TRIBUNAL DE JUSTICIA
DE LA UNIÓN EUROPEA

ES

Ficha temática

Protección de datos de carácter personal

Dirección de Investigación y Documentación

curia.europa.eu

Introducción

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 recogido en el Derecho primario, en particular en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), así como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE). 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.

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, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, [1] derogada desde 2018, constituía a este respecto el principal acto jurídico de la Unión en la materia.

La Directiva 2002/58/CE [2] vino a completar posteriormente la Directiva 95/46, armonizando las disposiciones de la legislación de los Estados miembros relativas a la protección del derecho a la intimidad, en particular en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas. [3] Debe señalarse que, con el fin de tener en cuenta las nuevas evoluciones tecnológicas y comerciales, el legislador de la Unión ha puesto en marcha, desde 2017, una revisión de esta Directiva, [4] que actualmente sigue en curso. [5]

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), versión consolidada de 20 de noviembre, derogada a partir del 25 de mayo de 2018 (véase la nota 6).

2 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37), versión consolidada de 19 de diciembre de 2009.

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

4 La Comisión presentó el 10 de enero de 2017 una propuesta con el fin de sustituir dicha Directiva por un reglamento relativo a la intimidad y a las comunicaciones electrónicas.

5 El 10 de febrero de 2021, el Consejo de la Unión Europea aprobó un mandato de negociación dirigido a la revisión de las normas en materia de protección de la intimidad y de la confidencialidad en la utilización de los servicios de comunicaciones electrónicas que permitía entablar negociaciones con el Parlamento Europeo. El texto de la Propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas está disponible en el *siguiente* enlace: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

En 2016, la Unión Europea reformó el marco jurídico global en la materia. A tal fin, adoptó el Reglamento (UE) 2016/679, [6] sobre la protección de datos personales (en lo sucesivo, «RGPD»), que deroga la Directiva 95/46 y es aplicable desde el 25 de mayo de 2018, así como la Directiva (UE) 2016/680, [7] relativa a la protección de dichos datos en materia penal, cuyas disposiciones son aplicables desde el 6 de mayo de 2018.

En lo tocante al tratamiento de datos personales por las instituciones y los órganos de la UE, la protección de esos datos está garantizada, desde el 11 de diciembre de 2018, por el Reglamento (UE) 2018/1725. [8] En aras de un enfoque coherente de la protección de los datos personales en el conjunto de la Unión, este nuevo Reglamento tiene por objeto armonizar en la medida de lo posible la normativa en la materia con el régimen establecido por el RGPD.

Por último, con el fin de afrontar los desafíos que plantean las nuevas tecnologías, el legislador de la Unión ha impulsado, desde 2020, la adopción de nuevas medidas legislativas [9] que se articulan con las disposiciones del Derecho de la Unión relativas a la protección de los datos personales.

Habida cuenta de la abundante jurisprudencia del Tribunal de Justicia en materia de protección de datos personales, la presente ficha temática tiene por objeto presentar una selección de sentencias pioneras en la materia, así como de sentencias que han contribuido significativamente al desarrollo de esta jurisprudencia, haciendo especial hincapié en las sentencias dictadas por la Gran Sala del Tribunal de Justicia. Más concretamente, esta ficha pretende abarcar tanto la jurisprudencia relativa a la normativa general en materia de protección de datos personales, derivada de la interpretación de la Directiva 95/46 y del RGPD, como la relativa a la normativa sectorial referida, en particular, al sector de las comunicaciones electrónicas y al Derecho penal. Asimismo, aspira a presentar una selección de las sentencias referidas a normas de

---

6 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DO 2016, L 119, p. 1).

7 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

8 Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO 2018, L 295, p. 39).

9 En este marco, deben destacarse especialmente tres iniciativas legislativas: *i)* el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) (DO 2022, L 152, p. 1) y el Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos) (DO 2023, L 2854, p. 1); *ii)* un paquete legislativo sobre los servicios y mercados digitales, compuesto por el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO 2022, L 277, p. 1) y por el Reglamento 2022/1925 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2022, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (DO 2022, L 265, p. 1); e *iii)* la primera propuesta legislativa dirigida a la creación de un marco normativo en materia de inteligencia artificial, que se concretó en un reglamento relativo a la inteligencia artificial (DO 2024, L, 1689).

aplicación transversal, al mismo tiempo que se pone de manifiesto, de entrada, el papel fundamental de la Carta en el desarrollo de la jurisprudencia.

Índice

I. El derecho a la protección de los datos de carácter personal reconocido en 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*)

En este asunto, en los litigios principales se enfrentaban unos agricultores y el Land Hessen (Estado Federado de Hesse), en relación con la publicación en el sitio de Internet de la Bundesanstalt für Landwirtschaft und Ernährung (Agencia Federal de Agricultura y Alimentación, Alemania) 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 Estado Federado de Hesse consideraba, por su parte, que la publicación de los citados datos se derivaba de los Reglamentos (CE) n.os 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 beneficiarias del FEAGA y del Feader.

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

El Tribunal de Justicia señaló, en lo referente a la adecuación entre el derecho a la protección de datos de carácter personal reconocido por la Carta y la obligación de transparencia en materia de fondos europeos, que la publicación en un sitio web de los datos nominales de los beneficiarios de los fondos y de los importes percibidos por estos constituye, debido al libre acceso de terceros al sitio web, un menoscabo del

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

[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 2008, L 76, p. 28), derogado por el Reglamento de Ejecución (UE) n.º 908/2014 de la Comisión, de 6 de agosto de 2014, por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 1306/2013 del Parlamento Europeo y del Consejo en relación con los organismos pagadores y otros organismos, la gestión financiera, la liquidación de cuentas, las normas relativas a los controles, las garantías y la transparencia (DO 2014, L 255, p. 59).

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.

Para estar justificado, tal menoscabo debe estar previsto por la ley, respetar el contenido esencial de dichos derechos y, con arreglo al principio de proporcionalidad, ser necesario y responder efectivamente a objetivos de interés general reconocidos por la Unión, debiendo establecerse las excepciones y limitaciones a tales derechos sin sobrepasar los límites de lo estrictamente necesario. En este contexto, el Tribunal de Justicia estimó que, si bien, en una sociedad democrática, los contribuyentes tienen derecho a ser informados de la utilización de los fondos públicos, no es menos cierto que el Consejo y la Comisión estaban obligados a ponderar equilibradamente los diversos intereses en conflicto, lo que requería, antes de adoptar las disposiciones controvertidas, verificar si la publicación de dichos datos en un sitio web único por el Estado miembro no iba más allá de lo necesario para alcanzar los objetivos legítimos perseguidos.

Así pues, el Tribunal de Justicia declaró inválidas ciertas disposiciones del Reglamento n.º 1290/2005 y el Reglamento n.º 259/2008 en su totalidad, en la medida en que obligaban, por lo que respecta a las personas físicas beneficiarias de ayudas del FEAGA y del Feader, a publicar datos de carácter personal de todos los beneficiarios, sin establecer distinciones en función de criterios pertinentes, tales como los períodos durante los cuales dichas personas habían percibido estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas. Sin embargo, el Tribunal de Justicia no impugnó 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.

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)

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

Mediante sus peticiones de decisión prejudicial, el tribunal irlandés y el austriaco preguntaron al Tribunal de Justicia sobre la validez de la Directiva 2006/24 con arreglo a los artículos 7, 8 y 11 de la Carta. Más concretamente, dichos órganos jurisdiccionales preguntaron al Tribunal de Justicia si la obligación de conservar durante un determinado período ciertos datos relativos a la vida privada de las personas y a sus comunicaciones y de permitir que accedieran a ellos las autoridades nacionales competentes, obligación impuesta por dicha Directiva a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, suponía una injerencia injustificada en esos derechos fundamentales. Los tipos de 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.

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

Sin embargo, el Tribunal de Justicia consideró que, al adoptar la Directiva sobre la 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 esta injerencia se limitara a lo estrictamente

necesario. En efecto, la Directiva 2006/24 se aplicaba de manera generalizada a todas las personas y a todos los medios de comunicación electrónica y datos relativos al tráfico, sin establecer diferenciación, limitación o excepción alguna en función del objetivo de lucha contra los delitos graves. Por lo demás, 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. 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 las personas afectadas o de su posible utilidad para el objetivo perseguido.

Asimismo, por lo que se refiere a las exigencias derivadas del artículo 8, apartado 3, de la Carta, el Tribunal de Justicia señaló que la Directiva 2006/24 no establecía garantías suficientes que permitieran proteger de manera eficaz los datos contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de tales datos, y tampoco obligaba 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.

Sentencia de 21 de junio de 2022 (Gran Sala), Ligue des droits humains (C-817/19, EU:C:2022:491)

Los datos PNR (Passenger Name Record) consisten en información de reservas almacenada por las compañías aéreas en sus sistemas de reservas y control de las salidas. La Directiva PNR [12] obliga a estas compañías a transferir los datos de todo pasajero que viaje en un vuelo exterior de la UE, operado entre un tercer país y la Unión Europea, a la Unidad de Información sobre los Pasajeros (en lo sucesivo, «UIP») del Estado miembro de destino o de salida del vuelo en cuestión para luchar contra los delitos de terrorismo y la delincuencia grave. Los datos PNR transferidos de este modo son objeto de una evaluación previa a cargo de la UIP [13] y seguidamente se conservan para una eventual evaluación posterior por parte de las autoridades competentes del Estado miembro de que se trate o de las autoridades de otro Estado miembro. Los

[12] Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (DO 2016, L 119, p. 132) (en lo sucesivo, «Directiva PNR»).

[13] Esta evaluación previa tiene por objeto la identificación de las personas respecto de las que es necesario un examen más en profundidad por parte de las autoridades competentes, habida cuenta de que pueden estar implicadas en un delito de terrorismo o en un delito grave. La evaluación se lleva a cabo de forma sistemática y por medios automatizados, comparando los datos PNR con bases de datos «pertinentes» o tratándolos a la luz de criterios preestablecidos en el artículo 6, apartado 2, letra a), y apartado 3, de la Directiva PNR.

Estados miembros pueden decidir aplicar la Directiva también a los vuelos interiores de la Unión. [14]

La Ligue des droits humains interpuso ante la Cour constitutionnelle (Tribunal Constitucional, Bélgica) un recurso de anulación contra la ley belga que transpone al Derecho nacional tanto la Directiva PNR como la Directiva API. [15] Según la recurrente, esta ley vulnera el derecho al respeto de la vida privada y a la protección de los datos personales. La recurrente critica, por una parte, la enorme amplitud de los datos PNR y, por otra parte, el carácter general de la recogida, la transferencia y el tratamiento de estos datos. A su juicio, la Ley también es contraria a la libre circulación de personas, ya que restablece indirectamente los controles en las fronteras al extender el sistema PNR a los vuelos interiores de la Unión y a los transportes realizados por otros medios en el interior de la Unión.

En este contexto, la Cour constitutionnelle (Tribunal Constitucional) planteó al Tribunal de Justicia diversas cuestiones prejudiciales relativas, en particular, a la validez de la Directiva PNR.

Mediante su sentencia, dictada en Gran Sala, el Tribunal de Justicia confirma la validez de la Directiva PNR siempre que se interprete de conformidad con la Carta.

A este respecto, el Tribunal de Justicia declara que, dado que la interpretación que hace de las disposiciones de la Directiva PNR a la luz de los derechos fundamentales garantizados en los artículos 7, 8, 21 y 52, apartado 1, de la Carta [16] garantiza la conformidad de la Directiva con esos artículos, el examen de las cuestiones prejudiciales planteadas no pone de manifiesto ningún elemento que pueda afectar a la validez de dicha Directiva.

Con carácter preliminar, el Tribunal de Justicia recuerda que un acto de la Unión debe interpretarse, en la medida de lo posible, de un modo que no cuestione su validez y de conformidad con el conjunto del Derecho primario y, en particular, con las disposiciones de la Carta, por lo que los Estados miembros deben procurar no basarse en una interpretación del mismo que entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico de la Unión o con los demás principios generales reconocidos en este ordenamiento jurídico. En relación con la Directiva PNR, el Tribunal de Justicia precisa que muchos de sus considerandos y disposiciones exigen que se lleve a cabo tal interpretación conforme, al hacer énfasis en la importancia que el legislador

---

14 Haciendo uso de la posibilidad contemplada en el artículo 2 de la Directiva PNR.

15 Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas (DO 2004, L 261, p. 24) (en lo sucesivo, «Directiva API»). Esta Directiva regula la comunicación por los transportistas aéreos a las autoridades nacionales competentes de información anticipada sobre los pasajeros (como el número y el tipo de documento de viaje utilizado y la nacionalidad) con objeto de mejorar los controles fronterizos y combatir la inmigración ilegal.

16 Con arreglo a esta disposición, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá ser establecida por la ley y respetar su contenido esencial. Asimismo, solo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

de la Unión atribuye, cuando se refiere a un elevado nivel de protección de los datos, al pleno respeto de los derechos fundamentales consagrados por la Carta.

El Tribunal de Justicia constata que la Directiva PNR comporta injerencias de una gravedad cierta en los derechos garantizados por los artículos 7 y 8 de la Carta, ya que tiene por objeto la implantación de un régimen de vigilancia continuo, no selectivo y sistemático que incluye la evaluación automatizada de datos de carácter personal de todas las personas que utilizan servicios de transporte aéreo. Recuerda que la posibilidad de que los Estados miembros justifiquen tal injerencia debe apreciarse ponderando su gravedad y comprobando que la importancia del objetivo de interés general perseguido se corresponda con esta gravedad.

El Tribunal de Justicia concluye que cabe considerar que la transferencia, el tratamiento, y la conservación de los datos PNR previstos por esta Directiva se limitan a lo estrictamente necesario para luchar contra los delitos de terrorismo y los delitos graves, siempre que las facultades previstas por esta Directiva sean objeto de una interpretación restrictiva. A este respecto, la sentencia dictada ese día precisa, en particular, que:

- El sistema establecido por la Directiva PNR únicamente debe comprender las informaciones claramente identificables y delimitadas en las categorías que figuran en su anexo I y que guardan relación con el vuelo realizado y el pasajero de que se trate, lo que implica que, respecto de determinadas categorías de ese anexo, solo estén cubiertas las informaciones contempladas expresamente. [17]

- La aplicación del sistema establecido por la Directiva PNR debe limitarse a los delitos de terrorismo y únicamente a los delitos graves que presenten un vínculo objetivo, cuando menos indirecto, con el transporte aéreo de pasajeros. Por lo que respecta a estos últimos delitos, la aplicación de este sistema no puede extenderse a delitos que, pese a cumplir el criterio previsto por esta Directiva relativo al umbral de gravedad y a estar contemplados en su anexo II, forman parte de la delincuencia común con arreglo a las particularidades del sistema penal nacional.

- La eventual extensión de la aplicación de la Directiva PNR a todos o parte de los vuelos interiores de la Unión, opción por la que un Estado miembro puede decantarse en ejercicio de la facultad prevista por esta Directiva, debe quedar limitada a lo estrictamente necesario. A tal efecto, esta extensión debe poder quedar sujeta al control efectivo de un órgano jurisdiccional o de un organismo administrativo independiente, cuyas resoluciones tengan efecto vinculante. A este respecto, el Tribunal de Justicia precisa que:

[17] Así, en particular, «todos los datos de pago, incluida la dirección de facturación» (apartado 6 del anexo) deben quedar limitados a los medios de pago y a la facturación del billete de avión, quedando excluida cualquier otra información sin relación directa con el vuelo, y las «observaciones generales» (apartado 12) solo pueden referirse a los datos expresamente recogidos en este apartado, relativo a los pasajeros menores de edad.

- Únicamente cuando dicho Estado miembro constate la existencia de circunstancias suficientemente concretas para considerar que se enfrenta a una amenaza terrorista que resulta real y actual o previsible, la aplicación de esta Directiva a todos los vuelos interiores de la Unión con origen o destino en este Estado miembro, por un período de tiempo limitado a lo estrictamente necesario, si bien prorrogable, no debe exceder los límites de lo estrictamente necesario. [18]

- Cuando no exista tal amenaza terrorista, la aplicación de dicha Directiva no puede extenderse a la totalidad de los vuelos interiores de la Unión, sino que debe limitarse a los vuelos interiores de la Unión que cubran determinadas conexiones aéreas o que respondan a determinados planes de viaje o que se refieran a determinados aeropuertos respecto de los que existan, según la apreciación del Estado miembro de que se trate, indicios que permitan justificar esa aplicación. El carácter estrictamente necesario de esta aplicación a los vuelos interiores de la Unión seleccionados de este modo debe ser objeto de un reexamen periódico, en función de la evolución de las circunstancias que justificaran su selección.

- A efectos de la evaluación previa de los datos PNR, destinada a identificar a las personas respecto de las que resulta necesario un examen más en profundidad antes de su llegada o partida y que, en una primera fase, se realiza mediante tratamientos automatizados, la UIP, por una parte, únicamente puede comparar esos datos con las bases de datos relativas a las personas u objetos buscados o bajo alerta. [19] Estas bases de datos deben ser no discriminatorias y deben utilizarse, por las autoridades competentes, en relación con la lucha contra los delitos de terrorismo y los delitos graves que presenten un vínculo objetivo, siquiera indirecto, con el transporte aéreo de pasajeros. Por lo que se refiere, por otra parte, a la evaluación previa con arreglo a criterios predeterminados, la UIP no tiene permitido utilizar tecnologías de inteligencia artificial en el marco de sistemas de autoaprendizaje («machine learning»), capaces de modificar, sin intervención y control humanos, el proceso de evaluación y, en particular, los criterios de evaluación en los que se basa el resultado de la aplicación de este procedimiento y la ponderación de estos criterios. Estos criterios deben determinarse de forma que su aplicación cribe específicamente a los individuos respecto de los cuales pueda existir una sospecha razonable de participación en

[18] En efecto, la existencia de esta amenaza permite, por sí misma, establecer una relación entre la transferencia y el tratamiento de los datos de que se trate y la lucha contra el terrorismo. Por lo tanto, prever la aplicación de la Directiva PNR a todos los vuelos interiores de la Unión con origen o destino en el Estado miembro de que se trate, por un período de tiempo limitado, no excede de los límites de lo estrictamente necesario, debiendo poder quedar sujeta la decisión que dispone esta aplicación a un control por un órgano jurisdiccional o por una entidad administrativa independiente.

[19] Esto es, las bases de datos sobre personas u objetos buscados o bajo alerta, en el sentido del artículo 6, apartado 3, letra a), de la Directiva PNR. En cambio, los análisis a partir de bases de datos diferentes podrían adoptar la forma de una exploración de datos (data mining) y podrían dar lugar a un uso desproporcionado de estos datos, proporcionando los medios para definir el perfil preciso de las personas de que se trate por la única razón de que tienen la intención de viajar en avión.

delitos de terrorismo o en delitos graves y de manera que se tengan en cuenta tanto los elementos «de cargo» como los elementos «de descargo», evitando en cualquier caso que se produzcan discriminaciones directas o indirectas. [20]

- Habida cuenta del porcentaje de error propio de tales tratamientos automatizados de los datos PNR y del elevado número de «falsos resultados positivos», registrados durante su aplicación a lo largo de los años 2018 y 2019, la idoneidad del sistema establecido por la Directiva PNR para alcanzar los objetivos perseguidos depende fundamentalmente del buen funcionamiento de la comprobación de los resultados positivos obtenidos a raíz de esos tratamientos que debe llevar a cabo la UIP, en un segundo momento, a través de medios no automatizados. A este respecto, los Estados miembros deben establecer reglas claras y precisas que permitan guiar y delimitar el análisis efectuado por los agentes de la UIP encargados de este reexamen individual con el fin de garantizar el pleno respeto de los derechos fundamentales consagrados en los artículos 7, 8 y 21 de la Carta y, en particular, de seguir una práctica administrativa coherente en el seno de la UIP que respete el principio de no discriminación. En particular deben asegurarse de que la UIP establece criterios de reexamen objetivos que permitan a sus agentes verificar, por una parte, si y en qué medida una concordancia positiva (hit) se refiere efectivamente a un individuo que puede estar implicado en delitos de terrorismo o en delitos graves y, por otra parte, el carácter no discriminatorio de los tratamientos automatizados. En este contexto, el Tribunal de Justicia destaca asimismo que las autoridades competentes deben asegurarse de que el interesado pueda comprender el funcionamiento de los criterios de evaluación preestablecidos y de los programas que aplican estos criterios, de forma que pueda decidir, con pleno conocimiento de causa, si ejerce o no su derecho a una acción judicial. Igualmente, en el marco de tal acción, el juez encargado del control de la legalidad de la resolución adoptada por las autoridades competentes y, salvo en los casos de amenazas para la seguridad del Estado, el propio interesado, deben poder acceder al conjunto tanto de los motivos como de las pruebas sobre la base de los cuales se ha adoptado esta resolución, incluyendo los criterios de evaluación preestablecidos y el funcionamiento de los programas que aplican estos criterios.

- La comunicación y la evaluación posteriores de los datos PNR, esto es, tras la llegada o la salida de la persona en cuestión, solo pueden realizarse con base en circunstancias nuevas y elementos objetivos que, o bien permitan dar credibilidad a una sospecha razonable de implicación de esta persona en delitos

[20] Los criterios predeterminados deben ser orientados, proporcionados y específicos y deben revisarse periódicamente (artículo 6, apartado 4, de la Directiva PNR). La evaluación previa a la luz de criterios predeterminados debe llevarse a cabo de forma no discriminatoria. Según el artículo 6, apartado 4, cuarta frase, de la Directiva PNR, los criterios no se basarán en ningún caso en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

graves que presenten un vínculo objetivo, siquiera indirecto, con el transporte aéreo de pasajeros, o bien permitan considerar que estos datos podrían, en un caso concreto, suponer una contribución activa a la lucha contra delitos de terrorismo que presentan tal vínculo. La comunicación de los datos PNR a efectos de tal evaluación posterior debe, en principio, salvo en casos de urgencia debidamente justificada, quedar supeditada a un control previo realizado por un órgano jurisdiccional o por una autoridad administrativa independiente a petición motivada de las autoridades competentes, y ello con independencia de si esta petición se presenta antes o después de la expiración del plazo de los seis meses siguientes a la transferencia de esos datos a la UIP. [21]

Sentencia de 22 de noviembre de 2022 (Gran Sala), Luxembourg Business Registers (C-37/20 y C-601/20, EU:C:2022:912)

En aras de la lucha y prevención contra el blanqueo de capitales y la financiación del terrorismo, la Directiva antiblanqueo [22] obliga a los Estados miembros a llevar un registro que contenga información sobre la titularidad real [23] de sociedades y otras entidades jurídicas constituidas en su territorio. A raíz de una modificación de esta Directiva por la Directiva 2018/843, [24] una parte de esa información debe estar en todos los casos a disposición de cualquier miembro del público en general. De conformidad con la Directiva antiblanqueo modificada de este modo (en lo sucesivo, «Directiva antiblanqueo modificada»), la legislación luxemburguesa creó un Registro de la Titularidad Real (en lo sucesivo, «RTR») destinado a conservar y poner a disposición una serie de datos sobre la titularidad real de las entidades registradas a los que toda persona tiene acceso.

En este contexto, el Tribunal d'arrondissement de Luxembourg (Tribunal de Distrito de Luxemburgo) conoce de dos demandas, presentadas respectivamente por WM y Sovim SA, por las que se impugna la denegación, por Luxembourg Business Registers, autoridad gestora del RTR, de sus solicitudes para impedir el acceso del público en general a los datos relativos, en el primer asunto, a WM como titular real de una sociedad civil inmobiliaria, y, en el segundo asunto, a la titularidad real de Sovim SA. En el marco de esos dos asuntos, el Tribunal d'arrondissement de Luxembourg (Tribunal de Distrito de Luxemburgo), al albergar dudas sobre la validez de las disposiciones del

[21] Con arreglo al artículo 12, apartados 1 y 3, de la Directiva PNR, tal control solo está expresamente previsto respecto de las solicitudes de comunicación de datos PNR presentadas una vez finalizado el período de seis meses tras la transferencia de estos datos a la UIP.

[22] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DO 2015, L 141, p. 73; en lo sucesivo, «Directiva antiblanqueo»).

[23] A tenor del artículo 3, punto 6, de la Directiva antiblanqueo, los titulares reales son la persona o personas físicas que tengan la propiedad o el control en último término del cliente o la persona o personas físicas por cuenta de las cuales se lleve a cabo una transacción o actividad.

[24] Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE (DO 2018, L 156, p. 43).

Derecho de la Unión que establecen el sistema de acceso público a la información sobre la titularidad real, planteó al Tribunal de Justicia una cuestión prejudicial de validez.

Mediante su sentencia, el Tribunal de Justicia, constituido en Gran Sala, declara inválida la Directiva 2018/843 en la medida en que modificó la Directiva antiblanqueo en el sentido de que los Estados miembros deberán garantizar que la información sobre la titularidad real de las sociedades y otras entidades jurídicas constituidas en su territorio esté en todos los casos a disposición de cualquier miembro del público en general. [25]

En primer lugar, el Tribunal de Justicia aprecia que el acceso del público en general a la información sobre la titularidad real, prevista por la Directiva antiblanqueo modificada, constituye una injerencia grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal, consagrados respectivamente en los artículos 7 y 8 de la Carta.

A este respecto, el Tribunal de Justicia observa que, toda vez que los datos de que se trata incluyen información sobre personas físicas identificadas, a saber, los titulares reales de las sociedades y otras entidades jurídicas constituidas en el territorio de los Estados miembros, el acceso de cualquier miembro del público en general a esta afecta al derecho fundamental al respeto de la vida privada. Además, su puesta a disposición del público en general constituye un tratamiento de datos personales. Añade que tal puesta a disposición del público en general constituye una injerencia en los dos derechos fundamentales antes citados, cualquiera que sea la utilización posterior de la información comunicada.

Por lo que respecta a la gravedad de esta injerencia, el Tribunal de Justicia señala que, en la medida en que la información puesta a disposición del público en general se refiere a la identidad del titular real y a la naturaleza y alcance de sus intereses reales en sociedades u otras entidades jurídicas, puede permitir elaborar un perfil sobre determinados datos personales identificativos y sobre la situación patrimonial del interesado y los sectores económicos, países y empresas específicos en los que ha invertido. Además, dicha información resulta accesible para un número potencialmente ilimitado de personas, de modo que tal tratamiento de datos personales también puede permitir el libre acceso a esos datos por parte de personas que, por razones ajenas al objetivo de interés general perseguido por la citada medida, pretendan informarse sobre la situación, en particular, material y económica de un titular real. Esta posibilidad resulta aún más plausible cuando los datos pueden consultarse en Internet. Por otra parte, las consecuencias que para las personas afectadas podrían derivarse de una posible utilización abusiva de sus datos personales se ven agravadas por el hecho de que esos datos, una vez puestos a disposición del público en general, no solo pueden ser libremente consultados, sino también conservados y difundidos, de manera que

[25] Invalidez del artículo 1, punto 15, letra c), de la Directiva 2018/843, por el que se modifica el artículo 30, apartado 5, párrafo primero, letra c), de la Directiva antiblanqueo.

para esas personas se hace aún más difícil, incluso ilusorio, defenderse eficazmente contra abusos.

En segundo lugar, en el marco del examen de la justificación de la injerencia de que se trata, el Tribunal de Justicia observa en primer término que, en el caso de autos, se respeta el principio de legalidad. En efecto, la limitación del ejercicio de los derechos fundamentales antes mencionados resultante del acceso del público en general a los datos sobre la titularidad real está prevista en un acto legislativo, a saber, la Directiva antiblanqueo modificada. Además, por un lado, esta Directiva precisa que dichos datos deben ser adecuados, exactos y actuales y enumera expresamente determinados datos a los que debe concederse acceso público. Por otro lado, establece las condiciones en las que los Estados miembros pueden establecer excepciones a tal acceso.

En segundo término, el Tribunal de Justicia precisa que la injerencia en cuestión no menoscaba el contenido esencial de los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta. Si bien es cierto que la Directiva antiblanqueo modificada no contiene una enumeración exhaustiva de los datos a los que debe permitirse el acceso a cualquier miembro del público en general y que los Estados miembros podrán dar acceso a información adicional, no lo es menos que solo la información adecuada sobre la titularidad real y los intereses reales ostentados puede obtenerse, conservarse y, por tanto, ponerse potencialmente a disposición del público, lo que excluye, en particular, la información que no guarda relación adecuada con las finalidades de la Directiva antiblanqueo modificada. Pues bien, no parece que la puesta a disposición del público en general de información que sí guarda ese tipo de relación menoscabe de algún modo el contenido esencial de los derechos fundamentales de que se trata.

En tercer término, el Tribunal de Justicia subraya que, al prever el acceso del público en general a la información sobre la titularidad real, el legislador de la Unión pretende prevenir el blanqueo de capitales y la financiación del terrorismo estableciendo, mediante una mayor transparencia, un entorno menos susceptible de ser utilizado con tales fines, lo que constituye un objetivo de interés general que puede justificar injerencias, incluso graves, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

En cuarto término, en el marco del examen del carácter idóneo, necesario y proporcionado de la injerencia en cuestión, el Tribunal de Justicia observa que, ciertamente, el acceso del público en general a la información sobre la titularidad real es idóneo para contribuir a la consecución de dicho objetivo.

No obstante, estima que esta injerencia no puede considerarse limitada a lo estrictamente necesario. Por una parte, no puede demostrarse la estricta necesidad de dicha injerencia basándose en el hecho de que el criterio del «interés legítimo» del que, según la Directiva antiblanqueo en su versión anterior a su modificación por la Directiva 2018/843, debía disponer cualquier persona que deseara acceder a la información sobre la titularidad real, era difícil de aplicar y su aplicación podía dar lugar a decisiones

arbitrarias. En efecto, la eventual existencia de dificultades para definir con precisión los supuestos y las condiciones en las que el público puede acceder a la información sobre la titularidad real no puede justificar que el legislador de la Unión prevea el acceso del público en general a esa información.

Por otra parte, las explicaciones que figuran en la Directiva 2018/843 tampoco pueden demostrar la estricta necesidad de la injerencia en cuestión. [26] En la medida en que, según esas explicaciones, el acceso del público en general a la información sobre la titularidad real posibilita un mayor control de la información por parte de la sociedad civil, en particular la prensa o las organizaciones de la sociedad civil, el Tribunal de Justicia señala que tanto la prensa como las organizaciones de la sociedad civil que presentan relación con la prevención y la lucha contra el blanqueo de capitales y la financiación del terrorismo tienen interés legítimo en acceder a la información de que se trata. Lo mismo sucede con las personas que desean conocer la identidad de los titulares reales de una sociedad o de otra entidad jurídica por el hecho de que pueden emprender transacciones con ellas, o incluso las instituciones financieras y las autoridades que participan en la lucha contra infracciones en materia de blanqueo de capitales o de financiación del terrorismo.

Además, la injerencia en cuestión tampoco presenta un carácter proporcionado. A este respecto, el Tribunal de Justicia declara que las normas sustantivas que delimitan esa injerencia no reúnen el requisito de claridad y precisión. En efecto, la Directiva antiblanqueo modificada prevé el acceso de cualquier miembro del público en general «como mínimo» a la información contemplada en esta disposición, y confiere a los Estados miembros la facultad de dar acceso a información adicional que incluirá, «como mínimo», la fecha de nacimiento o los datos de contacto del titular real en cuestión. Pues bien, al emplear la expresión «como mínimo», esta directiva autoriza la puesta a disposición del público de datos que no están suficientemente definidos ni son identificables.

Por lo demás, en lo que atañe a la ponderación entre la gravedad de esa injerencia y la importancia del objetivo de interés general perseguido, el Tribunal de Justicia reconoce que, habida cuenta de su importancia, este objetivo puede justificar injerencias, incluso graves, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

Sin embargo, por una parte, la lucha contra el blanqueo de capitales y la financiación del terrorismo incumbe prioritariamente a las autoridades públicas y a entidades como las entidades de crédito o las entidades financieras a las que, por razón de sus actividades, se imponen obligaciones específicas en la materia. Por este motivo, la Directiva antiblanqueo modificada prevé que la información sobre la titularidad real debe estar en todos los casos a disposición de las autoridades competentes y de las unidades de

[26] Se refiere a las explicaciones que figuran en el considerando 30 de la Directiva 2018/843.

inteligencia financiera, sin ninguna restricción, así como de las entidades obligadas, en el marco de la diligencia debida con respecto al cliente. [27]

Por otra parte, en comparación con un régimen anterior que preveía, además del acceso de las autoridades competentes y de ciertas entidades a la información sobre la titularidad real, el de toda persona u organización que pudiera demostrar un interés legítimo, el régimen introducido por la Directiva 2018/843 representa un menoscabo considerablemente más grave de los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta, sin que esta mayor gravedad se compense con los eventuales beneficios que, en lo que atañe a la lucha contra el blanqueo de capitales y la financiación del terrorismo, podrían resultar de este último régimen en comparación con el primero.

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

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

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

El día siguiente al pronunciamiento de la sentencia Digital Rights Ireland y Seitlinger y otros, la empresa de telecomunicaciones Tele2 Sverige notificó a la autoridad sueca de control de los servicios de correos y telecomunicaciones su decisión de no seguir conservando los datos y su intención de suprimir los datos ya registrados (asunto C-203/15). En efecto, el Derecho sueco obligaba a los proveedores de servicios de comunicaciones electrónicas a conservar de manera sistemática y continuada, sin ninguna excepción, todos los datos de tráfico y de localización de todos sus abonados y usuarios registrados, en relación con todos los medios de comunicación electrónica. En el asunto C-698/15, tres personas habían interpuesto recursos contra el régimen británico de conservación de datos, que permitía que el Ministro de Interior obligara a los operadores de telecomunicaciones públicas a conservar todos los datos relativos a las comunicaciones, exceptuando el contenido de dichas comunicaciones, durante un período máximo de doce meses.

[27] Artículo 30, apartado 5, párrafo primero, letras a) y b), de la Directiva antiblanqueo modificada.

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

En su sentencia, el Tribunal de Justicia comenzó por afirmar que el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11, y 52, apartado 1, de la Carta, se opone a una normativa nacional, como la sueca, que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Según el Tribunal de Justicia, una normativa nacional de este tipo sobrepasa 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.

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.

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 establecido. 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 que pueda delimitarse en la práctica de modo efectivo 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 dirigirse a 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.

II. El tratamiento de datos personales con arreglo a la normativa general en la materia

1. Ámbito de aplicación de la normativa general

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 estaban 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, [28] 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 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, [29] 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

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

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

datos PNR a las aduanas estadounidenses por parte de las compañías aéreas establecidas en el territorio de los Estados miembros de la Comunidad.

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

Por lo que se refiere a la Decisión de protección adecuada, el Tribunal de Justicia examinó, en primer lugar, si la Comisión podía adoptar tal Decisión sobre la base de la Directiva 95/46. En este contexto, señaló que se deducía de la Decisión de protección adecuada que la transferencia de los datos 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 PNR en el marco de una actividad sometida al Derecho de la Unión, a saber, la venta de un billete de avión que daba 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.

A este respecto, el Tribunal de Justicia señaló que el hecho de que los datos 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.

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

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 en cuestión, 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 por considerar que el editor había publicado legalmente la información en cuestión, pero la estimó, en cambio, 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.

En esta sentencia, el Tribunal de Justicia también se pronunció sobre el ámbito de aplicación territorial de la Directiva 95/46.

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

En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en un Estado miembro, a pesar de ser distintas, están 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.

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, República Checa), 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 debido a 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.

A este respecto, 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 limitaciones de esa protección no excedan de lo estrictamente necesario. Teniendo en cuenta que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que puede vulnerar las libertades fundamentales y, en particular, el derecho a la intimidad o la protección de la vida privada, deben necesariamente interpretarse 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. Además, el propio texto de esta disposición excluye del ámbito de aplicación de la Directiva 95/46 el tratamiento de datos efectuado en el ejercicio de actividades «exclusivamente» personales o domésticas. Ahora bien, en la medida en que una vigilancia por videocámara se extienda, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente «personal o doméstica», en el sentido de dicha disposición.

Sentencia de 16 de enero de 2024 (Gran Sala), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

El Nationalrat (Cámara Baja del Parlamento, Austria) constituyó una comisión de investigación (en lo sucesivo, «comisión de investigación BVT») para inquirir acerca de la existencia de una posible influencia política sobre la Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Agencia Federal de Protección Constitucional y Lucha contra el Terrorismo, Austria). [30] Esta comisión de investigación oyó a WK en calidad de testigo. A pesar de que ese testigo había solicitado permanecer en el anonimato, el acta de esta audiencia fue publicada en el sitio de Internet del Parlament Österreich (Parlamento austriaco) incluyendo su nombre y apellidos completos. Al estimar que tal divulgación de su identidad era contraria al RGPD y a la legislación austriaca, WK presentó una reclamación ante la Österreichische Datenschutzbehörde (Autoridad de Protección de Datos, Austria) (en lo sucesivo, «Datenschutzbehörde»). Mediante resolución de 18 de septiembre de 2019, la Datenschutzbehörde se declaró incompetente para pronunciarse sobre la reclamación por entender que el principio de separación de poderes excluía que, como órgano del poder ejecutivo, pudiera controlar la comisión de investigación BVT, la cual forma parte del poder legislativo.

Tras la resolución del Bundesverwaltungsgericht (Tribunal Federal de lo Contencioso-Administrativo, Austria) por la que se estimó el recurso interpuesto por WK y se anuló la resolución de la Datenschutzbehörde, esta última recurrió en casación ante el Verwaltungsgerichtshof (Tribunal Supremo de lo Contencioso-Administrativo, Austria).

En este contexto, el órgano jurisdiccional remitente preguntó al Tribunal de Justicia si las actividades de una comisión de investigación creada por el Parlamento de un Estado miembro están incluidas en el ámbito de aplicación del RGPD y si este Reglamento se aplica en caso de que estas actividades se refieran a la protección de la seguridad nacional.

En primer lugar, el Tribunal de Justicia recuerda que el artículo 2, apartado 2, letra a), del RGPD, según el cual ese Reglamento no se aplica al tratamiento de datos personales realizado en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, tiene como único objeto excluir de su ámbito de aplicación los tratamientos de datos personales efectuados por autoridades estatales en el marco de una actividad dirigida a preservar la seguridad nacional o una actividad que pueda incluirse en la misma categoría, de modo que el mero hecho de que una actividad sea propia del Estado o de una autoridad pública no basta para excluir automáticamente la aplicación del RGPD a tal actividad.

[30] El 1 de diciembre de 2021 esta entidad pasó a convertirse en la «Direktion Staatsschutz und Nachrichtendienst» (Dirección de Seguridad del Estado y Servicio de Información, Austria).

Esta interpretación, que ya se desprende del hecho de que no se establece distinción alguna en función de la identidad del autor del tratamiento en cuestión, queda confirmada por el artículo 4, punto 7, del RGPD. [31]

El Tribunal de Justicia precisa que la naturaleza parlamentaria de la comisión de investigación BVT no implica que sus actividades queden excluidas del ámbito de aplicación del RGPD. Así, la excepción prevista en el artículo 2, apartado 2, letra a), del RGPD se refiere únicamente a categorías de actividades que, por su naturaleza, no están comprendidas en el ámbito de aplicación del Derecho de la Unión, y no a categorías de personas. Por lo tanto, el hecho de que el tratamiento de datos personales sea efectuado por una comisión de investigación creada por el Parlamento de un Estado miembro en el ejercicio de su facultad de control del poder ejecutivo no permite, como tal, apreciar que dicho tratamiento se efectúa en el marco de una actividad que no está comprendida en el ámbito de aplicación del Derecho de la Unión.

En segundo lugar, el Tribunal de Justicia señala que, si bien corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizarla, [32] el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho. Pues bien, la excepción prevista en el artículo 2, apartado 2, letra a), del RGPD se refiere únicamente a categorías de actividades que, por su naturaleza, no están comprendidas en el ámbito de aplicación del Derecho de la Unión. A este respecto, el hecho de que el responsable del tratamiento sea una autoridad pública cuya actividad principal es garantizar la seguridad nacional no basta, como tal, para excluir del ámbito de aplicación del RGPD los tratamientos de datos personales que esta efectúe en el marco de sus demás actividades.

En el presente caso, el control político que lleva a cabo la comisión de investigación BVT no parece constituir, como tal, una actividad dirigida a preservar la seguridad nacional o que pueda incluirse en la misma categoría. En consecuencia, y sin perjuicio de que el órgano jurisdiccional remitente realice las comprobaciones oportunas, esta actividad no está excluida del ámbito de aplicación del RGPD.

Dicho lo anterior, una comisión parlamentaria de investigación puede tener acceso a datos personales que, por razones de seguridad nacional, deben gozar de una protección especial. A este respecto, es posible establecer limitaciones, a través de medidas legislativas, a las obligaciones y derechos previstos en el RGPD para garantizar, en particular, la seguridad nacional. [33] Así pues, con este fundamento pueden quedar justificadas limitaciones relativas a la recogida de datos personales, a la información de

[31] Este define el concepto de «responsable del tratamiento» o «responsable» en el sentido de que se refiere a «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento».

[32] Con arreglo al artículo 4 TUE, apartado 2.

[33] Según el artículo 23 del RGPD.

los interesados y a su acceso a dichos datos o, incluso, a la divulgación de estos, sin el consentimiento de los interesados, a personas distintas del responsable del tratamiento, siempre que tales limitaciones respeten en lo esencial los derechos y libertades fundamentales de los interesados y constituyan una medida necesaria y proporcionada en una sociedad democrática.

Sin embargo, el Tribunal de Justicia señala que de los autos que obran en su poder no se desprende que la comisión de investigación BVT haya alegado que la divulgación de los datos personales del interesado fuera necesaria para proteger la seguridad nacional y estuviera basada en una medida legislativa nacional prevista a tal efecto, extremo que, en su caso, corresponde comprobar al órgano jurisdiccional remitente.

2. Concepto de «datos de carácter personal»

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

El Sr. Breyer había presentado ante los tribunales civiles 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 al finalizar cada consulta de sitios de Internet de organismos federales alemanes. 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 una serie de 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*, relacionar, mediante ficheros accesibles al público, 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 Supremo de lo Civil y Penal, Alemania), que conocía del recurso de casación, planteó al Tribunal de Justicia la cuestión de si una dirección IP registrada por un proveedor de servicios de medios en línea con ocasión de un acceso a su sitio de Internet constituye para este un dato personal.

En primer lugar, el Tribunal de Justicia consideró que para que un dato pueda ser calificado de «dato personal» en el sentido del artículo 2, letra a), de la Directiva 95/46 no es preciso que toda la información que permita identificar al interesado se encuentre en poder de una sola persona. El hecho de que la información adicional necesaria para identificar al usuario de un sitio de Internet no esté en poder del proveedor de servicios

de medios en línea, sino del proveedor de acceso a Internet de ese usuario, no parece que pueda excluir que las direcciones IP dinámicas registradas por el proveedor de servicios de medios en línea constituyan, para este, datos personales en el sentido del artículo 2, letra a), de la Directiva 95/46.

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

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

El Sr. Nowak, un contable en prácticas, había suspendido el examen organizado por el Instituto de Auditores Públicos de Irlanda. Había presentado, 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 y que estaban en poder del Instituto de Auditores Públicos. Este último había remitido al Sr. Nowak ciertos documentos, pero rehusó enviarle su examen, basándose en que no contenía datos personales que le concernieran, a efectos de lo establecido en la Ley de Protección de Datos.

Como el Comisario de Protección de Datos tampoco tramitó su solicitud de acceso a dicho documento por los mismos motivos, el Sr. Nowak acudió ante los tribunales nacionales. La Supreme Court (Tribunal Supremo, Irlanda), al conocer 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 relativos al candidato, 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. Asimismo, afirmó que, en el supuesto de que el examinador no conozca la identidad del aspirante al evaluar las respuestas dadas por este en un examen, la entidad que organice el examen (en ese caso, el Instituto de Auditores Públicos) 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 manifiesta, en particular, en 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 aspirante durante el examen, son datos relativos a este aspirante, 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 declaró que las respuestas escritas de un aspirante en un examen profesional y las eventuales anotaciones al respecto del examinador pueden someterse a una comprobación, en particular, de su exactitud y de la necesidad de su conservación, a efectos del artículo 6, apartado 1, letras d) y e), de la Directiva 95/46, y pueden ser objeto de rectificación o de supresión, 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 última, 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 dicho aspirante tiene o no ese derecho de acceso también en virtud de la normativa nacional aplicable al procedimiento de examen. Sin embargo, el Tribunal de Justicia subrayó que los derechos de acceso y de 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 aspirante.

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.

3. Concepto de «tratamiento de datos personales»

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

La Sra. Lindqvist, que trabajaba como voluntaria en una parroquia de la Iglesia protestante de Suecia, había creado con su ordenador personal varias páginas web que contenían datos personales de diversas 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 sueca (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 sensibles.

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

El Tribunal de Justicia declaró que la operación consistente 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. En efecto, tal 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 la categoría de actividades que tienen 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.

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

En esta sentencia (véase asimismo la sección II.1., titulada «Ámbito de aplicación de la normativa general»), el Tribunal de Justicia tuvo ocasión de precisar el concepto de «tratamiento de datos personales» en Internet a la luz de la Directiva 95/46.

Así, el Tribunal de Justicia declaró que la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales» cuando esa información contiene datos personales. 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.

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

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

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

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

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

En virtud de la normativa letona sobre circulación vial, [34] la información relativa a los puntos impuestos a conductores inscritos en dicho registro es accesible al público y es comunicada por la CSDD a cualquier persona que lo solicite, sin que se tenga que justificar un interés específico en obtener dicha información, incluidos operadores económicos a efectos de reutilización. Al albergar dudas sobre la legalidad de esta

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

normativa, B interpuso un recurso de inconstitucionalidad ante la Latvijas Republikas Satversmes tiesa (Tribunal Constitucional, Letonia), para que este órgano jurisdiccional examinara la conformidad de dicha normativa con el derecho al respeto de la vida privada.

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

Mediante su sentencia, pronunciada en Gran Sala, el Tribunal de Justicia considera que el tratamiento de datos personales relativos a los puntos constituye un «tratamiento de datos personales relativos a condenas e infracciones penales», [35] para el que el RGPD prevé una mayor protección debido al carácter especialmente sensible de los datos en cuestión.

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

Así pues, por una parte, dicho tratamiento no está cubierto por la excepción relativa a la no aplicación del RGPD a un tratamiento efectuado en el marco de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión. [36] Debe considerarse que la citada excepción tiene como único objeto excluir del ámbito de aplicación de ese Reglamento al tratamiento de datos personales efectuado por autoridades estatales en el marco de una actividad dirigida a preservar la seguridad nacional o de una actividad que pueda incluirse en la misma categoría. Estas actividades comprenden, en particular, las que tienen por objeto proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad. Ahora bien, las actividades relativas a la seguridad vial no persiguen este objetivo y, por lo tanto, no pueden incluirse en la categoría de las actividades que tienen por objeto la preservación de la seguridad nacional.

Por otra parte, la comunicación de datos personales relativos a los puntos tampoco es un tratamiento comprendido por la excepción que prevé que no se aplique el RGPD al tratamiento de datos personales efectuado por las autoridades competentes en materia penal. [37] El Tribunal de Justicia observa, en efecto, que no puede considerarse que, en el ejercicio de dicha comunicación, la CSDD sea una de esas «autoridades competentes». [38]

---

35 Artículo 10 del RGPD.

36 Artículo 2, apartado 2, letra a), del RGPD.

37 Artículo 2, apartado 2, letra d), del RGPD.

38 Artículo 3, apartado 7, de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

Para determinar si el acceso a los datos personales relativos a infracciones de tráfico, como los puntos, constituye un tratamiento de datos personales relativos a «infracciones», [39] los cuales gozan de una mayor protección, el Tribunal de Justicia constata, basándose en particular en la génesis del RGPD, que este concepto se refiere exclusivamente a las infracciones penales. No obstante, el hecho de que, en el sistema jurídico letón, las infracciones de tráfico estén tipificadas como infracciones administrativas no es determinante para apreciar si tales infracciones están comprendidas en el concepto de «infracción penal», en la medida en que se trata de un concepto autónomo del Derecho de la Unión que exige, en toda la Unión, una interpretación autónoma y uniforme. Así pues, tras recordar los tres criterios pertinentes para apreciar el carácter penal de una infracción, a saber, la calificación jurídica de la infracción en Derecho interno, la naturaleza de la infracción y el grado de severidad de la sanción impuesta, el Tribunal de Justicia declara que las infracciones de tráfico en cuestión están comprendidas en el concepto de «infracción» en el sentido del RGPD. Por lo que respecta a los dos primeros criterios, el Tribunal de Justicia constata que, aunque las infracciones no se califiquen de «penales» en Derecho nacional, tal carácter puede derivarse de la naturaleza de la infracción y, especialmente, de la finalidad represiva que persiga la sanción que la infracción puede implicar. Pues bien, en el caso de autos, la atribución de puntos por infracciones de tráfico, al igual que las demás sanciones que la comisión de aquellas puede implicar, persiguen, entre otras cosas, tal finalidad represiva. En cuanto al tercer criterio, el Tribunal de Justicia observa que solo las infracciones de tráfico de cierta gravedad implican la imposición de puntos y que, por lo tanto, pueden dar lugar a sanciones de cierta severidad. Además, la imposición de tales puntos se suma generalmente a la sanción impuesta, y la acumulación de estos puntos conlleva consecuencias jurídicas que pueden incluso llegar a la prohibición de conducir.

Sentencia de 5 de diciembre de 2023 (Gran Sala), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

En 2020, para gestionar mejor la pandemia de COVID-19, las autoridades lituanas decidieron organizar la adquisición de una aplicación informática móvil. Esta aplicación debía contribuir a un seguimiento epidemiológico, permitiendo registrar y realizar un seguimiento de datos de las personas expuestas al virus de la COVID-19.

A tal fin, el Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Centro Nacional de Salud Pública adscrito al Ministerio de Sanidad, Lituania; en lo sucesivo, «CNSP»), encargado de dicha adquisición, se puso en contacto con la sociedad UAB IT sprendimai sėkmei (en lo sucesivo, «sociedad ITSS»), solicitándole la creación de tal aplicación móvil. Posteriormente, los empleados del CNSP remitieron a

[39] Artículo 10 del RGPD.

esta sociedad correos electrónicos, en particular, sobre las cuestiones que debían figurar en dicha aplicación.

Durante el período comprendido entre abril y mayo de 2020, la aplicación móvil creada por la empresa ITSS se puso a disposición del público. Por consiguiente, 3 802 personas hicieron uso de ella y proporcionaron diversos datos que les concernían, solicitados mediante esta aplicación. Sin embargo, debido a una falta de financiación, el CNSP no adjudicó a la sociedad ITSS ningún contrato público para la adquisición oficial de su aplicación móvil y puso fin al procedimiento correspondiente.

Mientras tanto, la autoridad nacional de control inició una investigación sobre el tratamiento de los datos personales resultantes de la utilización de dicha aplicación. Mediante decisión de dicha autoridad, adoptada al término de la investigación, se impusieron multas administrativas tanto al CNSP como a la sociedad ITSS, considerada corresponsable del tratamiento.

El CNSP impugnó esta resolución ante el Vilniaus apygardos administracinis teismas (Tribunal Regional de lo Contencioso-Administrativo de Vilna, Lituania). Al albergar dudas sobre la interpretación de varias disposiciones del RGPD, dicho órgano jurisdiccional planteó una petición de decisión prejudicial al Tribunal de Justicia.

En su sentencia, el Tribunal de Justicia, constituido en Gran Sala, aporta precisiones, entre otros, sobre el concepto de «tratamiento». A este respecto, indica que la utilización de datos personales para pruebas informáticas de una aplicación móvil constituye un tratamiento a efectos del RGPD. Sin embargo, no sería así si tales datos se hubieran anonimizado de modo que la persona a la que conciernen no fuera o ya no fuera identificable o si se tratara de datos ficticios que no se refiriesen a una persona física existente

En efecto, por una parte, la cuestión de si los datos personales se utilizan para realizar pruebas informáticas o para otro fin carece de incidencia en la calificación de la operación de «tratamiento». Por otra parte, solo un tratamiento que tenga por objeto datos personales puede calificarse de «tratamiento» en el sentido del RGPD. Ahora bien, los datos ficticios o anónimos no constituyen datos personales.

4. Concepto de «fichero de datos personales»

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

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

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

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

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

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

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

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

La autoridad alemana de protección de datos, en su condición de autoridad de control, en el sentido del artículo 28 de la Directiva 95/46, había ordenado a una empresa alemana, especializada en el ámbito de la educación y que ofrecía servicios de

formación mediante una página de fans alojada en el sitio de la red social Facebook, desactivar su página de fans. Según la citada autoridad, ni esa empresa ni Facebook habían informado a los visitantes de la página de fans de que esta recogía, mediante «cookies», datos personales relativos a ellos y de que después dicha empresa y Facebook trataban esos datos.

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

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

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

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

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

En primer lugar, el Tribunal de Justicia declaró que el administrador de un sitio de Internet, como Fashion ID, puede ser considerado responsable del tratamiento, en el sentido del artículo 2, letra d), de la Directiva 95/46. Sin embargo, esa responsabilidad se

limita a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente, a saber, la recogida y la comunicación por transmisión de datos en cuestión. En cambio, según el Tribunal de Justicia, cabe excluir en principio, que Fashion ID determine los fines y los medios de las operaciones ulteriores de tratamiento de datos personales, efectuadas por Facebook Ireland tras su transmisión a esta última, de modo que Fashion ID no puede ser considerada responsable de esas operaciones, en el sentido de dicho artículo 2, letra d).

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

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

Sentencia de 5 de diciembre de 2023 (Gran Sala), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

En este asunto (véase también la sección I.3, titulada «Concepto de “tratamiento de datos personales”»), el Tribunal de Justicia señala que una entidad que ha encargado a una empresa el desarrollo de una aplicación informática móvil y que, en este contexto, ha participado en la determinación de los fines y medios del tratamiento de datos personales realizado mediante esta aplicación puede ser considerada responsable del tratamiento. [40] Esta consideración no queda desvirtuada por el hecho de que la propia entidad no haya realizado operaciones de tratamiento de tales datos, de que no haya dado expresamente su consentimiento para la realización de las operaciones concretas de tal tratamiento o para la puesta a disposición del público de dicha aplicación móvil y de que no haya adquirido esa misma aplicación móvil, a menos que, antes de esa puesta a disposición del público, la referida entidad se haya opuesto expresamente a ella y al tratamiento de los datos personales resultante.

[40] En el sentido del artículo 4, punto 7, del RGPD.

6. Concepto de «corresponsable del tratamiento»

Sentencia de 5 de diciembre de 2023 (Gran Sala), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

En este asunto (véanse también las secciones I.3 y I.5, tituladas «Concepto de "tratamiento de datos personales"» y «Concepto de "responsable del tratamiento de datos personales"»), el Tribunal de Justicia señala que la calificación de dos entidades como corresponsables del tratamiento no presupone ni la existencia de un acuerdo entre esas entidades sobre la determinación de los fines y medios del tratamiento de datos personales ni la existencia de un acuerdo que establezca los requisitos relativos a la corresponsabilidad del tratamiento. Ciertamente, en virtud del RGPD, [41] los corresponsables del tratamiento deben determinar de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por dicho Reglamento. Sin embargo, la existencia de tal acuerdo no constituye un requisito previo para que dos o más entidades sean calificadas de «corresponsables del tratamiento», sino una obligación que el RGPD impone a los corresponsables del tratamiento, una vez calificados de tales, con el fin de garantizar el cumplimiento de los requisitos de dicho Reglamento que les incumben. Así pues, esta calificación se deriva del mero hecho de que varias entidades hayan participado en la determinación de los fines y medios del tratamiento.

En cuanto a la determinación conjunta, por las entidades de que se trate, de los fines y medios del tratamiento, el Tribunal de Justicia señala que su participación en esta determinación puede adoptar distintas formas y resultar tanto de una decisión común como de decisiones convergentes. Ahora bien, en este último caso, tales decisiones deben complementarse, de modo que cada una de ellas tenga un efecto concreto en la determinación de los fines y medios del tratamiento.

7. Requisitos de licitud de un tratamiento de datos personales

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

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,

[41] Artículo 26, apartado 1, del RGPD, interpretado a la luz de su considerando 79.

de sus competencias en materia de diligencias penales y de investigaciones relativas a comportamientos delictivos o que pusieran en peligro la seguridad pública.

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

En este contexto, el Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tribunal Superior de lo Contencioso-Administrativo del Estado federado de Renania del Norte-Westfalia, Alemania), al conocer 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 sujeto a limitaciones. Por lo tanto, el uso de un Registro de ese tipo en apoyo de las autoridades encargadas de aplicar la normativa en materia de derecho de residencia es, en principio, legítimo, y, habida cuenta de su naturaleza, compatible con la prohibición de la 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 datos personales, a esos efectos.

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

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

Por lo demás, con respecto a la cuestión del uso de los datos contenidos en el Registro para combatir la delincuencia, el Tribunal de Justicia señaló en particular que tal finalidad tiene por objeto la persecución de los crímenes y delitos cometidos, con independencia de la nacionalidad de sus autores. Así pues, a efectos 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 combatir la delincuencia, entre aquellos nacionales y estos ciudadanos de la Unión resultante 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.

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

En esta sentencia (véase también la sección II.2, titulada «Concepto de ”datos personales”»), el Tribunal de Justicia se pronunció igualmente sobre la cuestión de si el artículo 7, letra f), de la Directiva 95/46 se opone a una disposición nacional con arreglo a la cual, por una parte, un proveedor 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 posibilitar 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 sesión de consulta concreta.

El Tribunal de Justicia declaró que el artículo 7, letra f), de la Directiva 95/46 se opone a la normativa de que se trata. En efecto, según dicho artículo 7, letra f), el tratamiento de datos personales es lícito si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado. Ahora 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 de este principio establecido en el artículo 7, letra f), de la Directiva 95/46, impidiendo sopesar el objetivo de garantizar el funcionamiento general de los sitios del medio en línea, por una parte, y el interés o los derechos y libertades fundamentales de los usuarios, por otra.

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

En el litigio principal, el Sr. 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, República Eslovaca), a todas las delegaciones de Hacienda dependientes de ella y al Kriminálny úrad finančnej správy (Unidad de Delitos de la Administración Tributaria, República Eslovaca) 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 de Tributos y la Unidad de Delitos de la Administración Tributaria (en lo sucesivo, «la lista controvertida»). Además, había solicitado que se eliminara toda mención de su nombre en dichas listas y en el sistema informático de las autoridades financieras.

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

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

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 del nombre de los interesados son adecuadas para cumplir los objetivos que persiguen y si no existen medios menos gravosos para alcanzarlos.

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.

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

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

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

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

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

El Tribunal de Justicia recuerda, en primer lugar, que el Derecho de la Unión [42] establece una lista de los casos en que un tratamiento de datos personales puede considerarse lícito. En particular, el consentimiento del interesado ha de ser libre, específico, informado e inequívoco. [43] A este respecto, el consentimiento no se presta válidamente en caso de silencio, de casillas marcadas por defecto o de inacción.

Además, cuando el consentimiento del interesado se preste en el contexto de una declaración escrita que también se refiera a otros asuntos, dicha declaración debe presentarse de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. Para garantizar al interesado una verdadera libertad de elección, las estipulaciones contractuales no deben inducirle a error en lo que respecta a la

[42] Artículo 7, de la Directiva 95/46 y artículo 6, del RGPD.
[43] Artículo 2, letra h), de la Directiva 95/46 y artículo 4, punto 11, del RGPD.

posibilidad de celebrar el contrato pese a negarse a dar su consentimiento para el tratamiento de sus datos.

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

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

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

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

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

En este contexto, el Tribunal de Justicia subraya que la mejora de la seguridad vial que persigue la normativa letona es un objetivo de interés general reconocido por la Unión y que, por tanto, los Estados miembros pueden calificar la seguridad vial de «misión realizada en interés público». [44] Sin embargo, no se ha demostrado la necesidad del régimen letón de comunicación de datos personales relativos a los puntos para lograr el objetivo perseguido. En efecto, por una parte, el legislador letón dispone de numerosas vías de acción que le habrían permitido alcanzar este objetivo por otros medios menos atentatorios contra los derechos fundamentales de los interesados. Por otra parte, deben tenerse en cuenta el carácter sensible de los datos relativos a los puntos y el hecho de que su comunicación al público puede constituir una injerencia grave en los derechos al respeto de la vida privada y a la protección de los datos personales, ya que puede provocar la desaprobación de la sociedad y conllevar la estigmatización del interesado.

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

Por lo demás, por idénticas razones, el Tribunal de Justicia declara que el RGPD se opone también a la normativa letona en la medida en que autoriza a la CSDD a comunicar los datos relativos a los puntos impuestos a conductores por infracciones de tráfico a operadores económicos para que estos puedan reutilizarlos y comunicarlos al público.

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

Por último, el Tribunal de Justicia precisa que el principio de primacía del Derecho de la Unión se opone a que el órgano jurisdiccional remitente, que conoce del recurso interpuesto contra la normativa letona, calificada por el Tribunal de Justicia de incompatible con el Derecho de la Unión, decida mantener los efectos jurídicos de dicha normativa hasta la fecha en que dicho órgano jurisdiccional remitente dicte sentencia firme.

III. Tratamientos de datos personales con arreglo a la normativa sectorial

1. Tratamiento de datos personales en el sector de las comunicaciones electrónicas

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

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

Tras haber recordado que el acceso de autoridades públicas a los datos personales conservados por proveedores de servicios de comunicaciones electrónicas, en el marco de un procedimiento de instrucción penal, está incluido en el ámbito de aplicación de la Directiva 2002/58, el Tribunal de Justicia declaró que el acceso a los datos que permiten identificar a los titulares de las tarjetas SIM activadas con un teléfono móvil sustraído, tales como los nombres y apellidos y, en su caso, direcciones de esos titulares, constituye una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, consagrados por la Carta, aun a falta de circunstancias que permitan calificar dicha injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia. No obstante, el Tribunal de Justicia subrayó que esa injerencia no presenta una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación,

descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave. En efecto, si bien la Directiva 2002/58 enumera de forma exhaustiva los objetivos que pueden justificar una norma nacional que regule el acceso de las autoridades públicas a los datos en cuestión y que, por tanto, establezca una excepción al principio de confidencialidad de las comunicaciones electrónicas, de modo que dicho acceso ha de responder efectiva y estrictamente a uno de esos objetivos, el Tribunal de Justicia observa que, por lo que se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos, el tenor de la Directiva 2002/58 no limita este objetivo a la lucha contra los delitos graves, sino que se refiere a los «delitos» en general.

En este contexto, el Tribunal de Justicia precisó que aun cuando en su sentencia *Tele2 Sverige y Watson y otros*, [45] había declarado que solo la lucha contra la delincuencia grave puede justificar un acceso de las autoridades públicas a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en su conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados, tal interpretación venía motivada por el hecho de que el objetivo perseguido por una norma que regula este acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión que supone la operación. Por lo tanto, conforme al principio de proporcionalidad, una injerencia grave solo puede justificarse en este ámbito por el objetivo de luchar contra la delincuencia que a su vez deba calificarse de «grave». En cambio, cuando la injerencia no es grave, el referido acceso puede estar justificado por el objetivo de prevenir, investigar, descubrir y perseguir «delitos» en general.

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

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

La jurisprudencia relativa a la conservación y el acceso a los datos personales en el ámbito de las comunicaciones electrónicas, en particular la sentencia Tele2 Sverige y Watson y otros, en la que el Tribunal de Justicia consideró, en particular, que los Estados

[45] Sentencia del Tribunal de Justicia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, EU:C:2016:970).

miembros no podían imponer a los proveedores de servicios de comunicaciones electrónicas una obligación de conservación generalizada e indiferenciada de los datos de tráfico y de localización, suscitó las preocupaciones de algunos Estados, que temieron haber sido privados de un instrumento que consideran necesario para proteger la seguridad nacional y luchar contra la delincuencia.

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

Mediante dos sentencias dictadas en Gran Sala, el 6 de octubre de 2020, el Tribunal de Justicia declara, para empezar, que la Directiva 2002/58 se aplica a normativas nacionales que obligan a los proveedores de servicios de comunicaciones electrónicas a conservar datos de tráfico y localización o a transmitirlos a las autoridades nacionales de seguridad e inteligencia a efectos de protección de la seguridad nacional y de lucha contra la delincuencia.

A continuación, el Tribunal de Justicia recuerda que la Directiva 2002/58 [46] no permite que la excepción a la obligación de principio de garantizar la confidencialidad de las comunicaciones electrónicas y de los datos relativos a ellas y a la prohibición de almacenar esos datos se convierta en la regla. Ello supone que esta Directiva solo autoriza a los Estados miembros a adoptar, entre otras, por razones de seguridad nacional, medidas legales para limitar el alcance de los derechos y obligaciones previstos en dicha Directiva, en particular la obligación de garantizar la confidencialidad de las comunicaciones y de los datos de tráfico, [47] siempre que respeten los principios generales del Derecho de la Unión, entre los que figura el principio de proporcionalidad, y los derechos fundamentales garantizados por la Carta. [48]

En este contexto, el Tribunal de Justicia considera, por una parte, en el asunto Privacy International, que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas, con el fin de proteger la seguridad nacional, la transmisión generalizada e indiferenciada a las agencias de seguridad de información de los datos de tráfico y de

[46] Artículo 15, apartados 1 y 3, de la Directiva 2002/58.
[47] Artículo 5, apartado 1, de la Directiva 2002/58.
[48] En particular, los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

localización. Por otra parte, en los asuntos acumulados La Quadrature du Net y otros, así como en el asunto Ordre des barreaux francophones et germanophone y otros, el Tribunal de Justicia estima que esta misma Directiva se opone a medidas legislativas que imponen a los proveedores de servicios de comunicaciones electrónicas, con carácter preventivo, una conservación generalizada e indiferenciada de los datos de tráfico y de localización.

En efecto, estas obligaciones de transmisión y de conservación generalizada e indiferenciada de tales datos constituyen injerencias especialmente graves en los derechos fundamentales garantizados por la Carta, sin que el comportamiento de las personas cuyos datos se ven afectados guarde relación alguna con el objetivo perseguido por la normativa controvertida. De manera análoga, el Tribunal de Justicia interpreta el artículo 23, apartado 1, del RGPD, a la luz de la Carta, en el sentido de que este se opone a una normativa nacional que impone a los proveedores de acceso a los servicios de comunicación al público en línea y a los proveedores de servicios de almacenamiento la conservación generalizada e indiferenciada, en particular, de los datos personales correspondientes a dichos servicios.

En cambio, el Tribunal de Justicia estima que, en situaciones en las que el Estado miembro se enfrente a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a que se obligue a los proveedores de servicios de comunicaciones electrónicas a conservar de manera generalizada e indiferenciada datos de tráfico y de localización. En este contexto, el Tribunal de Justicia señala que la decisión que establezca dicho requerimiento, para un período temporalmente limitado a lo estrictamente necesario, debe ser objeto de un control efectivo, bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya resolución tenga efecto vinculante, con el fin de comprobar la existencia de una de esas situaciones y el cumplimiento de los requisitos y garantías previstos. En estas mismas circunstancias, dicha Directiva tampoco se opone al análisis automatizado de los datos, en particular los de tráfico y de localización, de todos los usuarios de medios de comunicaciones electrónicas.

El Tribunal de Justicia añade que la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a medidas legislativas que permitan el recurso a una conservación selectiva, temporalmente limitada a lo estrictamente necesario, de los datos de tráfico y de localización, que se delimite, sobre la base de elementos objetivos y no discriminatorios, en función de categorías de personas afectadas o mediante un criterio geográfico. Asimismo, esta Directiva no se opone a medidas de esta índole que dispongan una conservación generalizada e indiferenciada de las direcciones IP atribuidas a la fuente de una comunicación, siempre que el período de conservación se limite a lo estrictamente necesario, ni a las que dispongan esa conservación de los datos relativos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas. En este último caso, los Estados miembros no están obligados a limitar temporalmente la conservación. Por añadidura, dicha Directiva no se opone a una

medida legislativa que permita el recurso a una conservación rápida de los datos de que dispongan los proveedores de servicios cuando se produzcan situaciones en las que resulte necesario conservar dichos datos más allá de los plazos legales de conservación de estos con el fin de esclarecer infracciones penales graves o atentados contra la seguridad nacional, cuando tales infracciones o atentados ya hayan sido comprobados o cuando su existencia pueda sospecharse razonablemente.

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

Por último, el Tribunal de Justicia aborda la cuestión del mantenimiento de los efectos en el tiempo de una normativa nacional declarada incompatible con el Derecho de la Unión. A este respecto, considera que un órgano jurisdiccional nacional no puede aplicar una disposición de su Derecho nacional que le faculta para limitar en el tiempo los efectos de una declaración de ilegalidad que le incumbe, en relación con una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, considerada incompatible con la Directiva 2002/58, interpretada a la luz de la Carta.

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

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

En Estonia se incoó un proceso penal contra H. K. por los cargos de robo, utilización de la tarjeta bancaria de un tercero y violencia contra los intervinientes en un procedimiento judicial. Por estos delitos, H. K. fue condenada por un tribunal de primera instancia a una pena privativa de libertad de dos años, sentencia que fue posteriormente confirmada en apelación. Los atestados en los que se basa la apreciación de esos delitos fueron redactados, en particular, sobre la base de datos personales generados en el marco de la prestación de servicios de comunicaciones electrónicas. El Riigikohus (Tribunal Supremo, Estonia), ante el que H. K. interpuso un recurso de casación, albergaba dudas en cuanto a la compatibilidad con el Derecho de la Unión [49] de las condiciones en las que los servicios de investigación tuvieron acceso a esos datos.

Estas dudas se refieren, en primer lugar, a si la duración del período en el que los servicios de investigación tuvieron acceso a los datos constituye un criterio que permita evaluar la gravedad de la injerencia de dicho acceso en los derechos fundamentales de las personas afectadas. Así, cuando ese período es muy breve o la cantidad de datos recogidos es muy limitada, el órgano jurisdiccional remitente se preguntaba si el objetivo de lucha contra la delincuencia en general, y no solo de lucha contra la delincuencia grave, puede justificar tal injerencia. En segundo lugar, el órgano jurisdiccional remitente albergaba dudas sobre la posibilidad de considerar al Ministerio Fiscal estonio, habida cuenta de las distintas funciones que le atribuye la normativa nacional, como una autoridad administrativa «independiente», en el sentido de la sentencia Tele2 Sverige y Watson y otros, [50] que pueda autorizar el acceso de la autoridad investigadora a los datos en cuestión.

Mediante su sentencia, pronunciada en Gran Sala, el Tribunal de Justicia declara que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a una normativa nacional que autoriza el acceso de las autoridades públicas a datos de tráfico o de localización que pueden facilitar información sobre las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utilice y permitir extraer conclusiones precisas sobre su vida privada, a efectos de la prevención, la investigación, el descubrimiento y la persecución de delitos, sin que dicho acceso se limite a procedimientos que tengan por objeto la lucha contra la delincuencia grave o la prevención de amenazas graves contra la seguridad pública. Según el Tribunal de Justicia, la duración del período para el que se solicite acceder a esos datos y la cantidad o naturaleza de los datos disponibles en ese período es irrelevante al respecto. Además, el Tribunal de Justicia considera que esta misma

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

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

Directiva, en relación con la Carta, se opone a una normativa nacional que atribuye competencia al Ministerio Fiscal para autorizar el acceso de una autoridad pública a los datos de tráfico y de localización con el fin de realizar la instrucción penal.

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

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

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

A este respecto, el Tribunal de Justicia precisa que el control previo requiere, entre otras cosas, que el órgano jurisdiccional o la entidad encargada de efectuar dicho control disponga de todas las atribuciones y presente todas las garantías necesarias para conciliar los diferentes intereses y derechos de que se trate. En el caso concreto de la investigación penal, tal control exige que ese órgano jurisdiccional o esa entidad esté en

condiciones de ponderar adecuadamente, por una parte, los intereses relacionados con las necesidades de la investigación en el marco de la lucha contra la delincuencia y, por otra parte, los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales de aquellos a cuyos datos afecte el acceso. Cuando dicho control no lo lleve a cabo un órgano jurisdiccional sino una entidad administrativa independiente, esta debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad, y, para ello, ha de estar a resguardo de toda influencia externa.

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

Sentencia de 5 de abril de 2022 (Gran Sala), Commissioner of An Garda Síochána y otros (C-140/20, **EU:C:2022:258)**

La petición de decisión prejudicial del presente asunto fue planteada por la Supreme Court (Tribunal Supremo, Irlanda) en el contexto de un proceso civil entablado por una persona condenada a cadena perpetua por un asesinato cometido en Irlanda. Esta última cuestionaba la compatibilidad con el Derecho de la Unión de determinadas disposiciones de la ley nacional reguladora de la conservación de los datos generados en el marco de las comunicaciones electrónicas. Al amparo de dicha ley, los proveedores de servicios de comunicaciones electrónicas habían conservado datos de tráfico y de localización relativos a llamadas telefónicas del inculpado y habían permitido a las autoridades de la Policía acceder a ellos. Las dudas expresadas por el órgano jurisdiccional remitente se referían, en particular, a la compatibilidad con la Directiva 2002/58, interpretada a la luz de la Carta, de un régimen de conservación generalizada e indiferenciada de esos datos, en el contexto de la lucha contra la delincuencia grave.

Mediante su sentencia, pronunciada en Gran Sala, el Tribunal de Justicia confirma, a la vez que precisa su alcance, la jurisprudencia emanada de la sentencia La Quadrature du Net y otros, [51] recordando que no está autorizada, a efectos de la lucha contra la delincuencia grave y de la prevención de las amenazas graves contra la seguridad

[51] Sentencia de 6 de octubre de 2020, La Quadrature du Net y otros (C-511/18, C-512/18 y C-520/18, EU:C:2020:791).

pública, la conservación generalizada e indiferenciada de los datos de tráfico y de localización relativos a las comunicaciones electrónicas. Confirma igualmente la jurisprudencia emanada de la sentencia Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas), [52] en particular en cuanto a la obligación de supeditar el acceso de las autoridades nacionales competentes a dichos datos conservados a un control previo efectuado bien por un órgano jurisdiccional bien por una entidad administrativa independiente, respecto de un funcionario de la Policía.

El Tribunal de Justicia declara, en primer lugar, que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a medidas legislativas que establezcan, con carácter preventivo, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, una conservación generalizada e indiferenciada de los datos de tráfico y de localización. En efecto, habida cuenta, por un lado, de los efectos disuasorios sobre el ejercicio de los derechos fundamentales [53] que dicha conservación puede acarrear y, por otro lado, de la gravedad de la injerencia que a que da lugar, tal conservación debe constituir la excepción y no la regla del sistema establecido por dicha Directiva, de manera que esos datos no puedan ser objeto de una conservación sistemática y continua. La delincuencia, aunque sea especialmente grave, no puede asimilarse a una amenaza para la seguridad nacional, por cuanto tal asimilación podría introducir una categoría intermedia entre la seguridad nacional y la seguridad pública, para aplicar a la segunda las exigencias inherentes a la primera.

En cambio, la Directiva 2002/58, interpretada a la luz de la Carta, no se opone a medidas legislativas que, a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, establezcan una conservación selectiva de los datos de tráfico y de localización que esté delimitada, sobre la base de elementos objetivos y no discriminatorios, en función de las categorías de personas afectadas o mediante un criterio geográfico, para un período temporalmente limitado a lo estrictamente necesario, pero que podrá renovarse. Añade que tal medida de conservación referida a lugares o infraestructuras frecuentados regularmente por un número muy elevado de personas o lugares estratégicos, como aeropuertos, estaciones de ferrocarril, puertos marítimos o zonas de peajes, permite a las autoridades competentes obtener información sobre la presencia, en esos lugares o zonas geográficas, de las personas que utilizan en uno de esos lugares un medio de comunicación electrónica y extraer conclusiones sobre su presencia y su actividad en dichos lugares o zonas geográficas a efectos de la lucha contra la delincuencia grave. En cualquier caso, la eventual existencia de dificultades para definir con precisión los casos y las condiciones en que pueda realizarse una conservación selectiva no justifica que los Estados miembros establezcan una conservación generalizada e indiferenciada de datos de tráfico y de localización.

---

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

53 Consagrados en los artículos 7 a 11 de la Carta.

Esa Directiva, interpretada a la luz de la Carta, tampoco se opone a medidas legislativas que establezcan, con los mismos fines, una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión para un período temporalmente limitado a lo estrictamente necesario, así como de los datos relativos a la identidad civil de los usuarios de comunicaciones electrónicas. En lo tocante a este último aspecto, el Tribunal de Justicia indica, más concretamente, que ni la Directiva 2002/58 ni ningún otro acto del Derecho de la Unión se oponen a una normativa nacional que tenga por objeto la lucha contra la delincuencia grave, en virtud de la cual la adquisición de un medio de comunicación electrónica, como una tarjeta SIM de prepago, está supeditada a la comprobación de documentos oficiales que acrediten la identidad civil del comprador y al registro, por el vendedor, de la información obtenida por tal vía, estando el vendedor obligado, en su caso, a permitir a las autoridades nacionales acceder a esa información.

Lo mismo vale para las medidas legislativas que establezcan, también a efectos de la lucha contra la delincuencia grave y la prevención de amenazas graves contra la seguridad pública, el recurso a un requerimiento efectuado a los proveedores de servicios de comunicaciones electrónicas, mediante una decisión de la autoridad competente sujeta a un control jurisdiccional efectivo, para que procedan, durante un período determinado, a la conservación rápida («quick freeze») de los datos de tráfico y de localización de los que dispongan. En efecto, solo la lucha contra la delincuencia grave y, *a fortiori*, la protección de la seguridad nacional pueden justificar tal conservación, siempre que esa medida y el acceso a los datos conservados respeten los límites de lo estrictamente necesario. El Tribunal de Justicia recuerda que tal medida de conservación rápida puede ampliarse a los datos de tráfico y a los datos de localización relativos a personas distintas de las sospechosas de haber planeado o cometido un delito grave o un atentado contra la seguridad nacional, siempre que esos datos puedan contribuir, sobre la base de elementos objetivos y no discriminatorios, a la investigación de tal delito o de tal atentado contra la seguridad nacional, como los datos de la víctima de estos y los de su entorno social o profesional.

No obstante, el Tribunal de Justicia indica a continuación que todas las medidas legislativas antes mencionadas deben garantizar, mediante normas claras y precisas, que la conservación de los datos en cuestión esté supeditada al respeto de las condiciones materiales y procesales correspondientes y que las personas afectadas dispongan de garantías efectivas contra los riesgos de abuso. Las distintas medidas de conservación de los datos de tráfico y de localización pueden aplicarse conjuntamente, según la elección del legislador nacional y siempre que se respeten los límites de lo estrictamente necesario.

Además, el Tribunal de Justicia recalca que autorizar, con fines de lucha contra la delincuencia grave, un acceso a tales datos conservados de manera generalizada e indiferenciada para hacer frente a una amenaza grave para la seguridad nacional sería contrario a la jerarquía de los objetivos de interés general que pueden justificar una

medida adoptada al amparo de la Directiva 2002/58. En efecto, ello equivaldría a permitir que el acceso pudiera justificarse por un objetivo de una importancia menor que el que justificó la conservación, a saber, la protección de la seguridad nacional, con el consiguiente riesgo de vaciar de todo efecto útil la prohibición de efectuar una conservación generalizada e indiferenciada a efectos de la lucha contra la delincuencia grave.

En segundo lugar, el Tribunal de Justicia concluye que la Directiva 2002/58, interpretada a la luz de la Carta, se opone a una normativa nacional en virtud de la cual el tratamiento centralizado de una solicitud de acceso a datos conservados por los proveedores de servicios de comunicaciones electrónicas, procedente de la Policía en el marco de la investigación y de la persecución de delitos graves, incumbe a un funcionario de la Policía, aunque asistido por una unidad integrada en este mismo cuerpo, con cierto grado de autonomía en el ejercicio de sus funciones y cuyas decisiones pueden ser objeto de un control jurisdiccional ulterior. En efecto, por un lado, tal funcionario no cumple las exigencias de independencia e imparcialidad que se imponen a una autoridad administrativa que ejerce el control previo de una solicitud de acceso a los datos emanada de una autoridad nacional competente, pues no tiene la condición de tercero con respecto a esta última. Por otro lado, si bien la decisión de tal funcionario puede ser objeto de un control jurisdiccional ulterior, aquel control independiente y, salvo urgencia debidamente justificada, de carácter previo no puede ser sustituido por un control ejercido *a posteriori*.

En tercer lugar, el Tribunal de Justicia confirma finalmente su jurisprudencia según la cual el Derecho de la Unión se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde, en virtud del Derecho nacional, referida a una normativa nacional que impone a los proveedores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y de localización, en razón de la incompatibilidad de esa normativa con la Directiva 2002/58. Ahora bien, el Tribunal de Justicia recuerda que la admisibilidad de las pruebas obtenidas mediante tal conservación se rige, conforme al principio de autonomía procesal de los Estados miembros, por el Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad.

Sentencia de 20 de septiembre de 2022 (Gran Sala), VD y SR (C-339/20 y C-397/20, EU:C:2022:703)

A raíz de una investigación de la Autorité des marchés financiers (Autoridad de los Mercados Financieros, Francia; en lo sucesivo, «AMF»), se incoaron procesos penales contra VD y SR, dos personas físicas acusadas de delitos de uso de información privilegiada, encubrimiento de delitos de uso de información privilegiada, complicidad, corrupción y blanqueo de capitales. En el marco de esta investigación, la AMF había utilizado datos personales procedentes de llamadas telefónicas de VD y SR, generados

sobre la base del code des postes et des communications électroniques (Código de Correos y Comunicaciones Electrónicas) francés, en el contexto de la prestación de servicios de comunicaciones electrónicas.

En la medida en que sus respectivos procesamientos se basaban en los datos de tráfico facilitados por la AMF, VD y SR interpusieron sendos recursos ante la cour d'appel de Paris (Tribunal de Apelación de París, Francia), invocando, en particular, un motivo basado en la infracción del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7, 8, 11 y 52, apartado 1, de la Carta. Más concretamente, basándose en la jurisprudencia derivada de la sentencia Tele2 Sverige y Watson y otros, [54] VD y SR impugnaban que la AMF se hubiera basado, para recabar dichos datos, en las disposiciones nacionales controvertidas, pese a que —a su juicio— dichas disposiciones, por una parte, no eran conformes con el Derecho de la Unión, ya que preveían una conservación generalizada e indiferenciada de los datos de conexión y, por otra parte, no establecían ningún límite a la facultad de los investigadores de la AMF de solicitar los datos conservados.

Mediante dos sentencias de 20 de diciembre de 2018 y 7 de marzo de 2019, la cour d'appel de Paris (Tribunal de Apelación de París) desestimó los recursos de VD y SR. Para desestimar el motivo antes mencionado, los jueces que resolvieron sobre el fondo se basaron, en particular, en el hecho de que el Reglamento sobre abuso de mercado [55] permite a las autoridades competentes solicitar, en la medida en que lo permita la legislación nacional, los registros existentes sobre datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas, cuando existan razones para sospechar que se ha producido una infracción de la prohibición de usar información privilegiada y cuando dichos registros puedan ser relevantes para la investigación de dicha infracción.

VD y SR interpusieron recurso de casación ante la Cour de cassation (Tribunal de Casación, Francia), el órgano jurisdiccional remitente en los presentes asuntos.

En ese contexto, dicho órgano jurisdiccional se pregunta sobre la conciliación del artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de la Carta, con las exigencias derivadas del artículo 12, apartado 2, letras a) y d), de la Directiva sobre abuso de mercado [56] y del artículo 23, apartado 2, letras g) y h), del Reglamento sobre abuso de mercado. Esta cuestión tiene su origen en las medidas legislativas controvertidas en el litigio principal, que establecen, con carácter preventivo, para los operadores de servicios de comunicaciones electrónicas, una conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día del registro, a

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

[55] Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión (DO 2014, L 173, p. 1).

[56] Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado) (DO 2003, L 96, p. 16).

efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada. En el supuesto de que el Tribunal de Justicia considere que la normativa relativa a la conservación de los datos de conexión controvertida en el litigio principal no es conforme con el Derecho de la Unión, el órgano jurisdiccional remitente se plantea la cuestión del mantenimiento provisional de los efectos de dicha normativa, con el fin de evitar la inseguridad jurídica y de permitir que los datos previamente recabados y conservados se utilicen con fines de detección y persecución de las operaciones con información privilegiada.

Mediante su sentencia, el Tribunal de Justicia, constituido en Gran Sala, considera que la conservación generalizada e indiferenciada de los datos de tráfico durante un año a partir del día del registro por los operadores de servicios de comunicaciones electrónicas no está autorizada, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado. Asimismo, confirma su jurisprudencia según la cual el Derecho de la Unión se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar en relación con disposiciones legislativas nacionales incompatibles con el Derecho de la Unión.

El Tribunal de Justicia recuerda en primer lugar que, para la interpretación de una disposición del Derecho de la Unión, hay que tener en cuenta no solo el tenor de esta, sino también su contexto y los objetivos perseguidos por la normativa de la que forma parte.

En lo que respecta al tenor de las disposiciones a que se refieren las cuestiones prejudiciales, el Tribunal de Justicia observa que, mientras que el artículo 12, apartado 2, letra d), de la Directiva sobre abuso de mercado se refiere a la facultad de la AMF de «solicitar registros existentes sobre tráfico de datos y sobre datos telefónicos», el artículo 23, apartado 2, letras g) y h), del Reglamento sobre abuso de mercado remite a la facultad de dicha autoridad de solicitar, por una parte, las «grabaciones […] de tráfico de datos que mantengan las empresas de servicios de inversión, las entidades de crédito o las entidades financieras» y, por otra parte, «en la medida en que lo permita la legislación nacional, los registros existentes sobre tráfico de datos que mantenga una empresa de telecomunicaciones». Según el Tribunal de Justicia, del tenor de estas disposiciones se desprende inequívocamente que estas se limitan a delimitar la facultad de la AMF de «solicitar» los datos de que disponen dichas empresas, lo que corresponde al acceso a esos datos. Además, la referencia hecha a los registros «existentes», que «mantenga» una de dichas empresas, da a entender que el legislador de la Unión no pretendió regular la posibilidad de que el legislador nacional estableciera una obligación de conservación de tales registros. Según el Tribunal de Justicia, esta interpretación se ve corroborada, además, tanto por el contexto en el que se inscriben las citadas disposiciones, como por los objetivos perseguidos por la normativa de la que forman parte esas mismas disposiciones.

Por lo que respecta al contexto en el que se inscriben las disposiciones objeto de las cuestiones prejudiciales, el Tribunal de Justicia observa que, si bien, a tenor de las disposiciones pertinentes de la Directiva sobre abuso de mercado y del Reglamento sobre abuso de mercado, [57] el legislador de la Unión ha querido imponer a los Estados miembros la obligación de adoptar las medidas necesarias para que las autoridades competentes en materia financiera dispongan de un conjunto de herramientas, competencias y recursos adecuados, así como de las facultades de supervisión e investigación necesarias para garantizar la eficacia de sus tareas, esas disposiciones no se pronuncian ni sobre la eventual posibilidad de que los Estados miembros impongan, con ese objetivo, a los operadores de servicios de comunicaciones electrónicas una obligación generalizada e indiferenciada de conservar los datos de tráfico, ni sobre las condiciones en las que tales datos deben ser conservados por esos operadores a efectos de entregarlos, en su caso, a las autoridades competentes.

En cuanto a los objetivos perseguidos por la normativa controvertida, el Tribunal de Justicia señala que tanto de la Directiva sobre abuso de mercado como del Reglamento sobre abuso de mercado [58] se desprende que estos instrumentos tienen como finalidad proteger la integridad de los mercados financieros de la Unión y aumentar la confianza de los inversores en esos mercados, confianza que se basa, entre otras cosas, en la garantía de que estarán en igualdad de condiciones y estarán protegidos contra el uso ilícito de información privilegiada. La prohibición de las operaciones con información privilegiada establecida en dichos instrumentos [59] pretende garantizar la igualdad entre las partes contractuales que intervienen en una operación bursátil, evitando que uno de ellos, poseedor de una información privilegiada que lo sitúa en una posición ventajosa con respecto a los otros inversores, saque provecho de ello en detrimento de la otra parte que desconoce tal información. Si bien es cierto que, a tenor del Reglamento sobre abuso de mercado, [60] los registros de datos de conexión constituyen una prueba decisiva, a veces la única, para detectar y probar la existencia de operaciones con información privilegiada y de manipulación de mercado, no es menos cierto que dicho Reglamento solo se refiere a los registros «que mantengan» las empresas de servicios de comunicaciones electrónicas, así como a la facultad de la autoridad competente en materia financiera para «exigir» a esos operadores que comuniquen los datos «existentes». Así pues, de ese texto no se desprende en modo alguno que el legislador de la Unión haya querido reconocer a los Estados miembros, mediante dicho Reglamento, la facultad de imponer a los operadores de servicios de comunicaciones electrónicas una obligación general de conservar datos. De ello se deduce que ni la Directiva sobre abuso de mercado ni el Reglamento sobre abuso de mercado pueden constituir la base jurídica de una obligación general de conservación de los registros de

[57] Respectivamente, artículo 12, apartado 1, de la Directiva sobre abuso de mercado y artículo 23, apartado 3, del Reglamento sobre abuso de mercado, entendido a la luz de su considerando 62.

[58] Respectivamente, considerandos 2 y 12 de la Directiva sobre abuso de mercado y artículo 1 del Reglamento sobre abuso de mercado, entendido a la luz de sus considerandos 2 y 24.

[59] Artículo 2, apartado 1, de la Directiva sobre abuso de mercado y artículo 8, apartado 1, del Reglamento sobre abuso de mercado.

[60] Considerando 62 del Reglamento sobre abuso de mercado.

datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas a efectos del ejercicio de las facultades conferidas a la autoridad competente en materia financiera en virtud de dichos actos.

En segundo lugar, el Tribunal de Justicia recuerda que la Directiva 2002/58 constituye el acto de referencia en materia de conservación y, con carácter más general, de tratamiento de datos personales en el sector de las comunicaciones electrónicas, de modo que su interpretación, realizada a la luz de esta Directiva, regirá también los registros de datos de tráfico que mantengan los operadores de servicios de comunicaciones electrónicas que las autoridades competentes en materia financiera pueden solicitarles, en el sentido de la Directiva sobre abuso de mercado y del Reglamento sobre abuso de mercado. [61] La apreciación de la licitud del tratamiento de los registros que mantengan los operadores de servicios de comunicaciones electrónicas, [62] debe efectuarse, por tanto, a la luz de los requisitos establecidos por la Directiva 2002/58 y de la interpretación que de esa Directiva se haga en la jurisprudencia del Tribunal de Justicia.

De este modo, el Tribunal de Justicia considera que la Directiva sobre abuso de mercado y el Reglamento sobre abuso de mercado, en relación con la Directiva 2002/58 e interpretados a la luz de la Carta, se oponen a medidas legislativas que establecen, con carácter preventivo, a efectos de la lucha contra los delitos de abuso de mercado, entre los que se encuentran las operaciones con información privilegiada, una conservación temporal, a saber, de un año a partir del día de su registro, pero generalizada e indiferenciada, de los datos de tráfico por parte de los operadores de servicios de comunicaciones electrónicas.

Por último, el Tribunal de Justicia confirma su jurisprudencia según la cual el Derecho de la Unión se opone a que un órgano jurisdiccional nacional limite en el tiempo los efectos de una declaración de invalidez que le corresponde efectuar, en virtud del Derecho nacional, con respecto a disposiciones nacionales que, por un lado, imponen a los operadores de servicios de comunicaciones electrónicas una conservación generalizada e indiferenciada de los datos de tráfico y, por otro lado, permiten la comunicación de esos datos a la autoridad competente en materia financiera, sin autorización previa de un órgano jurisdiccional o de una autoridad administrativa independiente, debido a la incompatibilidad de esas disposiciones con la Directiva 2002/58, interpretada a la luz de la Carta. Ahora bien, el Tribunal de Justicia recuerda que la admisibilidad de las pruebas obtenidas mediante tal conservación se rige, conforme al principio de autonomía procesal de los Estados miembros, por el Derecho nacional, siempre que se respeten, en particular, los principios de equivalencia y de efectividad. Este último principio exige que el juez penal nacional descarte la información y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada incompatible con el Derecho

[61] Respectivamente, artículo 11 de la Directiva sobre abuso de mercado y artículo 22 del Reglamento sobre abuso de mercado.

[62] En el sentido del artículo 12, apartado 2, letra d), de la Directiva sobre abuso de mercado y del artículo 23, apartado 2, letras g) y h), del Reglamento sobre abuso de mercado.

de la Unión cuando las personas afectadas no estén en condiciones de comentar eficazmente tal información y tales pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y que pueden influir destacadamente en la apreciación de los hechos.

Sentencia de 30 de abril de 2024 (Pleno), La Quadrature du Net y otros (Datos personales y lucha contra la vulneración de derechos de propiedad intelectual) (C-470/21, EU:C:2024:370)

En respuesta a una petición de decisión prejudicial planteada por el Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), el Pleno del Tribunal de Justicia desarrolla su jurisprudencia sobre la Directiva 2002/58 aportando precisiones, por una parte, sobre las condiciones en las que puede no considerarse que una conservación generalizada de direcciones IP por parte de los proveedores de servicios de comunicaciones electrónicas supone una injerencia grave en los derechos al respeto de la vida privada, a la protección de los datos personales y a la libertad de expresión garantizados por la Carta, [63] así como, por otra parte, sobre la posibilidad de que una autoridad pública acceda a determinados datos personales conservados dentro del respeto de tales condiciones, en el marco de la lucha contra las vulneraciones de los derechos de propiedad intelectual cometidas en línea.

En el caso de autos, cuatro asociaciones presentaron ante el Premier ministre (Primer Ministro, Francia) una solicitud con objeto de que se derogase el decreto de tratamiento automatizado de datos personales. [64] Al no recibir contestación la solicitud, las asociaciones interpusieron ante el Conseil d'État (Consejo de Estado, Francia) un recurso de anulación contra esa resolución desestimatoria tácita. En su opinión, dicho decreto y las disposiciones que conforman su base legal [65] violan el Derecho de la Unión.

En virtud de la legislación francesa, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (Alta Autoridad para la Difusión de Obras y la Protección de los Derechos en Internet, Francia; en lo sucesivo, «Hadopi»), a fin de poder identificar a los responsables de vulneraciones de los derechos de autor o de los derechos afines a los derechos de autor cometidas en línea, tiene autorización para acceder a determinados datos que los proveedores de servicios de comunicaciones electrónicas están obligados a conservar. Se trata de una serie de datos de identidad

63 Artículos 7, 8 y 11 de la Carta.

64 Décret nº 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé «Système de gestion des mesures pour la protection des œuvres sur internet», (Decreto n.º 2010-236, de 5 de marzo de 2010, relativo al tratamiento automatizado de datos personales autorizado por el artículo L. 331-29 del Código de la Propiedad Intelectual denominado «Sistema de gestión de medidas para la protección de las obras en Internet») (JORF n.º 56 de 7 de marzo de 2010, texto n.º 19), en su versión modificada por el décret nº 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (Decreto n.º 2017-924, de 6 de mayo de 2017, relativo a la gestión de los derechos de autor y de los derechos afines por un organismo de gestión de derechos y por el que se modifica el Código de la Propiedad Intelectual) (JORF n.º 109 de 10 de mayo de 2017, texto n.º 176).

65 En particular, el artículo L. 331-21, párrafos tercero a quinto, del code de la propriété intellectuelle (Código de la Propiedad Intelectual).

civil de la persona correspondientes a su dirección IP previamente recabada por organizaciones de titulares de derechos. Una vez que se identifica al titular de la dirección IP utilizada para actividades de esta naturaleza, la Hadopi aplica el denominado «procedimiento de respuesta gradual». En concreto, está facultada para enviar a dicha persona dos recomendaciones, que se asemejan a advertencias, y, si las actividades continúan, una carta en la que se le notifica que sus actividades pueden dar lugar a la incoación de diligencias penales. Por último, la Hadopi tiene derecho a presentar denuncia ante el Ministerio Fiscal para que se incoen diligencias penales contra esa persona. [66]

En este contexto, el Conseil d'État (Consejo de Estado) preguntó al Tribunal de Justicia sobre la interpretación de la Directiva 2002/58, entendida a la luz de la Carta. [67]

En primer lugar, por lo que respecta a la conservación de los datos de identidad civil y de las direcciones IP correspondientes a estos datos, el Tribunal de Justicia subraya que no toda conservación generalizada e indiferenciada de direcciones IP constituye necesariamente una injerencia grave en los derechos al respeto de la vida privada, a la protección de los datos personales y a la libertad de expresión garantizados por la Carta.

La obligación de garantizar tal conservación puede estar justificada por el objetivo de luchar contra las infracciones penales en general cuando se excluye, de manera efectiva, que esa conservación pueda generar injerencias graves en la vida privada de la persona afectada debido a la posibilidad de extraer conclusiones precisas sobre ella, en particular asociando esas direcciones IP a un conjunto de datos de tráfico o de localización.

En consecuencia, un Estado miembro que pretenda imponer a los proveedores de servicios de comunicaciones electrónicas tal obligación debe cerciorarse de que las condiciones de conservación de esos datos excluyen que puedan extraerse conclusiones precisas sobre la vida privada de las personas afectadas.

El Tribunal de Justicia precisa que las condiciones de conservación deben atañer, a tal efecto, a la propia estructura de la conservación, que, en esencia, debe organizarse de modo que se asegure una separación en compartimentos estancos de las diferentes categorías de datos conservados. Así, las normas nacionales relativas a esas condiciones deben garantizar que cada categoría de datos, incluidos los datos de identidad civil y las direcciones IP, se conserve de forma totalmente separada de las demás categorías de datos conservados y que esa separación se haga en compartimentos estancos, con un sistema informático seguro y fiable. Además, en caso de que dichas normas prevean la

66 A partir del 1 de enero de 2022, se fusionó a la Hadopi con el Conseil supérieur de l'audiovisuel (CSA) (Consejo Superior de lo Audiovisual, Francia), otra autoridad pública independiente, para formar la Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) (Autoridad Reguladora de la Comunicación Audiovisual y Digital, Francia). No obstante, el procedimiento de respuesta gradual se mantuvo inalterado en lo esencial.

67 Artículo 15, apartado 1, de la Directiva 2002/58.

posibilidad de asociar las direcciones IP conservadas a la identidad civil de la persona de que se trate con fines de lucha contra infracciones, solo deben permitir tal asociación mediante la utilización de un procedimiento técnico efectivo que no suscite dudas sobre la eficacia de la separación en compartimentos estancos de esas categorías de datos. La fiabilidad de esa separación debe someterse al control periódico de una tercera autoridad pública. Siempre que en la legislación nacional aplicable se establezcan tales exigencias estrictas, la injerencia resultante de esa conservación de las direcciones IP no puede calificarse de «grave».

Consiguientemente, el Tribunal de Justicia concluye que, de existir un régimen legal que garantice que ninguna asociación de datos permitirá extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se conserven, la Directiva 2002/58, a la luz de la Carta, no se opone a que un Estado miembro imponga la obligación de conservación generalizada e indiferenciada de las direcciones IP, por un período que no exceda de lo estrictamente necesario, en pro del objetivo de luchar contra las infracciones penales en general.

En segundo lugar, por lo que respecta al acceso a datos de identidad civil correspondientes a direcciones IP, el Tribunal de Justicia declara que la Directiva 2002/58, a la luz de la Carta, no se opone, en principio, a una normativa nacional que permite el acceso, por parte de una autoridad pública, a esos datos conservados por los proveedores de servicios de comunicaciones electrónicas conforme a una separación en compartimentos estancos, con el solo propósito de que dicha autoridad pueda identificar a los titulares de esas direcciones sospechosos de ser responsables de vulneraciones de los derechos de autor y de los derechos afines a los derechos de autor en Internet y pueda adoptar medidas contra ellos. En tal caso, la normativa nacional debe prohibir a los agentes que dispongan de tal acceso, primero, divulgar de cualquier forma información sobre el contenido de los archivos consultados por esos titulares, salvo a los solos efectos de presentar denuncia ante el Ministerio Fiscal, segundo, realizar cualquier rastreo de la secuencia de navegación de esos titulares y, tercero, utilizar esas direcciones IP con fines distintos de la adopción de esas medidas.

En este contexto, el Tribunal de Justicia recuerda, en particular, que, aun cuando la libertad de expresión y la confidencialidad de los datos personales son preocupaciones primordiales, estos derechos fundamentales no son absolutos. En efecto, en el marco de la ponderación de los derechos e intereses en juego, deben en ocasiones ceder ante otros derechos fundamentales e imperativos de interés general, como la defensa del orden público y la prevención de las infracciones penales o la protección de los derechos y libertades de terceros. Así sucede, en particular, cuando la preponderancia que se reconoce a las referidas preocupaciones primordiales puede mermar la eficacia de una investigación penal, en particular haciendo imposible o excesivamente difícil que se identifique al autor de una infracción penal y se le imponga una sanción.

En este mismo contexto, el Tribunal de Justicia se refiere también a su jurisprudencia según la cual, cuando se trata de luchar contra las infracciones penales que vulneran los

derechos de autor o los derechos afines a los derechos de autor cometidas en línea, la circunstancia de que el acceso a las direcciones IP puede constituir el único método de investigación para identificar a la persona en cuestión lleva a demostrar que la conservación de esas direcciones y el acceso a ellas son estrictamente necesarios para la consecución del objetivo perseguido y, por tanto, cumplen la exigencia de proporcionalidad. No permitir tal acceso implicaría además un riesgo real de impunidad sistémica de infracciones penales cometidas en línea o cuya comisión o preparación se ve facilitada por las características propias de Internet. Pues bien, la existencia de tal riesgo constituye una circunstancia pertinente para apreciar, en el marco de la ponderación de los diferentes derechos e intereses en juego, si una injerencia en los derechos al respeto de la vida privada, a la protección de los datos personales y a la libertad de expresión es una medida proporcionada respecto al objetivo de luchar contra las infracciones penales.

En tercer lugar, al pronunciarse sobre si el acceso de la autoridad pública a datos de identidad civil correspondientes a una dirección IP debe sujetarse a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, el Tribunal de Justicia considera que la exigencia de tal control se impone cuando, en el contexto de una normativa nacional, ese acceso entrañe el riesgo de que se produzca una injerencia grave en los derechos fundamentales de la persona afectada, en el sentido de que podría posibilitar que dicha autoridad pública extraiga conclusiones precisas sobre su vida privada y, en su caso, establezca un perfil detallado de ella. A la inversa, esa exigencia de control previo no resulta de aplicación cuando la injerencia en los derechos fundamentales no pueda calificarse de grave.

A este respecto, el Tribunal de Justicia señala que, en el supuesto de que se establezca un sistema de conservación que garantice una separación en compartimentos estancos de las diferentes categorías de datos conservados, el acceso de la autoridad pública a los datos de identidad civil correspondientes a las direcciones IP conservadas no se condiciona, en principio, a la exigencia de control previo. En efecto, tal acceso con el solo propósito de identificar al titular de una dirección IP no constituye, por regla general, una injerencia grave en los mencionados derechos.

No obstante, el Tribunal de Justicia no excluye que, en situaciones atípicas, exista el riesgo de que, en el marco de un procedimiento como el de respuesta gradual controvertido en el litigio principal, la autoridad pública pueda extraer conclusiones precisas sobre la vida privada de la persona afectada, en particular cuando dicha persona realice actividades que vulneran los derechos de autor o los derechos afines a los derechos de autor en redes entre pares repetidamente, o incluso a gran escala, en relación con obras protegidas de clases particulares que revelen información, en su caso sensible, sobre su vida privada.

En el caso de autos, un titular de una dirección IP puede estar particularmente expuesto a tal riesgo cuando la autoridad pública tiene que decidir si denuncia o no los hechos al Ministerio Fiscal para que se incoen diligencias contra él. En efecto, la intensidad del

menoscabo del derecho al respeto de la vida privada puede incrementarse a medida que el procedimiento de respuesta gradual, que se desarrolla secuencialmente, vaya avanzando por sus distintas fases. El acceso de la autoridad competente al conjunto de los datos de la persona de que se trate acumulados a lo largo de las distintas fases de que consta ese procedimiento puede posibilitar que se extraigan conclusiones precisas sobre su vida privada. Por tanto, la normativa nacional debe contemplar asimismo un control previo que debe realizarse antes de que la autoridad pública pueda asociar los datos de identidad civil y tal conjunto de datos, y antes de la notificación en que se indica que esa persona ha cometido hechos que pueden dar lugar a la incoación de diligencias penales. Ese control debe asimismo preservar la eficacia del procedimiento de respuesta gradual, permitiendo, en particular, que se identifiquen los casos de posibles nuevas reiteraciones en el comportamiento infractor de que se trate. A tal fin, ese procedimiento debe organizarse y estructurarse de manera que los datos de identidad civil de una persona correspondientes a direcciones IP que se hayan recogido previamente en Internet no puedan automáticamente ser asociados, por las personas encargadas del examen de los hechos en la autoridad pública competente, a elementos de que esa autoridad ya disponga y que pudieran posibilitar que se extraigan conclusiones precisas sobre la vida privada de esa persona.

Además, por lo que atañe al objeto del control previo, el Tribunal de Justicia señala que, en los casos en que existan sospechas de que la persona en cuestión ha cometido una infracción penal encuadrada en la categoría de infracciones penales en general, el órgano jurisdiccional o la entidad administrativa independiente a cargo de dicho control debe denegar el acceso cuando este permita que la autoridad pública extraiga conclusiones precisas sobre la vida privada de esa persona. En cambio, incluso un acceso que haga posible extraer semejantes conclusiones precisas debería autorizarse en los casos en los que haya sospechas de que la persona en cuestión ha cometido infracciones penales que el Estado miembro de que se trate considere que afectan a un interés fundamental de la sociedad y, por tanto, que se encuadran en las formas graves de delincuencia.

El Tribunal de Justicia puntualiza asimismo que el control previo no puede en ningún caso automatizarse totalmente, ya que, cuando se trata de una investigación penal, tal control exige que se ponderen, por una parte, los intereses legítimos relacionados con la lucha contra la delincuencia y, por otra parte, el respeto de la vida privada y la protección de los datos personales. Tal ponderación requiere la intervención de una persona física, que es tanto más necesaria cuanto que la automaticidad y el carácter masivo del tratamiento de datos de que se trata comportan riesgos para la vida privada.

Así, el Tribunal de Justicia concluye que la posibilidad de que las personas encargadas del examen de los hechos en dicha autoridad pública asocien datos de identidad civil de una persona correspondientes a una dirección IP a los archivos que contengan elementos que permitan conocer el título de obras protegidas cuya puesta a disposición en Internet haya justificado la recogida de las direcciones IP por parte de organizaciones

de titulares de derechos debe condicionarse, en los casos en que la misma persona vuelva a reiterar una actividad que vulnere los derechos de autor o los derechos afines a los derechos de autor, al control de un órgano jurisdiccional o de una entidad administrativa independiente. Ese control no puede automatizarse totalmente y debe efectuarse antes de que se realice esa asociación, la cual, en tales casos, puede permitir que se extraigan conclusiones precisas sobre la vida privada de dicha persona cuya dirección IP se haya utilizado para actividades que pudieran ser constitutivas de vulneración de los derechos de autor o de los derechos afines a los derechos de autor.

En cuarto y último lugar, el Tribunal de Justicia indica que el sistema de tratamiento de datos utilizado por la autoridad pública tiene que someterse periódicamente al control de un organismo que sea independiente y tenga la condición de tercero respecto de dicha autoridad pública. En ese control se han de comprobar la integridad del sistema, incluidas las garantías efectivas contra los riesgos de acceso y uso abusivos o ilícitos de dichos datos, así como su eficacia y fiabilidad para detectar los posibles ilícitos.

En este contexto, el Tribunal de Justicia observa que, en el presente asunto, el tratamiento automatizado de los datos personales realizado por la autoridad pública sobre la base de información relativa a las vulneraciones del derecho de propiedad intelectual constatadas por las organizaciones de titulares de derechos puede dar lugar a un determinado número de falsos positivos y, sobre todo, al riesgo de que un número de datos que puede llegar a ser muy elevado sean desviados por terceros para finalidades abusivas o ilícitas, lo que explica la necesidad de tal control. El Tribunal de Justicia añade asimismo que ese tratamiento debe atenerse a las normas específicas de protección de los datos personales que se contemplan en la Directiva 2016/680. En efecto, en el presente asunto, aun cuando la autoridad pública no dispone de potestades de decisión propias en el denominado procedimiento de respuesta gradual, debe ser calificada de «autoridad pública» que participa en la prevención y la detección de infracciones penales y, por tanto, entra en el ámbito de aplicación de esta Directiva. Así pues, las personas implicadas en tal procedimiento deben disfrutar de un conjunto de garantías materiales y procedimentales que prescribe la Directiva 2016/680, correspondiendo al órgano jurisdiccional remitente comprobar si la legislación nacional recoge esas garantías.

2. Tratamiento de datos personales en materia penal

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

En 2012, la Organización Internacional de Policía Criminal (en lo sucesivo, «Interpol») publicó, a petición de los Estados Unidos y sobre la base de una orden de detención dictada por las autoridades de este país, una notificación roja referida a WS, de

nacionalidad alemana, con miras a su eventual extradición. Cuando se localiza en un Estado afiliado a Interpol a una persona objeto de una notificación roja, ese Estado debe, en principio, proceder a su detención preventiva o a vigilarla o limitar sus desplazamientos.

No obstante, antes de que se publicase dicha notificación roja, se había incoado contra WS en Alemania un procedimiento de investigación referido, según el órgano jurisdiccional remitente, a los mismos hechos que aquellos en los que se basaba dicha notificación roja. Este procedimiento se archivó con carácter firme en 2010, una vez que WS hubo abonado una determinada cantidad dineraria, acogiéndose a un procedimiento específico de transacción previsto en el Derecho penal alemán. Posteriormente, el Bundeskriminalamt (Oficina Federal de Policía Criminal, Alemania) informó a Interpol de que consideraba que, a la vista de ese procedimiento anterior, el principio *non bis in idem* era aplicable al caso de autos. Este principio, consagrado tanto en el artículo 54 del Convenio de aplicación del Acuerdo de Schengen [68] como en el artículo 50 de la Carta, prohíbe, en particular, que una persona que ya haya sido juzgada en sentencia firme sea procesada de nuevo por el mismo delito.

En 2017, WS interpuso un recurso contra la República Federal de Alemania ante el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania) con la pretensión de que se ordenara a esta adoptar las medidas necesarias para la retirada de la notificación roja. A este respecto, WS invoca, además de la violación del principio *non bis in idem*, la violación de su derecho a la libre circulación, garantizado por el artículo 21 TFUE, dado que no puede desplazarse a los Estados parte en el Acuerdo de Schengen o a los Estados miembros sin correr el riesgo de ser detenido. Aduce asimismo que, debido a estas violaciones, el tratamiento de sus datos personales consignados en la notificación roja es contrario a la Directiva 2016/680, relativa a la protección de los datos personales en materia penal. [69]

En este contexto, el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden) decidió consultar al Tribunal de Justicia sobre la aplicación del principio *non bis in idem* y, más concretamente, sobre la posibilidad de que se proceda a la detención preventiva de una persona objeto de una notificación roja en una situación como esta. Además, en caso de que este principio sea aplicable, dicho órgano jurisdiccional desea que se dilucide qué consecuencias se derivarían para el tratamiento por parte de los Estados miembros de los datos personales consignados en tal notificación.

---

[68] Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes (DO 2000, L 239, p. 19; en lo sucesivo, «CAAS»)

[69] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO 2016, L 119, p. 89).

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

En lo referente a la cuestión de los datos personales consignados en una notificación roja de Interpol, el Tribunal de Justicia indica que toda operación realizada sobre tales datos, como su registro en los ficheros de búsqueda de un Estado miembro, constituye un «tratamiento» comprendido en la Directiva 2016/680. [70] Estima además, por un lado, que ese tratamiento persigue un fin legítimo y, por otro, que no puede considerarse ilícito meramente porque el principio *non bis in idem* pudiera resultar aplicable a los hechos en los que se basa la notificación roja. [71] Por añadidura, tal tratamiento por parte de las autoridades de los Estados miembros puede resultar indispensable precisamente para comprobar si dicho principio resulta aplicable.

En estas circunstancias, el Tribunal de Justicia declara, asimismo, que la Directiva 2016/680, interpretada a la luz del artículo 54 del CAAS y del artículo 50 de la Carta, no se opone al tratamiento de los datos personales que figuran en una notificación roja mientras no se haya determinado en una resolución judicial firme que el principio *non bis in idem* resulta aplicable al caso. No obstante, tal tratamiento debe respetar los requisitos establecidos en dicha Directiva. Desde esta perspectiva, en particular, debe ser necesario para la ejecución de una tarea realizada por una autoridad nacional competente para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. [72]

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

70 Véanse los artículos 2, apartado 1, y 3, punto 2, de la Directiva 2016/680.

71 Véanse los artículos 4, apartado 1, letra b), y 8, apartado 1, de la Directiva 2016/680.

72 Véanse los artículos 1, apartado 1, y 8, apartado 1, de la Directiva 2016/680.

***Sentencia de 21 de junio de 2022 (Gran Sala), Ligue des droits humains (C-817/19*, EU:C:2022:491)**

En este asunto (véase también la sección I.1., titulada «Conformidad del Derecho derivado de la Unión con el derecho a la protección de los datos de carácter personal»), tras haber constatado la validez de la Directiva PNR, el Tribunal de Justicia aporta precisiones sobre la interpretación de algunas de sus disposiciones. [73]

En primer término, señala que la Directiva enumera de manera exhaustiva los objetivos perseguidos por el tratamiento de los datos PNR. En consecuencia, esta Directiva se opone a una normativa nacional que autoriza el tratamiento de datos PNR con fines distintos de la lucha contra el terrorismo y las formas graves de delincuencia. De ese modo, una normativa nacional que además admite, como uno de los fines del tratamiento de datos PNR, el seguimiento de las actividades objeto de la atención de los servicios de inteligencia y de seguridad puede ir en contra del carácter exhaustivo de esta enumeración. Asimismo, el sistema establecido por la Directiva PNR no puede destinarse a la mejora de los controles fronterizos y la lucha contra la inmigración clandestina. De lo anterior también se deduce que los datos PNR no pueden ser conservados en una base de datos única consultable para la consecución tanto de los fines de la Directiva PNR como de otros fines.

En segundo término, el Tribunal de Justicia explicita el concepto de autoridad nacional independiente, competente para comprobar si se cumplen los requisitos de comunicación de los datos PNR, con vistas a su posterior evaluación, y para aprobar tal comunicación. En particular, la autoridad creada como UIP no puede ser calificada como tal autoridad ya que no tiene la condición de tercero respecto de la autoridad que solicita el acceso a los datos. Así, dado que los miembros de su personal pueden ser agentes transferidos por las autoridades facultadas para solicitar tal acceso, la UIP está necesariamente vinculada a esas autoridades. En consecuencia, la Directiva PNR se opone a una normativa nacional con arreglo a la cual la autoridad creada como UIP reviste también la condición de autoridad nacional competente, facultada para aprobar la comunicación de los datos PNR tras la expiración del plazo de seis meses desde la transferencia de estos datos a la UIP.

En tercer término y por lo que se refiere al plazo de conservación de los datos PNR, el Tribunal de Justicia resuelve que el artículo 12 de la Directiva PNR, interpretado a la luz de los artículos 7, 8 y 52, apartado 1, de la Carta, se opone a una normativa nacional que prevé una duración general de conservación de estos datos de cinco años, aplicable a todos los pasajeros aéreos sin distinción.

Así, según el Tribunal de Justicia, tras la expiración del período de conservación inicial de seis meses, la conservación de los datos PNR no parece limitarse a lo estrictamente

[73] En particular, el artículo 2 («Aplicación de la [Directiva] a los vuelos interiores de la UE»), el artículo 6 («Tratamiento de los datos PNR»), y el artículo 12 («Período de conservación de los datos y despersonalización»), de la Directiva PNR.

necesario en lo que se refiere a los pasajeros aéreos respecto de los cuales ni la evaluación previa, ni las eventuales comprobaciones efectuadas durante el periodo de conservación inicial de seis meses, ni ninguna otra circunstancia, han revelado la existencia de elementos objetivos —como el hecho de que los datos PNR de los pasajeros en cuestión hayan dado lugar a una concordancia positiva verificada en el marco de la evaluación previa— que permitan apreciar la existencia de un riesgo en materia de delitos de terrorismo o de delitos graves que tengan una relación, siquiera indirecta, con el viaje aéreo realizado por esos pasajeros. Por el contrario, el Tribunal de Justicia, estima que, durante el período inicial de seis meses, la conservación de los datos PNR de todos los pasajeros aéreos cubiertos por el sistema establecido por esta Directiva no parece, en principio, exceder los límites de lo estrictamente necesario.

En cuarto término, el Tribunal de Justicia aporta precisiones acerca de una eventual aplicación de la Directiva PNR, con objeto de luchar contra delitos de terrorismo o delitos graves, a otros medios de transporte de pasajeros dentro de la Unión. Pues bien, esta Directiva, interpretada a la luz del artículo 3 TUE, apartado 2, del artículo 67 TFUE, apartado 2, y del artículo 45 de la Carta, se opone a un sistema de transferencia y de tratamiento del conjunto de los datos PNR de la totalidad de los transportes efectuados mediante otros medios dentro de la Unión, en ausencia de una amenaza terrorista real y actual o previsible a la que deba enfrentarse el Estado miembro en cuestión. En tal situación, al igual que respecto de los vuelos interiores de la Unión, la aplicación del sistema establecido por la Directiva PNR debe limitarse a los datos PNR de los transportes relativos, en particular, a determinadas conexiones o a determinados planes de viaje o a determinadas estaciones o puertos marítimos respecto de los que existan indicios que permitan justificar esta aplicación. Incumbe al Estado miembro de que se trate seleccionar los transportes respecto de los que existen estos indicios y reexaminar regularmente esta aplicación en función de la evolución de las circunstancias que justificaran su selección.

IV. Transferencia de datos personales a terceros países

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

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

El Tribunal de Justicia declaró que no existe una «transferencia de datos a un país tercero» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se

encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio de Internet en el que se puede consultar la página web y que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros.

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

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

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 Comisario para la protección de datos desestimó esa reclamación, en particular porque en su Decisión 2000/520/CE [74] la Comisión había estimado que, en el marco del régimen llamado de «puerto seguro» (en inglés, «safe harbour»), [75] Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos.

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

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

[75] 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.

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

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

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 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.

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. 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, 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. 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.

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 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 del registro de nombres de los pasajeros (Acuerdo 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 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, entre otros, 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 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 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 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. Tales 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.

Además, puso de relieve que, aun cuando algunos de los datos 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 que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas, etc.).

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. Ahora bien, en el caso de autos no existe 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.

En segundo lugar, el Tribunal de Justicia consideró que el almacenamiento continuado de los datos 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. En cambio, el almacenamiento de los datos PNR de los pasajeros aéreos respecto de los cuales se identifiquen elementos objetivos que permitan considerar que estos 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 es admisible aun después de concluida su estancia en ese país, incluso durante un período de cinco años.

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, 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 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 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.

Por lo tanto, en los supuestos en que concurren circunstancias objetivas que justifican la utilización de los datos PNR para luchar contra el terrorismo y la delincuencia grave de carácter transnacional y 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 PNR se comunican a otras autoridades públicas o a particulares. No obstante, únicamente debe procederse a esa información siempre que no pueda perjudicar a las investigaciones llevadas a cabo por las autoridades públicas contempladas en el acuerdo previsto.

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

El RGPD dispone que la transferencia de datos personales hacia un país tercero únicamente puede efectuarse, en principio, cuando el país tercero de que se trate garantice un nivel de protección adecuado de los mismos. Según el referido Reglamento, la Comisión puede constatar que un país tercero, a la vista de su legislación interna o de sus compromisos internacionales, garantiza un nivel de protección

adecuado. [76] A falta de esa decisión de adecuación, la mencionada transferencia solo podrá realizarse si el exportador de datos personales, establecido en la Unión, ofrece garantías adecuadas que pueden, en particular, derivarse de cláusulas tipo de protección de datos adoptadas por la Comisión y si los interesados cuentan con derechos exigibles y acciones legales efectivas. [77] Asimismo, el RGPD establece, de modo preciso, las condiciones en las que puede tener lugar esa transferencia en ausencia de una decisión de adecuación o de garantías adecuadas. [78]

El Sr. Maximilliam Schrems, nacional austriaco residente en Austria, es usuario de Facebook desde 2008. Como ocurre con el resto de usuarios residentes en la Unión, los datos personales del Sr. Schrems son transferidos, total o parcialmente, por Facebook Ireland a servidores pertenecientes a Facebook Inc., situados en el territorio de Estados Unidos, donde son objeto de tratamiento. El Sr. Schrems presentó una reclamación ante la autoridad irlandesa de control en la que solicitaba, en esencia, que se prohibiesen esas transferencias. Afirmó que el Derecho y las prácticas de los Estados Unidos no ofrecían una protección suficiente contra el acceso, por parte de las autoridades públicas, a los datos trasferidos a ese país. La reclamación fue desestimada, debido, en particular, a que la Comisión había declarado, en su Decisión 2000/520, [79] que los Estados Unidos ofrecían un nivel adecuado de protección. Mediante sentencia dictada el 6 de octubre de 2015, el Tribunal de Justicia, resolviendo una cuestión prejudicial planteada por la High Court (Tribunal Superior, Irlanda), declaró inválida dicha Decisión (en lo sucesivo, «sentencia Schrems I»). [80]

A raíz de la sentencia Schrems I y de la anulación consecutiva, por parte del órgano jurisdiccional irlandés, de la decisión por la que se desestimaba la reclamación del Sr. Schrems, la autoridad de control irlandesa instó a este a que modificase su reclamación, habida cuenta de la invalidación por el Tribunal de Justicia de la Decisión 2000/520. En su reclamación modificada, el Sr. Schrems sostiene que los Estados Unidos no ofrecen protección suficiente de los datos transferidos a dicho país. Solicita que en el futuro se suspendan o se prohíban las transferencias de sus datos personales desde la Unión a los Estados Unidos, que Facebook Ireland efectúa desde entonces basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión 2010/87/UE. [81] Al estimar que la tramitación de la reclamación del Sr. Schrems dependía, entre otros factores, de la validez de la Decisión 2010/87, la autoridad de control irlandesa inició un procedimiento ante la High Court (Tribunal Superior) con el fin de que

---

76 Artículo 45 del RGPD.

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

78 Artículo 49 del RGPD.

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

80 Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650.

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

esta plantease una petición de decisión prejudicial al Tribunal de Justicia. Tras la incoación de dicho procedimiento, la Comisión adoptó la Decisión (UE) 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. [82]

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

El Tribunal de Justicia constata que el examen de la Decisión 2010/87 a la luz de la Carta no ha puesto de manifiesto la existencia de ningún elemento que pueda afectar a su validez. En cambio, declara que la Decisión 2016/1250 es inválida.

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

Por lo que respecta al nivel de protección exigido respecto de dicha transferencia, el Tribunal de Justicia declara que las exigencias previstas en ese sentido por las disposiciones del RGPD, que se refieren a garantías adecuadas, derechos exigibles y acciones legales efectivas, deben interpretarse en el sentido de que las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos deben gozar de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por dicho Reglamento, interpretado a la luz de la Carta. En este contexto, el Tribunal de Justicia precisa que la evaluación de ese nivel de protección debe tener en cuenta tanto las estipulaciones contractuales acordadas entre el exportador de datos establecido en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país.

Por lo que respecta a las obligaciones que incumben a las autoridades de control en el contexto de tal transferencia, el Tribunal de Justicia declara que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, dichas autoridades

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

están obligadas, en concreto, a suspender o prohibir una transferencia de datos a un país tercero cuando consideren, a la luz de todas las circunstancias específicas de la referida transferencia, que las cláusulas tipo de protección de datos no se respetan o no pueden respetarse en ese país y que la protección de los datos transferidos, exigida por el Derecho de la Unión, no puede garantizarse mediante otros medios, si el exportador establecido en la Unión no ha suspendido la transferencia o puesto fin a esta por sí mismo.

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

El Tribunal examina, por último, la validez de la Decisión 2016/1250 atendiendo a las exigencias derivadas del RGPD, leído a la luz de las disposiciones de la Carta que garantizan el respeto de la vida privada y familiar, la protección de los datos personales y el derecho a la tutela judicial efectiva. A este respecto, el Tribunal de Justicia señala que dicha Decisión consagra, al igual que la Decisión 2000/520, la primacía de las exigencias relativas a la seguridad nacional, al interés público y al cumplimiento de la legislación americana, posibilitando de este modo las injerencias en los derechos fundamentales de las personas cuyos datos son transferidos a ese país tercero. Según el Tribunal de Justicia, las limitaciones de la protección de los datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización, por las autoridades estadounidenses, de los datos transferidos desde la Unión a dicho país tercero, y que la Comisión evaluó en la Decisión 2016/1250, no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas, en el Derecho de la Unión, por el principio de proporcionalidad, en la medida en que los programas de vigilancia basados en esa normativa no se limitan a lo estrictamente necesario. Basándose en las constataciones expuestas en dicha Decisión, el Tribunal de Justicia pone de manifiesto que, por lo que respecta a determinados programas de vigilancia, de la citada normativa no se desprende en modo alguno la existencia de limitaciones a la

habilitación que otorga para la ejecución de esos programas ni tampoco la existencia de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de los mismos. El Tribunal de Justicia añade que, si bien la misma normativa establece exigencias que las autoridades estadounidenses deben respetar al aplicar los programas de vigilancia de que se trata, esta no confiere a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales.

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

V. La protección de datos personales en Internet

1. Derecho de oposición al tratamiento de 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 esta sentencia (véanse también las secciones II.1. y II.3., tituladas «Ámbito de aplicación de la normativa general» y «Concepto de “tratamiento de datos personales”»), el Tribunal de Justicia precisó el alcance de los derechos de acceso y de oposición al tratamiento de los datos personales en Internet, previstos en la Directiva 95/46.

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

sido borrados previa o simultáneamente de esas páginas web y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.

Asimismo, al preguntársele sobre 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 de Justicia 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. 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. En este marco, la apreciación de la existencia del derecho del interesado a que la información relativa a su persona ya no esté vinculada a su nombre por una lista de resultados no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado.

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 resultara, por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, 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.

2. Tratamiento de datos personales y derechos de propiedad intelectual

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

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), [83] 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, [84] 2004/48/CE, relativa al respeto de los derechos de propiedad intelectual, [85] y 2002/58 no obligan a los Estados miembros a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Sin embargo, el Derecho de la Unión exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de estas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no solo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de estas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad.

---

83 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 del comercio electrónico en el mercado interior («Directiva sobre el comercio electrónico») (DO 2000, L 178, p. 1).

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

85 Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (DO 2004, L 157, p. 45; corrección de errores en DO 2004, L 195, p. 16, DO 2004, L 351, p. 44 y DO 2007, L 204, p. 27)

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

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

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

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

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, en particular, 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 el fin perseguido por dicho requerimiento fuera más importante que el daño o perjuicio que este pudiera causar a la persona afectada o a otros intereses contrapuestos.

El Tribunal de Justicia concluyó, por tanto, que las Directivas 2002/58 y 2004/48 no se oponen a una normativa nacional, como la controvertida en el 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.

3. Retirada de enlaces a datos personales

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

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

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

En primer término, el Tribunal de Justicia recordó que el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la pertenencia a sindicatos, así como el tratamiento de los datos

relativos a la salud o a la sexualidad, está prohibido, [86] salvo determinadas excepciones y restricciones a esta prohibición. Por lo que respecta al tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, en principio solo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías adecuadas y específicas en el Derecho nacional. [87]

El Tribunal de Justicia declaró que la prohibición y las restricciones relativas al tratamiento de esas categorías especiales de datos se aplican al gestor de un motor de búsqueda, al igual que a cualquier otro responsable del tratamiento de datos personales. En efecto, la finalidad de esas prohibiciones y restricciones consiste en garantizar una mayor protección frente a tales tratamientos, que, en atención a la particular sensibilidad de esos datos, pueden constituir una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales.

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

En segundo término, el Tribunal de Justicia consideró que, cuando el gestor reciba una solicitud de retirada de enlaces relativa a datos sensibles, está obligado en principio, salvo ciertas excepciones, a acceder a dicha solicitud. Por lo que respecta a esas excepciones, el gestor puede, en particular, negarse a acceder a tal solicitud cuando compruebe que los enlaces conducen a datos que han sido manifiestamente hechos públicos por el interesado, [88] siempre que la inclusión de tales enlaces cumpla los demás requisitos de legalidad de un tratamiento de datos personales y salvo que el interesado tenga derecho a oponerse a tal tratamiento por razones legítimas propias de su situación particular. [89]

En cualquier caso, cuando reciba una solicitud de retirada de enlaces, el gestor de un motor de búsqueda debe verificar si la inclusión en la lista de resultados del enlace a una página web en la que se han publicado datos sensibles, presentada tras una búsqueda efectuada a partir del nombre de esa persona, resulta estrictamente necesaria para proteger el derecho a la libertad de información de los internautas potencialmente interesados en acceder a esa página web mediante tal búsqueda. A este respecto, el Tribunal de Justicia subrayó que, aunque los derechos al respeto de la vida

[86] Artículo 8, apartado 1, de la Directiva 95/46 y artículo 9, apartado 1, del Reglamento 2016/679.
[87] Artículo 8, apartado 5, de la Directiva 95/46 y artículo 10 del Reglamento 2016/679.
[88] Artículo 8, apartado 2, letra e), de la Directiva 95/46 y artículo 9, apartado 2, letra e), del Reglamento 2016/679.
[89] Artículo 14, párrafo primero, letra a), de la Directiva 95/46 y artículo 21, apartado 1, del Reglamento 2016/679.

privada y a la protección de datos personales prevalecen, con carácter general, sobre la libertad de información de los internautas, este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate, del carácter sensible de esta para la vida privada del interesado y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que el interesado desempeñe en la vida pública.

En tercer término, el Tribunal de Justicia declaró que, en el marco de una solicitud de retirada de enlaces referida a datos sobre un procedimiento judicial en materia penal incoado contra el interesado, que hace referencia a una etapa anterior de ese procedimiento y que ya no corresponde a la situación actual, incumbe al gestor de un motor de búsqueda apreciar si, a la luz del conjunto de circunstancias del caso concreto, esa persona tiene derecho a que la información en cuestión ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre. Sin embargo, aun cuando este no sea el caso porque la inclusión del enlace controvertido es estrictamente necesaria para conciliar los derechos al respeto de la vida privada y a la protección de los datos del interesado con la libertad de información de los internautas potencialmente interesados, el gestor estará obligado, a más tardar en el momento de la solicitud de retirada de enlaces, a estructurar la lista de resultados de tal manera que la imagen global que resulte de ella para el internauta refleje la situación judicial actual, lo que requerirá, en particular, que en dicha lista se indiquen, en primer lugar, enlaces a páginas web que contengan información al respecto.

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

La Commission nationale de l'informatique et des libertés (Comisión Nacional de Informática y Libertades, Francia; en lo sucesivo «CNIL») requirió a Google para que, cuando esta empresa acceda a una solicitud de retirada de enlaces, suprima de la lista de resultados que aparece tras una búsqueda efectuada a partir del nombre de la persona de que se trate, los enlaces que dirijan a páginas web que incluyan datos personales relativos a esta en todas las extensiones de nombre de dominio de su motor de búsqueda. Tras negarse Google a atenerse a este requerimiento, la CNIL impuso a esta sociedad una sanción de 100 000 euros. El Conseil d'État (Consejo de Estado, actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), ante el que recurrió Google, solicitó al Tribunal de Justicia que precisase el alcance territorial de la obligación del gestor de un motor de búsqueda de aplicar el derecho a la supresión de enlaces en virtud de la Directiva 95/46.

El Tribunal de Justicia comenzó recordando que, basándose en el Derecho de la Unión, las personas físicas tienen la posibilidad de hacer valer su derecho a la retirada de enlaces frente al gestor de un motor de búsqueda que posea uno o varios establecimientos en el territorio de la Unión, con independencia de que el tratamiento

de datos personales (en este caso, el hecho de mostrar enlaces que dirigen a páginas web en las que figuran datos personales que conciernen a la persona que reivindica ese derecho) tenga lugar en la Unión o no. [90]

Por lo que respecta al alcance del derecho a la retirada de enlaces, el Tribunal de Justicia consideró que el gestor de un motor de búsqueda no está obligado a proceder a dicha retirada en todas las versiones de su motor de búsqueda, sino solo en las versiones de este que corresponden al conjunto de los Estados miembros. A este respecto, señaló que, si bien una retirada de enlaces universal respondería plenamente, habida cuenta de las características de Internet y de los motores de búsqueda, al objetivo del legislador de la Unión consistente en garantizar un elevado nivel de protección de los datos personales en toda la Unión, del Derecho de la Unión [91] no se desprende en modo alguno que, para alcanzar tal objetivo, el legislador haya optado por atribuir al derecho a la retirada de enlaces un alcance que vaya más allá del territorio de los Estados miembros. En particular, mientras que el Derecho de la Unión ha instaurado mecanismos de cooperación entre las autoridades de control de los Estados miembros para que estas lleguen a una decisión común basada en un equilibrio entre el derecho a la protección de la vida privada y de los datos personales, por un lado, y el interés del público de los distintos Estados miembros en tener acceso a una información, por otro lado, tales mecanismos no están previstos actualmente en lo que respecta al alcance de la retirada de enlaces fuera de la Unión.

En el estado actual del Derecho de la Unión, incumbe al gestor de un motor de búsqueda proceder a la retirada de enlaces solicitada no solo de la versión del motor de búsqueda correspondiente al Estado miembro de residencia del beneficiario de esa retirada de enlaces, sino de las versiones del motor correspondientes a todos los Estados miembros, en particular con el fin de garantizar un nivel coherente y elevado de protección en el conjunto de la Unión. Asimismo, incumbe a tal gestor tomar, en caso necesario, medidas lo suficientemente eficaces como para impedir o, al menos, dificultar seriamente a los internautas de la Unión el acceso, en su caso desde una versión del motor correspondiente a un tercer Estado, a los enlaces objeto de la retirada y será responsabilidad del órgano jurisdiccional nacional comprobar si las medidas adoptadas por el gestor responden a esta exigencia.

Por último, el Tribunal de Justicia subrayó que, aunque el Derecho de la Unión no exige al gestor de un motor de búsqueda proceder a una retirada de enlaces en todas las versiones de su motor, tampoco lo prohíbe. Por lo tanto, una autoridad de control o judicial de un Estado miembro sigue siendo competente para realizar, de conformidad con los estándares nacionales de protección de los derechos fundamentales, una ponderación entre, por un lado, los derechos del interesado al respeto de su vida privada y a la protección de sus datos personales y, por otro lado, el derecho a la

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

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

libertad de información y, al término de esta ponderación, exigir, en su caso, al gestor del motor de búsqueda que proceda a retirar los enlaces de todas las versiones de dicho motor.

Sentencia de 8 de diciembre de 2022 (Gran Sala), Google (Retirada de enlaces a contenido supuestamente inexacto) (C-460/20, EU:C:2022:962)

Los demandantes en el litigio principal, TU, que ocupa puestos de responsabilidad y posee participaciones en diferentes sociedades, y RE, que era su pareja, y hasta mayo de 2015 apoderada de una de estas sociedades, fueron objeto de tres artículos publicados en un sitio de Internet en 2015 por G LLC, que gestiona ese sitio de Internet. Esos artículos, uno de los cuales estaba ilustrado con cuatro fotografías que representaban a los demandantes y sugería que llevaban una vida de lujo, presentaban de manera crítica el modelo de inversión de varias de sus sociedades. Se podía acceder a esos artículos tecleando en el motor de búsqueda gestionado por Google LLC (en lo sucesivo, «Google») los nombres y apellidos de los demandantes, tanto solos como en combinación con determinados nombres de sociedades. La lista de resultados remitía a esos artículos, por medio de un enlace, y a las fotografías, mostradas en forma de imágenes de previsualización («thumbnails»).

Los demandantes en el litigio principal solicitaron a Google, como responsable del tratamiento de datos personales efectuado por su motor de búsqueda, por una parte, que retirara de la lista de resultados de búsqueda los enlaces a los artículos controvertidos, por entender que contenían alegaciones inexactas y opiniones difamatorias, y, por otra parte, que retirara las previsualizaciones de la lista de resultados de búsqueda. Google denegó dicha solicitud.

Al haber sido desestimadas sus pretensiones tanto en primera instancia como en apelación, los demandantes en el litigio principal plantearon ante el Bundesgerichtshof (Tribunal Supremo de lo Civil y Penal, Alemania) un recurso de casación en cuyo marco el Bundesgerichtshof planteó al Tribunal de Justicia una cuestión prejudicial sobre la interpretación del RGPD y de la Directiva 95/46. [92]

Mediante su sentencia, dictada en Gran Sala, el Tribunal de Justicia desarrolla su jurisprudencia sobre los requisitos aplicables a las solicitudes de retirada de enlaces dirigidas al gestor de un motor de búsqueda sobre la base de las normas de protección de datos personales. Concretamente, examina, por un lado, el alcance de las obligaciones y responsabilidades del gestor de un motor de búsqueda en la tramitación de una solicitud de retirada de enlaces basada en la supuesta inexactitud de la información que figura en el contenido indexado y, por otro, la carga de la prueba que recae sobre el interesado por lo que respecta a dicha inexactitud. Además, se pronuncia sobre la necesidad, a efectos del examen de una solicitud de supresión de fotografías

[92] Respectivamente, el artículo 17, apartado 3, letra a), del RGPD y los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46.

mostradas en forma de previsualizaciones en la lista de resultados de una búsqueda de imágenes, de tener en cuenta el contexto original de la publicación de dichas fotografías en Internet.

En primer lugar, el Tribunal de Justicia declara que, en la ponderación entre, por una parte, los derechos al respeto de la vida privada y a la protección de datos personales, y, por otra parte, el derecho a la libertad de expresión e información, [93] a efectos del examen de una solicitud de retirada de enlaces dirigida al gestor de un motor de búsqueda que tiene por objeto la supresión de la lista de resultados de una búsqueda de un enlace a un contenido que incluye información supuestamente inexacta, dicha retirada de enlaces no está supeditada a la aclaración siquiera provisional de la cuestión de la exactitud del contenido indexado mediante una demanda judicial presentada por el solicitante contra el proveedor de contenidos.

Con carácter preliminar, para examinar en qué condiciones está obligado el gestor de un motor de búsqueda a acceder a una solicitud de retirada de enlaces y, por lo tanto, a suprimir de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre del interesado el enlace a una página web en la que figuran alegaciones que dicha persona estima inexactas, el Tribunal de Justicia recuerda, en particular, lo siguiente:

• En la medida en que la actividad de un motor de búsqueda puede afectar, significativamente y de modo adicional a la de los editores de sitios de Internet, a los derechos fundamentales al respeto de la vida privada y a la protección de datos personales, el gestor de ese motor de búsqueda, como persona que determina los fines y los medios de esta actividad, debe garantizar, en el marco de sus responsabilidades, competencias y posibilidades, que las garantías establecidas por la Directiva 95/46 y el RGPD puedan tener pleno efecto y que puede llevarse a cabo efectivamente una protección eficaz y completa de los interesados.

• Cuando se le presente una solicitud de retirada de enlaces, el gestor de un motor de búsqueda debe comprobar si la inclusión del enlace a la página web en cuestión en la lista de resultados es necesaria para el ejercicio del derecho a la libertad de información de los internautas potencialmente interesados en acceder a dicha página web mediante tal búsqueda, protegida por el derecho a la libertad de expresión e información.

• El RGPD consagra expresamente la exigencia de una ponderación entre, por una parte, los derechos fundamentales al respeto de la vida privada y a la protección de datos personales y, por otra parte, el derecho fundamental a la libertad de información.

Para comenzar, el Tribunal de Justicia señala que, aunque los derechos al respeto de la vida privada y a la protección de datos personales del interesado prevalecen, con carácter general, sobre el interés legítimo de los internautas en acceder a la información

[93] Derechos fundamentales garantizados, respectivamente, por los artículos 7, 8 y 11 de la Carta.

en cuestión, dicho equilibrio puede depender de las circunstancias pertinentes del supuesto específico, y en concreto de la naturaleza de la información de que se trate y de su carácter sensible para la vida privada del interesado y del interés del público en disponer de esa información, que puede variar, en particular, en función del papel que el interesado desempeñe en la vida pública.

La exactitud o inexactitud del contenido indexado constituye también un elemento pertinente en el marco de esta apreciación. De ese modo, en determinadas circunstancias, el derecho a la información de los internautas y la libertad de expresión del proveedor de contenidos pueden prevalecer sobre los derechos a la protección de la vida privada y a la protección de los datos personales, en particular cuando el interesado desempeña un papel en la vida pública. Sin embargo, esta correlación se invierte cuando al menos una parte de la información a la que se refiere la solicitud de retirada de enlaces, que no presenta un carácter menor respecto del contenido en su conjunto, resulta inexacta. En ese supuesto, no pueden tenerse en cuenta los derechos a informar y ser informado, puesto que no pueden incluir el derecho a difundir y recibir ese tipo de información.

A continuación, por lo que se refiere, por una parte, a las obligaciones referidas a la determinación del carácter exacto o no de la información que figura en el contenido indexado, el Tribunal de Justicia precisa que la persona que solicita la retirada de enlaces debido a la inexactitud de tal información está obligada a acreditar su inexactitud manifiesta o, al menos, la inexactitud de parte de esa información que no presenta un carácter menor en relación con el conjunto de dicho contenido. No obstante, para evitar que recaiga sobre esa persona una carga excesiva que pueda menoscabar el efecto útil del derecho a la retirada de enlaces, únicamente le incumbe aportar las pruebas que, habida cuenta de las circunstancias del caso concreto, puede exigírsele razonablemente que busque. En principio, esa persona no puede estar obligada a presentar en apoyo de su solicitud de retirada de enlaces, ya antes de recurrir a los tribunales, una resolución judicial anterior dictada contra el editor del sitio de Internet, ni siquiera una resolución sobre medidas provisionales.

Por otra parte, en cuanto a las obligaciones y responsabilidades que recaen sobre el gestor del motor de búsqueda, el Tribunal de Justicia subraya que, para comprobar si un contenido puede seguir incluido en la lista de resultados de las búsquedas efectuadas a través de su motor de búsqueda tras una solicitud de retirada de enlaces, debe basarse en el conjunto de derechos e intereses en juego, así como en todas las circunstancias del caso concreto. Sin embargo, no puede obligarse a dicho gestor a investigar los hechos y, a tal efecto, a organizar un debate contradictorio con el proveedor de contenidos para obtener datos que le falten sobre la exactitud del contenido indexado. La obligación de contribuir a determinar si el contenido indexado es o no exacto haría recaer sobre dicho gestor una carga que excede de lo que razonablemente cabe esperar de él en relación con sus responsabilidades, competencias y posibilidades. Esa solución entrañaría un grave riesgo de que se retiraran enlaces a contenidos que responden a

una necesidad de información legítima y preponderante del público y que, de ese modo, resultara difícil encontrarlos en Internet. Así pues, existiría un riesgo real de efecto disuasorio sobre el ejercicio de la libertad de expresión e información si tal gestor efectuara la retirada de enlaces de manera casi sistemática con el fin de evitar tener que soportar la carga de investigar los hechos pertinentes para acreditar el carácter exacto o no del contenido indexado.

Por consiguiente, cuando el solicitante de retirada de enlaces presenta pruebas que demuestran la inexactitud manifiesta de la información que figura en el contenido indexado o, al menos, de una parte de esa información que no tiene carácter menor respecto del conjunto de esta, el gestor del motor de búsqueda está obligado a acceder a la solicitud. Lo mismo sucede cuando el solicitante presenta una resolución judicial adoptada contra el editor del sitio de Internet y que se basa en la constatación de que cierta información que figura en el contenido indexado, que no presenta un carácter menor respecto del conjunto de este, es, al menos a primera vista, inexacta. En cambio, si el carácter inexacto de tal información no resulta manifiesto a la vista de los elementos de prueba aportados por el solicitante, el gestor del motor de búsqueda no está obligado, a falta de tal resolución judicial, a acceder a la solicitud de retirada de enlaces. Cuando la información en cuestión puede contribuir a un debate de interés general, procede atribuir especial importancia al derecho a la libertad de expresión e información, tras considerar el conjunto de circunstancias del caso concreto.

Por último, el Tribunal de Justicia añade que, en caso de que el gestor del motor de búsqueda no acceda a la solicitud de retirada de enlaces, el interesado puede acudir a la autoridad de control o a los tribunales para que estos lleven a cabo las comprobaciones necesarias y ordenen a dicho responsable que adopte las medidas precisas en consecuencia. A ese respecto, son en particular las autoridades judiciales las que deben garantizar la ponderación de los intereses en pugna, ya que son las mejor situadas para efectuar una ponderación compleja y minuciosa que tenga en cuenta todos los criterios y elementos establecidos por la jurisprudencia pertinente.

En segundo lugar, el Tribunal de Justicia declara que, en la ponderación de los derechos fundamentales antes mencionados, a efectos del examen de una solicitud de retirada de enlaces que tiene por objeto que se eliminen de los resultados de una búsqueda de imágenes efectuada a partir del nombre de una persona física fotografías mostradas en forma de previsualizaciones que representan a esa persona, procede tener en cuenta el valor informativo de esas fotografías con independencia del contexto original de su publicación en la página web de la que proceden. Sin embargo, procede tomar en consideración cualquier elemento textual que acompañe directamente a esas fotografías cuando se muestran en los resultados de la búsqueda y que pueda arrojar luz sobre su valor informativo.

Para llegar a esa conclusión, el Tribunal de Justicia subraya que las búsquedas de imágenes efectuadas a través de un motor de búsqueda en Internet a partir del nombre de una persona están sujetas a los mismos principios que los aplicables a las búsquedas

de páginas de Internet y de información recogida en dichas páginas. Indica que mostrar fotografías del interesado en forma de previsualizaciones tras una búsqueda por nombre puede constituir una injerencia particularmente importante en los derechos a la protección de la vida privada y de los datos personales de esa persona.

Por lo tanto, cuando el gestor de un motor de búsqueda recibe una solicitud de retirada de enlaces con el fin de que se eliminen de los resultados de una búsqueda de imágenes efectuada a partir del nombre de una persona fotografías mostradas en forma de previsualizaciones que representan a esa persona, debe comprobar si mostrar las fotografías en cuestión es necesario para el ejercicio del derecho a la libertad de información de los internautas potencialmente interesados en tener acceso a esas fotografías mediante tal búsqueda.

Pues bien, en la medida en que el motor de búsqueda muestra fotografías del interesado fuera del contexto en el que se publican en la página web indexada, la mayoría de las veces con el fin de ilustrar los elementos textuales que contiene esa página, procede determinar si, no obstante, ese contexto debe tomarse en consideración en la ponderación de los derechos e intereses en pugna que debe efectuarse. En ese marco, la cuestión de si dicha evaluación debe incluir también el contenido de la página web en la que figura la fotografía cuya presentación en forma de previsualización se solicita que se suprima depende del objeto y de la naturaleza del tratamiento en cuestión.

Por lo que respecta, en primer término, al objeto del tratamiento de que se trata, el Tribunal de Justicia observa que la publicación de fotografías como medio de comunicación no verbal puede tener un impacto más importante en los internautas que las publicaciones textuales. En efecto, las fotografías son, como tales, un medio importante de atraer la atención de los internautas y pueden suscitar interés en acceder a los artículos que ilustran. Pues bien, debido, en particular, a que estas se prestan a menudo a varias interpretaciones, mostrarlas como previsualizaciones en la lista de resultados de búsqueda puede implicar una injerencia particularmente grave en el derecho del interesado a la protección de su imagen, lo cual debe tenerse en cuenta en el marco de la ponderación entre los derechos e intereses en conflicto. Es necesaria una ponderación diferenciada en función de que se trate, por un lado, de artículos provistos de fotografías publicadas por el editor de la página web y que, insertas en su contexto original, ilustran la información facilitada en esos artículos y las opiniones que en ellos se expresan, o, por otro, de fotografías mostradas en forma de previsualizaciones en la lista de resultados por el gestor de un motor de búsqueda fuera del contexto en el que fueron publicadas en la página web original.

A este respecto, el Tribunal de Justicia recuerda que no solo la razón que justifica la publicación de un dato personal en un sitio de Internet no coincide forzosamente con la que se aplica a la actividad de los motores de búsqueda, sino también que, aun cuando así sea, el resultado de la ponderación de los derechos e intereses en conflicto puede variar según se trate del tratamiento efectuado por el gestor de un motor de búsqueda

o del realizado por el editor de esa página web. Por una parte, los intereses legítimos que justifican esos tratamientos pueden ser diferentes y, por otra parte, las consecuencias de estos tratamientos sobre el interesado, en particular sobre su vida privada, no son necesariamente las mismas.

En cuanto, en segundo término, a la naturaleza del tratamiento realizado por el gestor del motor de búsqueda, el Tribunal de Justicia declara que, al encontrar las fotografías de personas físicas publicadas en Internet y mostrarlas por separado en los resultados de una búsqueda por imágenes en forma de previsualizaciones, el gestor de un motor de búsqueda ofrece un servicio en el que realiza un tratamiento de datos personales autónomo y distinto tanto del tratamiento efectuado por el editor de la página web de la que proceden las fotografías, como del correspondiente a la indexación de dicha página, del que el gestor es igualmente responsable.

Por consiguiente, es necesario proceder a una apreciación autónoma de la actividad del gestor del motor de búsqueda que consiste en mostrar los resultados de una búsqueda de imágenes en forma de previsualizaciones, ya que la injerencia adicional en los derechos fundamentales que resulta de tal actividad puede ser particularmente intensa, debido a la agregación, en una búsqueda por nombre, de toda la información referida al interesado que se encuentre en Internet. En esa apreciación autónoma procede tener en cuenta que mostrar esos resultados constituye en sí el resultado buscado por el internauta, con independencia de su decisión posterior de acceder o no a la página web original.

No obstante, el Tribunal de Justicia observa que tal ponderación específica, que tiene en cuenta la naturaleza autónoma del tratamiento que lleva a cabo el gestor del motor de búsqueda, se entiende sin perjuicio de la eventual pertinencia de elementos textuales que puedan acompañar directamente a la presentación de una fotografía en la lista de resultados de una búsqueda, pues esos elementos pueden arrojar luz sobre el valor informativo de dicha fotografía para el público y, por tanto, influir en la ponderación de los derechos e intereses que están en juego.

4. Consentimiento del usuario de un sitio de Internet al almacenamiento de información

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

Mediante esta sentencia, el Tribunal de Justicia declaró que el consentimiento para el almacenamiento de información o para el acceso a información a través de «cookies» instaladas en el equipo terminal del usuario de un sitio de Internet no se presta de manera válida cuando la autorización resulta de una casilla marcada por defecto, con independencia de que la información de que se trate consista o no en datos personales. Además, el Tribunal de Justicia precisó que el proveedor de servicios debe indicar al

usuario de un sitio de Internet el tiempo durante el cual estas «cookies» estarán activas, así como la posibilidad o imposibilidad de que los terceros accedan a esas «cookies».

El litigio principal versaba sobre la organización de un juego con fines promocionales por Planet49 en el sitio de Internet www.dein-macbook.de. Para participar, los internautas debían comunicar su nombre y dirección en una página web en la que figuraban una serie de casillas para marcar. La casilla que autorizaba la instalación de «cookies» estaba marcada por defecto. El Bundesgerichtshof (Tribunal Supremo de lo Civil y Penal, Alemania), que conocía del recurso interpuesto por la Federación de Organizaciones y Asociaciones de Consumidores, albergaba dudas acerca de la validez de la obtención del consentimiento de los usuarios mediante una casilla marcada por defecto y sobre el alcance de la obligación de información que recae sobre el proveedor de servicios.

La petición de decisión prejudicial tenía como objeto principal la interpretación del concepto de «consentimiento» contemplado en la Directiva 2002/58, [94] puesta en relación con la Directiva 95/46/CE, [95] y con el RGPD. [96]

En primer término, el Tribunal de Justicia observó que el artículo 2, letra h), de la Directiva 95/46, a la que se remite el artículo 2, letra f), de la Directiva 2002/58, define el consentimiento como «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». Señaló que el requisito de una «manifestación» de voluntad del interesado sugiere claramente un comportamiento activo y no pasivo. Pues bien, el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de Internet. Además, la génesis del artículo 5, apartado 3, de la Directiva 2002/58, que dispone desde su modificación por la Directiva 2009/136 que el usuario debe haber «dado su consentimiento» a la colocación de «cookies», muestra que el consentimiento del usuario ya no puede presumirse y debe resultar del comportamiento activo de este último. Por último, el consentimiento activo está expresamente previsto en la actualidad en el RGPD, [97] cuyo artículo 4, punto 11, exige una manifestación de voluntad que adopte la forma, concretamente, de una «clara acción afirmativa» y cuyo considerando 32 excluye expresamente que pueda haber consentimiento en caso de «silencio, [...] casillas ya marcadas o [...] inacción».

El Tribunal de Justicia declaró por lo tanto que el consentimiento no se presta de manera válida cuando el almacenamiento de información o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de Internet se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento. Añadió que el hecho de que ese

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

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

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

97 *Ibidem*.

usuario active el botón de participación en el juego con fines promocionales de que se trata no basta para considerar que el usuario ha dado de manera válida su consentimiento para la colocación de «cookies».

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

En tercer término, el Tribunal de Justicia señaló que el artículo 5, apartado 3, de la Directiva 2002/58 exige que el usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos. Pues bien, una información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa. A este respecto, el Tribunal de Justicia consideró que el tiempo durante el cual las «cookies» estarán activas y la posibilidad o imposibilidad de que terceros tengan acceso a ellas forman parte de la información clara y completa que el proveedor de servicios debe facilitar al usuario de un sitio de Internet.

5. Tratamiento de datos personales en las redes sociales en línea

Sentencia de 4 de julio de 2023 (Gran Sala), Meta Platforms y otros (Condiciones generales del servicio de una red social) (C-252/21, EU:C:2023:537)

La sociedad Meta Platforms es propietaria de la red social en línea «Facebook», gratuita para usuarios privados. El modelo de negocio de esta red social se basa en la financiación mediante la publicidad en línea, que se realiza a medida para sus usuarios individuales. Este tipo de publicidad tiene como fundamento técnico el establecimiento automatizado de perfiles detallados de los usuarios de la red y de los servicios en línea ofrecidos a nivel del grupo. Así pues, para poder utilizar dicha red social, los usuarios deben aceptar, en el momento de registrarse, las condiciones generales establecidas por Meta Platforms, que remiten a las políticas de utilización de los datos y de las «cookies» establecidas por dicha sociedad. En virtud de estas últimas, además de los datos que estos usuarios proporcionan directamente en el momento de su registro, Meta Platforms recoge también datos relativos a las actividades de dichos usuarios dentro y fuera de la red social y los relaciona con las cuentas de Facebook de los usuarios de que se trata. En cuanto a estos últimos datos, también denominados «datos “off” Facebook», se trata, por una parte, de los datos relativos a la consulta de páginas de Internet y de aplicaciones de terceros y, por otra parte, de los datos relativos a la

utilización de otros servicios en línea pertenecientes al grupo Meta (entre ellos, Instagram y WhatsApp). La visión global de los datos así recogidos permite extraer conclusiones detalladas sobre las preferencias e intereses de estos mismos usuarios.

Mediante resolución de 6 de febrero de 2019, el Bundeskartellamt (Autoridad Federal de Defensa de la Competencia, Alemania) prohibió a Meta Platforms, por un lado, supeditar, en las condiciones generales vigentes en ese momento, el uso de la red social Facebook por usuarios privados residentes en Alemania al tratamiento de sus datos «off» Facebook y, por otro lado, proceder, sin su consentimiento, al tratamiento de dichos datos. Además, la Autoridad Federal de Defensa de la Competencia le obligó a adaptar esas condiciones generales de modo que se desprendiera claramente de ellas que dichos datos no serían recogidos, puestos en relación con las cuentas de usuarios de Facebook y utilizados sin el consentimiento de los usuarios afectados. Por último, la citada autoridad subrayó que tal consentimiento no era válido cuando constituía un requisito para la utilización de la red social. Motivó su decisión por el hecho de que el tratamiento de los datos en cuestión, que no era conforme con el RGPD, constituía una explotación abusiva de la posición dominante de Meta Platforms en el mercado de las redes sociales en línea.

Meta Platforms recurrió esa resolución ante el Oberlandesgericht Düsseldorf (Tribunal Superior Regional de lo Civil y Penal de Düsseldorf, Alemania). Al albergar dudas, entre otros, sobre la interpretación y la aplicación de ciertas disposiciones del RGPD, el Oberlandesgericht Düsseldorf (Tribunal Superior Regional de lo Civil y Penal de Düsseldorf) planteó una petición de decisión prejudicial al Tribunal de Justicia.

Mediante su sentencia, el Tribunal de Justicia, constituido en Gran Sala, aporta precisiones sobre la posibilidad del tratamiento, por parte de un operador de una red social, de datos personales «sensibles» de sus usuarios, sobre las condiciones de licitud del tratamiento de datos efectuado por tal operador y sobre la validez del consentimiento, prestado por esos usuarios para tal tratamiento, a una empresa en posición dominante en el mercado nacional de las redes sociales en línea.

Por lo que respecta al tratamiento de categorías especiales de datos personales, [98] el Tribunal de Justicia estima que, en el supuesto de que un usuario de una red social en línea consulte sitios de Internet o aplicaciones en relación con una o con varias de estas categorías y, en su caso, introduzca datos en ellos registrándose o efectuando pedidos en línea, el tratamiento de datos personales por parte del operador de esa red social en línea [99] debe considerarse como un «tratamiento de categorías especiales de datos personales», con arreglo al artículo 9, apartado 1, del RGPD, cuando dicho tratamiento

[98] Contempladas en el artículo 9, apartado 1, del RGPD. Esta disposición establece que «quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.»

[99] Este tratamiento consiste en la recogida, mediante interfaces integradas, «cookies» o tecnologías de almacenamiento similares, de los datos procedentes de la consulta de esos sitios y aplicaciones, así como de los datos introducidos por el usuario, en la puesta en relación del conjunto de esos datos con la cuenta de la red social de este y en la utilización de dichos datos por ese operador.

de datos permita revelar información comprendida en alguna de esas categorías especiales, con independencia de que tal información afecte a un usuario de esa red o a cualquier otra persona física. Dicho tratamiento de datos está, en principio, prohibido, sin perjuicio de determinadas excepciones. [100]

A este último respecto, el Tribunal de Justicia precisa que, cuando un usuario de una red social en línea consulta sitios de Internet o aplicaciones en relación con una o con varias de dichas categorías especiales de datos, no hace manifiestamente públicos [101] los datos relativos a dicha consulta recogidos por el operador de esa red social en línea a través de «cookies» o de tecnologías de almacenamiento similares. Por otra parte, cuando introduce datos en esos sitios de Internet o aplicaciones o activa botones de selección integrados en ellos, como son los botones «me gusta» o «compartir» o los botones que permiten al usuario identificarse en esos sitios o aplicaciones utilizando los identificadores de conexión vinculados a su cuenta de usuario de la red social, su número de teléfono o su dirección de correo electrónico, tal usuario solo hace manifiestamente públicos los datos así introducidos o resultantes de la activación de esos botones en el supuesto de que haya manifestado explícitamente su opción previa, en su caso sobre la base de una configuración individual efectuada con pleno conocimiento de causa, de que los datos que le conciernen resulten accesibles públicamente a un número ilimitado de personas.

En lo que atañe más en general a los requisitos de licitud de un tratamiento de datos personales, el Tribunal de Justicia recuerda que, en virtud del RGPD, el tratamiento de datos personales solo será lícito si el interesado dio su consentimiento para uno o varios fines específicos. [102] A falta de tal consentimiento, o cuando este no se haya prestado de forma libre, específica, informada e inequívoca, tal tratamiento está, no obstante, justificado cuando cumple alguno de los requisitos de necesidad, [103] que deben interpretarse restrictivamente. Pues bien, el tratamiento de datos personales de sus usuarios efectuado por un operador de una red social en línea solo puede considerarse necesario para la ejecución del contrato en el que esos usuarios son partes si dicho tratamiento es objetivamente indispensable para conseguir un fin que forme parte

---

[100] Contempladas el artículo 9, apartado 2, del RGPD. Esta disposición enuncia lo siguiente: «el apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; […]

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

[…]».

[101] En el sentido del artículo 9, apartado 2, letra e), del RGPD.

[102] A tenor del artículo 6, apartado 1, párrafo primero, letra a), del RGPD.

[103] Mencionados en el artículo 6, apartado 1, párrafo primero, letras b) a f), del RGPD. En virtud de estas disposiciones, el tratamiento solo es lícito si es necesario, entre otras cosas, para la ejecución de un contrato en el que el interesado sea parte [artículo 6, apartado 1, párrafo primero, letra b), del RGPD], para el cumplimiento de una obligación legal aplicable al responsable del tratamiento [artículo 6, apartado 1, párrafo primero, letra c), del RGPD] o para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero [artículo 6, apartado 1, párrafo primero, letra f), del RGPD].

integrante de la prestación contractual destinada a esos mismos usuarios, de manera que el objeto principal del contrato no podría alcanzarse sin ese tratamiento.

Además, según el Tribunal de Justicia, el tratamiento de datos personales en cuestión solo puede considerarse necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero si dicho operador ha indicado a los usuarios de los que se han obtenido los datos un interés legítimo perseguido por el tratamiento de estos, si el referido tratamiento se lleva a cabo dentro de los límites de lo estrictamente necesario para la satisfacción de ese interés legítimo y si de una ponderación de los intereses en conflicto se desprende, habida cuenta de todas las circunstancias pertinentes, que los intereses o las libertades y los derechos fundamentales de esos usuarios no prevalecen sobre el citado interés legítimo del responsable del tratamiento o de un tercero. Ahora bien, el Tribunal de Justicia considera en particular que, a falta de consentimiento por parte de dichos usuarios, los intereses y los derechos fundamentales de estos prevalecen sobre el interés del operador de una red social en línea en la personalización de la publicidad mediante la que él financia su actividad.

Por último, el Tribunal de Justicia precisa que el tratamiento de datos de que se trata está justificado cuando sea efectivamente necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, en virtud de una disposición del Derecho de la Unión o del Derecho del Estado miembro de que se trate, cuando esta base jurídica responda a un objetivo de interés público y sea proporcionada al objetivo legítimo perseguido y cuando ese tratamiento se lleve a cabo sin sobrepasar los límites de lo estrictamente necesario.

Por lo que respecta a la validez del consentimiento de los usuarios afectados al tratamiento de sus datos en virtud del RGPD, el Tribunal de Justicia considera que el hecho de que el operador de una red social en línea ocupe una posición dominante en el mercado de las redes sociales en línea no impide, como tal, que los usuarios de tal red puedan prestar válidamente su consentimiento al tratamiento de sus datos personales efectuado por ese operador. No obstante, dado que puede afectar a la libertad de elección de esos usuarios y crear un desequilibrio claro entre estos y dicho operador, tal posición constituye un elemento relevante para determinar si el consentimiento ha sido efectivamente prestado válidamente y, en especial, libremente, lo que incumbe probar a dicho operador. [104]

En particular, los usuarios de la red social en cuestión deben disponer de la libertad de negarse individualmente, en el marco del proceso contractual, a dar su consentimiento a operaciones particulares de tratamiento de datos que no sean necesarias para la ejecución del contrato, sin estar no obstante obligados a renunciar íntegramente a la utilización de dicha red social en línea, lo que implica que se ofrezca a dichos usuarios,

[104] En virtud del artículo 7, apartado 1, del RGPD.

en su caso a cambio de una remuneración adecuada, una alternativa equivalente no acompañada de tales operaciones de tratamiento de datos. Además, debe poder darse un consentimiento independiente para el tratamiento de los datos «off» Facebook.

VI. Autoridades nacionales de control

1. Alcance de la exigencia de independencia

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

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

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

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

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 que corresponde a dichas autoridades de 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, por tanto, la tutela del Estado ejercida sobre las autoridades nacionales de control no es compatible con la exigencia de independencia.

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

En su recurso, la Comisión solicitó al Tribunal de Justicia que declarase que la República de Austria había incumplido las obligaciones que le incumbían en virtud del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 al no haber adoptado todas las medidas necesarias para que la normativa vigente en Austria cumpliera el requisito de independencia por lo que se refiere a la Datenschutzkommission (Comisión de protección de datos, Austria), 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 requisito de independencia de la autoridad de control, establecido por la Directiva 95/46, el Estado miembro que establece un marco normativo en virtud del cual el administrador de dicha autoridad es un funcionario del Estado sometido a supervisión jerárquica, su secretaría está integrada en la estructura orgánica del Gobierno nacional y el Jefe del Gobierno nacional tiene un derecho incondicional a informarse de todos los aspectos de la gestión de dicha autoridad.

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. Asimismo, habida cuenta del papel de guardianas del derecho a la intimidad que asumen las autoridades de control, sus decisiones y, por tanto, ellas mismas, deben estar por encima de toda sospecha de parcialidad.

El Tribunal de Justicia precisó que, para poder cumplir el requisito de independencia establecido en el citado artículo de la Directiva 95/46, no es necesario que la autoridad nacional de control disponga de una línea presupuestaria autónoma similar a la contemplada en el artículo 43, apartado 3, del Reglamento n.º 45/2001. En efecto, los Estados miembros no están obligados a reproducir en su normativa nacional disposiciones análogas a las del capítulo V del Reglamento n.º 45/2001 con el fin de garantizar la total independencia de su autoridad o autoridades de control y, por tanto, pueden establecer que, desde el punto de vista del Derecho presupuestario, la autoridad de control dependa de un Ministerio determinado. No obstante, la atribución de los medios humanos y materiales que necesita tal autoridad de control no debe impedir que ejerza sus funciones «con total independencia», en el sentido del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46.

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

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

El Tribunal de Justicia declaró que incumple las obligaciones que le incumben en virtud de la Directiva 95/46 un Estado miembro que pone fin antes de tiempo al mandato de la autoridad de control de la protección de los datos personales.

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.

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 tal terminación anticipada que planearía sobre esa autoridad durante todo su mandato

podría generar una forma de «obediencia» de esta al poder político incompatible con la citada exigencia 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.

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)

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

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

Por lo que respecta al Derecho nacional aplicable, el Tribunal de Justicia declaró que el artículo 4, apartado 1, letra a), de la Directiva 95/46 permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que este ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento. Para determinar si así ocurre, el órgano jurisdiccional remitente puede tener en cuenta, por un lado, el hecho de que la actividad del responsable de dicho tratamiento, en cuyo marco este tiene lugar, consiste en la gestión de sitios de Internet de anuncios de inmuebles situados en el territorio de dicho Estado miembro y redactados en la lengua de ese Estado y que, en consecuencia, se dirige principalmente, incluso íntegramente, a dicho Estado miembro. El órgano jurisdiccional remitente puede tener en cuenta igualmente, por otro lado, el hecho de que ese responsable dispone de un representante en el referido Estado miembro que se encarga de cobrar los créditos 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.

Por lo que se refiere a la competencia y a las facultades de la autoridad de control que entiende de las denuncias, de conformidad con el artículo 28, apartado 4, de la Directiva 95/46, el Tribunal de Justicia consideró que dicha autoridad puede examinar tales denuncias sea cual sea el Derecho aplicable, e incluso antes de saber cuál es el Derecho nacional aplicable al tratamiento de los datos de que se trate. 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, le corresponde instar, en ejecución de la obligación de cooperación que se establece en el artículo 28, apartado 6, de la citada Directiva, a la autoridad de control de ese otro Estado miembro a declarar una eventual infracción de ese Derecho y a imponer sanciones si este lo permite, basándose, en su caso, en la información que ella le haya remitido.

3. Facultades de las autoridades nacionales de control

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

En ese asunto (véase también la sección IV, titulada «Transferencia de 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, 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 de la capacidad de comparecer en juicio.

En lo que atañe a la facultad de controlar las transferencias de datos personales a terceros países, el Tribunal de Justicia declaró que del artículo 28, apartados 1 y 6, de la Directiva 95/46 resulta ciertamente 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 tercer país.

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

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

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

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

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

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

El 11 de septiembre de 2015, el presidente de la Commission belge de la protection de la vie privée (Comisión de protección de la vida privada, Bélgica; en lo sucesivo, «CPVP») ejercitó ante el Nederlandstalige rechtbank van eerste aanleg Brussel (Tribunal de Primera Instancia Neerlandófono de Bruselas, Bélgica) una acción de cesación contra Facebook Ireland, Facebook Inc. y Facebook Belgium, que tenía por objeto poner fin a infracciones de la legislación en materia de protección de datos supuestamente cometidas por Facebook. Estas infracciones consistían, en particular, en la recogida y utilización de información sobre los hábitos de navegación de los internautas belgas, poseedores o no de una cuenta Facebook, mediante diferentes tecnologías, como «cookies», complementos sociales [105] o píxeles.

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

El 2 de marzo de 2018, Facebook Ireland, Facebook Inc. y Facebook Belgium interpusieron recurso de apelación contra esa sentencia ante el Hof van beroep te Brussel (Tribunal de Apelación de Bruselas, Bélgica), que es el órgano jurisdiccional remitente en el presente asunto. Ante este órgano jurisdiccional, la Autorité belge de protection des données (Autoridad de Protección de Datos, Bélgica; en lo sucesivo, «APD») ha actuado como sucesor legal del presidente de la CPVP. El órgano jurisdiccional remitente se ha declarado únicamente competente para conocer del recurso de apelación interpuesto por Facebook Belgium.

El órgano jurisdiccional remitente albergaba dudas acerca de los efectos de la aplicación del mecanismo de «ventanilla única» previsto por el RGPD [106] en las competencias de la APD y, más concretamente, se preguntaba si, con respecto a los hechos posteriores a la entrada en vigor del RGPD, a saber, el 25 de mayo de 2018, la APD puede ejercitar acciones judiciales contra Facebook Belgium, dado que Facebook Ireland ha sido identificada como la responsable del tratamiento de los datos en cuestión. En efecto, desde esta fecha y, en particular, en aplicación del principio de «ventanilla única» establecido por el RGPD, el Comisario irlandés de protección de datos es el único competente para ejercitar una acción de cesación, bajo el control de los órganos jurisdiccionales irlandeses.

---

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

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

En su sentencia, dictada por la Gran Sala, el Tribunal de Justicia precisa los poderes de las autoridades nacionales de control en el marco del RGPD. De este modo, declara, en particular, que, en determinadas condiciones, este Reglamento autoriza a una autoridad de control de un Estado miembro a ejercer su facultad de poner en conocimiento de los órganos jurisdiccionales de ese Estado miembro cualquier supuesta infracción de RGPD y de iniciar o ejercitar acciones judiciales con respecto a un tratamiento de datos transfronterizo, [107] aunque no sea la autoridad de control principal en lo referente a ese tratamiento.

En primer lugar, el Tribunal de Justicia precisa las condiciones en las que una autoridad nacional de control, que no tiene la condición de autoridad principal con respecto a un tratamiento transfronterizo, debe ejercer su facultad de poner en conocimiento de los órganos jurisdiccionales de un Estado miembro cualquier supuesta infracción del RGPD y, si procede, iniciar o ejercitar acciones judiciales para garantizar la aplicación de este Reglamento. Así, por una parte, el RGPD debe conferir a dicha autoridad de control competencia para adoptar una decisión en la que se declare que dicho tratamiento incumple las normas que contiene ese Reglamento y, por otra parte, esa facultad debe ejercerse respetando los procedimientos de cooperación y de coherencia establecidos por dicho Reglamento. [108]

En efecto, en el caso de los tratamientos transfronterizos, el RGPD establece el mecanismo de «ventanilla única», [109] basado en un reparto de competencias entre una «autoridad de control principal» y las demás autoridades de control interesadas. Este mecanismo exige una cooperación estrecha, leal y efectiva entre estas autoridades, para garantizar una protección coherente y homogénea de las normas relativas a la protección de datos personales y preservar así su efecto útil. El RGPD establece a este respecto la competencia de principio de la autoridad de control principal para adoptar una decisión en la que se declare que un tratamiento transfronterizo incumple las normas establecidas en dicho Reglamento, [110] mientras que la competencia de las demás autoridades nacionales de control para adoptar tal decisión, incluso con carácter provisional, constituye la excepción. [111] No obstante, en el ejercicio de sus competencias, la autoridad de control principal no puede prescindir de un diálogo indispensable y de una cooperación leal y efectiva con las demás autoridades de control interesadas. Por ello, en el marco de esta cooperación, la autoridad de control principal no puede pasar por alto los criterios de las demás autoridades de control interesadas, y toda objeción pertinente y motivada formulada por una de estas últimas autoridades tiene por efecto bloquear, al menos temporalmente, la adopción del proyecto de decisión de la autoridad de control principal.

---

[107] En el sentido del artículo 4, punto 23, del RGPD.

[108] Establecidos en los artículos 56 y 60 del RGPD.

[109] Artículo 56, apartado 1, del RGPD.

[110] Artículo 60 apartado 7, RGPD.

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

El Tribunal de Justicia precisa, además, que el hecho de que una autoridad de control de un Estado miembro que no sea la autoridad de control principal con respecto a un tratamiento de datos transfronterizo solo pueda ejercer la facultad de poner en conocimiento de los órganos jurisdiccionales de ese Estado cualquier supuesta infracción del RGPD y de iniciar o ejercitar acciones judiciales respetando las reglas de reparto de las competencias decisorias entre la autoridad de control principal y las demás autoridades de control [112] es conforme con los artículos 7, 8 y 47 de la Carta, que garantizan al interesado, respectivamente, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva.

En segundo lugar, el Tribunal de Justicia declara que, en caso de tratamiento de datos transfronterizo, el ejercicio de la facultad de una autoridad de control de un Estado miembro, distinta de la autoridad de control principal, de iniciar o ejercitar acciones judiciales [113] no exige que el responsable o encargado del tratamiento transfronterizo de datos personales contra el que se ejercite dicha acción disponga de un establecimiento principal u otro establecimiento en el territorio de dicho Estado miembro. Sin embargo, el ejercicio de esta facultad debe estar comprendido en el ámbito de aplicación territorial del RGPD, [114] lo que supone que el responsable o el encargado del tratamiento transfronterizo disponga de un establecimiento en el territorio de la Unión.

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

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

---

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

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

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

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

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

Sentencia de 16 de enero de 2024 (Gran Sala), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

En este asunto (véase también la sección II.1., titulada «Ámbito de aplicación de la normativa general»), el Tribunal de Justicia señala que las disposiciones del RGPD relativas a la competencia de las autoridades de control nacionales y al derecho de reclamación [115] no requieren la adopción de medidas nacionales de aplicación y son lo suficientemente claras, precisas e incondicionales como para tener efecto directo. De ello se deduce que, si bien el RGPD reconoce un margen de apreciación a los Estados miembros en cuanto al número de autoridades de control que deben establecerse, [116] fija el alcance de sus competencias para vigilar la aplicación de dicho Reglamento. Así, en el supuesto de que un Estado miembro opte por crear una única autoridad de control, esta estará necesariamente dotada de todas las competencias previstas por ese Reglamento. Cualquier otra interpretación menoscabaría el efecto útil de esas disposiciones y podría debilitar el efecto útil de las demás disposiciones del RGPD que pueden verse afectadas por una reclamación.

[115] Respectivamente, los artículos 55, apartado 1, y 77, apartado 1, del RGPD.
[116] Con arreglo al artículo 51, apartado 1, del RGPD.

En relación con la circunstancia de que las disposiciones nacionales de rango constitucional excluyen la posibilidad de que una autoridad de control dependiente del poder ejecutivo supervise la aplicación del RGPD por un órgano que forma parte del poder legislativo, el Tribunal de Justicia destaca que, precisamente dentro del respeto de la estructura constitucional de los Estados miembros, el RGPD se limita a exigir a estos últimos que establezcan al menos una autoridad de control, ofreciéndoles al mismo tiempo la posibilidad de establecer varias. De este modo, el Reglamento reconoce a cada Estado miembro un margen de apreciación que le permite establecer tantas autoridades de control como lo requieran, en particular, las exigencias relativas a su estructura constitucional.

Asimismo, la invocación por un Estado miembro de disposiciones de Derecho nacional no puede afectar a la unidad y a la eficacia del Derecho de la Unión. Así, los efectos que se asocian al principio de primacía del Derecho de la Unión se imponen a todos los órganos de un Estado miembro, sin que las disposiciones internas, incluidas las de rango constitucional, puedan oponerse a ello.

Cuando un Estado miembro ha optado por establecer una única autoridad de control, este no puede invocar disposiciones de Derecho nacional, aunque sean de rango constitucional, para excluir de la vigilancia de dicha autoridad los tratamientos de datos personales comprendidos en el ámbito de aplicación del RGPD.

4. Requisitos para la imposición de multas administrativas

Sentencia de 5 de diciembre de 2023 (Gran Sala), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

En este asunto (véanse también las secciones II.3., II.5. y II.6., tituladas «Concepto de “tratamiento de datos personales”», «Concepto de “responsable del tratamiento de datos personales”» y «Concepto de “corresponsable del tratamiento”»), el Tribunal de Justicia declara que, en virtud del artículo 83 del RGPD, solo puede imponerse una multa administrativa a un responsable del tratamiento si se demuestra que ha cometido de forma intencionada o negligente una infracción de las normas contenidas en dicho Reglamento. [117]

A este respecto, precisa que el legislador de la Unión no ha dejado a los Estados miembros un margen de apreciación en lo que respecta a los requisitos materiales que debe respetar una autoridad de control cuando decide imponer una multa administrativa a un responsable del tratamiento en virtud de dicha disposición. El hecho de que el RGPD conceda a los Estados miembros la posibilidad de establecer

[117] Infracción contemplada en el artículo 83, apartados 4 a 6.

excepciones en relación con las autoridades y organismos públicos establecidos en su territorio, [118] así como requisitos relativos al procedimiento que deben seguir las autoridades de control para imponer una multa administrativa, [119] no significa en modo alguno que también estén facultados para establecer tales requisitos materiales.

Por lo que respecta a estos requisitos, el Tribunal de Justicia señala que entre los elementos enumerados en el RGPD para que la autoridad de control pueda imponer al responsable del tratamiento una multa administrativa figura «la intencionalidad o negligencia en la infracción». [120] En cambio, entre estos elementos no se menciona posibilidad alguna de exigir la responsabilidad del responsable del tratamiento cuando no exista una conducta culpable por su parte. Por lo tanto, solo las infracciones de las disposiciones del RGPD cometidas por el responsable del tratamiento de forma intencionada o negligente pueden dar lugar a que se le imponga una multa administrativa con arreglo al artículo 83 de dicho Reglamento.

El Tribunal de Justicia añade que esta interpretación se ve corroborada por la estructura general y la finalidad del RGPD. En este contexto, precisa que la existencia de un sistema de sanciones en virtud del RGPD que permita imponer, cuando las circunstancias específicas de cada caso lo justifiquen, una multa administrativa crea un incentivo para que los responsables y encargados del tratamiento cumplan el Reglamento y que, por su efecto disuasorio, las multas administrativas contribuyen a reforzar la protección de los interesados. Sin embargo, el legislador de la Unión no consideró necesario prever la imposición de multas administrativas cuando no exista culpabilidad. Toda vez que el RGPD tiene por objeto un nivel de protección tanto equivalente como homogéneo y que, a tal fin, debe aplicarse de manera coherente en toda la Unión, sería contrario a esta finalidad permitir a los Estados miembros establecer un régimen de esta índole para la imposición de una multa.

Además, el Tribunal de Justicia concluye que tal multa puede imponerse a un responsable del tratamiento en relación con las operaciones de tratamiento de datos personales efectuadas por un encargado del tratamiento por cuenta de este, salvo si, en el marco de esas operaciones, dicho encargado ha efectuado tratamientos para sus propios fines o ha tratado esos datos de manera incompatible con el marco o las modalidades del tratamiento tal como hayan sido determinados por el responsable del tratamiento, o de manera que no pueda considerarse razonablemente que dicho responsable hubiera dado su consentimiento. En este supuesto, debe considerarse que el encargado del tratamiento es responsable de tal tratamiento.

---

[118] En virtud del artículo 83, apartado 7, del RGPD, que establece que «[…] cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro».

[119] De conformidad con el artículo 83, apartado 8, del RGPD, interpretado a la luz de su considerando 129.

[120] Artículo 83, apartado 2, letra b), del RGPD.

Sentencia de 5 de diciembre de 2023 (Gran Sala), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE (en lo sucesivo, «DW») es una sociedad inmobiliaria que posee de forma indirecta, mediante participaciones en diferentes sociedades, numerosos locales comerciales y viviendas. En el marco de su actividad mercantil, lleva a cabo el tratamiento de datos personales de los arrendatarios de esos inmuebles.

A raíz de dos inspecciones realizadas en 2017 y 2019, la Berliner Beauftragte für den Datenschutz (Autoridad Competente de Berlín para la Protección de Datos, Alemania) constató que DW había cometido varias infracciones del RGPD. Mediante decisión de 30 de octubre de 2019, esta autoridad de control le impuso por esa razón una serie de multas administrativas.

DW interpuso recurso contra esta decisión ante el Landgericht Berlin (Tribunal Regional de lo Civil y Penal de Berlín, Alemania), que archivó el procedimiento. Dicho tribunal señaló que, en virtud de la ley alemana, [121] solo puede constatarse una infracción administrativa con respecto a una persona física y no con respecto a una persona jurídica. Además, en el supuesto de que se genere la responsabilidad de una persona jurídica, solo se le puede imputar la actuación de los miembros de sus órganos o de sus representantes. La Staatsanwaltschaft Berlin (Fiscalía de Berlín, Alemania) interpuso un recurso contra esta resolución ante el Kammergericht Berlin (Tribunal Superior Regional de lo Civil y Penal de Berlín, Alemania). En este contexto, dicho órgano jurisdiccional planteó al Tribunal de Justicia una petición de decisión prejudicial sobre la interpretación del RGPD.

En su sentencia, el Tribunal de Justicia, constituido en Gran Sala, se pronuncia sobre los requisitos de imposición de multas administrativas con arreglo al RGPD. En primer lugar, examina la cuestión de si los Estados miembros pueden supeditar la imposición de una multa administrativa a una persona jurídica al requisito de que la infracción de dicho Reglamento se impute previamente a una persona física concreta. En segundo lugar, también trata la cuestión, al igual que la sentencia Nacionalinis visuomenės sveikatos centras (véase *supra*) de si la infracción sancionada de las disposiciones del RGPD debe cometerse de forma intencionada o negligente.

Por lo que respecta a la imposición de una multa administrativa en virtud del RGPD a una persona jurídica, el Tribunal de Justicia señala, para empezar, que los principios, prohibiciones y obligaciones previstos en el RGPD se dirigen, en particular, a los «responsables del tratamiento», cuya responsabilidad se extiende a cualquier tratamiento de datos personales realizado por ellos mismos o por su cuenta. Es esa responsabilidad la que constituye, cuando se infringen las disposiciones del RGPD, el fundamento de la imposición de una multa administrativa al responsable del

[121] Gesetz über Ordnungswidrigkeiten (Ley de Infracciones Administrativas), de 24 de mayo de 1968 (BGBl. 1968 I, p. 481), en la versión de la Comunicación de 19 de febrero de 1987 (BGBl. 1987 I, p. 602), en su versión modificada por la Ley de 19 de junio de 2020 (BGBl. 2020 I, p. 1350).

tratamiento con arreglo al artículo 83 de dicho Reglamento. Sin embargo, el legislador de la Unión no ha establecido, a efectos de la determinación de tal responsabilidad, una distinción entre las personas físicas y las personas jurídicas, ya que esta responsabilidad está sujeta únicamente al requisito de que estas, solas o conjuntamente con otras, determinen los fines y los medios del tratamiento de datos personales. [122] Por tanto, en principio, toda persona que cumpla este requisito será responsable, en particular, de cualquier infracción del RGPD, cometida por ella misma o en su nombre. Ello implica, por una parte, que las personas jurídicas son responsables no solo de las infracciones cometidas por sus representantes, directores o gestores, sino también por cualquier otra persona que actúe en el ámbito de la actividad empresarial de esas personas jurídicas y en su nombre. Por otra parte, las multas administrativas previstas en el RGPD en caso de que se produzcan tales infracciones deben poder imponerse directamente a personas jurídicas cuando estas puedan ser calificadas de responsables del tratamiento.

A continuación, el Tribunal de Justicia observa que ninguna disposición del RGPD permite considerar que la imposición de una multa administrativa a una persona jurídica como responsable del tratamiento esté sujeta a la constatación previa de que esa infracción ha sido cometida por una persona física concreta. Además, el legislador de la Unión no ha dejado a los Estados miembros un margen de apreciación a este respecto. El hecho de que el RGPD conceda a estos la posibilidad de establecer requisitos relativos al procedimiento que deben seguir las autoridades de control para imponer una multa administrativa [123] no significa en modo alguno que también estén facultados para establecer requisitos materiales adicionales a los fijados en el RGPD.

En este contexto, el Tribunal de Justicia precisa que permitir a los Estados miembros exigir, de manera unilateral y como condición necesaria para la imposición de una multa administrativa con arreglo al artículo 83 del RGPD a un responsable del tratamiento que es una persona jurídica, que la infracción en cuestión sea imputada o imputable, con carácter previo, a una persona física concreta sería contrario a la finalidad del RGPD. Además, tal exigencia adicional podría, en definitiva, debilitar la efectividad y el efecto disuasorio de las multas administrativas impuestas a personas jurídicas como responsables del tratamiento.

Por último, el Tribunal de Justicia subraya que el concepto de «empresa», en el sentido de los artículos 101 TFUE y 102 TFUE, [124] no tiene incidencia sobre si puede imponerse una multa administrativa en virtud del RGPD a un responsable del tratamiento que es una persona jurídica y en qué condiciones y solo es pertinente para determinar el importe de tal multa.

[122] Conforme al artículo 4, punto 7, del RGPD.

[123] Como se desprende de los artículos 58, apartado 4, y 83, apartado 8, del RGPD, interpretados a la luz de su considerando 129.

[124] Al que se remite el considerando 150 del RGPD.

Así pues, el Tribunal de Justicia concluye que el RGPD [125] se opone a una normativa nacional en virtud de la cual solo puede imponerse una multa administrativa a una persona jurídica en su condición de responsable del tratamiento por una infracción del referido Reglamento [126] si dicha infracción ha sido imputada previamente a una persona física concreta.

Por lo que respecta a si los Estados miembros pueden prever la imposición de una multa administrativa aun cuando la infracción sancionada no se haya cometido de forma intencionada o negligente, el Tribunal de Justicia recuerda, para empezar, que los requisitos materiales que una autoridad de control debe respetar cuando impone tal multa a un responsable del tratamiento pertenecen únicamente al ámbito del Derecho de la Unión y que los Estados miembros no disponen de ningún margen de maniobra a este respecto. Siguiendo un razonamiento idéntico al adoptado en la sentencia Nacionalinis visuomenės sveikatos centras antes citada, el Tribunal de Justicia declara que, en virtud del artículo 83 del RGPD, solo puede imponerse una multa administrativa si se demuestra que el responsable del tratamiento, que es a la vez una persona jurídica y una empresa, ha cometido, de forma intencionada o negligente, una infracción de las normas contenidas en dicho Reglamento.

5. Articulación de las competencias de las autoridades nacionales de control con las competencias de las restantes autoridades nacionales

Sentencia de 4 de julio de 2023 (Gran Sala), Meta Platforms y otros (Condiciones generales del servicio de una red social) (C-252/21, EU:C:2023:537)

En este asunto (véase asimismo la sección V.5., titulada «Tratamiento de datos personales en las redes sociales en línea»), al pronunciarse sobre la competencia de una autoridad de defensa de la competencia para constatar la falta de conformidad con el RGPD de un tratamiento de datos personales, el Tribunal de Justicia señala que, sin perjuicio del cumplimiento de su obligación de cooperación leal [127] con las autoridades de control de la protección de datos, tal autoridad puede concluir, en el marco del examen de un abuso de posición dominante por parte de una empresa, [128] que las condiciones generales del servicio fijadas por dicha empresa en materia de tratamiento de los datos personales y la aplicación de esas condiciones no son conformes con el citado Reglamento, cuando esa conclusión sea necesaria para declarar la existencia de ese abuso. No obstante, cuando una autoridad de defensa de la competencia señala una infracción del RGPD en el marco de la declaración de un abuso de posición dominante, no suplanta a las autoridades de control.

---

125 Artículos 58, apartado 2, letra i), y 83, apartados 1 a 6, del RGPD.
126 Contemplada en el artículo 83, apartados 4 a 6, del RGPD.
127 Consagrada en el artículo 4 TUE, apartado 3.
128 En el sentido del artículo 102 TFUE.

Así pues, habida cuenta del principio de cooperación leal, cuando las autoridades de defensa de la competencia se ven obligadas, en el ejercicio de sus competencias, a examinar la conformidad con las disposiciones del RGPD de una actividad de una empresa, deben ponerse de acuerdo y cooperar lealmente con las autoridades de control nacionales interesadas o con la autoridad de control principal. Todas estas autoridades están entonces obligadas a respetar sus respectivos poderes y competencias, de modo que se observen las obligaciones derivadas del RGPD y los objetivos de este y quede preservado su efecto útil. De ello se deduce que cuando, en el examen destinado a comprobar la existencia de un abuso de posición dominante por parte de una empresa, una autoridad de defensa de la competencia considera necesario examinar la conformidad de una actividad de dicha empresa con las disposiciones del RGPD, dicha autoridad debe comprobar si esa actividad o una actividad similar ya ha sido objeto de una decisión por parte de la autoridad de control nacional competente o por parte de la autoridad de control principal, o incluso por parte del Tribunal de Justicia. Si es así, la autoridad de defensa de la competencia no puede apartarse de ella, aunque conserva su libertad para deducir sus propias conclusiones desde el punto de vista de la aplicación del Derecho de la competencia.

Cuando albergue dudas sobre el alcance de la apreciación efectuada por la autoridad nacional de control competente o por la autoridad de control principal, o cuando la actividad en cuestión o una actividad similar sean, al mismo tiempo, objeto de examen por parte de esas autoridades, o incluso cuando considere, en ausencia de investigación de tales autoridades, que una actividad de una empresa no es conforme con las disposiciones del RGPD, la autoridad de defensa de la competencia debe consultar a esas autoridades y solicitar su cooperación, con el fin de disipar sus dudas o de determinar si, antes de iniciar su propia apreciación, no procede esperar a la adopción de una decisión por parte de la autoridad de control interesada. Si no plantean objeciones ni responden en un plazo razonable, la autoridad nacional de defensa de la competencia puede proseguir su propia investigación.

TRIBUNAL DE JUSTICIA
DE LA UNIÓN EUROPEA

Dirección de Investigación y Documentación

Julio 2024