

Asunto C-215/20

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:

19 de mayo de 2020

Órgano jurisdiccional remitente:

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

Fecha de la resolución de remisión:

13 de mayo de 2020

Parte demandante:

JV

Parte demandada:

Bundesrepublik Deutschland (República Federal de Alemania)

Objeto del procedimiento principal

Admisibilidad de la transferencia de los datos de los pasajeros aéreos

Objeto y fundamento jurídico de la petición de decisión prejudicial

Interpretación del Derecho de la Unión, artículo 267 TFUE

Cuestiones prejudiciales

- 1) La 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»), en virtud de la cual las empresas de transporte aéreo transfieren extensos registros de datos relativos a todos los pasajeros sin excepción a las Unidades de Información

sobre los Pasajeros establecidas por los Estados miembros, donde los datos se utilizan sin motivos en una comparación automatizada con las bases de datos y patrones y se conservan a continuación durante cinco años, ¿es, habida cuenta del objetivo perseguido por la Directiva PNR y de los requisitos de precisión y proporcionalidad, compatible con la Carta de los Derechos Fundamentales, y en particular con los artículos 7, 8 y 52 de esta?

2) En particular:

- a) ¿Es compatible con los artículos 7 y 8 de la Carta el artículo 3, punto 9, de la Directiva PNR, en relación con el anexo II de la misma Directiva, en la medida en que establece que se entenderán por «delitos graves» a efectos de la Directiva los delitos incluidos en su anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al Derecho nacional de un Estado miembro, desde la óptica de la exigencia de suficiente precisión y del requisito de proporcionalidad?
- b) ¿Son los datos del registro de nombres de los pasajeros que han de transferirse (en lo sucesivo, «datos del PNR»), en la medida en que exigen la transferencia de los nombres y apellidos (artículo 8, apartado 1, primera frase, en relación con anexo I, punto 4, de la Directiva PNR) y de la información sobre viajeros asiduos (artículo 8, apartado 1, primera frase, en relación con anexo I, punto 8, de la Directiva PNR) y exigen que se cumplimente un campo de texto libre con observaciones generales (artículo 8, apartado 1, primera frase, en relación con anexo I, punto 12, de la Directiva PNR), suficientemente precisos como para poder justificar una injerencia en los derechos consagrados en los artículos 7 y 8 de la Carta?
- c) ¿Es compatible con los artículos 7 y 8 de la Carta y con la finalidad de la Directiva PNR que se registren también, además de los datos de los pasajeros, datos de terceros, como de la agencia de viajes/del operador de viajes (anexo I, punto 9, de la Directiva PNR), de los acompañantes de menores (anexo I, punto 12, de la Directiva PNR) y de otros viajeros (anexo I, punto 17, de la Directiva PNR)?
- d) En la medida en que según la Directiva PNR son objeto de transferencia, tratamiento y almacenamiento los datos del PNR de menores, ¿es dicha Directiva compatible con los artículos 7, 8 y 24 de la Carta?
- e) A la luz del principio de minimización de datos, ¿es compatible con los artículos 8 y 52 de la Carta el artículo 8, apartado 2, de la Directiva PNR (en relación con el anexo I, punto 18, de la Directiva), según el cual las empresas de transporte aéreo transferirán datos API a las

Unidades de Información sobre los Pasajeros de los Estados miembros, aunque sean idénticos a los datos del PNR?

- f) ¿Constituye el artículo 6, apartado 4, de la Directiva PNR, como base jurídica para determinar los criterios de comparación de los registros de datos (es decir, los denominados «patrones»), un fundamento legítimo suficiente, previsto por la ley, a los efectos de los artículos 8, apartado 2, y 52 de la Carta, así como del artículo 16 TFUE, apartado 2?
 - g) ¿Está el artículo 12 de la Directiva PNR limitando la injerencia en los derechos consagrados en los artículos 7 y 8 de la Carta a lo estrictamente necesario, si los datos transferidos se conservan en las Unidades de Información sobre los Pasajeros de los Estados miembros durante un período de cinco años?
 - h) ¿Reduce la despersonalización prevista en el artículo 12, apartado 2, de la Directiva PNR los datos personales a lo que con arreglo a los artículos 8 y 52 de la Carta es lo necesario, si no se trata sino de una seudonimización que es reversible en cualquier momento?
 - i) ¿Deben interpretarse los artículos 7, 8 y 47 de la Carta en el sentido de que exigen que los pasajeros cuyos datos vuelvan a ser personalizados en el marco del tratamiento de los datos de los pasajeros (artículo 12, apartado 3, de la Directiva PNR) sean informados sobre dicho extremo, brindándoles así la posibilidad de una revisión judicial?
- 3) ¿Es compatible el artículo 11 de la Directiva PNR con los artículos 7 y 8 de la Carta en la medida en que permite la transferencia de datos del PNR a terceros países que no disponen de un nivel adecuado de protección de datos?
- 4) ¿Brinda el artículo 6, apartado 4, cuarta frase, de la Directiva PNR protección suficiente contra el tratamiento de categorías especiales de datos personales, a los efectos del artículo 9 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 (DO 2016, L 119, p. 1; en lo sucesivo, «RGPD»), y del artículo 10 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), si en el marco del campo de texto libre «observaciones generales» (anexo I, punto 12, de la

Directiva PNR) se puede comunicar, por ejemplo, la comida solicitada, que permite extraer conclusiones sobre dichas categorías especiales de datos personales?

- 5) ¿Es compatible con el artículo 13 del RGPD que la página web de las empresas de transporte aéreo simplemente remita a los pasajeros a la normativa nacional de transposición [en este caso, la Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 [Ley sobre tratamiento de los datos de pasajeros de transposición de la Directiva (UE) 2016/681], de 6 de junio de 2017, BGBl. I, p. 1484 (en lo sucesivo, «Fluggastdatengesetz» o «FlugDaG»)]?

Disposiciones del Derecho de la Unión invocadas

Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), artículos 7, 8, 24, 47 y 52

Art. 16 TFUE

Directiva PNR

Directiva 2016/680

RGPD

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 283, p. 31)

Disposiciones de Derecho nacional invocadas

FlugDaG

Breve exposición de los hechos y del procedimiento principal

- 1 El 10 de junio de 2017 entró en vigor la FlugDaG, que adapta el Derecho alemán a la Directiva PNR. Esta Directiva regula la transferencia de datos del PNR en vuelos desde los Estados miembros de la Unión Europea a terceros países y desde terceros países a los Estados miembros de la Unión, así como el tratamiento de dichos datos.
- 2 A tenor del artículo 1, apartado 2, de la Directiva PNR, esta persigue los fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves. El artículo 4 de la Directiva obliga a cada Estado miembro a establecer su Unidad de Información sobre los Pasajeros (en lo sucesivo, «UIP»),

responsable de recoger los datos del PNR de las compañías aéreas, almacenar y procesar esos datos y transferirlos a las autoridades competentes, así como de intercambiar tanto los datos del PNR como los resultados de su tratamiento. Con arreglo al artículo 8, en relación con el anexo I, de la Directiva PNR, los Estados miembros deben obligar a todas las compañías aéreas a transmitir un conjunto definido de datos del PNR a la UIP del Estado miembro en cuyo territorio aterrice o de cuyo territorio salga el vuelo. En virtud del artículo 9 de la Directiva PNR, los Estados miembros pueden solicitar y transmitir entre ellos los datos del PNR. En las condiciones previstas en el artículo 11 de la Directiva también es posible una transferencia de datos a terceros países. Con arreglo al artículo 12, apartado 2, de la Directiva, los datos conservados de los pasajeros que deban serlo durante un período de cinco años deberán ser «despersonalizados» al finalizar un plazo de seis meses, lo que implica que se enmascararán los datos que podrían servir para identificar directamente al pasajero. No obstante, es posible una nueva personalización de estos elementos de datos en las condiciones previstas en el artículo 12, apartado 3, de la Directiva. El artículo 6 de la Directiva regula el tratamiento de los datos, que debe efectuarse, en particular, mediante la comparación automatizada de los datos con bases de datos y criterios predeterminados (denominados «patrón» en la FlugDaG).

- 3 El 28 de abril de 2019 el demandante voló con la compañía aérea Lufthansa desde Fráncfort del Meno (Alemania) a Bogotá (Colombia) y el 7 de mayo de 2019 retornó a Fráncfort del Meno desde Río de Janeiro (Brasil). Para estos vuelos, el demandante pretende la supresión de los datos de los que disponga la demandada sobre él.

Breve exposición de los motivos de la petición de decisión prejudicial

- 4 La solución del litigio principal depende de si la Directiva PNR es total o parcialmente contraria a la Carta. En tal caso, la FlugDaG, como Ley de transposición, no sería aplicable, de modo que el tratamiento de datos controvertido sería inadmisibles y el demandante tendría derecho a la supresión de los datos.

Acercas de la primera cuestión: ¿Es la Directiva PNR es en su conjunto compatible con la Carta?

- 5 Los diferentes tratamientos de datos del PNR previstos por la Directiva del PNR y por la FlugDaG invaden el ámbito de protección del derecho fundamental al respeto de la vida privada garantizado en el artículo 7 de la Carta, pues dicho derecho se extiende a toda información sobre una persona física identificada o identificable (véase la sentencia de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 52), y por tanto también a la información relativa a las personas afectadas por el tratamiento de los datos del PNR a la que se refiere el anexo I de la Directiva PNR. Además, el artículo 8 de la Carta es también aplicable a los tratamientos de datos del PNR

contemplados por la Directiva PNR, porque constituyen tratamientos de datos de carácter personal en el sentido de dicho artículo y, en consecuencia, deben cumplir necesariamente los requisitos de protección de los datos previstos en él (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 123).

- 6 En efecto, como ya ha declarado el Tribunal de Justicia, la comunicación de datos personales a un tercero, como puede ser una autoridad pública, constituye una injerencia en el derecho fundamental consagrado en el artículo 7 de la Carta, cualquiera que sea la utilización posterior de la información comunicada. Lo mismo puede decirse de la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas. A este respecto, carece de relevancia que la información de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 124). Lo mismo sucede con el artículo 8 de la Carta en lo que respecta al tratamiento de datos de carácter personal (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 126).
- 7 Es cierto que los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 136). Los objetivos de interés general, entre los que figura la lucha contra los delitos de terrorismo y otros delitos graves, pueden justificar una limitación de estos derechos (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 149). No obstante, las injerencias en los derechos fundamentales deben ser apropiadas y necesarias para alcanzar dichos objetivos y no resultar desproporcionadas en el sentido estricto del término. Además, con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades de la Unión reconocidos por esta deberá ser establecida por la ley y respetar su contenido esencial. Dentro del respeto del principio de proporcionalidad, 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 (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 138).
- 8 Según jurisprudencia reiterada del Tribunal de Justicia, el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 46). En lo que respecta al derecho a la intimidad, la protección de este derecho fundamental exige, en cualquier caso, conforme a la jurisprudencia del Tribunal de Justicia, que las excepciones y restricciones a la protección de los datos personales se establezcan sin sobrepasar los límites de lo estrictamente necesario (sentencia de 8 de abril de

2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 52).

- 9 Para cumplir estos requisitos, la normativa que contenga la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas. Las personas cuyos datos hayan sido transferidos deberán disponer de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado. Esto es aplicable, en particular, a la protección de la categoría especial de los datos sensibles de carácter personal (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55).
- 10 Existen serias dudas sobre si la Directiva PNR cumple todos estos requisitos.
- 11 En virtud de lo dispuesto en la Directiva PNR, las empresas de transporte aéreo están obligadas a transferir, para cada vuelo concreto, los datos del PNR de todos los pasajeros sin excepción a las UIP de los Estados miembros, en las que dichos datos serán tratados de forma automatizada y conservados de forma duradera. A tal efecto no es necesario un motivo determinado, como podría ser, por ejemplo, la existencia de indicios concretos de un vínculo con el terrorismo internacional o con la delincuencia organizada. Ello conduce a que en breves períodos de tiempo se traten y almacenen cientos de billones de registros de datos. Por lo tanto, la «conservación de datos» de pasajeros afecta de un modo evidente a los derechos fundamentales de una gran parte del conjunto de la población europea.
- 12 Los datos del registro que deben transferirse, establecidos en el artículo 8, apartado 1, primera frase, de la Directiva PNR, en relación con el anexo I de esta, son muy extensos e incluyen, además del nombre, los apellidos y la dirección de los pasajeros, así como del desarrollo previsto del viaje, también información relativa a su equipaje, a sus acompañantes, todo tipo de información de pago, así como «observaciones generales» no definidas en detalle. Del conjunto de estos datos se pueden extraer conclusiones muy precisas sobre la vida privada y profesional de los interesados. En efecto, de los datos se desprende quién viajó en qué fecha en compañía de qué personas a qué lugar, qué medio de pago utilizó a tal fin y qué datos de contacto indicó, así como si la persona en cuestión viajó con mucho o poco equipaje. Se pueden obtener otros datos, cuyo alcance es totalmente opaco (véase *infra*), por medio del campo de texto libre «observaciones generales».
- 13 El órgano jurisdiccional remitente considera que el tratamiento y el almacenamiento de los datos del PNR son comparables a la conservación de datos

en el ámbito de las telecomunicaciones. Respecto de este último, el Tribunal de Justicia precisó que la injerencia que supone en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta resulta de gran magnitud y debe considerarse especialmente grave, pues un almacenamiento masivo y sin motivos de extensos registros de datos que permita extraer conclusiones sobre la vida privada y profesional de las personas afectadas puede generar en estas el sentimiento de que su vida privada es objeto de una vigilancia constante (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 37).

- 14 En su primera sentencia sobre la conservación de datos, el Tribunal de Justicia declaró que esta era contraria a los derechos fundamentales debido, en particular, a que deben mantenerse incluso datos de personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 58). Lo mismo sucede con el tratamiento y almacenamiento de los datos del PNR, lo que demuestra que lo dispuesto en la Directiva PNR excede de los límites de lo necesario para alcanzar los objetivos perseguidos por dicha Directiva y es, por tanto, desproporcionado en el sentido de la jurisprudencia del Tribunal de Justicia. A esto se suma que, a diferencia de los datos de tráfico de telecomunicaciones en el marco de la conservación de datos, los datos del PNR no solo se conservan sin motivos, sino que también son objeto de tratamiento posterior, es decir, son objeto de comparaciones automatizadas con bases de datos y con los denominados «patrones».

Acerca de la segunda cuestión, letra a): concepto de «delitos graves»

- 15 También resultan cuestionables la precisión y la proporcionalidad de la recopilación y del tratamiento de los datos del PNR en relación con las infracciones que con esta forma de proceder se pretende combatir. Los fines declarados de la Directiva PNR son la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de los delitos graves. En el artículo 3, punto 9, de la Directiva, los «delitos graves» son definidos como los delitos incluidos en el anexo II que son punibles con una pena privativa de libertad o un auto de internamiento de una duración máxima no inferior a tres años con arreglo al Derecho nacional de un Estado miembro. El anexo II de la Directiva PNR contiene una lista con veintiséis de los delitos a que se refiere el artículo 3, punto 9. Ahí se incluyen, por ejemplo, la corrupción (punto 6), el fraude (punto 7), los delitos informáticos/ciberdelincuencia (punto 9), así como los delitos contra el medio ambiente (punto 10).
- 16 De inicio, procede cuestionar la precisión de esas normas. Así, por ejemplo, el Derecho penal alemán no conoce un delito de «corrupción», sino que es un término superpuesto que designa un gran número de delitos. Lo mismo sucede con los conceptos de «fraude», de «delitos informáticos» y de «delitos contra el medio ambiente».

- 17 Esto y la referencia que el artículo 3, punto 9, de la Directiva PNR hace a las penas aplicables en cada Estado miembro conducen a incoherencias en la utilización de los datos del PNR en los diferentes Estados miembros de la Unión. En efecto, cada Estado miembro es libre de incluir o de no incluir determinados delitos como «delitos graves» en el sentido de la Directiva, sirviéndose para ello de la pena prevista en el código penal nacional.
- 18 También es dudoso, en lo que concierne al carácter proporcional de la normativa, la duración máxima no inferior a tres años de pena privativa de libertad, fijada en el artículo 3, punto 9, de la Directiva PNR. En el Derecho penal alemán esto comprende un conjunto enorme de infracciones cuya calificación como «delitos graves» parece muy discutible. Así, con arreglo al artículo 263 del Strafgesetzbuch (Código Penal alemán; en lo sucesivo, «StGB»), la pena máxima por un fraude no cualificado ya alcanza los cinco años de pena privativa de libertad. Lo mismo sucede, por ejemplo, con la receptación (artículo 259 del StGB), con el fraude informático (artículo 263a del StGB) o con la administración desleal (artículo 266 del StGB). Todas estas infracciones se pueden incluir en los actos punibles enumerados en el anexo II de la Directiva PNR (en particular, en el «fraude» a que se refiere el punto 6). Pues bien, tales infracciones forman parte de la «delincuencia cotidiana», que es tan frecuente, y pueden ser casos de menor gravedad. Si es así, su inclusión en la Directiva PNR es ajena a la prevención y el enjuiciamiento de los delitos graves.

Acerca de la segunda cuestión, letra b): precisión de los datos del PNR

- 19 Habida cuenta de que el Tribunal de Justicia exige que la normativa controvertida establezca reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 141), algunos de los datos del PNR que las empresas de transporte aéreo deben transferir a las UIP de los Estados miembros no son determinados de manera suficientemente precisa en el anexo I de la Directiva PNR.
- 20 No se aprecia con claridad qué debe entenderse por los «nombre(s) y apellido(s)» que deben transmitirse (anexo I, punto 4, de la Directiva PNR). Así se desprende de la adaptación alemana del Derecho interno en el artículo 2, puntos 1 y 9, de la FlugDaG, según los cuales deben comunicarse el apellido, el apellido de nacimiento, los nombres y un posible título de doctor, así como la mención de otros elementos de los nombres. En el lenguaje corriente, a la pregunta por nombres y apellidos no se responde indicando también el apellido de nacimiento. Así pues, no queda claro que este esté comprendido en la expresión «nombre(s) y apellido(s)» mencionada en el punto 4 del anexo I de la Directiva PNR. También resulta dudoso si un título académico debe considerarse un componente del nombre en el sentido de la Directiva.
- 21 Por lo que respecta a la transmisión y el tratamiento de la información sobre viajeros asiduos (anexo I, punto 8, de la Directiva PNR), existe asimismo una falta

de precisión en la normativa. No está claro, en particular, si esto se refiere a la mera participación en programas de recompensas para viajeros frecuentes o también a información específica sobre vuelos y reservas de la persona que participa en dicho programa.

- 22 La expresión «observaciones generales [incluida [...]]» que figura en el anexo I, punto 12, de la Directiva PNR está formulada de manera muy amplia y no resulta palpable. Como se desprende del término «incluida», se trata únicamente de una enumeración ilustrativa y no taxativa. Además, al rellenar este campo de texto libre, también podría comunicarse información carente de relación alguna con la finalidad de la transferencia de datos del PNR (véase, en este sentido, el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 160). Esta redacción también podría permitir, en particular, transmitir información que la Directiva PNR no pretende admitir, a saber, datos sensibles, que, según el considerando 15 de la Directiva, no deben recopilarse (véase también, a este respecto, la cuarta cuestión).

Acerca de la segunda cuestión, letra c): terceros afectados

- 23 Con arreglo al artículo 1, apartado 1, de la Directiva PNR, esta regula la transferencia por las compañías aéreas de datos del PNR de vuelos exteriores de la UE y el tratamiento de estos datos por los Estados miembros. Conforme al artículo 3, punto 4, de la Directiva, es pasajero toda persona, incluidos los pasajeros en tránsito o en conexión y exceptuados los miembros de la tripulación, transportada o que vaya a ser transportada a bordo de una aeronave con el consentimiento de la compañía aérea, lo cual se manifiesta en la inclusión de la persona en la lista de pasajeros. Sin embargo, en el anexo I de la Directiva PNR se mencionan varios datos que deben transferirse y que no se refieren a «pasajeros» así definidos, de modo que, a este respecto, las normas de la Directiva presentan una contradicción interna.
- 24 Así, es contrario al artículo 3, punto 4, de la Directiva PNR que el anexo I, punto 9, de dicha Directiva prevea la recopilación, en el marco del tratamiento de los datos del registro de nombres de los pasajeros, de información relativa a la agencia de viajes y al operador de viajes en dicha agencia. En virtud del punto 12 del anexo I de la Directiva, debe facilitarse en el marco del campo de texto libre «observaciones generales» especialmente información relativa a los acompañantes de los menores en el momento de la salida y a la llegada, así como a los agentes.
- 25 Es evidente que todos esos datos no están comprendidos en la categoría de «pasajeros» que define el artículo 3, punto 4, de la Directiva PNR. Aun así, dichos datos deben ser transferidos por las empresas de transporte aéreo a las UIP de los Estados miembros y almacenados por estas. A este respecto, el órgano jurisdiccional remitente considera que todas estas normas no se limitan a lo estrictamente necesario en el sentido de la jurisprudencia del Tribunal de Justicia (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 141). Además, para todos los terceros afectados se suscita la cuestión de cómo deben ser

informados del tratamiento de sus datos personales según lo previsto en el artículo 14 del RGPD.

- 26 Según el punto 17 del anexo I de la Directiva PNR, los datos del PNR de otros viajeros también deben transferirse y tratarse. Por lo que respecta a esos otros viajeros, ello conduce a un doble registro, pues ya se ven afectados, como pasajeros, por el tratamiento de los datos del registro de nombres de los pasajeros. Por lo tanto, aquí se incumple gravemente el principio de minimización de datos [véase el artículo 5, apartado 1, letra c), del RGPD].

Acerca de la segunda cuestión, letra d): menores

- 27 En virtud de la Directiva PNR, las empresas de transporte aéreo están obligadas a transferir sin excepción los datos del PNR de todos los pasajeros a las respectivas UIP de los Estados miembros, de modo que también se ven afectados los pasajeros menores de edad.
- 28 El tratamiento de los datos de menores puede efectuarse, por una parte, con el fin de actuar con carácter preventivo o represivo contra los menores (presuntamente) implicados en actos terroristas o en delitos graves y, por otra parte, por razones de protección de menores, como la detección o el enjuiciamiento del tráfico de menores. Estos dos objetivos distintos requieren regulaciones diferenciadas. Así lo ilustra el artículo 6 de la Directiva 2016/680, según el cual, en la medida de lo posible, procede establecer una distinción clara entre los datos personales de las distintas categorías de interesados. Entre las categorías que se diferenciarán están, en particular, las personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal en un futuro próximo [artículo 6, letra a), de la Directiva 2016/680] y las víctimas de una infracción penal o personas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal [artículo 6, letra c), de la Directiva 2016/680].
- 29 Pues bien, en la medida en que los datos se recopilen y traten a efectos de actuaciones represivas o preventivas contra menores, procede señalar que el enjuiciamiento penal con base en la información obtenida del tratamiento de los datos del registro de nombres de los pasajeros solo se podrá contemplar para adolescentes en edad penal. A este respecto, la Directiva PNR se excede de lo estrictamente necesario en la medida en que no contiene una limitación a los datos de los menores en edad penal.
- 30 Por lo que se refiere a la recopilación y al tratamiento de los datos del PNR con fines de protección de menores, debe tenerse en cuenta que los niños y los adolescentes tienen una necesidad particular de protección. Así lo ilustra el artículo 24 de la Carta, que les confiere derechos fundamentales de la Unión propios para su protección particular. Esta necesidad particular de protección se aplica también al tratamiento de sus datos personales. En la medida en que la recogida y el tratamiento de los datos del PNR de los pasajeros menores deba

servir a la prevención o al enjuiciamiento de crímenes dirigidos contra menores, las disposiciones de la Directiva PNR no parecen adecuadas a tal efecto. El tratamiento de los datos del PNR está enfocado a encontrar o identificar a personas sospechosas. A tal efecto, los datos del PNR son comparados de manera automatizada con bases de datos y patrones con el fin de detectar a personas sospechosas (véase artículo 6, apartado 2, de la Directiva PNR). Pues bien, en el contexto de la protección de los menores contra el tráfico de menores, los datos de los menores precisamente no son datos de sospechosos, sino, por el contrario, datos de quien necesita protección. Por lo tanto, también deberían ser tratados de modo diferente y precisamente no existirá la necesidad de realizar comparaciones con patrones. A este respecto, parece que la Directiva PNR no establece normas suficientemente matizadas en lo que se refiere al tratamiento de los datos del PNR de los pasajeros menores de edad.

Acerca de la segunda cuestión, letra e): datos API

- 31 El artículo 8, apartado 2, de la Directiva PNR establece que los Estados miembros adoptarán las medidas necesarias para garantizar que se envíen a las UIP también los datos de información anticipada sobre los pasajeros en el sentido del anexo I, punto 18, de la Directiva (datos API), incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada. A este respecto, existen numerosos solapamientos entre los datos API y los datos del PNR, que deben transferirse de todos modos, como los datos de la salida prevista (anexo I, punto 3, de la Directiva), los nombre(s) y apellido(s) (anexo I, punto 4, de la Directiva) o el itinerario completo del viaje (anexo I, punto 7, de la Directiva).
- 32 Este tratamiento duplicado de los datos de los pasajeros es contrario al principio de minimización de datos consagrado, entre otras, en la Directiva 2016/680. Este se deduce, en primer lugar, del artículo 4, apartado 1, letra c), de la Directiva 2016/680, que establece que los datos personales no deberán ser excesivos en relación con los fines para los que son tratados. El artículo 20, apartado 1, de la Directiva 2016/680 concreta este principio en el sentido de que los Estados miembros deben disponer que el responsable del tratamiento tome las medidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva. Además, el artículo 20, apartado 2, de la misma Directiva establece que solo deberán ser objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Acerca de la segunda cuestión, letra f): base jurídica de los patrones

- 33 Con arreglo al artículo 6, apartado 3, letra b), de la Directiva PNR, los datos transmitidos por las empresas de transporte aéreo a las UIP de los Estados

miembros deberán compararse con criterios predeterminados (los denominados patrones). El artículo 6, apartado 4, frases segunda y cuarta, de la Directiva PNR dispone que los criterios predeterminados deben ser orientados, proporcionados y específicos y que los criterios no se basarán 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. De conformidad con el artículo 6, apartado 4, tercera frase, de la Directiva PNR, el establecimiento de los patrones incumbe a la UIP de cada Estado miembro.

- 34 En consecuencia, toda la configuración de la comparación a partir de patrones queda plenamente en manos, en cuanto a su contenido, del poder ejecutivo de cada Estado miembro. Esto lleva necesariamente a que los Estados miembros de la Unión apliquen patrones diferentes y, por tanto, a que los pasajeros, según el destino del viaje, se vean sometidos a patrones diferentes que pueden conducir a resultados completamente diferentes.
- 35 Resulta dudoso que esto sea conforme con los artículos 8, apartado 2, y 52 de la Carta, así como con artículo 16 TFUE, apartado 2. Con arreglo al artículo 8, apartado 2, de la Carta, los datos de carácter personal se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Según el artículo 52, apartado 1, primera frase, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos en ella debe ser establecida por la ley. A tenor del artículo 16 TFUE, apartado 2, el Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.
- 36 Para justificar la injerencia en los derechos fundamentales de la Unión se requiere no solo la existencia de algún tipo de normativa, sino que además esta debe ser suficientemente precisa (véase la sentencia de 21 de diciembre de 2016, *AGET Iraklis*, C-201/15, EU:C:2016:972, apartado 99). El justiciable debe poder prever las consecuencias de la ley, entendiéndose que una normativa abierta debe aceptarse cuando una normativa más precisa no sea posible por el objeto de esta (sentencia de 20 de mayo de 2003, *Österreichischer Rundfunk* y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 77).
- 37 El artículo 6, apartado 4, de la Directiva PNR no cumple esos requisitos. En cuanto al artículo 6, apartado 4, segunda frase, de la Directiva, se trata de palabras vagas de contenido, indeterminadas, con las que se finge una concreción de los criterios que, en realidad, no existe. El artículo 6, apartado 4, tercera frase, de la Directiva deja íntegramente en manos de los distintos Estados miembros la decisión esencial y, por relevante, importante de qué datos deben emplearse para establecer criterios o, en su caso, patrones, a los efectos de la comparación automatizada. Pues bien, esto no es estrictamente necesario por razón del objeto

de la normativa. Al legislador europeo le habría sido perfectamente posible establecer determinados datos o criterios que se utilizarán o no en la preparación de los patrones. A este respecto, ni la criminalidad o el terrorismo que hay en los diferentes Estados miembros ni los criterios que permiten detectar a los sospechosos son distintos entre un Estado miembro y otro.

- 38 Como único mecanismo de control de la proporcionalidad de los patrones desarrollados por los Estados miembros se establece, en el artículo 6, apartado 7, de la Directiva PNR, en relación con el artículo 5 de esta, que el responsable de la protección de datos en la UIP tenga acceso a dichos patrones. Sin embargo, con arreglo al artículo 5, apartado 1, de la Directiva, el responsable de la protección de datos es designado y, por regla general, empleado por la propia UIP, de modo que, *a priori*, no queda garantizada su independencia (sobre la independencia de la oficina supervisora de protección de datos, véanse las sentencias de 9 de marzo de 2010, Comisión/Alemania, C-518/07, EU:C:2010:125, y de 16 de octubre de 2012, Comisión/Austria, C-614/10, EU:C:2012:631).

Acerca de la segunda cuestión, letra g): plazo de almacenamiento de los datos

- 39 Con arreglo al artículo 12, apartado 1, de la Directiva PNR, los datos del PNR se almacenan durante un período de cinco años. Según la segunda frase del considerando 25 de la Directiva, dada la naturaleza y la utilización de los datos del PNR, es necesario que se almacenen durante un período suficientemente largo. Sin embargo, no se explica por qué es necesario un período de almacenamiento de cinco años.
- 40 El órgano jurisdiccional remitente no logra apreciar por qué es necesario un período de almacenamiento tan largo. Después de que los pasajeros hayan sido objeto de evaluación antes de su llegada o salida programada del Estado miembro de que se trate con arreglo al artículo 6, apartado 4, primera frase, de la Directiva PNR, sin que se haya detectado nada llamativo, no existe ningún indicio objetivo que permita considerar que puedan tener una relación, ni siquiera indirecta, con delitos de terrorismo o delitos graves. Así pues, no existe un vínculo suficiente entre el almacenamiento de los datos y los objetivos perseguidos por la Directiva. Solo en el caso de indicios concretos de un peligro con origen en determinados pasajeros parece adecuado un almacenamiento duradero (véase el dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartados 204 y ss.). En cambio, la mera posibilidad teórica de que los datos en algún momento puedan ser relevantes en materia de seguridad no deberá bastar para justificar una profunda injerencia en los derechos fundamentales como es el almacenamiento de los datos personales durante años.
- 41 En el marco de la conservación de datos (otra forma de almacenamiento masivo y sin motivos de datos de carácter personal), el Tribunal de Justicia ya ha declarado que una directiva que establece un período de conservación de hasta 24 meses no limita la injerencia a lo estrictamente necesario (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:2014:238, apartado 63).

Si un período de 24 meses ya es demasiado largo en el caso de la conservación de datos, con mayor razón lo será un período de cinco años, como en el caso de autos.

Acerca de la segunda cuestión, letra h): despersonalización

- 42 Según el considerando 25 de la Directiva PNR, la denominada «despersonalización» tiene por finalidad garantizar un alto nivel de protección de datos. Eso parece pero que muy dudoso. La «despersonalización» de los datos, así llamada también en el artículo 12, apartado 2, de la Directiva, que debe producirse transcurridos seis meses, no altera en absoluto el carácter desproporcionado del período de almacenamiento.
- 43 Procede señalar, de inicio, que la denominación de «despersonalización» es ajena a la sistemática de la normativa y es engañosa. Se trata simplemente de una seudonimización de datos en el sentido del artículo 3, punto 5, de la Directiva 2016/680. Se distingue de la anonimización en que, a diferencia de esta, la opción de vincular los datos a una persona determinada no es imposibilitada de un modo permanente ni definitivo, sino que sigue siendo posible su nueva personalización (véase el artículo 12, apartado 3, de la Directiva PNR), es decir, puede restablecerse fácilmente un vínculo directo con la persona de que se trate. Por lo tanto, no se entiende por qué no se recurre al concepto de seudonimización, como en la Directiva 2016/680. Pues bien, debido a su carácter reversible, la seudonimización reduce considerablemente menos que una verdadera anonimización la intensidad de la injerencia en los derechos fundamentales.
- 44 También debe tenerse en cuenta el artículo 4, apartado 1, letra e), de la Directiva 2016/680. Según dicha disposición, los datos personales serán conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados. En el caso de lo que el artículo 12, apartado 2, de la Directiva PNR denomina despersonalización, la identificación del interesado sigue siendo posible durante todo el período de almacenamiento quinquenal, como demuestra el artículo 12, apartado 3, de la Directiva PNR, que regula la divulgación (o la recuperación de la divulgación) una vez transcurrido un período de seis meses. Pues bien, no se aprecia que ello sea indispensable para los fines de la Directiva PNR ni ha sido fundamentado en ese sentido por el legislador de la Unión.

Acerca de la segunda cuestión, letra i): información al interesado tras nueva personalización

- 45 No existe en la Directiva PNR una regulación que prevea que las personas afectadas deban ser informadas cuando sus datos, conservados por las UIP de los Estados miembros, sean de nuevo personalizados de conformidad con el artículo 12, apartado 3, de la Directiva. Únicamente se regula que la nueva personalización debe ser aprobada por una «autoridad judicial» o por otra autoridad nacional [artículo 12, apartado 3, letra b), de la Directiva].

- 46 El Tribunal de Justicia ya señaló, en su dictamen relativo al Acuerdo UE-Canadá, que, si bien el Acuerdo previsto establecía que los pasajeros aéreos debían ser informados en una página web del tratamiento general de sus datos en el marco de los controles de seguridad y de los controles en las fronteras, esa información general no les daba la posibilidad de saber si sus datos han sido utilizados, al margen de esos controles, por la autoridad competente (dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 223). El dictamen del Tribunal de Justicia continúa literalmente: «Así pues, en los supuestos [...] en los que concurren circunstancias que justifican tal utilización 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 del PNR de los pasajeros aéreos se comunican a otras autoridades públicas o a particulares» (dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 223).
- 47 El órgano jurisdiccional remitente considera que esta apreciación del Tribunal de Justicia es extrapolable a la Directiva PNR y opina, en consecuencia, que los afectados deben ser informados individualmente de la nueva personalización de sus datos. Si el Tribunal de Justicia considerase que la notificación inmediata a los interesados de la nueva personalización podría menoscabar excesivamente el objetivo perseguido de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de los delitos graves, el órgano jurisdiccional remitente considera que sería necesario informar a los interesados a más tardar en el momento en que ya no exista riesgo de comprometer el objetivo de la nueva personalización, por ejemplo, debido a la finalización de las medidas de investigación.
- 48 Asimismo, en virtud del artículo 47 de la Carta, el interesado tiene derecho a la revisión por un juez independiente e imparcial, establecido previamente por la ley, y no por una «autoridad judicial». En cambio, en el caso de autos se excluye toda vía de recurso.

Acerca de la tercera cuestión: transferencia a terceros países

- 49 Con arreglo al artículo 11, apartado 1, de la Directiva PNR, los datos del PNR y el resultado del tratamiento de dichos datos podrán transferirse caso por caso a un tercer país si se cumplen las condiciones establecidas en el artículo 13 de la Decisión marco 2008/977/JAI, la transmisión es necesaria para los fines de la Directiva, el tercer país acuerda transmitir los datos a otro tercer país únicamente si fuera estrictamente necesario para los fines de la Directiva y solo con la autorización expresa del Estado miembro, y se reúnen las condiciones establecidas en el artículo 9, apartado 2, de la Directiva.
- 50 El artículo 11, apartado 2, de la Directiva PNR contiene una excepción a esta exigencia al disponer que, no obstante lo dispuesto en el artículo 13, apartado 2, de la Decisión marco 2008/977/JAI (actualmente artículo 38 de la Directiva 2016/680), las transmisiones de datos del PNR a terceros países sin

consentimiento previo del Estado miembro del que fueron obtenidos se permitirán en circunstancias excepcionales y solamente si son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país y el consentimiento previo no puede obtenerse a su debido tiempo.

- 51 En la medida en que, mediante la transmisión a terceros países, las autoridades de dichos países obtienen acceso a los datos del PNR, todos los principios relativos a la utilización de esos datos, dirigidos a garantizar la proporcionalidad de las injerencias que implican en los derechos fundamentales y un nivel de protección adecuado de los datos personales, deben aplicarse también a los terceros países. A este respecto, el Tribunal de Justicia precisó, en su dictamen sobre el Acuerdo UE-Canadá, que solo puede efectuarse una transmisión de datos personales de la Unión a un país tercero si ese país garantiza un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión. Con ello se persigue la finalidad de evitar que el nivel de protección establecido en dicho Acuerdo pueda eludirse mediante la transmisión de datos de carácter personal a otros países y de garantizar la continuidad del nivel de protección que ofrece el Derecho de la Unión (dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 214). El Tribunal de Justicia dedujo de ahí que esa comunicación de datos personales requiere o bien un acuerdo entre la Unión y el país tercero de que se trate equivalente al Acuerdo UE-Canadá, o bien una decisión de la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46 (actualmente artículo 45, apartado 3, del RGPD), por la que se declare que el citado país tercero garantiza un nivel de protección adecuado con arreglo al Derecho de la Unión y que comprenda a las autoridades a las que se pretendan transferir los datos del PNR (dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 214).
- 52 El artículo 11 de la Directiva PNR burla estos requisitos. El artículo 11, apartado 1, letra a), de la Directiva se remite al artículo 13 de la Decisión marco 2008/977/JAI, derogada por la Directiva 2016/680. Las referencias a la Decisión marco se entenderán hechas a la Directiva 2016/680 (véase el artículo 59 de esta última Directiva). El artículo 13 de la Decisión marco 2008/977/JAI, derogada, se corresponde, en esencia, con los artículos 35 a 38 de la Directiva 2016/680.
- 53 De conformidad con el artículo 35, apartado 1, letra d), de la Directiva 2016/680, la transferencia de datos a un tercer Estado está supeditada a que la Comisión haya adoptado una decisión de adecuación con arreglo al artículo 36 de la Directiva o, a falta de tal decisión y de las garantías apropiadas de conformidad con el artículo 37, a que concurra una situación excepcional prevista en el artículo 38. En ese sentido, la remisión que hace el artículo 11, apartado 1, letra a), de la Directiva PNR al artículo 13 de la Decisión marco 2008/977/JAI y, por tanto, al artículo 35 de la Directiva 2016/680 no garantiza un nivel de protección adecuado de los datos en el tercer país, al permitir, mediante la remisión también al artículo 38 de la Directiva 2016/680, la transferencia de datos del PNR a terceros países, aun cuando no existan una decisión de adecuación ni garantías apropiadas. Esto se

debe, en particular, a que el concepto de situación excepcional en el sentido del artículo 38 de la Directiva 2016/680 se concibe de manera muy amplia. En efecto, esta disposición permite transferir datos del PNR a terceros países sin un nivel adecuado de protección de datos cuando sea necesario, en el caso concreto, para los fines del artículo 1, apartado 1, de la Directiva 2016/680 (la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención) o para el establecimiento, el ejercicio o la defensa de acciones legales en relación con los fines expuestos [véase el artículo 38, apartado 1, letras d) y e), de la Directiva 2016/680].

Acerca de la cuarta cuestión: solicitud de comida en el marco del campo de texto libre

- 54 Con arreglo al artículo 6, apartado 4, cuarta frase, de la Directiva PNR, los criterios con los que las UIP de los Estados miembros comparan de forma automatizada los datos del PNR 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.
- 55 Sin embargo, esta disposición solo contiene una declaración de intenciones, que es contrarrestada, en particular, por el anexo I, punto 12, de la Directiva PNR. En efecto, mediante el campo de texto libre «observaciones generales», que debe transmitirse a las UIP obligatoriamente, sin excepción, puede transmitírseles una variedad inabarcable de información que podrá ser utilizada por ellas, también datos especialmente sensibles. Así, por medio de dicho campo de texto libre puede comunicarse, por ejemplo, que un pasajero ha solicitado alimentación kósher o comida halal. Pues bien, esta información permite deducir las creencias religiosas del interesado, de modo que se trata de un dato especialmente sensible en el sentido antes mencionado.

Acerca de la quinta cuestión: información facilitada por las empresas de transporte aéreo

- 56 Con arreglo al artículo 13, apartado 3, de la Directiva PNR, la Directiva se entenderá sin perjuicio de la aplicabilidad de la Directiva 95/46 al tratamiento de datos personales por las compañías aéreas, en particular sus obligaciones de tomar las medidas técnicas y de organización adecuadas para proteger la seguridad y la confidencialidad de los datos personales. También el artículo 21, apartado 2, de la Directiva PNR aclara que esta se entiende sin perjuicio de la aplicabilidad de la Directiva 95/46 al tratamiento de datos personales por las compañías aéreas.
- 57 La Directiva 95/46 fue sustituida por el RGPD (véase el artículo 94, apartado 2, del Reglamento, según el cual las referencias a la Directiva 95/46 se entenderán hechas al RGPD).

- 58 Conforme al artículo 13 del RGPD, cuando los datos personales se obtengan del interesado se le deberá facilitar la información allí indicada. El concepto de «datos personales» se define en el artículo 4, punto 1, del mismo Reglamento. La recopilación por las empresas de transporte aéreo de los datos del PNR de los pasajeros y de terceros interesados constituye una obtención de datos personales en ese mismo sentido, de modo que, en el caso de autos, el artículo 13 del RGPD se aplica a las empresas de transporte aéreo.
- 59 El órgano jurisdiccional remitente estima que, habida cuenta de la gravedad ya expuesta de las injerencias en los derechos fundamentales que implica el tratamiento de los datos del PNR, deben aplicarse criterios estrictos en lo que respecta a las obligaciones de información.
- 60 En opinión del órgano jurisdiccional remitente, incumbe a las empresas de transporte aéreo informar a los interesados conforme a los artículos 13 y 14 del RGPD, pues en caso contrario existiría una laguna normativa incompatible con los artículos 7 y 8 de la Carta. En consecuencia, parece necesario que las empresas de transporte aéreo informen expresamente a los pasajeros de todos los datos del PNR recogidos por ellas, de la transmisión prevista a las UIP de los Estados miembros y del tratamiento posterior de los datos en dichas unidades, incluidos el período de almacenamiento quinquenal y sus derechos concretos en calidad de interesados. En efecto, sin esta información, los pasajeros afectados difícilmente podrán ejercer sus derechos en calidad de interesados. Sin embargo, la Directiva PNR no contiene disposiciones a este respecto.
- 61 El Tribunal de Justicia ya ha precisado, en su dictamen sobre el Acuerdo UE-Canadá, que, para garantizar el respeto de esos derechos, es importante que los pasajeros aéreos sean informados de la transmisión de sus datos del PNR a Canadá 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 del PNR que les conciernan y, en su caso, su rectificación, así como a interponer, con arreglo al artículo 47, párrafo primero, de la Carta, un recurso efectivo ante un tribunal (dictamen 1/15, de 26 de julio de 2017, EU:C:2017:592, apartado 220).
- 62 Como ejemplo de la información insuficiente facilitada a los pasajeros por las empresas de transporte aéreo procede señalar aquí las indicaciones de la línea aérea utilizada por el demandante. La información recogida por Lufthansa AG en su página web (<https://www.lufthansa.com/xx/de/informationen-zum-datenschutz>, última consulta de 11 de mayo de 2020) es la siguiente:

«¿Quién es el responsable?»

Deutsche Lufthansa [...] le informa a continuación del tratamiento de sus datos personales [...]

[...]

¿A quién puedo dirigirme?

Si tiene [...] dudas sobre la protección de datos [...], póngase en contacto con nuestro delegado de protección de datos:

[...]

¿En virtud de qué [...] obligaciones trataremos sus datos?

Tratamos los datos de los pasajeros en virtud de las obligaciones legales conforme al artículo 6, apartado 1, primera frase, letra c), del RGPD:

En la medida en que estemos obligados legalmente, trataremos datos personales con el fin de [...] cumplir exigencias en materia de seguridad [...]

Transferencias a **autoridades de control de entrada**:

- *En virtud del Acuerdo sobre datos de pasajeros celebrado entre UE y EEUU o, en su caso, Canadá*
- *En virtud de la Fluggastdatengesetz en Alemania*
- *API* (Advance Passenger Information) Transferencia de datos si estamos obligados a participar en actividades de control en el ámbito del tráfico internacional de viajeros*

**Los datos de la zona mecánicamente legible del pasaporte o del documento de identidad*

Las autoridades competentes le podrán aportar información adicional.

[...]

¿Quién recibe sus datos?

[...] Sus datos podrán comunicarse a las siguientes categorías de destinatarios:

[...]

autoridades y organismos estatales, por ejemplo, en virtud de normas de entrada al país o de actividades policiales o de investigación.

Puede suceder, en este contexto, que se transfieran datos personales a terceros países o a organizaciones internacionales. Para su protección y la protección de sus datos personales, en el marco de dichas transferencias

están previstas garantías adecuadas con arreglo a los requisitos previstos legalmente.

Cuando dichas transferencias no se basen en un fundamento legal o se efectúen hacia un país para el que no exista una decisión de adecuación adoptada por la Comisión Europea, utilizaremos las cláusulas contractuales estándar de la UE.

¿Qué derechos tiene usted en materia de protección de datos?

Para Lufthansa, es importante configurar nuestros procesos de tratamiento de forma equitativa y transparente. Por consiguiente, es importante para nosotros que, en las condiciones legales aplicables, los interesados, además del derecho de oposición, puedan ejercer los siguientes derechos:

Derecho de acceso, artículo 15 del RGPD

Derecho de rectificación, artículo 16 del RGPD

Derecho de supresión («derecho al olvido»), artículo 17 del RGPD

Derecho a la limitación del tratamiento, artículo 18 del RGPD

Derecho a la portabilidad de los datos, artículo 20 del RGPD

Derecho de oposición, artículo 21 del RGPD

[...]»

- 63 Esta información seguramente sea insuficiente e induzca a error. Así, en particular, es manifiestamente incompleta la indicación de que los datos API solo se refieren a la parte de lectura mecánica del pasaporte o del documento de identidad. En efecto, con arreglo al punto 18 del anexo I de la Directiva PNR, deben transmitirse los datos API en la medida en que sean recogidos, incluidos, en particular, la compañía aérea, el número de vuelo y los días, horarios y lugares de llegada y salida, es decir, no solo las partes de lectura mecánica de los documentos de identidad. Por otra parte, no se hace referencia alguna a la Directiva PNR, sino únicamente a la FlugDaG. También falta cualquier referencia al contenido de la Directiva PNR o de la FlugDaG. Así, las personas afectadas, antes de una reserva de vuelo, no pueden apreciar con transparencia quién es la UIP del Estado miembro de que se trate, ni cómo dirigirse a dicha unidad, cómo son tratados los datos del PNR en la unidad, ni el período durante el cual esta puede almacenar sus datos. En esa medida, la información facilitada por Lufthansa AG a los pasajeros no se ajusta a los requisitos del artículo 13 del RGPD, por no hablar de las demás personas cuyos datos también deben facilitarse.