Asunto C-60/22

Resumen de la petición de decisión prejudicial con arreglo al artículo 98, apartado 1, del Reglamento de Procedimiento del Tribunal de Justicia

Fecha de presentación:

1 de febrero de 2022

Órgano jurisdiccional remitente:

Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania)

Fecha de la resolución de remisión:

27 de enero de 2022

Parte demandante:

UZ

Parte demandada:

Bundesrepublik Deutschland (República Federal de Alemania)

Objeto del procedimiento principal

Protección de datos — Reglamento 2016/679 (Reglamento General de Protección de Datos) — Artículo 5, apartado 2 — Responsabilidad proactiva — Artículos 17, apartado 1, letra d), y 18, apartado 1, letra b) — Legalidad del tratamiento — Derecho de supresión y limitación — Utilización de los datos tratados

Objeto y fundamento jurídico de la petición de decisión prejudicial

Interpretación del Derecho de la Unión, artículo 267 TFUE

Cuestiones prejudiciales

1) ¿Implica la ausencia total o parcial de responsabilidad proactiva de un responsable del tratamiento en el sentido del artículo 5 del 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 (Reglamento general de protección de datos; en lo sucesivo, «RGPD»), por ejemplo, por la ausencia total o parcial de un registro de actividades de tratamiento con arreglo al artículo 30 del RGPD o por falta de un acuerdo sobre un procedimiento conjunto con arreglo al artículo 26 del RGPD, la ilicitud del tratamiento a efectos de los artículos 17, apartado 1, letra d), y 18, apartado 1, letra b), del RGPD, de modo que asiste al interesado un derecho de supresión o limitación?

2) En caso de respuesta afirmativa a la primera cuestión: ¿Implica la existencia de un derecho de supresión o limitación que los datos tratados no deban ser tenidos en cuenta en un procedimiento judicial? ¿Es así, al menos, cuando el interesado se ha opuesto a la utilización de los datos en el procedimiento judicial?

3) En caso de respuesta negativa a la primera cuestión: ¿Implica la infracción de los artículos 5, 30 o 26 del RGPD por parte del responsable del tratamiento que, a efectos de la utilización judicial del tratamiento de datos, un órgano jurisdiccional nacional solo puede tener en cuenta los datos si el interesado ha dado su consentimiento expreso al tratamiento?

Disposiciones del Derecho de la Unión invocadas

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 (Reglamento General de Protección de Datos) (DO 2016, L 119, p. 1); considerando 82 y artículos 5, 9, 17, 18, 26, 30 y 94

Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional (DO 2013, L 180, p. 60); considerando 52

Carta de los Derechos Fundamentales de la Unión Europea, artículos 7 y 8

Disposiciones de Derecho nacional invocadas

Bundesdatenschutzgesetz (Ley federal de protección de datos; en lo sucesivo, «BDSG») (BGBl. I, p. 2097), artículo 43, apartado 3

Breve exposición de los hechos y del procedimiento principal

1 El demandante impugna una decisión desestimatoria del Bundesamt für Migration und Flüchtlinge (Organismo Federal de Migración y Refugiados) y solicita el reconocimiento de la condición de refugiado con arreglo al artículo 3 de la Asylgesetz (Ley de asilo; en lo sucesivo, «AsylG»). La decisión de la demandada

se basa en el denominado expediente electrónico federal MARIS, que se transmite al tribunal, en particular, en el caso de un procedimiento conjunto con arreglo al artículo 26, por medio del Elektronisches Gerichts- und Verwaltungspostfach (Buzón Electrónico de Comunicación Judicial y Administrativa; en lo sucesivo, «EGVP»). Respecto a las cuestiones relativas a la transmisión íntegra de expedientes, se hace remisión a las cuestiones prejudiciales ya planteadas al Tribunal de Justicia (asunto C-564/21).

2 Existen dudas acerca de si el llamado «expediente electrónico MARIS» de la demandada constituye un registro de actividades de tratamiento, parcial o completo, en el sentido del artículo 30 del RGPD. No existe ningún acuerdo ni regulación legal a efectos del artículo 26 del RGPD respecto al procedimiento de transmisión electrónica de expedientes y a la determinación del responsable del tratamiento en dicho procedimiento. El órgano jurisdiccional remitente requirió la correspondiente documentación en el curso del procedimiento. Sin embargo, la demandada denegó su presentación alegando, en particular, que respecto al EGVP no existe acuerdo alguno con arreglo al artículo 26 del RGPD.

Breve exposición de la fundamentación de la petición de decisión prejudicial

3 Se plantea la cuestión, al menos en caso de ilicitud (formal) del tratamiento de los datos personales del demandante por la demandada, de cómo ha de proceder el tribunal con dichos datos, ya que, de conformidad con la Directiva 2013/32, el RGPD es aplicable al procedimiento de asilo con arreglo al Derecho nacional. Ni la AsylG ni la Verwaltungsgerichtsordnung (Ley de la jurisdicción contencioso-administrativa) dicen nada al respecto.

4 De acuerdo con el considerando 52 de la Directiva 2013/32, el tratamiento de los datos personales en el procedimiento de asilo en los Estados miembros con arreglo a dicha Directiva se somete a la 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. La Directiva 95/46 fue derogada por el artículo 94, apartado 1, del RGPD con efectos a partir del 25 de mayo de 2018. No obstante, de conformidad con el artículo 94, apartado 2, del RGPD, las referencias a la derogada Directiva 95/46 se entenderán hechas a este Reglamento. Por lo tanto, el RGPD es plenamente aplicable al procedimiento de reconocimiento de la protección internacional.

5 Ya la Directiva 95/46 preveía la documentación de los tratamientos automatizados: la llamada «notificación» con arreglo al artículo 18 de la Directiva. El contenido de la notificación de conformidad con el artículo 19 de la Directiva 95/46 se correspondía esencialmente con el actual artículo 30 del RGPD, si bien la nueva disposición hace referencia a todas las formas de tratamiento, incluidos los ficheros.

6 Durante la vigencia de la Directiva 95/46, la demandada disponía de un rudimentario registro de tratamientos como notificación a efectos de la Directiva 95/46 (artículo 4e de la BDSG, versión antigua) respecto al expediente electrónico MARIS. Dicho registro de tratamientos (notificación) no contenía ninguna disposición específica sobre el tratamiento de categorías especiales de datos personales en el sentido del artículo 9 del RGPD (artículo 8 de la Directiva 95/46). Cabe considerar que actualmente tampoco existen tales disposiciones especiales relativas al tratamiento de los datos a que se refieren los artículos 9 y 10 del RGPD, ya que los datos sobre salud y religión, así como los antecedentes penales, se recogen con carácter general en el expediente electrónico MARIS como «documentos normales». No parece que haya una protección especial de la seguridad de datos, aunque sí existe un registro de acceso. En todo caso, el expediente de un solicitante de asilo puede ser consultado por cualquier delegación de la demandada en toda Alemania, como por la propia central.

7 Precisamente en relación con la gestión de los expedientes y su presentación ante los tribunales, el órgano jurisdiccional remitente alberga serias dudas sobre la conformidad de la actuación de la demandada con el artículo 5, apartado 1, del RGPD en relación con, por ejemplo, los artículos 26 y 30 de este Reglamento. Pese al requerimiento del tribunal, la demandada no presentó el registro de actividades de tratamiento. A este respecto, el tribunal tiene intención de tomar declaración al director de la entidad responsable, es decir, de la demandada, una vez haya recaído la resolución del Tribunal de Justicia respecto a la responsabilidad proactiva de la demandada con arreglo al artículo 5, apartado 2, del RGPD.

8 No obstante, antes de que se produzca dicha declaración es preciso dilucidar si el incumplimiento de las obligaciones que impone el RGPD y la consiguiente ilicitud del tratamiento dan lugar a una sanción, como la supresión de los datos con arreglo al artículo 17, apartado 1, letra d), del RGPD, o a una limitación del tratamiento en virtud del artículo 18, apartado 1, letra b), del RGPD, al menos cuando así lo solicita el interesado, en este caso el demandante. De lo contrario, el tribunal se vería obligado a participar en un tratamiento de datos ilícito dentro del procedimiento judicial, y la Administración podría infringir impunemente el RGPD en cualquier ocasión.

9 En tal caso, solamente podría intervenir la autoridad de control con arreglo al artículo 58 del RGPD, pero el Derecho nacional no prevé la posibilidad de imponer una sanción al Organismo Federal de Migración y Refugiados. Con arreglo al artículo 43, apartado 3, de la BDSG, basado en el artículo 83, apartado 7, del RGPD, no se imponen sanciones pecuniarias a las autoridades y demás organismos públicos. No existiría ningún incentivo para que la Administración actuase conforme a la ley. Esto tendría como consecuencia que se incumpliesen las disposiciones de la Directiva 2013/32 tanto como las del propio RGPD.

10 El Tribunal de Justicia ya ha declarado que en el momento del tratamiento ha de existir ya una notificación (actualmente, un registro de actividades de tratamiento)

completa, pero no antes (sentencia de 9 de noviembre de 2011, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartados 95 y siguientes). En el presente caso, los datos personales del demandante ya fueron objeto de tratamiento por la demandada desde el momento en que solicitó asilo (el 7 de mayo de 2019). Por lo tanto, al menos conforme a la jurisprudencia del Tribunal de Justicia, desde ese momento debió haber existido un registro de actividades de tratamiento en relación con el expediente MARIS (y, por ende, respecto al expediente de asilo del demandante). Sin embargo, no fue así.

11 Lo que ha de suceder en tal situación no ha sido resuelto hasta la fecha por el Tribunal de Justicia, ya sea con arreglo a la Directiva 95/46 o al RGPD. Si se tiene en cuenta que, para demostrar el cumplimiento del RGPD, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad (considerando 82 del RGPD), se plantea la cuestión de qué consecuencias ha de tener el incumplimiento de esta obligación por parte de la entidad responsable, pues impide cumplir también con la responsabilidad proactiva con arreglo al artículo 5 del RGPD.

12 Si bien el artículo 83, apartado 5, letra a), del RGPD establece que la infracción de la responsabilidad proactiva prevista en el artículo 5 del mismo Reglamento se sancionará con multas de hasta 20 000 000 euros, como ya se ha señalado, el artículo 43, apartado 3, de la BSDG excluye de esta posibilidad a las autoridades federales. No obstante, con arreglo al artículo 17, apartado 1, letra d), del RGPD, los datos personales que hayan sido tratados ilícitamente deben ser suprimidos, al menos a instancia del interesado.

13 A juicio del órgano jurisdiccional remitente, la ausencia total o parcial del registro de actividades de tratamiento, cuando menos a la luz del artículo 5 del RGPD, implica la ilicitud «formal» del tratamiento. Así pues, se plantea la cuestión de si en tal caso no ha lugar a la supresión o, al menos, al bloqueo de los datos, como sanción por la infracción del artículo 5 del RGPD en relación con el artículo 30 del mismo Reglamento. De lo contrario, en defecto de toda sanción posible, podría frustrarse la aplicación efectiva del RGPD.

14 En cualquier caso, que conozca el tribunal, la República Francesa, por ejemplo, durante la vigencia de los artículos 18 y siguientes de la Directiva 95/46, disponía en su Derecho nacional que en el procedimiento judicial estaba estrictamente prohibido por ley utilizar los datos personales que no se hubiesen recogido en una notificación de la autoridad responsable a la autoridad de control (CNIL), ya que era ilícita la utilización de los datos en defecto de documentación. Por lo tanto, en tal situación al menos existía una sanción consistente en no poder tratar y utilizar los datos ante un tribunal. Bajo la vigencia del RGPD, parece que también en Portugal y en otros Estados miembros la ausencia de un registro de actividades de tratamiento implica la prohibición de utilizar los datos, posibilidad que en la República Federal de Alemania no existía con la transposición de la Directiva 95/46 y tampoco existe bajo la vigencia del RGPD. Antes bien, aquí se sentaron las bases para una «tolerancia» de la omisión de la notificación.

15 La transmisión electrónica del expediente y de los escritos de la demandada constituye también un tratamiento de datos en el sentido del artículo 4, punto 2, del RGPD, en el que se han de observar los principios establecidos en el artículo 5 de este. Por lo tanto, también a este respecto resulta dudosa la licitud formal del tratamiento de datos mediante la transmisión del expediente electrónico federal y de los escritos de la demandada mediante el correspondiente canal. Tampoco en este caso existe un registro de actividades de tratamiento ni está regulada la corresponsabilidad. Es cierto que existe un Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach, de 24 de noviembre de 2017 (BGBl. I, p. 3803, modificado por el artículo 6 de la Ley de 5 de octubre de 2021, BGBl. I, p. 4607) (Reglamento sobre el marco de requisitos técnicos del tráfico jurídico electrónico y el Buzón Electrónico Especial de la Administración). En él se regula la transmisión de documentos electrónicos a los tribunales de los Länder (Estados federados) y del Bund (Federación). El Reglamento autoriza a los organismos públicos establecidos por las máximas autoridades de la Federación o por los gobiernos regionales dentro de sus ámbitos territoriales a comprobar la identidad de las autoridades o las personas jurídicas de Derecho público a fin de concederles el acceso al Buzón Electrónico Especial de la Administración (el llamado «BeBPo»). Las máximas autoridades de la Federación o varios Gobiernos regionales también pueden designar conjuntamente un organismo público para sus ámbitos territoriales. No se establece cuál ha de ser este organismo. En último término probablemente se trate del llamado Bund-Länder-Arbeitsgruppe der Justizministerien [Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) Arbeitsgruppe IT-Standards in der Justiz) [Grupo de Trabajo de los Ministerios de Justicia Federación-Estados federados [Comisión Federación-Estados federados para la tecnología de la información en la Justicia, Grupo de Trabajo sobre normas IT en la Justicia]. No se conoce ni está documentado qué autoridad o autoridades son responsables del servicio de registros del EGVP o del BeBPo, o siquiera de la necesaria infraestructura de servidores.

16 Tampoco existe la correspondiente normativa legal o de otro tipo entre los tribunales y la Administración, como exige el artículo 26 del RGPD, que regule las responsabilidades. Incluso en los Estados federados que han elegido en sus ordenamientos jurídicos el modelo del procedimiento conjunto no se dispone de la correspondiente transposición en materia de protección de datos. En el reglamento vigente en Hesse se establece incluso que el buzón electrónico se utilice exclusivamente en los servidores del «centro de datos» de la justicia, es decir, en la Hessische Zentrale für Datenverarbeitung (Central de Tratamiento de Datos de Hesse, HZD). Pero la HZD no está integrada en el sistema judicial y, a lo sumo, se puede considerar como encargada del tratamiento en su condición de intermediario, con arreglo al artículo 28 del RGPD.

17 Solo se conoce que, en la práctica, el Landesamt für Datensicherheit in Nordrhein-Westfalen (Organismo de Seguridad de Datos del Land de Renania del Norte-Westfalia], como «intermediario», es competente para la administración y funcionamiento del servidor de registros interregional S.A.F.E. Según parece, el

ID de SAFE es invariable y se asigna una sola vez (véase SAFE: http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). Además, los buzones del EGVP se designan con un número de identificación único (el llamado «ID Govello»). Según la información de que dispone el órgano jurisdiccional remitente, estos ID se registran en un servicio de registros gestionado por Renania del Norte-Westfalia (IT-NRW). No está establecido a quién le corresponde la asignación efectiva del ID Govello en el marco de esta colaboración entre la Federación y los Estados federados.

18 Tampoco se conoce el fundamento del EGVP en cuanto a la protección de datos. Respecto a la existencia de un acuerdo con arreglo al artículo 26 del RGPD, la demandada se ha negado a dar ninguna explicación y a presentar acuerdo alguno. Tampoco está claro si, dado que no se han asignado responsabilidades en virtud de dicha disposición, es posible una transmisión lícita por medio del Buzón Electrónico Especial de la Administración, incluso desde el punto de vista de la seguridad de datos, pues ningún documento está cifrado en el canal de transmisión.

19 A juicio del órgano jurisdiccional remitente no es determinante si, con arreglo al actual Derecho positivo, es obligatorio el uso de un cifrado de extremo a extremo para el Buzón Electrónico Especial de la Abogacía. Al menos en Hesse, entre el intermediario (la HZD) y cada tribunal (incluido el Verwaltungsgericht Wiesbaden [Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania]) no se hace cifrado alguno de los mensajes que se transmiten.

20 En cualquier caso, esto no es relevante en el presente asunto, pues el procedimiento principal versa sobre un envío por correo electrónico. Sobre el servicio por internet Gmail, el Tribunal de Justicia ha declarado que no se trata de un servicio de comunicaciones, ya que no incluye el acceso a Internet, no consiste en su totalidad o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas y no constituye, por tanto, un «servicio de comunicaciones electrónicas» (sentencia de 13 de junio de 2019, Google, C-193/18, EU:C:2019:498). Por consiguiente, el EGVP no es un servicio sometido a la Directiva 2002/58/CE (artículo 2, apartado 4, del RGPD), de modo que está sujeto al RGPD, lo que significa que el EGVP y los procedimientos asociados deben estar recogidos en un registro de actividades de tratamiento, y las respectivas responsabilidades relativas a un procedimiento con múltiples responsables se han de acordar con arreglo al artículo 26 del RGPD. Nada de ello se cumple en el presente caso, por lo que existen dudas acerca de la licitud de la trasmisión de los datos.

21 El EGVP es un procedimiento de las administraciones judiciales, que pertenecen al segundo poder, el Ejecutivo, y a la demandada, que también es parte de este poder. En consecuencia, a juicio del tribunal, la demandada está obligada a velar por que el procedimiento electrónico de transmisión de datos relativos a los escritos y expedientes se lleve a cabo de conformidad con el RGPD.

22 Así pues, al órgano jurisdiccional remitente se le plantea la cuestión, dentro de la actividad jurisdiccional, de cómo se ha de proceder respecto a los datos proporcionados mediante el sistema EGVP a través del llamado «Buzón de la Administración», cuando el procedimiento aplicado por el EGVP y el correspondiente tratamiento de datos, en sí mismos, no son conformes con el RGPD.

23 El órgano jurisdiccional remitente debe respetar y atenerse al RGPD en su actividad jurisdiccional.

24 Dicho órgano jurisdiccional no tiene ningún control sobre la legalidad del tratamiento de datos que lleva a cabo la administración judicial, pues esta es ajena a la «actividad jurisdiccional» y pertenece al segundo poder, el Ejecutivo. No obstante, el órgano jurisdiccional remitente debe observar y hacer cumplir el Derecho de la Unión. Cuando las partes del procedimiento lo infringen, no debería ser admisible que el tribunal utilizase los datos, pues, de lo contrario, estaría participando en un tratamiento de datos ilícito. En el presente caso, esto se ve agravado por el hecho de que la demandada, según se desprende de la correspondencia mantenida hasta la fecha, probablemente esté incumpliendo (de forma consciente) el Derecho de la Unión.

25 Tampoco concurre un supuesto en que la utilización judicial esté justificada en virtud del artículo 17, apartado 3, letra e), del RGPD, para la formulación, el ejercicio o la defensa de reclamaciones por parte de la demandada. Si bien los datos de la demandada sirven para el cumplimiento de una obligación legal que requiere el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplica al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público, o en el ejercicio de poderes públicos conferidos al responsable, de conformidad con el artículo 17, apartado 3, letra b), del RGPD, con ello también se estaría legalizando de forma permanente una actuación contraria a la legislación sobre protección de datos.

26 Por lo tanto, las cuestiones prejudiciales planteadas adquieren especial relevancia cuando se trata de la aplicación del RGPD en el procedimiento judicial. Se vería menoscabado el objetivo formulado en el artículo 1, apartado 2, del RGPD, de proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

27 Al menos en caso de respuesta negativa a la primera cuestión prejudicial, debería ser necesaria la aquiescencia o, mejor aún, el consentimiento expreso del interesado (en este caso, del demandante) para la utilización de sus datos en el procedimiento judicial, a pesar de haber sido objeto de un tratamiento formalmente ilícito.

28 No obstante, la consecuencia de ello sería también que, si se denegase este consentimiento, el tribunal no podría tratar (utilizar) los datos tratados por la demandada y presentados por esta en forma de expediente electrónico MARIS.

Asimismo, esto implicaría que, hasta la subsanación de las deficiencias documentales, no habría ningún elemento en que fundamentar la resolución del asunto, y la decisión impugnada de la demandada habría de ser anulada en todos los casos. Mientras no se produjera dicha subsanación no sería posible resolver sobre la solicitud de asilo presentada.