y de «datos relativos a la intimidad» no se confunden, el Tribunal de Justicia consideró, además, inoperante la alegación de ClientEarth y PAN Europe según la cual la información discutida no formaba parte de la intimidad de los expertos interesados (apartados 29 y 32).

En segundo lugar, el Tribunal de Justicia examinó el argumento de ClientEarth y PAN Europe basado en la existencia de un ambiente de desconfianza hacia la EFSA, acusada a menudo de parcialidad a causa de su recurso a expertos con intereses personales derivados de sus vínculos con los medios empresariales, y en la necesidad de garantizar la transparencia del proceso decisorio de esa autoridad. Este argumento estaba apoyado por un estudio que ponía de manifiesto los vínculos que ligaban a la mayoría de los expertos miembros de un grupo de trabajo de la EFSA con grupos de presión empresariales. A este respecto, el Tribunal de Justicia consideró que la obtención de la información controvertida se revelaba necesaria para

[93] Reglamento (CE) n.º 1107/2009 del Parlamento Europeo y del Consejo, de 21 de octubre de 2009, relativo a la comercialización de productos fitosanitarios y por el que se derogan las Directivas 79/117/CEE y 91/414/CEE del Consejo (DO 2009, L 309, p. 1).

[94] Sentencia del Tribunal General de 13 de septiembre de 2013, ClientEarth y PAN Europe/EFSA (T-214/11, EU:T:2013:483).

comprobar en concreto la imparcialidad de cada uno de los expertos en el cumplimiento de su función científica al servicio de la EFSA. En consecuencia, el Tribunal de Justicia anuló la sentencia del Tribunal General, declarando que este había estimado erróneamente que el mencionado argumento de ClientEarth y de PAN Europe no era suficiente para demostrar la necesidad de la transmisión de la información controvertida (apartados 57 a 59).

En tercer lugar, para apreciar la legalidad de la decisión impugnada de la EFSA, el Tribunal de Justicia examinó si existía o no una razón para suponer que esa transmisión habría podido perjudicar los intereses legítimos de las personas afectadas. A este respecto, el Tribunal de Justicia hizo constar que la alegación de la EFSA de que la divulgación de la información controvertida habría podido perjudicar la intimidad y la integridad de esos expertos constituía una consideración general, no sustentada de otra forma por ningún factor propio del caso específico. El Tribunal de Justicia estimó, por el contrario, que esa divulgación habría permitido por sí misma disipar las sospechas de parcialidad referidas o habría ofrecido a los expertos potencialmente afectados la ocasión de refutar el fundamento de esas alegaciones de parcialidad, en su caso a través de los medios de acción judicial disponibles. A la vista de estos elementos, el Tribunal de Justicia anuló igualmente la decisión de la EFSA (apartados 69 y 73).

* * *

Las sentencias que figuran en esta ficha están indizadas en el Repertorio de jurisprudencia en las rúbricas 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07 y 4.11.11.01.