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 noventa, de diversos instrumentos destinados a garantizar la protección de los datos personales. La Directiva 95/46/CE, [1] 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, adoptada sobre la base del artículo 100 A CE, constituye a este respecto el principal acto jurídico de la Unión en la materia. En ella se establecen las condiciones generales para la licitud del tratamiento de los datos y los derechos de los interesados, y se dispone 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/CE, armonizando las disposiciones de la legislación de los Estados miembros relativas a la protección del derecho a la

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 L 281 de 23.11.1995, p. 31), con versión consolidada de 20.11.2003, y 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 L 201 de 31.7.2002, p. 37), con versión consolidada de 19.12.2009.

intimidad, en particular en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas. [3]

Además, en el campo del espacio de libertad, seguridad y justicia (antiguos artículos 30 TUE y 31 TUE), la Decisión marco 2008/977/JAI [4] regula (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.

La Unión Europea ha elaborado recientemente un nuevo marco jurídico global en la materia. A tal fin, la Comisión ha adoptado en 2016 el Reglamento (UE) 2016/679, [5] sobre la protección de datos, que deroga la Directiva 95/46/CE y será directamente aplicable a partir del 25 de mayo de 2018, así como la Directiva (UE) 2016/680, [6] 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 expira 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 queda garantizada por el Reglamento (CE) n.º 45/2001. [7] Este Reglamento ha permitido la creación, en 2004, del Supervisor Europeo de Protección de Datos. En enero de 2017, la Comisión ha presentado la propuesta [8] de un nuevo Reglamento que derogue el Reglamento n.º 45/2001 y la Decisión n.º 1247/2002/CE, con objeto de modernizar las normas en esta materia y de armonizarlas con el nuevo régimen establecido por el Reglamento (UE) 2016/679.

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 L 105 de 13.4.2006, p. 54). Esta Directiva ha sido 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 la razón de que vulneraba 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 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 L 350 de 30.12.2008, p. 60), que quedará derogada a partir del 6 de mayo de 2018 (véase la nota 6).

5 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 L 119 de 4.5.2016, p. 1), aplicable a partir del 25 de mayo de 2018.

6 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 L 119 de 4.5.2016, p. 89).

7 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 L 8 de 12.1.2001, p. 1).

8 Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE [COM (2017) 8 final].

# 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)* [9]

En dicho 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 [10] y 259/2008, [11] 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 (CE) n.º 1290/2005 y a la del Reglamento (CE) 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).

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

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

10 Reglamento (CE) n.º 1290/2005 du Consejo, de 21 de junio de 2005, sobre la financiación de la política agrícola común (DO L 209 de 11.8.2005, 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 L 347 de 20.12.2013, p. 549).

11 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 L 76 de 19.3.2008, 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 L 255 de 28.8.2014, p. 59).

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 (CE) n.º 1290/2005 y el Reglamento (CE) 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, [12] 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 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).

12 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 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 L 142 de 6.6.2009, p. 1).

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)* [13]

Ese asunto tiene su origen en unas 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 unos 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/CE en Derecho austriaco.

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/CE 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/CE 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

13 Esta sentencia fue mencionada en el Informe Anual de 2014, p. 60.

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/CE 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 del artículo 8, apartado 3, de la Carta, el Tribunal de Justicia afirmó que la Directiva 2006/24/CE 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-98/15, EU:C:2016:970)* [14]

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

14 Esta sentencia fue mencionada en el Informe Anual de 2016, p. 62.

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 del 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], solicitaban al el Tribunal de Justicia que se pronunciara sobre la interpretación del artículo 15, apartado 1, de la Directiva 2002/58/CE, 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 confidencialidad de las comunicaciones el artículo 15, apartado 1, de la Directiva 2002/58/CE, 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 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 Directiva 95/46/CE

## 1. Tratamiento de datos personales excluidos del ámbito de aplicación de la Directiva 95/46/CE

### *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 operaran en rutas con destino u origen en Estados Unidos o que atravesaran 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, [15] 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, [16] 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.

15 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 L 235 de 6.7.2004, p. 11).

16 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 L 183 de 20.5.2004, p. 83, y corrección de errores en DO L 255, de 30.9.2005, p. 168).

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/CE. 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 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/CE, 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/CE 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/CE, 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/CE 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)* [17]

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.

En este contexto, el Bundesgerichtshof (Tribunal Federal de Justicia, 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

17 Esta sentencia fue mencionada en el Informe Anual de 2016, p. 61.

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 / 95/CE (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/CE, 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 (C-434/16, EU:C:2017:582)*

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.

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.

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/CE, 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.

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/CE.

## 3. Concepto de «tratamiento de datos personales»

### *Sentencia de 6 de noviembre de 2003 (Pleno), 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 varias 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/CE.

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 ha tenido la ocasión de precisar el concepto de «tratamiento de datos personales» en Internet con arreglo a la Directiva 95/46/CE.

El Tribunal de Justicia ha declarado 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).

## 4. Condiciones generales para la licitud del tratamiento de datos personales con arreglo al artículo 7 de la Directiva n.º 95/46/CE

### *Sentencia de 16 de diciembre de 2008 (Gran Sala), Huber (C-524/06, EU:C:2008:724)* [18]

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.

18 Esta sentencia fue mencionada en el Informe Anual de 2008, p. 45.

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), que conoce del litigio, pidió al Tribunal de Justicia que se pronunciase sobre la compatibilidad con el 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 acompañado de 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/CE, 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/CE, 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/CE, 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 tratamiento, 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/CE.

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/CE 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/CE, 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/CE 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/CE. 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 ha pronunciado igualmente sobre la cuestión de si el artículo 7, letra f), de la Directiva 95/46/CE 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/CE 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/CE, 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/CE 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/CE 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 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/CE 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/CE 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/CE 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).

# III. Transferencia de datos personales a países terceros

### *Sentencia de 6 de noviembre de 2003 (Pleno), Lindqvist (C-101/01, EU:C:2003:596)* [19]

En ese 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/CE 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 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/CE y, por otro, la inexistencia de criterios aplicables al uso de 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)* [20]

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 [21] la Comisión había estimado que, en el marco del régimen llamado de «puerto seguro» (en inglés, «safe harbour»), [22] Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos.

En este contexto, la High Court (Tribunal Superior, Irlanda) recurrió al Tribunal de Justicia por una demanda de interpretación del artículo 25, apartado 6, de la Directiva 95/46/CE, 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

19 Esta sentencia fue mencionada en el Informe Anual de 2003, p. 67.

20 Esta sentencia fue mencionada en el Informe Anual de 2015, p. 53.

21 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 L 215 du 25.8.2000, p. 7).

22 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.

2000/520/CE, adoptada por la Comisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

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/CE, el artículo 1 de esta vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46/CE, 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/CE 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 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/CE, 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/CE, 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. El Tribunal llegó a la conclusión de que la invalidez de los artículos 3 y 1 de la Decisión 2000/520/CE 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).

# IV. 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/CE.

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/CE, 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 9 de enero de 2008 (Gran Sala), Promusicae (C-275/06, EU:C:2008:54)* [23]

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 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), [24] 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, [25] 2004/48/CE, relativa al respeto de los derechos de propiedad intelectual, [26] y 2002/58/CE 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 comunitario 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).

23 Esta sentencia fue mencionada en el Informe Anual de 2008, p. 46.

24 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 L 178 du 17.7.2000, p. 1).

25 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 L 167 du 22.6.2001, p. 10).

26 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 L 157 du 30.4.2004, p. 45, y corrección de errores en DO L 195 de 2.6.2004, p. 16).

### *Sentencia de 24 de noviembre de 2011, Scarlet Extended (C-70/10, EU:C:2011:771)* [27]

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 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/CE, 2000/31/CE, 2001/29/CE, 2002/58/CE y 2004/48/CE, 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/CE, 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

27 Esta sentencia fue mencionada en el Informe Anual de 2011, p. 37.

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/CE y 2004/48/CE 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/CE, 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/CE y 2004/48/CE 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).

# V. 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)* [28]

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/CE, 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/CE 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/CE.

El Tribunal de Justicia estimó que la garantía de independencia de las autoridades de control nacionales establecida en la Directiva 95/46/CE 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 dicho 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 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,

28 Esta sentencia fue mencionada en el Informe Anual de 2010, p. 34.

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/CE 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/CE, 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/CE, 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 (CE) 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 (CE) 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 95/95/CE (apartado 58).

### *Sentencia de 8 de abril de 2014 (Gran Sala), Comisión/Hungría (C-288/12, EU:C:2014:237)* [29]

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/CE al poner fin antes de tiempo al mandato de la autoridad de control de la protección de los datos personales.

29 Esta sentencia fue mencionada en el Informe Anual de 2014, p. 62.

El Tribunal de Justicia declaró que incumple las obligaciones que le incumben en virtud de la Directiva 95/46/CE 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

### *Sentencia de 1 de octubre de 2015, Weltimmo (C-230/14, EU:C:2015:639)* [30]

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/CE.

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/CE. 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 4/46/CE 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

30 Esta sentencia fue mencionada en el Informe Anual de 2015, p. 55.

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/CE, 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, 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 III, titulada «Transferencia de datos personales a terceros países»), 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/CE, 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/CE, 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).

# VI. 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 [véase también en las secciones II.3, titulada «Concepto de "tratamiento de datos personales"», y IV.1, titulada «Derecho de oposición al tratamiento de datos personales ("derecho al olvido")»], el Tribunal de Justicia se ha pronunciado igualmente sobre el ámbito geográfico de aplicación de la Directiva 95/46/CE.

Así, el Tribunal de Justicia ha indicado ya 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/CE, 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).

# VII. 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 relativo a la protección de los datos personales.

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 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 ante el Tribunal de Justicia un recurso de casación contra esa sentencia.

El Tribunal de Justicia señaló en primer lugar que, cuando una solicitud basada en el Reglamento (CE) n.º 1049/2001, [31] relativo al acceso del público a los documentos, pretende obtener el acceso a documentos que contienen datos personales, el Reglamento (CE) 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 (CE) 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). [32]

31 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 L 145 du 31.5.2001, p. 43).

32 Esta sentencia fue mencionada en el Informe Anual de 2010, p. 14.

### *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) n.º 1107/2009, [33] 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 (CE) n.º 1049/2001 y a la legislación de la Unión sobre la protección de los datos personales, en especial el Reglamento (CE) 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 (CE) 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. [34]

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 (CE) n.º 45/2001. Dado que los conceptos de «datos personales», en el sentido del artículo 2, letra a), del Reglamento (CE) 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 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).

33 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 L 309 de 24.11.2009, p. 1).

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

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 se revisarán en el Repertorio de jurisprudencia en las rúbricas 1.04.03.07, 1.04.03.08, 1.04.03.11, 2.04, 2.05.00, 4.11.01 y 4.11.07.*