Asunto C-817/19

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:

31 de octubre de 2019

Órgano jurisdiccional remitente:

Cour constitutionnelle (Tribunal Constitucional, Bélgica)

Fecha de la resolución de remisión:

17 de octubre de 2019

Parte recurrente:

ASBL «Ligue des droits humains»

I. Objeto del recurso y pretensiones de las partes

1 El legislador belga adoptó la loi du 25 décembre 2016 relative au traitement des données des passagers (Ley de 25 de diciembre de 2016 relativa al tratamiento de datos de los pasajeros) (*Moniteur belge* de 25 de enero de 2017; también denominada en lo sucesivo «Ley PNR») con el fin de transponer esencialmente:

– 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 […] para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (en lo sucesivo, también, «Directiva PNR»).

– la 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 (en lo sucesivo, también, «Directiva API»).

2 La Ley PNR impone a diferentes sectores de transporte de personas de carácter internacional (aéreo, ferroviario, internacional por carretera y marítimo) y operadores de viajes que transmitan los datos de sus pasajeros a un banco de datos gestionado por el Servicio Público Federal de Interior (Ministerio del Interior).

3 A tal efecto, la Ley crea en el Servicio Público Federal de Interior una «Unidad de Información sobre los Pasajeros» (artículos 12 a 14) integrada, entre otros, por miembros adscritos a los servicios de policía, de seguridad del Estado, de inteligencia y seguridad y de aduanas, y encargada, en particular, de la recogida, conservación y tratamiento de los datos de los pasajeros transmitidos por las compañías de transporte y los operadores de viajes.

4 El «banco de datos de pasajeros» contiene, por una parte, los datos de reserva y, por otra parte, los datos de facturación y de embarque [los llamados datos «API» (Advance Passenger Information), y los llamados datos «PNR» (Passenger Name Record)] (artículo 9).

5 Estos datos son tratados en particular con fines de investigación, enjuiciamiento y ejecución de penas, relativas a delitos contemplados en la Ley, así como con fines de prevención de atentados graves contra la seguridad pública en el marco de la radicalización violenta, seguimiento de las actividades llevadas a cabo por los servicios de inteligencia y seguridad y con vistas a mejorar los controles de personas en las fronteras exteriores y luchar contra la inmigración ilegal (artículo 8).

6 El tratamiento de datos puede tener lugar en el marco de la evaluación previa de los pasajeros (antes de su salida o su llegada) (artículos 24 a 26) o en el marco de investigaciones puntuales (artículo 27).

7 La Ley establece que los datos de los pasajeros se conservarán en el banco de datos de los pasajeros durante un período máximo de cinco años a partir de su registro (artículos 18 a 23).

8 La asociación sin ánimo de lucro «Ligue des droits humains» cuestiona la Ley en los siete aspectos siguientes:

– las modalidades de ejecución de la Ley de 25 de diciembre de 2016 (artículos 3, apartado 2, y 7, apartado 3);

– los conceptos de «documentos de identidad» y de «documentos de viaje» (artículo 7, apartados 1 y 2);

– los datos a que se refiere la Ley (artículos 4, punto 9.º, y 9);

– el concepto de «pasajero» (artículo 4, punto 10.º);

– los fines del tratamiento de los datos «PNR» (artículo 8);

– la gestión del banco de datos de los pasajeros y el tratamiento de datos en el marco de la evaluación previa de los pasajeros y de las investigaciones puntuales (artículos 12 a 16, 24 a 27, 50 y 51);

– la duración del período de conservación de los datos PNR (artículo 18).

9 Denuncia irregularidades en estos aspectos y ha interpuesto ante la Cour constitutionnelle (Tribunal Constitucional, Bélgica) un recurso de anulación basado en dos motivos.

10 El primer motivo se basa esencialmente en el artículo 23 del Reglamento (UE) 2016/679, [1] los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), y el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, «CEDH»).

11 Sostiene, en esencia, que la injerencia en el derecho al respeto de la vida privada y en el derecho a la protección de los datos personales es ilícita en la medida en que no cumple los criterios de legalidad, necesidad y proporcionalidad.

12 En primer lugar, la Ley PNR confiere un amplio margen de apreciación al Poder Ejecutivo, al cual encomienda la labor de definir, mediante Real Decreto, determinados elementos esenciales en menoscabo del principio de legalidad, el cual exige que la injerencia esté prevista por ley o, en caso de habilitación para el desarrollo reglamentario, que los elementos esenciales estén previstos por la ley de manera suficientemente precisa y detallada.

Por otro lado, aduce que la Ley impugnada no persigue un objetivo legítimo. Afirma que la citada Ley prevé, en efecto, una evaluación previa llamada «*pre-screening*», que consiste en evaluar el riesgo que representan los pasajeros, antes de su llegada, salida o tránsito por el territorio nacional.

13 La recurrente niega a continuación la necesidad de adoptar las medidas impugnadas para alcanzar el objetivo perseguido.

Sostiene que el establecimiento de un cotejo de datos, mucho menos intrusivo en la vida privada que la creación de un banco de datos, también permitiría alcanzar la finalidad perseguida.

14 Por último, arguye que la Ley impugnada no respeta el principio de proporcionalidad, en la medida en que los operadores recogen los datos de manera indiscriminada y generalizada y dichos datos se transmiten a las autoridades competentes para su conservación durante cinco años, sin ninguna distinción, diferenciación, limitación o excepción en función del objetivo perseguido.

15 Más concretamente, la Ley incumple el principio de proporcionalidad, habida cuenta de (a) su ámbito de aplicación y las categorías de datos a que se refiere, (b) los tratamientos de datos que instaura, (c) sus finalidades y (d) la duración del período de conservación de los datos.

[1] 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) (en lo sucesivo, también «RGPD»).

16 En primer lugar, la Ley impugnada define de manera muy amplia los datos recogidos, los cuales van más allá de lo estrictamente necesario.

17 La recurrente declara que parece —si bien la Ley no es clara— que el *pre-screening* debe efectuarse en el banco de datos centralizado en la UIP (Unidad de Información sobre los Pasajeros), con ayuda de criterios predeterminados que sirven de indicadores de amenazas. Pues bien, la Ley PNR no define ni la naturaleza precisa de los bancos de datos utilizados para la correlación, ni las modalidades de esta última. La Ley PNR tampoco establece que dicha correlación se limita a las bases de datos utilizadas en relación con la lucha contra el terrorismo y la delincuencia grave.

18 La recurrente critica asimismo las investigaciones puntuales que contempla la Ley sin precisar los datos efectivamente accesibles.

19 Denuncia además que los fines del tratamiento de datos, como los de combatir la inmigración ilegal y actividades que pueden suponer una amenaza para los intereses fundamentales del Estado o luchar contra la «radicalización violenta», definida únicamente en una circular, son considerablemente más amplios que los determinados por la Directiva PNR.

20 Por último, la recurrente cuestiona la duración del período de cinco años de conservación de los datos. El legislador no ha justificado en modo alguno la elección del tiempo máximo autorizado por la Directiva PNR, que pone de manifiesto el carácter desproporcionado de la medida.

21 El Conseil des ministres (Consejo de Ministros) (que defiende la Ley) sostiene, con carácter principal, que el primer motivo de recurso es inadmisible en la medida en que se basa en la infracción del artículo 23 del RGPD, por cuanto tanto del considerando 19 del RGPD como del artículo 1 de la Directiva PNR se desprende claramente que el tratamiento de los datos «PNR» no está comprendido en el ámbito de aplicación del RGPD, sino en el ámbito de la cooperación judicial y policial entre los Estados miembros y de la Directiva (UE) 2016/680. [2]

22 Por otro lado, sostiene que no se infringe el principio de legalidad puesto que la Ley contiene los elementos esenciales de las medidas que establece y enuncia de manera suficientemente precisa los supuestos de habilitación para el desarrollo reglamentario en esta materia. Además, según el Tribunal Europeo de Derechos Humanos, la exigencia de legalidad se entiende en un sentido material, de manera que los actos reglamentarios están comprendidos en el concepto de «ley» en el sentido del Convenio Europeo de Derechos Humanos.

[2] 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 lo sucesivo, «Directiva 2016/680).

La Ley PNR tiene por objeto garantizar la seguridad pública, permitiendo no solo el enjuiciamiento de delitos terroristas o de determinadas formas de delincuencia grave, sino también, gracias a una evaluación previa de los datos obtenidos, la prevención de dichos delitos. El Tribunal de Justicia ha reconocido que dichos objetivos son legítimos en el sentido del artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, tanto en su sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), como en su dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592).

23 El Consejo de Ministros estima que las medidas impugnadas son proporcionadas.

24 En lo que se refiere a la creación de un banco de datos de «nombres de los pasajeros», el Consejo de Ministros señala que la parte recurrente se limita a afirmar, sin acreditarlo, que el establecimiento de una correlación entre los datos habría permitido alcanzar el objetivo perseguido con una menor injerencia en el derecho al respeto de la vida privada. Añade que una simple correlación entre datos no basta para efectuar las evaluaciones previas destinadas a identificar los riesgos para la seguridad. La creación de una base de datos permite además responder al contenido del considerando 25 de la Directiva PNR, que insta a conservar los datos durante el período necesario a la luz de los objetivos perseguidos.

25 En cuanto atañe a la correlación entre las diferentes bases de datos, el Consejo de Ministros recuerda que los artículos 24 y 25 de la Ley PNR transponen el artículo 6 de la Directiva PNR. Por otro lado, de los trabajos preparatorios se desprende que el legislador no pretende establecer una correlación entre el banco de datos de «nombres de los pasajeros» y el conjunto de bancos de datos a los que las autoridades competentes tienen acceso, sino únicamente entre el banco de datos de «nombres de los pasajeros» y los que corresponden a los fines perseguidos por la Ley impugnada. Estas medidas son conformes con las conclusiones que se derivan del dictamen 1/15 del Tribunal de Justicia, ya que el artículo 6, apartado 3, de la Directiva PNR tampoco precisa entre qué bancos de datos cabe establecer una correlación. La facultad discrecional tampoco es incompatible con el principio de legalidad, según interpreta este principio el Tribunal Europeo de Derechos Humanos.

Por otro lado, el objetivo de la Ley no se podría alcanzar si los viajeros conocieran de antemano los criterios que llevan a la obtención de un resultado positivo en la correlación, puesto que podrían adaptar su comportamiento en consecuencia. El artículo 16 de la Ley impugnada indica además claramente que el *pre-screening* debe efectuarse en el banco de datos «de nombres de los pasajeros», extremo que, por consiguiente, es conforme con el principio de legalidad.

26 En lo referente a la duración del período de conservación de los datos, el Consejo de Ministros considera que no resulta desproporcionado establecer un período de conservación de cinco años, el cual, además, corresponde a la duración del plazo

mínimo de prescripción de la acción pública para los delitos de menos gravedad, de que conocen los tribunaux correctionnels.

Por tanto, el período de conservación de dichos datos, que es conforme con el período establecido por la Directiva PNR, en absoluto es desproporcionado.

27 El segundo motivo de recurso, formulado con carácter subsidiario, se basa en esencia en el incumplimiento de lo dispuesto en el artículo 3 TFUE, apartado 2, en relación con el artículo 45 de la Carta.

28 La recurrente sostiene que los artículos 3, apartado 1, y 8, apartado 2, y el capítulo 11, que contiene los artículos 28 a 31 de la Ley PNR, son contrarios a la libre circulación de las personas, en la medida en que no solo se refieren a los transportes exteriores de la UE, sino también a los transportes interiores de la UE (incluidas las escalas). En otras palabras, la parte recurrente estima que, al hacer extensivo el sistema «PNR» a los vuelos interiores de la UE, las disposiciones impugnadas restablecen indirectamente controles en las fronteras que son contrarios a la libre circulación de las personas.

29 El Consejo de Ministros considera que la Ley impugnada no vuelve a instaurar ningún control en las fronteras y que no vulnera en modo alguno la libre circulación de las personas. Aduce que la Directiva PNR no se aplica a la inmigración ilegal y que la Ley impugnada no solo transpone la Directiva PNR, sino también la Directiva API.

El motivo de recurso, según se encuentra formulado, se refiere únicamente a los artículos 3, apartado 1, y 8, apartado 2, y al capítulo 11 de la Ley impugnada. Pues bien, de la definición del concepto de «fronteras exteriores» se desprende que la Ley PNR solo se refiere a los controles exteriores de la UE. Además, la Ley PNR transpone la Directiva 2004/82/CE, de forma que no puede interpretarse en el sentido de que vuelve a instaurar controles en las fronteras del espacio Schengen.

Con carácter subsidiario de segundo grado, el considerando 10 de la Directiva PNR establece expresamente la posibilidad de ampliar la utilización de los datos «PNR» a los vuelos interiores de la UE, lo que demuestra que dicha medida no es en sí misma contraria a la libre circulación ni al Reglamento (CE) n.º 562/2006.

II. Marco jurídico

Convenio Europeo de Derechos Humanos

30 El artículo 8 establece:

«1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás.»

Derecho de la Unión

Carta de los Derechos Fundamentales de la Unión Europea

31 El artículo 7 de la Carta («Respeto de la vida privada y familiar») dispone:

«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.»

32 Con arreglo al artículo 8 de la Carta («Protección de datos de carácter personal»):

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

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

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

33 El artículo 52, apartado 1, de la Carta establece lo siguiente:

«Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones 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.»

Reglamento general de protección de datos (RGPD)

34 De conformidad con el artículo 2, apartado 2, letra d), de este Reglamento:

«2. El presente Reglamento no se aplica al tratamiento de datos personales:

[…]

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de

ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.»

35 El artículo 23 establece:

«1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) 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;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.»

Directiva PNR

36 Su artículo 3 está redactado de la siguiente manera:

A efectos de la presente Directiva, se entenderá por:

«[…]

4) "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».

37 El artículo 4 establece:

«Unidad de Información sobre los Pasajeros

1. Cada Estado miembro establecerá o designará una autoridad competente para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves, o una sucursal de esa autoridad, para actuar como su Unidad de Información sobre los Pasajeros ("UIP").

2. La UIP será responsable de:

a) recoger los datos PNR de las compañías aéreas, almacenar y procesar esos datos y transferir dichos datos o el resultado de su tratamiento a las autoridades competentes a que hace mención el artículo 7;

b) intercambiar tanto los datos PNR como […] los resultados de su tratamiento con las UIP de otros Estados miembros y con Europol, de conformidad con los artículos 9 y 10.

[…]»

38 A tenor del artículo 6:

«1. Los datos PNR transmitidos por las compañías aéreas serán recopilados por la UIP del Estado miembro que corresponda, con arreglo a lo dispuesto en el artículo 8. Si los datos PNR transmitidos por las compañías aéreas incluyeran datos distintos de los enumerados en el anexo I, la UIP los suprimirá inmediatamente y de manera definitiva en el momento de su recepción.

2. La UIP tratará los datos PNR solo para realizar:

a) una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro, a fin de identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes a que se refiere el artículo 7 y, en su caso, por Europol, de conformidad con el artículo 10, ante la posibilidad de que pudiera estar implicada en un delito de terrorismo o delito grave;

b) responder, en cada caso particular, a las peticiones debidamente razonadas y con suficiente base de las autoridades competentes de que se suministren y traten datos PNR en casos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y facilitar a las autoridades competentes o, en su caso, a Europol, los resultados de dicho tratamiento, y

c) analizar los datos PNR con el fin de actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave.

[…]»

39 En virtud del artículo 12:

«1. Los Estados miembros se asegurarán de que los datos PNR proporcionados por las compañías aéreas a la UIP se conservan en una base de datos de la Unidad durante un plazo de cinco años a partir de su transmisión a la UIP del Estado miembro en cuyo territorio tenga su punto de aterrizaje u origen el vuelo.

2. Al finalizar un plazo de seis meses desde la transmisión de datos PNR mencionada en el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento de los siguientes elementos que podrían servir para identificar directamente al pasajero al que se refieren los datos PNR:

a) nombre(s) y apellido(s), incluidos los de otros pasajeros que figuran en el PNR y número de personas que figuran en el PNR que viajan juntas;

b) dirección y datos de contacto;

c) todos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, o a cualquier otra persona;

d) información sobre viajeros asiduos;

e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el PNR, y

f) toda la API recopilada.

3. Al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la divulgación de los datos PNR completos cuando:

a) se crea razonablemente que es necesario a los efectos establecidos en el artículo 6, apartado 2, letra b), y

b) haya sido aprobado por:

i) una autoridad judicial, u

ii) otra autoridad nacional competente para verificar si se cumplen las condiciones para la divulgación conforme al derecho nacional, con sujeción a la información y revisión *a posteriori* del responsable de la protección de datos de la UIP.

4. Los Estados miembros se asegurarán de que los datos PNR sean suprimidos de modo permanente al finalizar el período a que se refiere el apartado 1. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente y se estén utilizando en el marco de un asunto específico a efectos de prevenir, detectar, investigar o enjuiciar los actos de terrorismo o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por el derecho nacional.

5. Los resultados del tratamiento a que se refiere el artículo 6, apartado 2, letra a), serán conservados por la UIP únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y, de conformidad con el artículo 9, apartado 1, a las UIP de otros Estados miembros. Cuando el resultado de un tratamiento automatizado, tras un examen individual por medios no automatizados, contemplado en el artículo 6, apartado 5, arroje un resultado negativo, este se podrá almacenar para evitar falsos resultados positivos mientras los datos de base no se hayan eliminado con arreglo al apartado 4 del presente artículo.»

40 El anexo I de la Directiva PNR, titulado «Datos del registro de nombres de los pasajeros recopilados por las compañías aéreas» indica, en particular:

«[…]

12. Observaciones generales (incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada)

[…]

18. Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema 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)

[…]»

Directiva API

41 El artículo 1 de esta Directiva establece:

«La presente Directiva tiene por objeto mejorar los controles fronterizos y combatir la inmigración ilegal mediante la comunicación previa por los transportistas a las autoridades nacionales competentes de los datos de las personas transportadas.»

Derecho belga

42 Las disposiciones pertinentes de la **Ley PNR** (en su versión modificada por las Leyes de 15 y de 30 de julio de 2018 y por la Ley de 2 de mayo de 2019) son las siguientes:

«CAPÍTULO 2. Ámbito de aplicación

Art. 3. 1. La presente Ley determina las obligaciones que incumben a los transportistas y operadores de viajes en relación con la comunicación de los datos de los pasajeros con destino o procedencia en el territorio nacional o en tránsito por dicho territorio.

2. Mediante Real Decreto aprobado en Consejo de Ministros, se determinarán, por sector de transporte y respecto a los operadores de viajes, los datos de los pasajeros que deberán transmitirse y sus modalidades de transmisión, previo dictamen de la autoridad competente en materia de control de los tratamientos de datos personales. […]

CAPÍTULO 3. Definiciones

Art. 4. A efectos de la aplicación de la presente Ley y de sus decretos de ejecución, se entenderá por:

[…]

9. "PNR": relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información mencionada en el artículo 9 necesaria para el tratamiento y el control de las reservas por parte de las compañías de transporte y los operadores de viajes que las realizan y participan en el sistema PNR, por cada viaje reservado por una persona o en su nombre, ya estén contenidos en sistemas de reservas, en sistemas de control de salidas utilizados para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades;

10. "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 por la compañía de transporte con el consentimiento de esta, lo cual se manifiesta en la inclusión de la persona en la lista de pasajeros;

[…]

CAPÍTULO 5. Fines del tratamiento de datos

Art. 8. 1. Los datos de los pasajeros serán tratados con los fines siguientes:

1.º la investigación y el enjuiciamiento de los delitos que figuran [en el] Code d'Instruction criminelle (Código de Enjuiciamiento Criminal), incluida la ejecución de las penas o medidas restrictivas de libertad relativas a dichos delitos;

2.º la investigación y el enjuiciamiento de los delitos que figuran [en el] Code pénal (Código Penal), incluida la ejecución de las penas o medidas restrictivas de libertad relativas a dichos delitos;

3.º la prevención de atentados graves contra la seguridad pública en el marco de la radicalización violenta mediante el seguimiento de fenómenos y agrupaciones de conformidad con el artículo 44/5, apartados 1, puntos 2.º y 3.º, y 2, de la loi du 5 août 1992 sur la fonction de police (Ley de 5 de agosto de 1992 sobre la función policial);

4.º el seguimiento de las actividades enumeradas en los artículos 7, puntos 1.º y 3.º/1, y 11, apartado 1, puntos 1.º a 3.º y 5.º, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Ley Orgánica de 30 de noviembre de 1998 relativa a los servicios de inteligencia y seguridad);

5.º la investigación y el enjuiciamiento de los delitos incluidos [en distintas leyes].

2. Con arreglo a las condiciones establecidas en el capítulo 11, los datos de los pasajeros también serán tratados a efectos de mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal.

CAPÍTULO 6. — Datos de los pasajeros

Art. 9. 1. En lo que concierne a la información relativa a la reserva, se recopilarán, como máximo, los siguientes datos de los pasajeros:

1.º localizador del registro PNR;

2.º fecha de reserva y emisión del billete;

3.º fechas de viaje previstas;

4.º nombres y apellidos y fecha de nacimiento;

5.º dirección y datos de contacto (número de teléfono, dirección de correo electrónico);

6.º datos de pago, incluida la dirección de facturación;

7.º itinerario completo del pasajero específico;

8.º información relativa a los "viajeros registrados", es decir, los viajeros asiduos;

9.º agencia de viajes u operador de viajes;

10.º situación del vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva;

11.º información PNR escindida o dividida;

12.º observaciones generales, incluida toda la información disponible sobre menores de 18 años no acompañados, como nombre y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada;

13.º información sobre el billete, incluidos el número de billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos;

14.º datos del asiento, incluido el número;

15.º información sobre códigos compartidos;

16.º toda la información relativa al equipaje;

17.º número de viajeros y otros nombres de viajeros que figuran en el PNR;

18.º cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API), indicada en el apartado 2;

19.º todo el historial de cambios de los datos indicados en los puntos 1.º a 18.º;

2. En relación con los datos de facturación y de embarque, la información recogida de forma anticipada a que se refiere el apartado 1, punto 18.º, será la siguiente:

1.º tipo de documento de viaje;

2.º número de documento;

3.º nacionalidad;

4.º país de emisión del documento;

5.º fecha de expiración del documento;

6.º apellidos, nombre, sexo, fecha de nacimiento;

7.º compañía de transporte/operador de viajes;

8.º número de transporte;

9.º fecha de salida, fecha de llegada;

10.º lugar de salida, lugar de llegada;

11.º hora de salida, hora de llegada;

12.º número total de personas transportadas;

13.º número de asiento;

14.º localizador de registro PNR;

15.º número, peso y localizador del equipaje;

16.º paso fronterizo utilizado para entrar en el territorio nacional.

[…]

CAPÍTULO 7. Unidad de Información sobre los Pasajeros

Art. 12. Por el presente se establece, como entidad dependiente del Servicio Público Federal Interior, la Unidad de Información sobre los Pasajeros.

Art. 13. 1. La UIP será responsable de:

1.º recoger, almacenar y procesar los datos relativos a los pasajeros comunicados por las compañías de transporte y los operadores de viajes, así como gestionar el banco de datos de los pasajeros;

2.º intercambiar tanto los datos de los pasajeros como los resultados de su tratamiento con las UIP de otros Estados miembros de la Unión Europea, Europol, y terceros países, de conformidad con el capítulo 12.

2. Sin perjuicio de otras disposiciones legales, la UIP no podrá utilizar los datos almacenados en virtud del capítulo 9 con fines distintos a los que figuran en el artículo 8.

Art. 14. 1. La UIP estará integrada por:

1.º un funcionario […] que se encargará de:

a) la organización y el funcionamiento de la UIP;

b) el control del cumplimiento de las obligaciones que incumben a las compañías de transporte y los operadores de viajes con arreglo al capítulo 4;

c) la gestión y la utilización del banco de datos de los pasajeros;

d) el tratamiento de los datos de los pasajeros;

e) el respeto de la legalidad y de la regularidad de todo tratamiento de datos a que se refiere el capítulo 10;

[…].

2.º personal enviado en comisión de servicios procedente de los servicios […] siguientes:

a) Servicios de policía […];

b) Seguridad del Estado […];

c) Servicio General de Inteligencia y Seguridad […];

d) Administración […] de Derechos de Aduana e Impuestos Especiales […]
[…].

CAPÍTULO 8. Banco de datos de los pasajeros

Art. 15. 1. Por el presente se crea un banco de datos de los pasajeros gestionado por el Servicio Público Federal Interior en el que se registrarán los datos de los pasajeros.

[…].

4. Todo tratamiento de datos de los pasajeros efectuado en virtud de la presente Ley estará sujeto a la Ley relativa a la protección de datos. La autoridad competente en materia de control del tratamiento de datos personales ejercerá las competencias indicadas en la Ley relativa a la protección de la vida privada. […]

[…]

CAPÍTULO 9. Sobre los plazos de conservación

Art. 18. Los datos de los pasajeros se conservarán en el banco de datos de los pasajeros durante un período máximo de cinco años a partir de su registro. Transcurrido dicho período, se destruirán.

[…]

CAPÍTULO 10. Tratamiento de datos

Sección I. Tratamiento de datos de los pasajeros en el marco de la evaluación previa de los pasajeros

Art. 24. 1. Los datos de los pasajeros serán tratados para realizar una evaluación previa de los pasajeros antes de su llegada o salida programada del territorio nacional o su tránsito por este, a efectos de identificar a toda persona que deba ser examinada de nuevo.

[métodos de evaluación previa]

Art. 25. […]

2. La evaluación de los pasajeros antes de su llegada o salida del territorio nacional o su tránsito por este con arreglo a los criterios predeterminados se realizará de forma no discriminatoria. Dichos criterios no podrán tener por objeto la identificación de una persona y deberán ser orientados, proporcionados y específicos.

3. Los criterios no se basarán en ningún caso en datos que revelen 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.

[…]

Sección 2. — Tratamiento de datos en el marco de investigaciones puntuales

Art. 27. Los datos de los pasajeros se utilizarán para llevar a cabo investigaciones puntuales con los fines indicados en el artículo 8, apartado 1, puntos 1.º, 2.º, 4.º y 5.º, y conforme a las condiciones establecidas en el artículo 46 *septies* del Código

de Enjuiciamiento Criminal, el artículo 16/3 de la Ley Orgánica de 30 de noviembre de 1998 relativa a los servicios de inteligencia y seguridad o el artículo 281, apartado 4, de la loi générale sur les douanes et accises (Ley general en materia de derechos de aduana e impuestos especiales), refundida el 18 de julio de 1977.

CAPÍTULO 11. Tratamiento de datos de los pasajeros a efectos de mejorar los controles fronterizos y combatir la inmigración ilegal

Art. 28. 1. El presente capítulo se aplica al tratamiento de datos de los pasajeros por parte de los servicios de policía encargados del control de las fronteras y de la Office des étrangers (Oficina de Extranjería) a efectos de mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal.

[…]

Art. 29. 1. […]

2. Únicamente se transmitirán los datos [API] referidos a las siguientes categorías de pasajeros:

1.º los pasajeros que tengan previsto entrar o hayan entrado en el territorio por las fronteras exteriores de Bélgica;

2.º los pasajeros que tengan previsto salir o hayan salido del territorio por las fronteras exteriores de Bélgica;

3.º los pasajeros que tengan previsto pasar o hayan pasado por una zona internacional de tránsito situada en Bélgica o se encuentren en dicha zona.

3. Los datos de los pasajeros a que hace referencia el apartado 2 se transmitirán a los servicios de policía indicados en el artículo 14, apartado 1, punto 2.º, letra a), inmediatamente después de su registro en el banco de datos de pasajeros. Dichos servicios conservarán esos datos en un fichero temporal y los destruirán en las veinticuatro horas siguientes a su transmisión.

4. […] los datos de los pasajeros a que hace referencia el apartado 2 se transmitirán a la Oficina de Extranjería inmediatamente después de su registro en el banco de datos de pasajeros. Dicha Oficina conservará esos datos en un fichero temporal y los destruirá en las veinticuatro horas siguientes a su transmisión.

[…].

Art. 31. En las veinticuatro horas siguientes a la finalización del transporte a que se refiere el artículo 4, puntos 3.º a 6.º, las compañías de transporte y los operadores de viajes destruirán todos los datos de los pasajeros enumerados en el artículo 9, apartado 1, punto 18.º, […].

[…]

CAPÍTULO 15. Disposiciones modificativas

Sección I. Modificación del Código de Enjuiciamiento Criminal

Art. 50. En el Código de Enjuiciamiento Criminal se insertará el artículo 46 *septies*, el cual tendrá el siguiente tenor:

"Art. 46 *septies*. En el marco de las investigaciones de los delitos a que se refiere el artículo 8, apartado 1, puntos 1.º, 2.º y 5.º, de la Ley de 25 de diciembre de 2016 relativa al tratamiento de datos de los pasajeros, el Ministerio Fiscal, mediante decisión escrita y motivada, podrá encargar al agente de la policía judicial que solicite a la UIP la comunicación de los datos de los pasajeros de conformidad con el artículo 27 de la Ley de 25 de diciembre de 2016 relativa al tratamiento de datos de los pasajeros.

[…]".

Sección 2. Modificación de la Ley Orgánica de 30 de noviembre de 1998 relativa a los servicios de inteligencia y seguridad

Art. 51. En el capítulo III, sección I.ª, subsección 2, de la Ley Orgánica de 30 de noviembre de 1998 relativa a los servicios de inteligencia y de seguridad se insertará el artículo 16/3 con el siguiente tenor:

"Art. 16/3. 1. Mediante decisión debidamente motivada y en aras de ejercer sus funciones, los servicios de inteligencia y seguridad podrán acceder a los datos de los pasajeros a que se refiere el artículo 27 de la Ley de 25 de diciembre de 2016 relativa al tratamiento de datos de los pasajeros […]".»

III. Apreciación de la Cour constitutionnelle

43 La Cour constitutionnelle señala, en primer lugar, que al examinar el recurso es preciso tener en consideración las modificaciones introducidas en la Ley de 25 de diciembre de 2016 por las Leyes de 15 y de 30 de julio de 2018 y por la Ley de 2 de mayo de 2019.

44 En segundo lugar, la Cour constitutionnelle reduce el alcance del recurso de anulación al determinar que el primer motivo de recurso se refiere únicamente al artículo 3, apartado 2, al artículo 4, puntos 9.º y 10.º, a los artículos 7 a 9, a los artículos 12 a 16, al artículo 18, a los artículos 24 a 27 y a los artículos 50 y 51 de la Ley, y que con el segundo motivo de recurso se impugnan el artículo 3, apartado 1, el artículo 8, apartado 2, y los artículos 28 a 31 de la Ley.

1. Sobre la admisibilidad del primer motivo de recurso: ¿es el artículo 23 del RGPD aplicable a la Ley PNR?

45 El órgano jurisdiccional remitente recuerda que la protección que brinda el RGPD se basa en el artículo 16 TFUE, apartado 2, y que, en principio, el 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 no está comprendido en el ámbito de aplicación del RGPD, sino en el de la Directiva 2016/680. Dicha Directiva establece unas normas específicas relativas 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, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, respetando la naturaleza específica de estas actividades.

46 La Ley PNR regula la recogida y la transmisión de los datos PNR, la creación de un banco de datos de pasajeros, gestionado por la UIP, los fines del tratamiento de los datos almacenados en dicho banco de datos y el acceso a este último. Transpone esencialmente la Directiva PNR, si bien su contenido va más allá de esta transposición.

47 En referencia al dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), el órgano jurisdiccional remitente declara que las disposiciones que regulan la recogida, la transmisión y el tratamiento de datos «PNR» pueden estar comprendidas tanto en el ámbito de la protección de datos (artículo 16 TFUE) como en el ámbito de la cooperación policial (artículo 87 TFUE).

Señala asimismo que el considerando 5 de la Directiva PNR indica que los objetivos de dicha Directiva son «*entre otras cosas, garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes*». El considerando 38 de esta misma Directiva indica, sin embargo, que los objetivos de la Directiva son «*la transferencia de datos PNR por las compañías aéreas y su tratamiento a efectos de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y la delincuencia grave*», lo que puede conferir a estos objetivos un carácter preponderante respecto al objetivo de la protección de datos.

Por otro lado, observa que el Derecho nacional no excluye la totalidad de la Ley PNR del ámbito de aplicación del artículo 23 del RGPD.

48 La Cour constitutionnelle concluye, por consiguiente, que al efecto de dilucidar si los requisitos que establece el artículo 23 del RGPD se aplican a la Ley PNR, que transpone, entre otras y principalmente, la Directiva PNR, procede plantear al Tribunal de Justicia una primera cuestión prejudicial.

2. Sobre el fondo del primer motivo de recurso

La Cour constitutionnelle examina a continuación el fondo del motivo de recurso en lo que se refiere a los siete aspectos mencionados en el punto 8 del presente resumen. Considera que las dos primeras imputaciones formuladas contra las «modalidades de ejecución» y contra los conceptos de «documentos de identidad» y «documento de viaje» son infundadas. Prosigue su examen de las otras cinco imputaciones y expone sus dudas tanto sobre la interpretación que ha de darse a determinadas disposiciones de la Directiva PNR como sobre la validez de estas a la luz de la Carta.

Sobre los datos a que se refiere la Ley PNR (artículos 4, punto 9.º, y 9 de la Ley PNR)

49 La parte recurrente estima que el extenso ámbito de aplicación relativo a los datos de los pasajeros a que se refieren los artículos 4, punto 9.º, y 9 de la Ley PNR es manifiestamente desproporcionado a la luz del objetivo perseguido. En su opinión, los datos de que se trata pueden revelar datos sensibles, como la pertenencia a un sindicato, las afinidades personales y las relaciones personales o profesionales.

50 El órgano jurisdiccional remitente recuerda que la injerencia de los poderes públicos en el ejercicio del derecho al respeto de la vida privada no solo debe basarse en una disposición legislativa suficientemente precisa, sino también responder a una necesidad social imperiosa en una sociedad democrática y ser proporcional al objetivo legítimo perseguido. El legislador goza en la materia de una facultad de apreciación que, sin embargo, no es ilimitada: para que una norma sea compatible con el derecho al respeto de la vida privada, es preciso que el legislador haya establecido un equilibrio justo entre los derechos e intereses de que se trate.

En su dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), el Tribunal de Justicia recordó que la injerencia en el derecho a la protección de datos personales debe limitarse a lo «estrictamente necesario» (véanse los apartados 140 y 141).

51 La Cour constitutionnelle señala que la Ley PNR tiene por objeto garantizar la seguridad pública, mediante el establecimiento de normas relativas a la transmisión y la utilización de datos de los pasajeros, en el marco de la lucha contra los delitos de terrorismo y la delincuencia grave de carácter transnacional. Dichos objetivos constituyen objetivos de interés general que pueden justificar injerencias en el derecho al respeto de la vida privada y en el derecho a la protección de datos personales (sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 42). Por otro lado, el Tribunal de Justicia confirmó que dichos objetivos de interés general pueden justificar el tratamiento y la transferencia de datos del registro de nombres de los pasajeros [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 148 y 149].

52 Acto seguido, el órgano jurisdiccional remitente examina si dichas injerencias están reguladas de manera suficientemente precisa y proporcional y si se limitan a lo «estrictamente necesario», teniendo en consideración la amplitud de los datos a que se refiere la Ley PNR.

La recogida de los datos de los pasajeros a que se refiere la Ley PNR va acompañada de garantías por lo que respecta a su contenido. En efecto, estos datos se encuentran enunciados con carácter exhaustivo en el artículo 9 de la Ley PNR. Se trata de información directamente vinculada al viaje que da lugar al transporte comprendido en el ámbito de aplicación de la Ley PNR, información de la que, en principio, ya disponen las compañías de transporte y los operadores de viajes. Además, dichos datos se corresponden con el anexo I de las directrices recomendadas por la Organización de Aviación Civil Internacional (OACI). Por consiguiente, son pertinentes a la luz de los objetivos perseguidos por la Ley PNR.

Por otro lado, los artículos 10 y 11, no impugnados, de la Ley PNR establecen que los datos de los pasajeros no pueden referirse al 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. Cuando los datos de los pasajeros transmitidos por las compañías de transporte y los operadores de viajes incluyen datos distintos a los enumerados en el artículo 9 o datos enumerados en el artículo 10, la UIP suprime dichos datos adicionales en el momento de su recepción y de manera definitiva. Dichas disposiciones garantizan que los datos sensibles no puedan, en principio, ser recogidos o conservados como «datos de pasajeros».

53 En su dictamen 1/15, antes citado, de 26 de julio de 2017, el Tribunal de Justicia también consideró, en cuanto atañe a los datos sensibles, que «*los artículos 7, 8 y 21 así como el artículo 52, apartado 1, de la Carta se oponen tanto a la transferencia de datos sensibles a Canadá como al marco regulador negociado por la Unión con ese Estado tercero sobre los requisitos relativos al uso y la conservación de tales datos por las autoridades de dicho Estado tercero*» (apartado 167).

Esta observación es extrapolable al caso de autos. Si bien existen garantías en amparo de los datos de los pasajeros a que se refiere la Ley PNR, procede preguntarse si dichas garantías son suficientes, habida cuenta de la amplitud de los datos de que se trata. Los datos enunciados en el artículo 9, apartado 1, de la Ley PNR, el cual reproduce los datos a que se refiere el anexo I de la Directiva PNR, incluyen, en efecto, además de los datos de facturación y de embarque, datos de amplio alcance, en particular: el itinerario completo del pasajero, la agencia de viajes, el número de asiento, toda la información relativa al equipaje, información relativa a los métodos de pago, incluida la dirección de facturación, observaciones generales, «incluida la información disponible sobre los menores de 18 años no acompañados».

En su dictamen 1/15 de 26 de julio de 2017, antes citado, el Tribunal de Justicia también observó que, «*aun cuando algunos de los datos del PNR, aisladamente considerados, no parezcan poder revelar información importante sobre la vida privada de las personas afectadas, no deja de ser cierto que, conjuntamente considerados, 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 define en el artículo 2, letra e), del Acuerdo previsto*» (apartado 128).

En su dictamen de 19 de agosto de 2016 sobre las implicaciones para la protección de datos del tratamiento de los registros de nombres de pasajeros (en lo sucesivo, «dictamen de 19 de agosto de 2016»), el Comité Consultivo del Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (en lo sucesivo, «Comité Consultivo del Convenio n.º 108») observó asimismo que «*los registros de nombres de pasajeros contienen información destinada a facilitar el viaje de los pasajeros, y pueden incluir ciertos datos sensibles (datos que pueden servir para identificar el origen racial, las opiniones políticas, las creencias religiosas y de otra índole, el estado de salud o la orientación sexual de una persona), no solo en forma de información "codificada", sino también en campos de información abiertos que contienen observaciones generales (tales como las necesidades dietéticas y médicas, o el hecho de que una asociación política o religiosa ha obtenido billetes a precio reducido para el transporte de sus miembros), lo que podría dar lugar a una discriminación directa*» [Consejo de Europa, dictamen de 19 de agosto de 2016, T-PD(2016)18rev, p. 7].

La Agencia de los Derechos Fundamentales de la Unión Europea también señaló que los datos PNR «*pueden incluir datos sensibles o especiales bajo la categoría de "observaciones generales"*» [dictamen 1/2011 de la Agencia de los Derechos Fundamentales de la Unión Europea sobre la propuesta de Directiva relativa a la utilización de datos del registro de nombres de pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave [COM(2011) 32 final], 14 de junio de 2011, p. 8; véase asimismo *ibid*, p. 13].

54 Habida cuenta de la extensión de su ámbito de aplicación, los datos a que se refiere el artículo 9 de la Ley PNR, si bien no pueden incluir directamente datos sensibles, pueden poner de manifiesto, indirectamente, elementos sensibles amparados por la protección de datos personales y por el respeto de la vida privada. Teniendo en consideración el dictamen 1/15 del Tribunal de Justicia, la Cour constitutionnelle se pregunta si dichos datos, que incluyen los enunciados en el anexo I de la Directiva PNR, no sobrepasan los límites de lo «estrictamente necesario» para alcanzar los objetivos perseguidos por esta misma Directiva. Por consiguiente, decide plantear al Tribunal de Justicia una segunda cuestión prejudicial.

55 En su dictamen 1/15, antes citado, de 26 de julio de 2017, el Tribunal de Justicia expuso además las observaciones siguientes en lo que respecta a la exigencia de definir de manera clara y precisa los datos a que se refiere el proyecto de Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros:

«*156.A este respecto, si bien las 19 categorías de datos del PNR enumeradas en el anexo del Acuerdo previsto se corresponden, según las observaciones de la Comisión, con el anexo I de las directrices de la Organización de la Aviación Civil Internacional (OACI) relativas a los datos del PNR, conviene subrayar no obstante, como ha señalado el Abogado General en el punto 217 de sus conclusiones, que la categoría 5, relativa a "información sobre viajeros frecuentes y ventajas correspondientes (billetes gratuitos, paso a la categoría superior, etc.)", y la categoría 7 que comprende "toda la información de contacto disponible (incluida la información del expedidor)", no definen de forma suficientemente clara y precisa los datos del PNR que han de transferirse.*

157. En efecto, en el caso de la categoría 5, el empleo del vocablo "etc." no especifica suficientemente el alcance de los datos que han de transferirse. Además, el enunciado de esta categoría no permite determinar si se refiere exclusivamente a la información relativa al estatus de los pasajeros aéreos en los programas de fidelización o si, por el contrario, se refiere a la totalidad de la información relativa a los viajes aéreos y a las transacciones efectuadas en el contexto de tales programas.

158. Del mismo modo, la categoría 7, al emplear los términos "toda la información de contacto disponible", no determina suficientemente el alcance de los datos que han de transferirse. En particular, no especifica el tipo de datos de contacto a que se refiere, ni si esos datos de contacto incluyen asimismo, como puede deducirse de la respuesta escrita de la Comisión a las preguntas formuladas por el Tribunal de Justicia, los de los terceros que hayan efectuado la reserva del vuelo para el pasajero aéreo, los de aquellos por medio de los cuales pueda entrarse en contacto con el pasajero aéreo, o los de aquellos que deban ser informados en caso de urgencia.

159. Por lo que respecta a la categoría 8, esta tiene por objeto "todos los datos de pago y facturación (excluidos los demás detalles de la transacción relacionados con una tarjeta de crédito o cuenta y no relacionados con la transacción correspondiente al viaje)". Es cierto que esta categoría podría parecer particularmente amplia por cuanto emplea la expresión "todos los datos". No obstante, como se desprende de la respuesta de la Comisión a las preguntas formuladas por el Tribunal de Justicia, debe considerarse que dicha categoría únicamente se refiere a la información relativa a los medios de pago y a la facturación del billete de avión, excluyendo cualquier otra información que no esté directamente relacionada con el vuelo. Interpretada en este sentido, la categoría 8 puede considerarse acorde con los requisitos de claridad y precisión.

160. En cuanto a la categoría 17, esta tiene por objeto las "observaciones generales, incluida la información sobre otros servicios (OSI), información sobre servicios especiales (SSI) y sobre servicios especiales solicitados (SSR)". Según las explicaciones facilitadas, en particular, por la Comisión, esta categoría es de las denominadas "de texto libre" (free text), y está destinada a incluir "toda la información adicional", además de la ya enumerada en otras categorías del anexo. Así pues, una categoría de este tipo no proporciona indicación alguna sobre la naturaleza y el alcance de la información que debe transmitirse, e incluso parece poder englobar información carente de relación alguna con la finalidad de la transferencia de datos del PNR. Además, puesto que la información a que se refiere esta categoría únicamente se facilita a modo de ejemplo, como lo demuestra el empleo del término "incluida", dicha categoría no establece limitación alguna en cuanto a la naturaleza y el alcance de la información que puede figurar en ella. En consecuencia, no puede considerarse que la categoría 17 se halle delimitada con la suficiente claridad y precisión.

161. Por último, en lo que se refiere a la categoría 18, esta tiene por objeto "cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API) a efectos de la reserva". Según las aclaraciones facilitadas por el Consejo y la Comisión, esta información se corresponde con la contemplada en el artículo 3, apartado 2, de la Directiva 2004/82, a saber, el número y tipo de documento de viaje utilizado, la nacionalidad, el nombre y apellidos, la fecha de nacimiento, el paso fronterizo de entrada en el territorio de los Estados miembros, el código de transporte, la hora de salida y de llegada del transporte, el número total de personas transportadas en ese medio y el lugar inicial de embarque. Esta categoría, siempre que se interprete en el sentido de que únicamente comprende la información expresamente contemplada en esta última disposición, puede considerarse acorde con los requisitos de claridad y precisión.

162. Las disposiciones del artículo 4, apartado 3, del Acuerdo previsto, que establecen la obligación de Canadá de suprimir cualquier dato del PNR que le haya sido transferido si no figura en la lista del anexo del mismo Acuerdo, no permiten paliar la imprecisión de que adolecen las categorías 5, 7 y 17 de dicho anexo. En efecto, en la medida en que esa lista no delimita, por sí misma, con la suficiente claridad y precisión, los datos del PNR que han de transferirse, aquellas disposiciones no pueden subsanar la incertidumbre en cuanto a los datos del PNR que han de ser objeto de la transferencia.

163. Por lo tanto, en lo que respecta a los datos del PNR que han de transferirse a Canadá, las categorías 5, 7 y 17 del anexo del Acuerdo previsto no delimitan de manera suficientemente clara y precisa el alcance de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta».

56 Dado que algunas de estas observaciones pueden ser extrapolables al caso de autos, por lo que respecta al carácter ilustrativo y no taxativo de determinados datos que figuran en el anexo I de la Directiva PNR, el cual incorpora al Derecho

nacional el artículo 9 de la Ley PNR, el órgano jurisdiccional remitente decide plantear una tercera cuestión prejudicial.

Sobre el concepto de «pasajero» (artículo 4, punto 10.º de la Ley PNR)

57 La parte recurrente critica la amplitud del concepto de «pasajero», que da lugar a un tratamiento automatizado sistemático, no selectivo, de los datos de todos los pasajeros.

58 De la definición del concepto de «pasajero» (artículo 4, punto 10.º, de la Ley PNR) se desprende que la recogida, la transferencia y el tratamiento de los datos PNR de los «pasajeros» constituyen obligaciones generales e indiferenciadas, las cuales se aplican a toda persona transportada o que deba ser transportada y registrada en la lista de pasajeros. Las obligaciones que impone la Ley PNR se aplican, por tanto, independientemente de que existan motivos fundados para presumir que las personas afectadas han cometido o van a cometer un delito, o han sido condenadas por un delito.

59 En su dictamen de 19 de agosto de 2016, el Comité Consultivo del Convenio n.º 108 observó a este respecto que «*el tratamiento de los datos PNR —que brinda la ventaja única de permitir la identificación de las personas objeto de interés— constituye una criba general y no selectiva de todos los pasajeros, incluidos los no sospechosos de haber cometido una infracción penal, por parte de las distintas autoridades competentes, e incluye datos recogidos inicialmente con fines comerciales por entidades privadas. Habida cuenta de la magnitud de la restricción del derecho a la vida privada y del derecho a la protección de datos que se deriva del tratamiento de los datos PNR, ha de quedar claramente acreditado que dicho tratamiento constituye una medida necesaria que responde a una finalidad legítima en una sociedad democrática; además, es preciso que se apliquen las garantías adecuadas. Es indispensable que se demuestre expresamente la necesidad de la recogida de los datos PNR y su utilización ulterior*» [dictamen de 19 de agosto de 2016, T-PD(2016)18rev, p. 5].

60 En el ámbito de las comunicaciones electrónicas, el Tribunal de Justicia se pronunció sobre una normativa nacional que establecía 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 y obligaba a los proveedores de servicios de comunicaciones electrónicas a conservar esos datos de manera sistemática y continuada, sin ninguna excepción (sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970).

Consideró que, «*si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la*

conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha» (apartado 103).

El Tribunal de Justicia estimó, por una parte, que tal normativa tienen por efecto que la conservación de los datos de tráfico y de localización constituya la norma, mientras que el sistema instaurado por la Directiva 2002/58 exige que dicha conservación de datos sea la excepción, y, por otra parte, que «*una normativa nacional* […] *que cubre de manera generalizada a todos los abonados y usuarios registrados y que tiene por objeto todos los medios de comunicación electrónica así como todos los datos de tráfico, no establece ninguna diferenciación, limitación o excepción en función del objetivo que se pretende lograr. Esta normativa afecta globalmente a todas las personas que hacen uso de servicios de comunicaciones electrónicas, aunque no se encuentren, ni siquiera indirectamente, en una situación que justifique una acción penal. Por tanto, esa normativa se aplica incluso a las personas de las que no existe ningún indicio para pensar que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves. Además, no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas a secreto profesional conforme al Derecho nacional (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartados 57 y 58).*

106. Una normativa de este tipo no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública. En particular, no está limitada a una conservación de datos referentes a un período temporal, una zona geográfica o un círculo de personas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la lucha contra la delincuencia (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 59).

107. Una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta.

108. En cambio, el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, no se opone a que un Estado miembro adopte una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido.

109. Para cumplir los requisitos enumerados en el apartado anterior de la presente sentencia, dicha normativa nacional debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a 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 (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 54 y jurisprudencia citada).

110. En segundo lugar, en relación con los requisitos materiales que debe cumplir una normativa nacional que permita, en el contexto de la lucha contra la delincuencia, la conservación con carácter preventivo de datos de tráfico y de localización, para garantizar que se limita a lo estrictamente necesario, debe señalarse que, si bien tales requisitos pueden variar en función de las medidas adoptadas a efectos de la prevención, investigación, descubrimiento y persecución de la delincuencia grave, la conservación de los datos debe responder en todo caso 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.

111. Por lo que se refiere a la delimitación de una medida de este tipo en cuanto al público y a las situaciones potencialmente afectadas, 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. Tal delimitación puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas.

112. Habida cuenta de las anteriores consideraciones, procede responder a la primera cuestión prejudicial en el asunto C-203/15 que el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica».

A la segunda cuestión prejudicial en el asunto C-203/15 y a la primera cuestión prejudicial en el asunto C-698/15, el Tribunal de Justicia respondió que el artículo 15, apartado 1, de la Directiva 2002/58/CE, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta, debe interpretarse «*en el sentido de que se opone 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» (apartado 125).

61 Por su parte, el TEDH se pronunció entretanto sobre la normativa sueca relativa a la interceptación masiva de comunicaciones electrónicas con arreglo al artículo 8 del Convenio Europeo de los Derechos Humanos, en su sentencia *Centrum for Rättvisa c. Suecia*, de 19 de junio de 2018. En particular, declaró lo siguiente:

«*El Tribunal ha expresamente reconocido que las autoridades nacionales disponen de un amplio margen de apreciación para elegir los medios para proteger la seguridad nacional* […]. *En los asuntos Weber y Saravia y Liberty y otros, el Tribunal admitió que las reglas de interceptación masiva no rebasaban, en sí, ese margen. Habida cuenta del razonamiento del Tribunal en esas sentencias y de las amenazas que actualmente enfrentan numerosos Estados parte (en particular el terrorismo mundial y otras formas graves de delincuencia, como el tráfico de drogas, la trata de personas, la explotación sexual de los menores y la ciberdelincuencia), de las mejoras tecnológicas que han permitido a los terroristas y a los delincuentes eludir más fácilmente su detección en Internet y de la imposibilidad de prever las vías por las que se transmiten las comunicaciones electrónicas, el Tribunal considera que la decisión de recurrir a un sistema de interceptación masiva para identificar amenazas para la seguridad nacional hasta hoy desconocidas es una decisión que está comprendida en el margen de discrecionalidad de los Estados*» (TEDH, 19 de junio de 2018, Centrum for Rättvisa c. Suecia, § 112).

Sin embargo, el mismo TEDH declaró que la normativa inglesa relativa a la interceptación de las comunicaciones constituía una vulneración del artículo 8 del CEDH, puesto que no cumplía los criterios enunciados en su jurisprudencia. Consideró asimismo que «*en principio, pertenece al ámbito de la facultad discrecional del Estado establecer el funcionamiento de los regímenes de interceptación masiva. La interceptación masiva, por definición, es de carácter no selectivo, y supeditarla a la existencia de una "sospecha razonable" impediría su ejercicio*» (TEDH, 13 de septiembre de 2018, Big Brother Watch y otros c. Reino Unido, § 317).

62 Se plantea la cuestión de saber en qué medida la jurisprudencia citada, que se refiere a la conservación generalizada e indiferenciada de datos en materia de comunicaciones electrónicas, puede extrapolarse a la recogida, la transferencia y el tratamiento generalizados e indiferenciados de los datos de los pasajeros, según se encuentran regulados por la Ley de 25 de diciembre de 2016.

63 En su dictamen 1/15, antes citado, de 26 de julio de 2017, el Tribunal de Justicia se pronunció sobre un sistema PNR análogo, si bien con un ámbito de aplicación más reducido, puesto que el proyecto de Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros preveía la «*transferencia sistemática y continua de los datos del PNR de la totalidad de los pasajeros aéreos que tomen vuelos entre la Unión y Canadá*» (apartado 127). Consideró que «*la transferencia de los datos del PNR a Canadá y los tratamientos posteriores de estos pueden considerarse idóneos para lograr el objetivo perseguido por el Acuerdo previsto consistente en garantizar la protección y la seguridad públicas*» (apartado 153).

En lo que se refiere a los pasajeros afectados, el Tribunal de Justicia estimó lo siguiente:

«*186.El Acuerdo previsto abarca los datos del PNR de la totalidad de los pasajeros aéreos que tomen vuelos entre la Unión y Canadá. La transferencia de esos datos a Canadá se lleva a cabo con independencia de cualquier elemento objetivo que permita considerar que los pasajeros pueden presentar un riesgo para la seguridad pública en Canadá.*

187. A este respecto, es de señalar que, como se ha recordado en los apartados 152 y 169 del presente dictamen, los datos del PNR están principalmente destinados a someterse a un tratamiento automatizado. Pues bien, como han expuesto diversos intervinientes, ese tratamiento tiene por objeto identificar el riesgo para la seguridad pública que podrían presentar personas que, hasta ese momento, no son conocidas por los servicios competentes y que, debido a ese riesgo, podrían ser sometidas a un examen exhaustivo. En este sentido, el tratamiento automatizado de esos datos previamente a la llegada de los pasajeros a Canadá facilita y acelera los controles de seguridad, especialmente en las fronteras. Por otra parte, la exclusión de determinadas categorías de personas o de determinadas zonas de origen podría obstaculizar la realización del objetivo del tratamiento automatizado de los datos del PNR, que es la identificación, mediante la comprobación de esos datos, de aquellas personas que puedan presentar un riesgo para la seguridad pública entre el conjunto de los pasajeros aéreos, y permitir que se eludiese esa comprobación.

188. Por lo demás, con arreglo al artículo 13 del Convenio de Chicago, al que se han referido en particular el Consejo y la Comisión en sus respuestas a las preguntas formuladas por el Tribunal de Justicia, todos los pasajeros aéreos deben, a la entrada, en el interior y a la salida del territorio de un Estado contratante, cumplir las leyes y reglamentos de ese Estado relativos a la entrada o la salida de los pasajeros aéreos de su territorio. La totalidad de los pasajeros aéreos que deseen entrar o salir de Canadá están por tanto sujetos, en virtud de dicho artículo, a los controles fronterizos y obligados a cumplir los requisitos de entrada y de salida prescritos por el Derecho canadiense vigente. Además, como se desprende de los apartados 152 y 187 del presente dictamen, la identificación, mediante los datos del PNR, de los pasajeros que puedan presentar un riesgo

para la seguridad pública forma parte de los controles fronterizos. Por consiguiente, dado que son objeto de dichos controles, los pasajeros aéreos que deseen entrar y permanecer en Canadá están, por la propia naturaleza de esa medida, sujetos a la comprobación de sus datos del PNR.

189. En tales circunstancias, no consta que el Acuerdo previsto exceda de lo estrictamente necesario por cuanto permite la transferencia de los datos del PNR de la totalidad de los pasajeros aéreos a Canadá».

64 La Cour constitutionnelle se pregunta si estas consideraciones pueden hacerse extensivas respecto a la Directiva PNR y a una normativa nacional, como la Ley PNR, la cual, al incorporar la Directiva PNR al Derecho nacional, establece un sistema para la recogida, la transferencia y la utilización generalizadas e indiferenciadas de los datos «PNR» de todos los pasajeros que utilicen el transporte aéreo, ferroviario o de autobús para viajar, con independencia del cruce de los pasos fronterizos exteriores de la Unión. En efecto, dicho sistema se aplica a personas respecto a las que no existe ningún indicio para presumir que su comportamiento pueda tener una relación, incluso indirecta o remota, con la comisión de delitos graves y es más amplio que el sistema que se establece mediante el Acuerdo «PNR» con Canadá. Habida cuenta de la amplitud de los datos a que se refiere dicha Ley, se plantea la cuestión de si esta medida respeta los límites de lo «estrictamente necesario». Antes de resolver en cuanto al fondo, la Cour constitutionnelle decide, por tanto, plantear al Tribunal de Justicia una cuarta cuestión prejudicial.

Sobre los fines del tratamiento de los datos «PNR» (artículo 8 de la Ley PNR)

65 La parte recurrente critica la definición de los fines del tratamiento de los datos «PNR», contenida en el artículo 8 de la Ley PNR, que es mucho más amplia que la correspondiente a los «fines específicos», los cuales, por su parte, únicamente se refieren a los delitos de terrorismo y la delincuencia grave que menciona la Directiva PNR. Estima que dichos fines exceden los límites de lo «estrictamente necesario».

Los fines del tratamiento de los datos «PNR», que figuran en los artículos 1, apartado 2, y 6, apartado 2, de la Directiva PNR, constituyen únicamente objetivos de prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (véase asimismo el considerando 7 de la Directiva PNR).

Algunos de los fines del tratamiento de datos a que se refiere el artículo 8 de la Ley PNR corresponden a los delitos que se enumeran en el anexo II de la Directiva PNR, en consonancia con los objetivos de prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y de la delincuencia grave que persigue dicha Directiva. Sin embargo, la referida Ley incorpora fines del tratamiento de los datos «PNR» que son adicionales a los contemplados por la Directiva. Así sucede, por ejemplo, en lo que respecta al «seguimiento de las

actividades enumeradas en los artículos 7, puntos 1.º y 3.º/1, y 11, apartado 1, puntos 1.º a 3.º y 5.º, de la Ley Orgánica de 30 de noviembre de 1998 relativa a los servicios de inteligencia y seguridad» (artículo 8, apartado 1, punto 4.º).

El órgano jurisdiccional remitente examina si estos otros fines se encuentran contemplados en normas claras, precisas y limitadas a lo estrictamente necesario y alberga dudas en lo que respecta al fin a que se refiere el artículo 8, apartado 1, punto 4.º, de la Ley PNR.

La exposición de motivos de la Ley PNR indica que este «fin guarda relación con las competencias de los servicios de inteligencia, a saber, la Sûreté de l'État (Servicio de Seguridad del Estado) y el Service général de Renseignement et de Sécurité (Servicio General de Inteligencia y Seguridad; SGRS). Para llevar a cabo sus tareas de investigación, análisis y tratamiento de la información relativa a las actividades que pueden suponer una amenaza para los intereses fundamentales del Estado, dichos servicios deben poder analizar los datos de los pasajeros con objeto de detectar lo antes posible amenazas concretas, llevar a cabo el seguimiento de los desplazamientos de personas concretas o elaborar análisis de fenómenos o tendencias de más amplio alcance. Las actividades relativas a la investigación, el análisis y el tratamiento de la información relativa a las actividades de los servicios de inteligencia extranjeros en el territorio belga están comprendidas en este fin» (Doc. parl., Cámara, 2018-2019, DOC 54-3652/001, pp. 19-20).

Si bien las actividades de los servicios de inteligencia y de seguridad contribuyen, con carácter general, a la seguridad nacional e internacional, el tratamiento de los datos «PNR» con arreglo al fin a que se refiere el artículo 8, apartado 1, punto 4.º, de la Ley PNR parece muy vago y genérico.

Este fin, además, en lo que se refiere a la evaluación previa de los pasajeros, recibe el mismo trato que los fines que figuran en el artículo 8, apartado 1, puntos 1.º, 2.º y 5.º, de la Ley PNR (artículos 24, apartado 2, y 26, apartado 2).

En estas circunstancias, la Cour constitutionnelle decide plantear al Tribunal de Justicia una quinta cuestión prejudicial al efecto de dilucidar si dicho fin está redactado de manera suficientemente clara y precisa y se limita a lo estrictamente necesario.

Sobre la gestión del banco de datos de los pasajeros y el tratamiento de datos en el marco de la evaluación previa de los pasajeros y de las investigaciones puntuales (artículos 16, 24 a 27, 50 y 51 de la Ley PNR)

66 La parte recurrente estima que los diferentes tratamientos y flujos de datos personales son manifiestamente desproporcionados.

67 El artículo 16 de la Ley PNR establece que, en el marco de los fines que se enuncian en el artículo 8, apartado 1, los datos de los pasajeros son objeto de los tratamientos a que se refieren los artículos 24 a 27.

– *Evaluación previa de los pasajeros (artículos 24 a 26)*

68 Los datos de los pasajeros son tratados con el fin de efectuar una evaluación previa (*pre-screening)* de los pasajeros antes de su entrada en el territorio nacional, su salida de dicho territorio o su paso por este, a efectos de determinar qué personas deben ser objeto de un control adicional. «Se trata de evaluar la posible amenaza y determinar qué pasajeros son objeto de interés para la actuación de estos servicios o, por ejemplo, han de ser objeto de medidas (ejecución de una orden de detención, registro, etc.)». (Doc. parl., Cámara, 2018-2019, DOC 54-3652/001, p. 28).

La evaluación previa se asienta en dos pilares: por una parte, la correlación entre los datos de los pasajeros y los bancos de datos, y, por otra parte, la correlación entre los datos y ciertos criterios predeterminados.

69 En lo que respecta a la correlación con los bancos de datos, los trabajos preparatorios de la Ley PNR indican que «el primer pilar consiste en la búsqueda de resultados positivos mediante la detección de correlaciones entre los datos de los pasajeros y los datos tratados en los bancos de datos gestionados por los servicios competentes. Ello permite, por ejemplo, evaluar si una persona presenta un grado elevado de peligrosidad, al estar fichada en un banco de datos policial en el marco de un expediente terrorista y al desprenderse de sus datos de pasajero que se desplaza con regularidad a países que albergan campos de entrenamiento de terroristas o a países de tránsito hacia tales emplazamientos. También puede tratarse de una persona respecto a la cual la información de que disponen los servicios de inteligencia indica que está preparando una toma de rehenes y que, a la luz de los datos del transporte, se desplaza a un país cuyos servicios de inteligencia saben, sobre la base de la información recibida, que dicha persona podría reclutar a personas en ese país con el fin de ejecutar sus planes. Además, cuantos más resultados positivos detecten los distintos servicios con respecto a una misma persona, más real será la probabilidad de que exista la amenaza de que se trate.

Los resultados positivos también pueden desencadenar la necesidad de la adopción de alguna medida por parte de las autoridades judiciales, como la ejecución de una orden de detención de una persona que se dispone a abandonar el territorio de Bélgica.

Por otro lado, los resultados positivos pueden resultar de una correlación con bases de datos internacionales, como SIS II, Interpol (SLTD).

El objetivo no es, evidentemente, vincular todos los bancos de datos de los distintos servicios con el banco de datos de los pasajeros, sino limitar técnicamente las correlaciones con los bancos de datos que guardan una relación directa con los fines que determina la Ley.

[…]

Las correlaciones podrán establecerse asimismo sobre la base de listados de personas elaborados específicamente por los servicios competentes a estos efectos. De conformidad con la Ley relativa a la protección de la vida privada y, más concretamente, conforme a su artículo 4, apartado 1, punto 4.º, dichos listados deberán ser objeto de actualizaciones periódicas» (Doc. parl., Cámara, 2015-2016, DOC 54-2069/001, pp. 28 y 29).

70 En cuanto atañe a la correlación con criterios predeterminados, los trabajos preparatorios de la Ley PNR disponen lo siguiente:

«El segundo pilar consiste en la búsqueda de resultados positivos mediante la aplicación a los datos de los pasajeros de (uno o varios) criterios predeterminados por la UIP. Dichos criterios están compuestos por uno o varios indicadores objetivos sobre la base de los cuales se puede deducir que las personas que son objeto de la evaluación presentan un comportamiento de riesgo específico que puede constituir una amenaza con arreglo a los fines que figuran en el artículo 8, apartado 1, puntos 1.º, 4.º y 5.º, de la Ley.

Esos criterios pueden englobar, por ejemplo, determinados comportamientos concretos en materia de reserva de viajes o del propio viaje.

La ventaja de su utilización reside en la posibilidad de descubrir perfiles de pasajeros de riesgo que los servicios competentes desconocen o que no constan en los bancos de datos de dichos servicios.

Tales criterios se refieren, por ejemplo, a un país de salida o de llegada, junto a determinada información relativa al viaje, como el medio de pago y la fecha de la reserva» (Doc. parl., Cámara, 2018-2019, DOC 54-3652/001, pp. 29 y 30).

«La evaluación previa efectuada en el marco del fin relativo al seguimiento de fenómenos de relevancia policial y de agrupaciones vinculadas a la radicalización violenta está sujeta a condiciones mucho más restrictivas que los demás fines […] En la evaluación previa efectuada en el marco de los demás fines está permitido el acceso a todos los datos de los pasajeros que se enumeran en el artículo 9» (*ibid.*, p. 31).

«Todo resultado positivo debe ser validado por la UIP. En efecto, para garantizar el pleno respeto del derecho a la protección de datos personales […] no se pueden adoptar decisiones que conlleven consecuencias jurídicas para una persona o que ocasionen a esta un grave perjuicio simplemente sobre la base del tratamiento automatizado de los datos del fichero que contiene información relativa a su viaje. En consecuencia, la evaluación humana precederá en todo caso a la adopción de cualquier decisión vinculante para la persona afectada.

Para acceder al banco de datos de los pasajeros, dicha validación deberá efectuarse en un plazo de 24 horas.

Una vez validado el resultado positivo, los servicios que lo hayan detectado deberán garantizar un seguimiento eficaz y adecuado del mismo. Ese seguimiento eficaz puede consistir en una intervención activa (registro, detención, etc.), pero también puede implicar la abstención con carácter provisional de este tipo de intervención. Corresponderá exclusivamente a los servicios competentes determinar el procedimiento operativo» (*ibid*., pp. 30 y 31).

71 En cuanto a los criterios de evaluación predeterminados por la UIP, no podrán basarse en datos que pongan de manifiesto 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. La evaluación de los pasajeros antes de su entrada en territorio nacional, su salida desde este o su paso por él a la luz de criterios predeterminados se llevará a cabo de manera no discriminatoria. Dichos criterios no podrán tener por objeto la identificación de una persona y deberán ser orientados, proporcionados y específicos.

72 En su dictamen de 19 de agosto de 2016, el Comité Consultivo del Convenio n.º 108 señaló lo siguiente:

«*El tratamiento de datos personales puede afectar a todos los pasajeros y no solo a las personas seleccionadas sospechosas de estar implicadas en un delito penal o de suponer una amenaza inmediata para la seguridad del Estado o para el orden público.*

[…]

La evaluación de los pasajeros mediante el cotejo de datos puede suscitar la cuestión de la previsibilidad, en particular cuando se efectúa sobre la base de algoritmos predictivos que utilizan criterios dinámicos susceptibles de evolucionar permanentemente en función de las capacidades de autoaprendizaje.

El desarrollo de algoritmos de extracción de datos debe basarse en los resultados de evaluaciones periódicas del posible impacto del tratamiento de datos en los derechos y libertades fundamentales de las personas afectadas.

La estructura básica de los análisis debe basarse en indicadores de riesgo claramente establecidos de antemano.

La pertinencia de los resultados individuales de dichas evaluaciones automáticas debe examinarse cuidadosamente caso por caso, por una persona y de forma no automatizada» [dictamen de 19 de agosto de 2016, T-PD(2016)18rev. p. 8].

73 En el caso de autos, los bancos de datos a que se refiere el artículo 24 se encuentran definidos con precisión y guardan una relación directa con los fines que figuran en el artículo 8 de la Ley PNR. En efecto, se trata de bancos de datos de los «servicios competentes», esto es, los servicios de Policía, Seguridad del Estado, Servicio General de Inteligencia y de Seguridad y Aduanas.

Además, el artículo 24, apartados 4 y 5, de la Ley PNR garantiza que, en caso de que se verifique un resultado positivo, el tratamiento sistemático automatizado es objeto de una comprobación individual a través de medios no automatizados, al efecto de apreciar si la autoridad competente debe adoptar medidas en virtud del Derecho nacional, como exige el artículo 6, apartado 5, de la Directiva PNR.

74 En su dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), el Tribunal de Justicia también insistió en la posibilidad de llevar a cabo un nuevo examen individual por medios no automatizados antes de adoptar una medida individual (apartado 173).

La exigencia de la intervención humana, tras producirse un resultado positivo, constituye una garantía susceptible de asegurar que la evaluación previa no se basa únicamente en medios automatizados, y, consecuentemente, contribuye a la eficacia del sistema.

Por consiguiente, una evaluación previa sistemática de los pasajeros constituye, en principio, una medida pertinente habida cuenta del objetivo consistente en identificar y prevenir amenazas para la seguridad pública.

Como declaró, sin embargo, el Tribunal de Justicia en su dictamen 1/15 de 26 de julio de 2017 antes citado, los tratamientos que se derivan de la evaluación previa «*pueden proporcionar información adicional sobre la vida privada de los pasajeros aéreos*» (apartado 131); además, «*dichos análisis se llevan a cabo sin que existan razones basadas en circunstancias individuales que permitan considerar que las personas afectadas podrían suponer un riesgo para la seguridad pública*» (*ibid.*, apartado 132).

Al tiempo que declaró que el tratamiento automatizado de los datos «PNR», basado en modelos y criterios predeterminados, presenta un porcentaje de error no desdeñable (*ibid*, apartados 169 y 170), el Tribunal de Justicia consideró, sin embargo, que «*los modelos y los criterios predeterminados deben ser, por una parte, específicos y fiables, de manera que permitan obtener […] resultados relativos a personas concretas respecto de las que pueda existir una sospecha razonable en cuanto a su implicación en delitos de terrorismo o delitos graves de carácter transnacional y, por otra parte, no discriminatorios*» y que «*las bases de datos con las que se cotejan los datos PNR deben ser fiables, actuales y limitadas a bases de datos utilizadas por Canadá en relación con la lucha contra el terrorismo y los delitos graves de carácter transnacional*» (*ibid*., apartado 172). Por último, para garantizar que la evaluación no presenta un carácter discriminatorio y se limita a lo estrictamente necesario, el Tribunal de Justicia consideró que «*la fiabilidad y la actualidad de dichos modelos y criterios predeterminados y de las bases de datos utilizadas deben ser objeto del examen conjunto resultante de la aplicación del Acuerdo previsto, teniendo en consideración los datos estadísticos y los resultados obtenidos de la investigación de ámbito internacional*», un año después de su entrada en vigor y, en lo sucesivo, con carácter periódico (*ibid*, apartado 174).

75 Por lo demás, parece técnicamente imposible definir de antemano con mayor precisión los criterios que vayan a servir para determinar los perfiles de riesgo. Como se ha expuesto anteriormente, dichos criterios deben ser específicos, fiables y no discriminatorios.

76 Si bien la Directiva PNR y la Ley PNR no contienen indicación alguna en cuanto a la manera en que la UIP establece de antemano los criterios en que ha de basarse la evaluación previa, las garantías que acompañan la elaboración de dichos criterios parecen suficientes para que la medida impugnada no sea considerada desproporcionada. Sin embargo, para determinar si dicha evaluación previa sistemática es suficientemente clara y precisa y se limita a lo estrictamente necesario, procede plantear al Tribunal de Justicia una sexta cuestión prejudicial.

– *Investigaciones puntuales (artículos 27, 50 y 51)*

77 El artículo 27 de la Ley PNR autoriza el tratamiento de datos de los pasajeros para llevar a cabo investigaciones puntuales con los fines indicados en el artículo 8, apartado 1, puntos 1.º, 2.º, 4.º y 5.º, y conforme a las condiciones establecidas en el artículo 46 *septies* del Código de Enjuiciamiento Criminal o en el artículo 16/3 de la Ley de 30 de noviembre de 1998, incorporados respectivamente por los artículos 50 y 51 de la Ley PNR. De conformidad con el artículo 20 de la Ley PNR, los requisitos de aplicación del artículo 27 también se aplican a las peticiones de acceso [a los datos] tras la expiración del plazo de seis meses establecido en el artículo 19.

78 El artículo 46 *septies* del Código de Enjuiciamiento Criminal se refiere a las investigaciones puntuales llevadas a cabo en el marco del fin que figura en el artículo 8, apartado 1, puntos 1.º, 2.º y 5.º, de la Ley PNR. Esta medida lleva aparejada diversas garantías, como la autorización previa del Ministerio Fiscal.

79 El artículo 16/3 de la Ley de 30 de noviembre de 1998 se refiere a las investigaciones puntuales llevadas a cabo en el marco del fin que figura en el artículo 8, apartado 1, punto 4.º, de la Ley PNR. Esta medida lleva aparejada diversas garantías, como la información y el control del Comité Permanente R.

80 La parte recurrente estima que los miembros en comisión de servicios de los servicios de policía que pertenecen a la UIP no gozan de la independencia necesaria para responder a las peticiones de acceso en el marco de dichas investigaciones puntuales.

81 El artículo 14, apartado 1, de la Ley PNR determina la composición de la UIP. A este respecto, los trabajos preparatorios exponen lo siguiente: «*El modelo belga se basa en un concepto de unidad multidisciplinaria integrada por un funcionario directivo que cumple una función de dirección, personal administrativo y personal enviado en comisión de servicios procedente de los servicios competentes.*

La UIP estará integrada por:

– *un funcionario directivo, asistido por un servicio de apoyo que, en el Servicio Público Federal de Interior, se encargará de supervisar, en particular, la gestión del banco de datos, el cumplimiento de las obligaciones que incumben a las compañías de transporte y los operadores de viajes, la rendición de informes, la celebración de protocolos con los servicios competentes y el cumplimiento de los requisitos del tratamiento de datos. El servicio de apoyo estará integrado principalmente por analistas, juristas, expertos de TIC y por el responsable de la protección de datos, quienes dispondrán de las habilitaciones de seguridad necesarias.*

– *personal enviado en comisión de servicios procedente de los servicios competentes taxativamente enumerados en el punto 2 del apartado 1, a saber: los servicios de policía, los servicios de inteligencia y los servicios de aduanas. Los fines específicos constituyen como tales la primera limitación. Por ejemplo, en el ámbito de los servicios de la unidad de policía integrada, es evidente que en ningún caso podrá un policía de barrio de la policía local conocer datos de los pasajeros, puesto que los fines en cuestión no entran en el ámbito de sus competencias.*

El envío en comisión de servicios de personal de los servicios competentes tiene por objeto garantizar un nivel de conocimientos técnicos determinados, pero no excluye en modo alguno la celebración de acuerdos entre estos servicios al efecto de intercambiar personal en comisión de servicios» (Doc. parl., Cámara, 2015-2016, DOC 54-2069/001, p. 22).

El ministre de la Sécurité et de l'Intérieur (Ministro de Seguridad y del Interior) añadió que «*también se nombrará a un* data protection officer *que será responsable de informar a la Commission de la protection de la vie privée (Comisión de la Protección de la Vida Privada)*» (Doc. parl., Cámara, 2015-2016, DOC 54-2069/003, p. 24).

El arrêté royal du 21 décembre 2017 (Real Decreto de 21 de diciembre de 2017) relativo a la ejecución de la Ley PNR establece las modalidades de composición y de organización de la UIP. El informe al Rey que precede a dicho Real Decreto precisa que «*solo podrá consultarse el banco de datos* […] *en la UIP, y únicamente por los miembros de la UIP, en el marco del ejercicio de sus funciones, así como por el responsable de la protección de datos*». [3]

El procedimiento de envío en comisión de servicios se encuentra regulado en los artículos 12 a 21 de este mismo Real Decreto. El hecho de que las personas enviadas en comisión de servicios procedentes de los servicios competentes intervengan en el funcionamiento de la UIP tiene por objeto garantizar que dicha UIP esté integrada por personal que posea unos conocimientos técnicos

[3] *Moniteur belge* de 29 de diciembre de 2017, segunda edición, p. 116833.

determinados, para de este modo reforzar la eficacia de la UIP. Esta posibilidad de envío en comisión de servicios está, por otro lado, expresamente prevista por el artículo 4, apartado 3, de la Directiva PNR.

No hay nada que permita considerar que dichas personas, aun cuando conserven su estatuto en el servicio del que proceden, no ejercen sus funciones en la UIP con independencia. Los miembros de la UIP están además sujetos a sanciones penales en el supuesto de que no respeten el secreto profesional o de que retengan consciente y voluntariamente información o datos que comprometan los fines establecidos en el artículo 8 (artículos 48 y 49).

82 En lo que atañe al acceso a los datos «PNR» en el marco de investigaciones puntuales tras la expiración de un plazo de seis meses, el Tribunal de Justicia consideró, en su dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (EU:C:2017:592), que la utilización de los datos PNR así almacenados debe «*basarse en criterios objetivos que definan las circunstancias y las condiciones en que las autoridades canadienses contempladas en el Acuerdo previsto están autorizadas para utilizarlos*» y que, «*salvo en casos de urgencia debidamente justificados, la utilización de dichos datos ha de estar supeditada a un control previo efectuado bien por un órgano judicial, bien por una entidad administrativa independiente que adopte su decisión de autorización sobre la base de una petición razonada de las referidas autoridades, presentada, en particular, en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos*» (apartado 208).

83 A efectos de comprobar si la UIP puede ser considerada como esa «otra autoridad nacional competente» en el sentido del artículo 12, apartado 3, de la Directiva PNR, procede, con carácter previo a un pronunciamiento, plantear al Tribunal de Justicia una séptima cuestión prejudicial.

Sobre el período de conservación de los datos «PNR» (artículo 18 de la Ley PNR)

84 La parte recurrente considera que el período de cinco años durante el cual se conservan los datos «PNR» es desproporcionado.

85 El considerando 25 de la Directiva PNR dispone:

«El período durante el cual deben conservarse los datos PNR debe ser el necesario y debe ser proporcional a las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves. Dada la naturaleza de los datos y su utilización, es necesario que los datos PNR se conserven durante un período suficientemente largo para realizar análisis y utilizarlos en las investigaciones. Para evitar una utilización desproporcionada es necesario que, después del período inicial de conservación, los datos PNR se despersonalicen mediante enmascaramiento de elementos de los datos. Con el fin de garantizar el más alto nivel de protección de datos, el acceso al conjunto total de datos PNR,

que permiten la identificación directa del interesado, solo debe poder autorizarse en condiciones muy estrictas y limitadas tras dicho período inicial.»

86 Según la jurisprudencia del Tribunal de Justicia, el período de conservación de los datos debe «responder en todo caso a criterios objetivos y ha de existir una relación entre los datos personales que deban conservarse y el objetivo que se pretende lograr» [sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 93; auto de 16 de marzo de 2017, Tele2 Sverige y Watson y otros, C-203/15 REC y C-698/15 REC, EU:C:2017:222, apartado 110; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 191].

87 En cuanto atañe más concretamente a los datos «PNR», el Tribunal de Justicia consideró, en su dictamen 1/15, antes citado, de 26 de julio de 2017, que la duración de cinco años «*no parece exceder los límites de lo estrictamente necesario a efectos de la lucha contra el terrorismo y contra los delitos graves de carácter transnacional*» (apartado 209), con la salvedad de que «*en lo que se refiere a los pasajeros aéreos respecto de los cuales no se haya identificado tal riesgo a su llegada a Canadá ni hasta su partida de dicho país tercero, no parece que exista, una vez que hayan abandonado el país, relación alguna, siquiera indirecta, entre sus datos del PNR y el objetivo perseguido por el Acuerdo previsto que justifique […] un almacenamiento continuado de los datos del PNR de la totalidad de los pasajeros aéreos después de su partida de Canadá a efectos del eventual acceso a dichos datos, con independencia de todo vínculo con la lucha contra el terrorismo y los delitos graves de carácter transnacional (véase, por analogía, la 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 119)*» (apartado 205).

88 El artículo 18 de la Ley PNR establece que los datos de los pasajeros se conservarán en el banco de datos de los pasajeros por un período máximo de cinco años a partir de su registro y que, tras la expiración de dicho período, se destruirán. De conformidad con el artículo 21, apartado 1, de esta misma Ley, la UIP se asegurará de que los datos de los pasajeros sean borrados de su banco de datos con carácter definitivo al finalizar el período establecido en el artículo 18.

No obstante, el período de cinco años ha de entenderse en relación con los artículos 19 y siguientes de la referida Ley, los cuales regulan asimismo las modalidades de conservación de los datos. El propio artículo 19 debe leerse en combinación con el artículo 4, punto 14.º, que establece que la definición de la expresión «despersonalización mediante enmascaramiento de elementos de los datos» es «hacer invisibles para un usuario aquellos elementos de los datos que servirían para identificar directamente al interesado, como indica el artículo 19».

El artículo 20 de la Ley PNR establece que, tras la expiración del período de seis meses a que se refiere el artículo 19, solo se permitirá la divulgación de los datos PNR completos para el tratamiento de los datos prescrito por el artículo 27 y únicamente con arreglo a las condiciones establecidas en dicha disposición.

Por otro lado, los resultados del tratamiento a que se refiere el artículo 24 serán conservados por la UIP únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y a las UIP de otros Estados miembros (artículo 21, apartado 3, párrafo primero).

El artículo 22 de la PNR garantiza que el funcionario directivo y el responsable de la protección de datos solo tendrán acceso a todos los datos pertinentes en el marco del desempeño de sus funciones.

Por último, el tratamiento de datos es objeto de registro y guarda una relación directa con los fines establecidos en el artículo 8 (artículo 23, apartado 1). La UIP velará por dicho registro conservando durante cinco años la documentación relativa a todos los sistemas y procedimientos de tratamiento aplicados bajo su responsabilidad (artículo 23, apartado 2, párrafo primero).

89 El período de conservación de los datos de los pasajeros deberá determinarse tomando en consideración los fines del tratamiento de dichos datos, en relación directa con las finalidades de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves.

90 La Comisión de la Protección de la Vida Privada declaró, sin embargo, que, cuando el período de conservación de los datos es largo y los datos son almacenados en masa, «aumenta el riesgo de que se elaboren perfiles de las personas afectadas, así como el riesgo de desviación del fin del tratamiento (*fonction creep*), es decir, la desviación potencial de la utilización de datos en relación con otros delitos respecto a los cuales no existía inicialmente un acuerdo (político) de intercambio de datos» [Comisión de Protección de la Vida Privada, dictamen de iniciativa n.º 01/2010 de 13 de enero de 2010 relativo al proyecto de ley por la que se aprueba el Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (Acuerdo PNR 2007)], hecho en Bruselas el 23 de julio de 2007 y en Washington el 26 de julio de 2007, punto 3.3, pp. 17 y 18).

En su dictamen n.º 55/2015 de 16 de diciembre de 2015 sobre el anteproyecto de ley que pasó a ser la Ley PNR, la Comisión de Protección de la Vida Privada estimó también que la necesidad de conservar los datos durante un período de cinco años debía justificarse de manera más precisa y razonada.

En su dictamen de 19 de agosto de 2016, el Comité Consultivo del Convenio n.º 108 también señaló que «los datos enmascarados pueden servir para identificar a las personas y continúan siendo en este aspecto datos personales, y que su conservación debe limitarse en el tiempo a efectos de evitar una vigilancia permanente generalizada» [dictamen de 19 de agosto de 2016, T-PD(2016)18rev, p. 9].

91 La Cour constitutionnelle considera que para comprobar si, habida cuenta de las consideraciones anteriores y de las diversas garantías que se enumeran en el apartado 88 anterior, dicho período de conservación de cinco años, autorizado por la Directiva PNR, es compatible con las observaciones del Tribunal de Justicia mencionadas en el apartado 87 anterior, dado que, en el marco de la evaluación previa, no se distingue a los pasajeros afectados en función de si pueden o no suponer un riesgo para la seguridad pública, es preciso plantear al Tribunal de Justicia una octava cuestión prejudicial.

3. Sobre el segundo motivo de recurso

92 La parte recurrente estima que al hacer extensivo el sistema «PNR» a los vuelos interiores de la UE, las disposiciones impugnadas restablecen indirectamente controles en las fronteras que son contrarios a la libre circulación de las personas.

93 En lo que se refiere al ámbito de aplicación de la Ley PNR, en los trabajos preparatorios se expone lo siguiente:

«La inclusión [de los vuelos] interiores de la UE en la recogida de datos permitirá obtener una imagen más completa de los desplazamientos de los pasajeros que representan una posible amenaza para la seguridad intracomunitaria y nacional. La práctica ya ha demostrado que determinados "*returnees*" (también llamados *foreign fighters* que regresan a Europa) embarcan a bordo de diferentes vuelos antes de alcanzar su destino final.

La Directiva UE PNR ofrece expresamente a los Estados miembros la posibilidad de tratar los datos de los pasajeros de la Unión en relación con el tráfico internacional dentro de la Unión Europea. Además, todos los Estados miembros aprobaron, el 21 de abril de 2016 en el Consejo de Justicia y Asuntos de Interior, una declaración de transposición de la Directiva PNR a los ordenamientos jurídicos nacionales también en lo que se refiere al tráfico dentro de la Unión Europea» (Doc. parl., Cámara, 2015-2016, DOC 54-2069/001, p. 7).

94 La Cour constitutionnelle señala que los pasajeros a que se refiere el capítulo 11 de la Ley PNR, así como los datos y el período de conservación contemplados, son limitados.

En los trabajos preparatorios se indica, en efecto, que «[…] solo se verán afectados los pasajeros que deseen cruzar o hayan cruzado las fronteras exteriores de Bélgica para entrar o salir del territorio de este Estado, y ello independientemente del tipo de transporte utilizado (marítimo, ferroviario, terrestre, aéreo). Solo los datos de dichos pasajeros serán tratados por los servicios de policía encargados del control en las fronteras y por la Oficina de Extranjería.

También se verá afectados los pasajeros que pretendan pasar por la zona internacional de tránsito, por ejemplo, de un aeropuerto situado en Bélgica en la medida en que también se aplica a dichos pasajeros la normativa sobre la entrada

en territorio belga, la estancia, la residencia y la expulsión de extranjeros. En este sentido, estas personas deben disponer de los documentos de viaje necesarios. Algunas personas están sujetas a la obligación de visado de tránsito aeroportuario; en esta zona están autorizados los controles y, en determinados casos, estos pueden implicar la adopción de medidas de devolución.

[…] en virtud del presente capítulo solo se transmitirán a los servicios de policía y a la Oficina de Extranjería los llamados datos "API". Dichos datos se encuentran enumerados en el artículo 9, apartado 2, del anteproyecto de Ley.

Corresponden, en esencia, a los datos que las compañías aéreas ya están obligadas a transmitir en virtud del arrêté royal du 11 décembre 2006 (Real Decreto de 11 de diciembre de 2006).

[…]

El tiempo de utilización de los datos también está limitado a veinticuatro horas. Transcurrido ese tiempo, si la Oficina de Extranjería necesitara acceder a los datos de los pasajeros en el marco del ejercicio de sus funciones legales, remitirá a la UIP una petición razonada» (*ibid*., pp. 34 y 35).

95 Como se ha expuesto anteriormente, el considerando 10 de la Directiva PNR autoriza a hacer extensivo el sistema «PNR» a los vuelos interiores de la UE. El artículo 2 de la Directiva PNR regula el procedimiento por el que se amplía el ámbito de aplicación.

El fin de combatir la inmigración ilegal y mejorar los controles fronterizos solo se refiere a las categorías de pasajeros enunciadas en el artículo 29, apartado 2, de la Ley PNR, y se limita a los datos «API» que contempla el artículo 9, apartado 1, punto 18.º, de esta misma Ley. Los tratamientos efectuados en el marco de este fin también son limitados. Las disposiciones impugnadas se inscriben en el contexto de la transposición de la Directiva «API», que también persigue los objetivos de combatir la inmigración ilegal y mejorar los controles fronterizos.

96 Sin embargo, en su dictamen n.º 55/2015 de 16 de diciembre de 2015 sobre el anteproyecto de ley que pasó a ser la Ley PNR, la Comisión de Protección de la Vida Privada se pregunta si el principio de la libre circulación es compatible con el sistema «PNR» aplicado, que tiene por objeto «tanto los transportes con destino y salida en el espacio Schengen (extra-Schengen) como los transportes que tienen lugar dentro del espacio Schengen (intra-Schengen)», lo que puede desembocar «indirectamente en un restablecimiento de los controles en las fronteras interiores» (puntos 21 a 25).

97 Al albergar dudas en cuanto a la interpretación y la validez de la Directiva 2004/82 «API» a la luz de la Carta y del TUE, la Cour constitutionnelle decide plantear una novena cuestión prejudicial al Tribunal de Justicia.

98 La Cour constitutionnelle plantea una última cuestión prejudicial relativa a la eventual regulación de los efectos de su sentencia en el tiempo.

IV. Cuestiones prejudiciales

La Cour constitutionnelle plantea, por consiguiente, las siguientes cuestiones prejudiciales:

1) ¿Debe interpretarse el artículo 23 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 — RGPD), en relación con el artículo 2, apartado 2, letra d), de dicho Reglamento, en el sentido de que se aplica a una normativa nacional como la loi du 25 décembre 2016 relative au traitement des données des passagers (Ley de 25 de diciembre de 2016, relativa al tratamiento de datos de los pasajeros), que transpone 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, la 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, y la Directiva 2010/65/UE del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, sobre las formalidades informativas exigibles a los buques a su llegada o salida de los puertos de los Estados miembros y por la que se deroga la Directiva 2002/6/CE?

2) ¿Es el anexo I de la Directiva (UE) 2016/681 compatible con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, en la medida en que los datos que enumera son muy amplios —en particular, los datos a que se refiere el punto 18 del anexo I de la Directiva (UE) 2016/681, que van más allá de los enunciados en el artículo 3, apartado 2, de la Directiva 2004/82/CE— y en la medida en que, considerados conjuntamente, podrían revelar datos sensibles y, en consecuencia, sobrepasar los límites de lo «estrictamente necesario»?

3) ¿Son los puntos 12 y 18 del anexo I de la Directiva (UE) 2016/681 compatibles con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, en la medida en que, habida cuenta de los términos «incluida» e «incluidos», los datos a que se refieren se enuncian a modo de ejemplo y no con carácter taxativo, de manera que no cumplen los requisitos de claridad y precisión de las normas que constituyen una injerencia en el derecho al respeto de la vida privada y en el derecho a la protección de los datos personales?

4) ¿Son compatibles el artículo 3, punto 4, de la Directiva (UE) 2016/681 y el anexo I de esta misma Directiva con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, en la medida en que el sistema de recogida, transmisión y tratamiento generalizados de datos de los pasajeros instaurado por dichas disposiciones afecta a toda persona que utilice el medio de transporte de que se trate, al margen de cualquier elemento objetivo que permita considerar que esa persona puede suponer un riesgo para la seguridad pública?

5) ¿Debe interpretarse el artículo 6 de la Directiva (UE) 2016/681, en relación con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea en el sentido de que se opone a una normativa nacional como la Ley impugnada, la cual permite, como fin del tratamiento de los datos «PNR», el seguimiento de las funciones desempeñadas por los servicios de inteligencia y de seguridad, integrando en este sentido dicho fin en la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave?

6) ¿Es compatible el artículo 6 de la Directiva (UE) 2016/681 con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, en la medida en que la evaluación previa que regula, a través de una correlación con las bases de datos y criterios predeterminados, se aplica de manera sistemática y generalizada a los datos de los pasajeros, al margen de cualquier elemento objetivo que permita considerar que dichos pasajeros pueden suponer un riesgo para la seguridad pública?

7) ¿Puede interpretarse el concepto de «otra autoridad nacional competente» a que se refiere el artículo 12, apartado 3, de la Directiva (UE) 2016/681 en el sentido de que se refiere a la UIP creada por la Ley de 25 de diciembre de 2016, la cual, en consecuencia, podría aprobar el acceso a los datos «PNR», transcurrido un período de seis meses, en el marco de investigaciones puntuales?

8) ¿Debe interpretarse el artículo 12 de la Directiva (UE) 2016/681, en relación con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea en el sentido de que se opone a una normativa nacional como la Ley impugnada que establece, con carácter general, un período de conservación de los datos de cinco años, sin distinguir si, conforme al resultado obtenido en el marco de la evaluación previa, los pasajeros afectados pueden suponer o no un riesgo para la seguridad pública?

9) a) ¿Es la Directiva 2004/82/CE compatible con el artículo 3, apartado 2, del Tratado de la Unión Europea y con el artículo 45 de la Carta de los Derechos Fundamentales de la Unión Europea, en la medida en que las obligaciones que establece se aplican a los vuelos interiores de la Unión Europea?

b) ¿Debe interpretarse la Directiva 2004/82/CE, en relación con el artículo 3, apartado 2, del Tratado de la Unión Europea y con el artículo 45 de la Carta de los Derechos Fundamentales de la Unión Europea, en el sentido de que se opone a una normativa nacional como la Ley impugnada, la cual, a efectos de combatir la inmigración ilegal y mejorar los controles en las fronteras, autoriza un sistema de recogida y de tratamiento de los datos de los pasajeros «con destino o procedencia en el territorio nacional o en tránsito por dicho territorio», lo que puede implicar indirectamente un restablecimiento de los controles en las fronteras interiores?

10) En caso de que, sobre la base de las respuestas a las cuestiones prejudiciales anteriores, la Cour constitutionnelle concluya que la Ley impugnada, que transpone en particular la Directiva (UE) 2016/681, incumple una o varias de las obligaciones que se derivan de las disposiciones mencionadas en dichas cuestiones prejudiciales, ¿puede este órgano jurisdiccional mantener provisionalmente los efectos de la Ley de 25 de diciembre de 2016, relativa al tratamiento de los datos de los pasajeros, con objeto de evitar la inseguridad jurídica y permitir que los datos recogidos y almacenados previamente puedan seguir utilizándose para los fines previstos por dicha Ley?