Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. GIOVANNI PITRUZZELLA
presentadas el 27 de enero de 2022 [1]

Asunto C-817/19

Ligue des droits humains
contra
Conseil des ministres

[Petición de decisión prejudicial planteada por la Cour constitutionnelle (Tribunal Constitucional, Bélgica)]

«Procedimiento prejudicial — Protección de los datos de carácter personal — Tratamiento de los datos del registro de nombres de los pasajeros (PNR) — Reglamento (UE) 2016/679 — Ámbito de aplicación — Directiva (UE) 2016/681 — Validez — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y artículo 52, apartado 1»

Índice

I. Introducción 3

II. Marco jurídico 4

A. Derecho de la Unión 4

1. Carta 4

2. RGPD 5

3. Directiva PNR 5

4. Otros actos pertinentes del Derecho de la Unión 8

B. Derecho belga 8

C. Litigio principal, cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia 10

[1] Lengua original: francés.

III. Análisis . . . 13

A. Sobre la primera cuestión prejudicial . . . 13

B. Sobre las cuestiones prejudiciales segunda, tercera, cuarta, sexta y octava . . . 20

1. Sobre los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta . . . 20

2. Sobre la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta . . . 22

3. Sobre la justificación de la injerencia dimanante de la Directiva PNR . . . 26

a) Sobre el cumplimiento del requisito de que cualquier limitación al ejercicio de un derecho fundamental previsto por la Carta debe estar establecida por la ley . . . 27

b) Sobre el respeto del contenido esencial de los derechos consagrados en los artículos 7 y 8 de la Carta . . . 28

c) Sobre el cumplimiento del requisito de que la injerencia debe favorecer el interés general . . . 31

d) Sobre el respeto del principio de proporcionalidad . . . 32

1) Sobre la idoneidad de los tratamientos de los datos PNR a que se refiere la Directiva PNR en relación con el objetivo perseguido . . . 33

2) Sobre el carácter estrictamente necesario de la injerencia . . . 34

i) Sobre la delimitación de los fines del tratamiento de los datos PNR . . . 34

ii) Sobre las categorías de datos PNR mencionadas por la Directiva PNR (cuestiones prejudiciales segunda y tercera) . . . 39

– Sobre el carácter suficientemente claro y preciso de los puntos 12 y 18 del anexo I (tercera cuestión prejudicial) . . . 39

– Sobre el alcance de los datos enumerados en el anexo I (segunda cuestión prejudicial) . . . 47

– Sobre los datos sensibles . . . 50

iii) Sobre el concepto de «pasajero» (cuarta cuestión prejudicial) . . . 53

iv) Sobre el carácter suficientemente claro, preciso y limitado a lo estrictamente necesario de la evaluación previa de los pasajeros (sexta cuestión prejudicial) . . . 60

– Sobre la comparación con bases de datos en el sentido del artículo 6, apartado 3, letra a), de la Directiva PNR . . . 61

– Sobre el tratamiento de los datos PNR con arreglo a criterios predeterminados . . . 63

– Sobre las garantías que lleva aparejado el tratamiento automatizado de los datos PNR 65

– Conclusión sobre la sexta cuestión prejudicial 67

v) Sobre la conservación de los datos PNR (octava cuestión prejudicial) 67

4. Conclusiones sobre las cuestiones prejudiciales segunda, tercera, cuarta, sexta y octava 73

C. Sobre la quinta cuestión prejudicial 73

D. Sobre la séptima cuestión prejudicial 75

E. Sobre la novena cuestión prejudicial 77

F. Sobre la décima cuestión prejudicial 81

IV. Conclusión 82

I. Introducción

1. Mediante la presente petición de decisión prejudicial, la Cour constitutionnelle (Tribunal Constitucional, Bélgica) plantea al Tribunal de Justicia una serie de diez cuestiones prejudiciales, que versan sobre la interpretación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo sucesivo, «RGPD»),[2] así como sobre la validez y la interpretación de 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 (en lo sucesivo, «Directiva PNR»)[3] y de 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, «Directiva API»).[4] Estas cuestiones prejudiciales han sido formuladas en el contexto de un recurso interpuesto por la asociación sin ánimo de lucro Ligue des droits humains (LDH), por el que solicita la anulación total o parcial de 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; en lo sucesivo, «Ley PNR»),[5] que transpone al Derecho belga la Directiva PNR y la Directiva API.

2. Las cuestiones prejudiciales que Tribunal de Justicia tendrá que resolver en el presente asunto se inscriben en el marco de uno de los dilemas principales del constitucionalismo liberal democrático contemporáneo: ¿cómo definir el equilibrio entre el individuo y la colectividad en la era de los datos, cuando las tecnologías digitales permiten la recogida, la conservación, el tratamiento y el análisis de ingentes cantidades de datos de carácter personal con fines predictivos? Los algoritmos, el análisis de los *big data* y la inteligencia artificial utilizados por las autoridades públicas pueden servir para la promoción y la protección de los intereses

2 DO 2016, L 119, p. 1.

3 DO 2016, L 119, p. 132.

4 DO 2004, L 261, p. 24.

5 *Moniteur belge* de 25 de enero de 2017, p. 12905.

fundamentales de la sociedad, con una eficacia otrora inimaginable: desde la protección de la salud pública hasta la sostenibilidad medioambiental, desde la lucha contra el terrorismo hasta la prevención de la delincuencia, en particular, la delincuencia grave. Al mismo tiempo, la recogida indiferenciada de datos de carácter personal y la utilización de las tecnologías digitales por parte de los poderes públicos puede generar un panóptico digital, es decir, un poder público que ve todo sin ser visto. Un poder omnisciente capaz de controlar y prever los comportamientos de todos y cada uno y de adoptar las medidas necesarias hasta llegar al paradójico resultado, imaginado por Steven Spielberg en la película *Minority Report*, de privar preventivamente de libertad al autor de un delito que aún no ha sido cometido. Como se sabe, en algunos países, la sociedad prima sobre el individuo y la utilización de los datos personales permite realizar legítimamente una vigilancia en masa eficaz dirigida a proteger los intereses públicos considerados fundamentales. En cambio, el constitucionalismo europeo —nacional y supranacional—, con el lugar central que concede al individuo y a sus libertades, representa un obstáculo de gran importancia al advenimiento de una sociedad de la vigilancia en masa, sobre todo, tras el reconocimiento de los derechos fundamentales a la protección de la vida privada y a la protección de los datos personales. Pero, ¿en qué medida cabe erigir tal obstáculo sin grave menoscabo de algunos intereses fundamentales de la sociedad —como los que se han citado anteriormente a título de ejemplo—, que pueden, no obstante, tener conexiones constitucionales? Estamos en el meollo de la cuestión de la relación entre individuo y colectividad en la sociedad digital. Una cuestión que requiere, por un lado, la búsqueda y la instauración de delicados equilibrios entre los intereses de la colectividad y los derechos de los individuos, partiendo de la importancia capital de estos últimos en el patrimonio constitucional europeo y, por otro lado, la aplicación de garantías frente a los abusos. Nos hallamos, también en este punto, ante la versión contemporánea de un tema clásico del constitucionalismo, pues, como afirmaba, de forma lapidaria, *El Federalista*, los hombres no son ángeles y, por esta razón, se precisan mecanismos jurídicos para limitar y controlar el poder público.

3. Estas son las cuestiones de carácter general que se inscriben en el contexto de las presentes conclusiones, las cuales habrán de circunscribirse a la interpretación del Derecho de la Unión a la luz de la jurisprudencia anterior del Tribunal de Justicia, utilizando técnicas muy asentadas, entre las que se cuenta la de la interpretación conforme. En las presentes conclusiones, se recurrirá con frecuencia a esta técnica cuando resulte posible jurídicamente, con objeto de hallar el necesario equilibrio, desde el punto de vista constitucional, entre las finalidades públicas que subyacen en el sistema de transferencia, de recogida y de tratamiento de los datos del registro de nombres de los pasajeros (en lo sucesivo, «datos PNR») y los derechos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

II. Marco jurídico

A. Derecho de la Unión

1. Carta

4. A tenor del artículo 7 de la Carta, «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

5. A tenor del artículo 8 de la Carta:

«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.»

6. Conforme al artículo 52, apartado 1, de la Carta, «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».

2. RGPD

7. El artículo 2, apartado 2, letra d), del RGPD excluye del ámbito de aplicación de dicho reglamento el tratamiento de datos personales efectuado «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 de protección frente a amenazas a la seguridad pública y su prevención».

8. A tenor del artículo 23, apartado 1, letra d), del RGPD:

«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:

[…]

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».

3. Directiva PNR

9. Me limitaré aquí a ofrecer una breve panorámica del funcionamiento del sistema instaurado por la Directiva PNR. En el análisis jurídico, se darán más detalles sobre el contenido de las disposiciones de la Directiva PNR pertinentes a los efectos de la respuesta que se ha de dar a las cuestiones prejudiciales.

10. Con arreglo a su artículo 1, la Directiva PNR, adoptada sobre la base del artículo 82 TFUE, apartado 1, letra d) y del artículo 87 TFUE, apartado 2, letra a), organiza, a escala de la Unión Europea, un sistema de transferencia por las compañías aéreas de los datos PNR de vuelos exteriores de la UE,[6] así como de recogida, de tratamiento y de conservación de dichos datos por las autoridades competentes de los Estados miembros a efectos de lucha contra el terrorismo y la delincuencia grave.

11. A tenor del artículo 3, punto 5), de la referida Directiva, el «registro de nombres de los pasajeros» o «PNR» es una «relación de los requisitos de viaje impuestos a cada pasajero, que incluye toda la información necesaria para el tratamiento y el control de las reservas por parte de las compañías aéreas 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 utilizado para embarcar a los pasajeros en el vuelo o en sistemas equivalentes que posean las mismas funcionalidades».

12. El anexo I de la Directiva PNR (en lo sucesivo, «anexo I»), enumera los datos del registro de nombres de los pasajeros recopilados por las compañías aéreas que son objeto de transferencia en el sentido del artículo 8 de dicha Directiva y según los requisitos establecidos en dicho artículo.

13. El anexo II de la Directiva PNR (en lo sucesivo, «anexo II») contiene la lista de los delitos que constituyen «delitos graves», en el sentido del artículo 3, punto 9, de dicha Directiva.

14. El artículo 2 de la Directiva PNR prevé la posibilidad de que los Estados miembros decidan aplicar esa Directiva también a los «vuelos interiores de la UE»[7] o a algunos de los que considere «necesarios» a fin de perseguir los objetivos de la citada Directiva.

15. A tenor del artículo 4, apartado 1, de la Directiva PNR, «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")». Conforme al apartado 2, letra a), de dicho artículo 4, la UIP será responsable, en particular, de recoger los datos PNR de las compañías aéreas, almacenar y procesar esos datos, así como de transferir dichos datos o el resultado de su tratamiento a las autoridades competentes a que hace mención el artículo 7 de la Directiva PNR. A tenor del apartado 2, del mencionado artículo 7, dichas autoridades serán «[las] del Estado miembro competentes para la prevención, detección, investigación o enjuiciamiento de los delitos de terrorismo y delitos graves».[8]

6 A tenor del artículo 3, punto 2), de la Directiva PNR, un «vuelo exterior de la UE» es «cualquier vuelo, programado o no programado por una compañía aérea, procedente de un tercer país que tenga previsto aterrizar en el territorio de un Estado miembro o volar procedente del territorio de un Estado miembro y que tenga previsto aterrizar en un tercer país, incluidos en ambos casos los vuelos que hagan escala en el territorio de Estados miembros o de terceros países».

7 A tenor del artículo 3, punto 3), de la Directiva PNR, constituye un «vuelo interior de la Unión» «cualquier vuelo, programado o no programado por una compañía aérea, procedente del territorio de un Estado miembro y que tenga previsto aterrizar en el territorio de otro u otros Estados miembros, sin escalas en el territorio de un tercer país».

8 El artículo 7, apartado 1, de la Directiva PNR establece que cada Estado miembro elaborará la lista de autoridades competentes para solicitar o recibir datos PNR o el resultado del tratamiento de los mismos de las UIP, a fin de seguir examinando esa información o de tomar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves. La Comisión publicó esta lista en 2018 (DO 2018, C 194, p. 1; corrección de errores en DO 2020, C 366, p. 55).

16. A tenor del artículo 6, apartado 1, segunda frase, de la Directiva PNR, «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». El apartado 2 de dicho artículo está redactado en los siguientes términos:

«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.»

17. El artículo 12 de la Directiva PNR contiene disposiciones relativas a la conservación de los datos PNR.

18. El artículo 5 de la Directiva PNR establece que cada UIP designará un responsable de la protección de datos para controlar el tratamiento de los datos PNR y aplicar las garantías oportunas. Asimismo, cada Estado miembro está obligado, con arreglo al artículo 15 de esta Directiva, a encargar a la autoridad nacional de control a que se refiere el artículo 25 de la Decisión Marco 2008/977/JAI,[9] sustituida por la Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos o (en lo sucesivo, «Directiva Policía»),[10] que controle la aplicación, en su territorio, de las disposiciones adoptadas de conformidad con dicha Directiva. Esta autoridad, que ejerce sus tareas con el fin de proteger los derechos fundamentales relativos al tratamiento de los datos personales,[11] será responsable, en particular, de una parte, de conocer las reclamaciones presentadas por cualquier interesado, de investigar el asunto y de informar al interesado de los progresos y del resultado de su reclamación en un plazo de tiempo razonable y, de otra parte, de verificar la legalidad del tratamiento de los datos, de realizar investigaciones, inspecciones y auditorías de conformidad con el Derecho nacional, bien por propia iniciativa, bien sobre la base de la reclamación.[12]

9 Decisión Marco del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO 2008, L 350, p. 60).

10 DO 2016, L 119, p. 89. El artículo 25 de la Decisión Marco 2008/977 ha sido sustituido por el artículo 41 de la Directiva Policía.

11 Véase el artículo 15, apartado 2, de la Directiva PNR.

12 Véase el artículo 15, apartado 3, letras a) y b), de la Directiva PNR.

4. Otros actos pertinentes del Derecho de la Unión

19. El marco jurídico del presente asunto se completa con la Directiva API y la Directiva Policía. Para hacer más sencilla la lectura de las presentes conclusiones, se irá exponiendo el contenido de las disposiciones pertinentes de dichos actos en la medida en que resulte preciso para tratar las cuestiones que a los mismos se refieren o, más en general, por necesidades del análisis jurídico.

B. Derecho belga

20. Conforme al artículo 22 de la Constitución belga, «todos tienen derecho al respeto de su vida privada y familiar, salvo en los casos y condiciones establecidos por la ley».

21. A tenor de su artículo 2, la Ley PNR transpone la Directiva API, la Directiva PNR y, parcialmente, la Directiva 2010/65/UE. [13]

22. Conforme a su artículo 3, apartado 1, la Ley PNR «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». A tenor del artículo 4, puntos 1 y 2, de la citada Ley, se entiende por «transportista» «toda persona física o jurídica que lleva a cabo, con carácter profesional, el transporte de personas por vía aérea, marítima, ferroviaria o terrestre» y por «operador de viajes» «cualquier organizador o intermediario de viajes, en el sentido de la Ley de 16 de febrero de 1994, por la que se regula el Contrato de Organización de Viajes y el Contrato de Intermediación de Viajes».

23. El artículo 8 de la Ley PNR dispone:

«l. 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 artículo 90 *ter*, apartado 2, puntos […] 7.º, […] 8.º, […] 11.º, […] 14.º, […] 17.º, 18.º y 19.º, y apartado 3, del Code d'Instruction criminelle (Código de Procedimiento Penal belga), 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 los artículos 196, en lo que se refiere a los delitos de falsedad en documento público u oficial, 198, 199, 199 *bis*, 207, 213, 375 y 505 del Code penal (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, apartado 1, puntos 2.º y 3.º, y apartado 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

[13] Directiva 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 (DO 2010, L 283, p. 1).

renseignement et de sécurité (Ley Orgánica de 30 de noviembre de 1998 relativa a los Servicios de Inteligencia y Seguridad); [14]

5.º la investigación y el enjuiciamiento de los delitos contemplados en el artículo 220, apartado 2, de la loi générale sur les douanes et accises du 18 juillet 1977 (Ley General de 18 de julio de 1977 sobre Aduanas e Impuestos Especiales) y en el artículo 45, apartado 3, de la loi du 22 décembre 2009 relative au régime général d'accise (Ley de 22 de diciembre de 2009 sobre el Régimen General de los Impuestos Especiales) […]

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.»

24. El artículo 9 de la Ley PNR contiene la lista de los datos de los pasajeros que son objeto de transferencia. Estos datos corresponden a los enumerados en el anexo I.

25. Conforme al artículo 18 de la Ley PNR, «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».

26. El artículo 19 de la citada Ley establece que, «al finalizar un plazo de seis meses, contados desde el registro de los datos de los pasajeros en el banco de datos de los pasajeros, todos los datos de los pasajeros serán despersonalizados mediante enmascaramiento de los elementos de información».

27. El artículo 24 de la Ley PNR establece:

«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 de su tránsito por este, a efectos de identificar a toda persona que deba ser examinada de nuevo.

2. En el marco de los fines a que se refiere el artículo 8, apartado 1, puntos 1.º, 4.º y 5.º, o relativos a las amenazas mencionadas en los artículos 8, punto 1.º, letras a), b), c), d), f), g), y 11, apartado 2, 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), la evaluación previa de los pasajeros se basa en una correspondencia positiva, resultante de una correlación entre los datos de los pasajeros y:

1.º los bancos de datos gestionados por los servicios competentes o directamente disponibles o accesibles para ellos en el ejercicio de sus funciones o listados de personas elaborados por los servicios competentes en el ejercicio de sus funciones.

2.º los criterios de evaluación predeterminados por la UIP, a que se refiere el artículo 25.

3. En el marco de los fines contemplados en el artículo 8, apartado 1, punto 3.º, la evaluación previa de los pasajeros se basa en una correspondencia positiva, resultante de una correlación entre los datos de los pasajeros y las bases de datos mencionadas en el apartado 2, punto 1.º. […]»

[14] *Moniteur belge* de 18 de diciembre de 1998, p. 40312.

28. El artículo 25 de la Ley PNR recoge el contenido del artículo 6, apartado 4, de la Directiva PNR.

29. El capítulo 11 de la Ley PNR contiene las disposiciones que regulan el tratamiento de los datos de los pasajeros con el fin de mejorar el control de fronteras y combatir la inmigración ilegal. Estas disposiciones constituyen la transposición al Derecho belga de la Directiva API.

30. El artículo 44 de la Ley PNR prevé que la UIP designe un responsable de la protección de datos dentro del service public fédéral intérieur (Ministerio del Interior, Bélgica). La Commission de la protection de la vie privée (Comisión de la Protección de la Vida Privada) es la encargada de velar por la aplicación de las disposiciones de la Ley PNR.

31. El artículo 51 de la Ley PNR modifica 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), insertando el artículo 16/3, cuyo tenor dice:

«1. Mediante resolución 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 7 de la Ley [PNR].

2. El director del servicio adoptará la resolución a que se refiere el apartado 1 y la comunicará por escrito a la Unidad de Información de Pasajeros a que se refiere el capítulo 7 de la Ley antes mencionada. La resolución se notificará al Comité permanente R junto con su motivación.

El Comité permanente R prohibirá a los servicios de inteligencia y de seguridad que utilicen los datos recogidos en condiciones que no se ajusten a los requisitos legales.

La resolución puede referirse a un conjunto de datos relacionados con una indagación específica. En este caso, la lista de consultas de datos de los pasajeros se comunicará una vez al mes al Comité permanente R.»

C. Litigio principal, cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia

32. Mediante un escrito dirigido a la Cour constitutionnelle (Tribunal Constitucional) el 24 de julio de 2017, la LDH interpuso un recurso por el que solicita la anulación total o parcial de la Ley PNR. En apoyo de su recurso, invoca dos motivos.

33. Mediante su primer motivo, formulado con carácter principal y basado en la infracción del artículo 22 de la Constitución belga, en relación con el artículo 23 del RGPD, los artículos 7, 8, y el artículo 52, apartado 1, de la Carta, así como el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950 (en lo sucesivo, «CEDH»), la LDH considera que la Ley impugnada no respeta el principio de proporcionalidad en lo que respecta a su ámbito de aplicación y las categorías de datos a que se refiere, los tratamientos de datos que instaura, sus finalidades y la duración del período de conservación de los datos. En particular, sostiene que la definición de los datos PNR es excesivamente amplia y que puede llevar a que se revelen datos sensibles y que la definición del concepto de «pasajero» contenida en dicha Ley permite un tratamiento sistemático no selectivo de los datos de todos los pasajeros afectados. Además, la LDH considera que la Ley PNR no define con suficiente claridad la naturaleza y las particularidades del método de *pre-screening* de las bases de datos de pasajeros, ni los criterios que sirven de «indicadores de amenaza». Por

último, considera que la Ley PNR excede de los límites de lo estrictamente necesario, en el sentido de que los fines que persigue el tratamiento de los datos PNR son más amplios que los que permite la Directiva PNR y de que el período de cinco años de conservación de los datos PNR es desproporcionado. Mediante su segundo motivo, formulado con carácter subsidiario y basado en la infracción del artículo 22 de la Constitución belga, en relación con el artículo 3 TUE, apartado 2, y con el artículo 45 de la Carta, la LDH impugna las disposiciones del capítulo 11 de la Ley PNR que transponen la Directiva API.

34. El Consejo de Ministros del Reino de Bélgica, que se ha personado ante la Cour constitutionnelle (Tribunal Constitucional), se opone al recurso de la LDH, cuestionando la admisibilidad y la procedencia de los dos motivos invocados en apoyo de este.

35. Por su parte, la Cour constitutionnelle (Tribunal Constitucional) expone las siguientes consideraciones.

36. En cuanto al primer motivo, se pregunta, en primer lugar, si la definición de los datos PNR que figura en el anexo I es suficientemente clara y precisa. Considera que la descripción de algunos de estos datos reviste un carácter ilustrativo y no taxativo. A continuación, la Cour constitutionnelle (Tribunal Constitucional) señala que la definición del concepto de «pasajero» que figura en el artículo 3, punto 4, de la Directiva PNR supone la recogida, la transferencia, el tratamiento y la conservación de los datos PNR de toda persona transportada o que deba ser transportada y registrada en la lista de pasajeros, independientemente de que existan motivos fundados para presumir que la persona afectada haya cometido o vaya a cometer un delito, o haya sido condenada por un delito. En cuanto a los tratamientos de los datos PNR, observa que estos últimos son sistemáticamente objeto de una evaluación previa que implica el cruce de los datos PNR de todos los pasajeros con bases de datos o criterios predeterminados, con vistas a establecer resultados positivos. No obstante, la Cour constitutionnelle (Tribunal Constitucional) precisa que, si bien los criterios deben ser específicos, fiables y no discriminatorios, le parece técnicamente imposible definir de antemano con mayor precisión los criterios que vayan a servir para determinar los perfiles de riesgo. Por lo que se refiere al período de conservación de los datos PNR establecido en el artículo 12, apartado 1, de la Directiva PNR, con arreglo al cual dichos datos pueden conservarse durante un plazo de cinco años, el órgano jurisdiccional remitente considera que los datos PNR se conservan sin tener en cuenta la cuestión de si, a tenor de la evaluación previa, los pasajeros afectados pueden suponer o no un riesgo para la seguridad pública. En estas circunstancias, el órgano jurisdiccional remitente se interroga acerca de la cuestión de si, a la luz del criterio jurisprudencial establecido, en particular, por la sentencia de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros [15] y del Dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, [16] puede considerarse que el sistema de recogida, transmisión, tratamiento y conservación de los datos PNR establecido por la Directiva PNR sobrepasa los límites de lo estrictamente necesario. En este contexto, dicho órgano jurisdiccional se interroga asimismo sobre la cuestión de si la Directiva PNR se opone a una normativa nacional, como la que resulta del artículo 8, apartado 1, punto 4), de la Ley PNR, que autoriza el tratamiento de los datos PNR para fines distintos que los previstos en esa Directiva. Por último, se pregunta si la UIP puede ser considerada «otra autoridad nacional» autorizada, en virtud del artículo 12, apartado 3, letra b), inciso ii), de la Directiva PNR, a permitir la divulgación de los datos PNR completos transcurrido un período de seis meses. En cuanto al segundo motivo, el órgano jurisdiccional remitente pone de relieve que este se formula respecto del artículo 3, apartado 1, el artículo 8, apartado 2, y de los artículos 28 a 31 de la Ley PNR, que regulan la recogida y el tratamiento de los datos de los

15 C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2 Sverige», EU:C:2016:970.

16 En lo sucesivo, «Dictamen 1/15», EU:C:2017:592.

pasajeros para combatir la inmigración ilegal y mejorar los controles fronterizos. Al tiempo que recuerda que, a tenor de la primera de las disposiciones mencionadas, la Ley citada abarca los vuelos con destino o procedencia en el territorio nacional o en tránsito por dicho territorio, dicho órgano jurisdiccional precisa que el legislador nacional incluyó los vuelos «interiores de la UE» en el ámbito de aplicación de dicha Ley para obtener «una imagen más completa de los […] pasajeros que representan una posible amenaza para la seguridad [dentro de la Unión] y nacional», basándose en la posibilidad que brinda el artículo 2 de la Directiva PNR en relación con su considerando 10.

37. En este contexto, la Cour constitutionnelle (Tribunal Constitucional) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) ¿Debe interpretarse el artículo 23 del [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 Ley [PNR], que transpone la Directiva [PNR], la Directiva [API] y la Directiva 2010/65?

2) ¿Es el anexo I [de la Directiva PNR] compatible con los artículos 7, 8 y 52, apartado 1, de la [Carta], en la medida en que los datos que enumera son muy amplios —en particular, los datos a que se refiere el punto 18 de [dicho anexo I], que van más allá de los enunciados en el artículo 3, apartado 2, de la Directiva [API]— 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 PNR] compatibles con los artículos 7, 8, y el artículo 52, apartado 1, de la [Carta], 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 [PNR] y el anexo I [de la misma] con los artículos 7, 8, y el artículo 52, apartado 1, de la [Carta], 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 [PNR], en relación con los artículos 7, 8, y el artículo 52, apartado 1, de la [Carta] 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 actividades 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 [PNR] con los artículos 7, 8, y el artículo 52, apartado 1, de la [Carta], 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 [PNR] en el sentido de que se refiere a la UIP creada por la Ley [PNR], 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 [PNR], en relación con los artículos 7, 8, y el artículo 52, apartado 1, de la [Carta] 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 [API] compatible con el artículo 3 [TUE], apartado 2, y el artículo 45 de la [Carta], en la medida en que las obligaciones que establece se aplican a los vuelos interiores de [la Unión]?

   b) ¿Debe interpretarse la Directiva [API], en relación con el artículo 3 [TUE], apartado 2, y con el artículo 45 de la [Carta], 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 [(Tribunal Constitucional)] concluya que la Ley impugnada, que transpone en particular la Directiva [PNR], 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 [PNR] 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?»

38. La LDH, los Gobiernos belga, checo, danés, alemán, estonio, irlandés, español, francés, chipriota, letón, neerlandés, austriaco, polaco, finlandés, así como el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea presentaron observaciones escritas con arreglo al artículo 23 del Estatuto del Tribunal de Justicia de la Unión Europea. Conforme al artículo 24 del Estatuto del Tribunal de Justicia de la Unión Europea, se instó a la Comisión, al Supervisor Europeo de Protección de Datos (SEPD) y a la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) a contestar por escrito a las preguntas planteadas por el Tribunal de Justicia. El 13 de julio de 2021, se celebró la vista oral.

III. Análisis

A. Sobre la primera cuestión prejudicial

39. Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si el artículo 2, apartado 2, letra d), del RGPD debe interpretarse en el sentido de que ese Reglamento y, en particular, su artículo 23, apartado 1, a tenor del cual el Derecho de la Unión o los Derechos de los Estados miembros pueden limitar, a través de medidas

legislativas, por razones enumeradas de forma taxativa, el alcance de las obligaciones y de los derechos establecidos en dicho Reglamento, es aplicable a los tratamientos de datos efectuados con arreglo a una legislación nacional como la Ley PNR, que transpone al Derecho interno la Directiva PNR, la Directiva API y la Directiva 2010/65.

40. El artículo 2, apartado 2, del RGPD establece excepciones al ámbito de aplicación de ese Reglamento, definido en términos muy amplios [17] en el apartado 1 del artículo 2. [18] En la medida en que suponen no aplicar una normativa que regula el tratamiento de datos personales, que puede lesionar las libertades fundamentales, estas excepciones deben interpretarse en sentido estricto. [19]

41. El artículo 2, apartado 2, letra d), del RGPD recoge, en particular, una cláusula de exclusión a tenor de la cual dicho Reglamento no se aplica al tratamiento de datos personales «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 de protección frente a amenazas a la seguridad pública y su prevención». Esta cláusula de exclusión se basa en un doble criterio subjetivo y objetivo. Así, quedan excluidos del ámbito de aplicación del citado Reglamento los tratamientos de datos efectuados, primero, por las «autoridades competentes» y, segundo, con los fines que se enumeran en dicha disposición. En consecuencia, es preciso apreciar los distintos tipos de tratamiento de datos contemplados en la Ley PNR en relación con ese doble criterio.

42. En primer lugar, por lo que se refiere a los tratamientos de datos llevados a cabo por los transportistas (aéreos, ferroviarios, terrestres y marítimos) en la UIP o por los operadores de viajes *a efectos de la prestación de servicios o comerciales*, siempre y cuando estén contemplados en la citada Ley, siguen rigiéndose por el RGPD, al no cumplirse ni el aspecto subjetivo ni el aspecto objetivo del criterio de exclusión establecido en el artículo 2, apartado 2, letra d), de dicho Reglamento.

43. Por lo que se refiere, en segundo lugar, a la *transmisión por parte de los transportistas o de los operadores de viajes de los datos PNR a la UIP*, que constituye, en sí misma, un «tratamiento» en el sentido del artículo 4, punto 2, del RGPD, [20] su inclusión en el ámbito de aplicación del referido Reglamento es menos evidente.

44. En efecto, de una parte, esta transmisión no la lleva a cabo una «autoridad competente» en el sentido del artículo 3, punto 7), de la Directiva Policía, a la que debe acudirse por analogía, al no existir en el RGPD una definición de ese concepto. [21] Un operador económico, como una compañía de transporte o una agencia viaje, al que solo incumbe una obligación legal de

17 Véase, en este sentido, la sentencia de 22 de junio de 2021, Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504), apartado 61.

18 A tenor del artículo 2, apartado 1, del RGPD, «el presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».

19 Véanse las sentencias de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 84, y de 22 de junio de 2021, Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504), apartado 62.

20 Véase, en este sentido, la sentencia de 6 de octubre de 2020, Privacy International (C-623/17, en lo sucesivo, «sentencia Privacy International», EU:C:2020:790), apartado 41 y jurisprudencia citada. A tenor del artículo 4, punto 2), del RGPD, constituye un «tratamiento» «cualquier operación […] sobre datos personales o conjuntos de datos personales […], como […] la comunicación por transmisión».

21 Véase, en este sentido, la sentencia de 22 de junio de 2021, Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504), apartado 69. A tenor del artículo 3, punto 7, letras a) y b), de la Directiva Policía, es una «autoridad competente» «a) toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública, o b) cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas» a esos mismos efectos.

transmisión de datos personales y al que no se ha encomendado ninguna competencia pública, [22] no puede considerarse un órgano o entidad o entidad en el sentido del mencionado artículo 3, punto 7, letra b). [23]

45. Por otra parte, la transmisión de los datos PNR por parte de las compañías de transporte y de los operadores de viajes se efectúa para cumplir una obligación impuesta por la Ley dirigida a que puedan perseguirse los fines enumerados en el artículo 2, apartado 2, letra d), del RGPD.

46. Pues bien, a mi juicio, de la redacción de la citada disposición se desprende claramente que solo quedan fuera del ámbito de aplicación del RGPD los tratamientos que responden a la vez al aspecto subjetivo y al aspecto objetivo del criterio de exclusión que enuncia. En consecuencia, la transmisión de los datos PNR a la UIP impuesta por la Ley PNR a las compañías de transporte y a los operadores de viajes queda sujeta a dicho Reglamento.

47. En lo tocante a las disposiciones de la Ley PNR que transponen la Directiva PNR, esta conclusión se ve corroborada por el artículo 21, apartado 2, de la citada Directiva, que establece que esta «se entenderá sin perjuicio de la aplicabilidad de la Directiva 95/46/CE [24] al tratamiento de datos personales por las compañías aéreas». Considero que no cabe aceptar la interpretación de esta disposición sugerida, en particular, por el Gobierno francés, con arreglo a la cual esta se limita a establecer que los transportistas siguen sujetos a las obligaciones establecidas por el RGPD en relación con los tratamientos de datos no contemplados por la Directiva PNR. En efecto, a la vista de su redacción, el alcance de esa «reserva» es amplio y se define únicamente en relación con el autor del tratamiento, sin que se haga mención alguna a la finalidad del tratamiento o al contexto en el que se produce, ni a si se lleva a cabo en el ejercicio de la actividad comercial del transportista o en cumplimiento de una obligación legal. Debo señalar asimismo que el artículo 13, apartado 3, de la Directiva PNR recoge una reserva del mismo tenor, que se refiere muy especialmente a las obligaciones impuestas a los transportistas aéreos con arreglo al RGPD «de tomar las medidas técnicas y de organización adecuadas para proteger la seguridad y la confidencialidad de los datos personales». Pues bien, esta disposición figura entre las que regulan la protección de datos personales tratados en virtud de la Directiva PNR y sigue al artículo 13, apartado 1, de dicha Directiva, que, de manera general, somete cualquier tratamiento de datos efectuado con arreglo a esta a las disposiciones de la Decisión marco 2008/977 que menciona. Contrariamente a lo que alega el Gobierno francés, esta combinación normativa permite, de una parte, interpretar el apartado 3 del mencionado artículo 13 como una cláusula que somete al RGPD únicamente el tratamiento de datos previsto por la Directiva PNR que no se lleva a cabo por «autoridades competentes» en el sentido de la Directiva Policía y, de otra parte, entender la referencia al respeto de las obligaciones impuestas por dicho Reglamento en materia de

22 No hay ningún indicio en este sentido en la resolución de remisión.

23 Tal operador tampoco puede calificarse de «encargado del tratamiento» o «encargado» en el sentido del artículo 4, punto 8, del RGPD o del artículo 3, punto 9, de la Directiva Policía, tratándose más bien del «responsable del tratamiento» en el sentido del artículo 4, punto 7, segunda frase, del RGPD. A tenor del artículo 4, punto 8, del RGPD y del artículo 3, punto 9, de la Directiva Policía, que están redactados en idénticos términos, el «encargado del tratamiento» o el «encargado» es la «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento». En el sentido del artículo 4, punto 7, primera frase, del RGPD, el «responsable del tratamiento» o «responsable» es «la persona física o jurídica, autoridad pública, servicio u otro organismo que […] determine los fines y medios del tratamiento», la segunda frase de esta disposición precisa que «si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros».

24 Directiva del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31). Esta Directiva fue derogada y sustituida por el RGPD (véase el artículo 94 de dicho Reglamento).

seguridad y de confidencialidad de los datos como un recordatorio de las garantías que deben imperativamente debe llevar aparejadas la transferencia de los datos PNR a las UIP por parte de los transportistas.

48. La conclusión enunciada en el punto 46 de las presentes conclusiones no se ve puesta en tela de juicio por el considerando 19 del RGPD ni por el considerando 11 de la Directiva Policía, a los que se refieren, entre otros, los Gobiernos alemán, irlandés y francés a los efectos de respaldar la naturaleza de *lex specialis* de la Directiva PNR. En este sentido, es ciertamente verdad que esta Directiva instaura, en relación con los tratamientos de datos personales a los que se refiere, un marco de protección para estos datos autónomo en relación con el RGPD. Sin embargo, este marco específico solo se aplica a los tratamientos de los datos PNR efectuados por las «autoridades competentes», en el sentido del artículo 3, punto 7, de la Directiva Policía, entre las que se cuentan, en particular, las UIP, mientras que la transferencia de los datos PNR a las UIP sigue sujeta al marco general establecido por el RGPD con arreglo, entre otras, a la «reserva» prevista en el artículo 21, apartado 2, de la Directiva PNR.

49. En apoyo de la tesis de que el RGPD no se aplica a la transferencia de los datos PNR a las UIP por parte de los transportistas y los operadores de viajes, los Gobiernos belga, irlandés, francés y chipriota se remiten a la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión,[25] en la que el Tribunal de Justicia declaró que la transferencia de los datos PNR por compañías aéreas comunitarias a las autoridades de los Estados Unidos de América, en el marco de un acuerdo negociado entre estos últimos y la Comunidad Europea, constituía un tratamiento de datos personales, en el sentido del artículo 3, apartado 2, primer guion, de la Directiva 95/46[26] y, en consecuencia, no estaba comprendida en el ámbito de aplicación de esa Directiva. Para llegar a tal conclusión, el Tribunal de Justicia tuvo en cuenta la *finalidad de la transferencia*, así como el hecho de que esta «se inserta[ba] en un marco creado por los poderes públicos», aunque los datos se recogieran y se transfirieran por operadores privados.[27]

50. En este sentido, basta con señalar que, en la sentencia de 6 de octubre de 2020, La Quadrature du Net y otros,[28] el Tribunal de Justicia consideró, en esencia, que la sentencia Parlamento/Consejo no podía extrapolarse al ámbito del RGPD.[29]

25 C-317/04 y C-318/04, en lo sucesivo, «sentencia Parlamento/Consejo», EU:C:2006:346. En los asuntos que dieron lugar a dicha sentencia, el Parlamento había solicitado, de una parte, que se anulara la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (DO 2004, L 183, p. 83, y corrección de errores DO 2005, L 255, p. 168) y, de otra parte, que se anulara la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (DO 2004, L 235, p. 11).

26 A tenor del artículo 3, apartado 2, primer guion, de la Directiva 95/46, dicha Directiva no era aplicable al tratamiento de datos personales «efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, *en cualquier caso*, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal» (el subrayado es mío).

27 Sobre el «enfoque teleológico» y «contextual» del Tribunal de Justicia en la sentencia Parlamento/Consejo, véanse las conclusiones del Abogado General Campos Sánchez-Bordona presentadas en los asuntos acumulados La Quadrature du Net y otros (C-511/18 y C-512/18, EU:C:2020:6), puntos 47 y 62.

28 C-511/18, C-512/18 y C-520/18, en lo sucesivo, sentencia «La Quadrature du Net», EU:C:2020:791.

29 Véase la sentencia La Quadrature du Net, apartados 100 a 102.

51. Por otra parte, en el apartado 102 de la sentencia La Quadrature du Net,[30] el Tribunal de Justicia afirmó, haciendo una aplicación analógica del razonamiento seguido en las sentencias Tele2 Sverige y de 2 de octubre de 2018, Ministerio Fiscal,[31] que, «aunque [el RGPD] precisa, en su artículo 2, apartado 2, letra d), que no se aplica a los tratamientos "por parte de las autoridades competentes" con fines, en particular, de prevención y detección de infracciones penales, incluid[o el] de protección frente a amenazas a la seguridad pública y su prevención, del artículo 23, apartado 1, letras d) y h), del mismo Reglamento se desprende que los tratamientos de datos personales efectuados con estos mismos fines por particulares están comprendidos en el ámbito de aplicación de este».[32]

52. Por las razones que ya se han expuesto, estoy convencido de que la conclusión de que la transferencia de los datos PNR por parte de las compañías de transporte y los operadores de viajes a las UIP está sujeta al RGPD ya se desprende con claridad de la redacción del artículo 2, apartado 2, letra d), del RGPD, que solo se refiere a los tratamientos «por parte de las autoridades competentes», sin necesidad de referirse a la reserva establecida en el artículo 23, apartado 1, de dicho Reglamento.[33] No obstante, la afirmación contenida en el apartado 102 de la sentencia La Quadrature du Net constituye una meridiana toma de posición del Tribunal de Justicia en favor de esta conclusión.

53. Dado que la transferencia de los datos PNR por parte de las compañías de transporte y los operadores de viajes está comprendida en el ámbito de aplicación del RGPD, una normativa nacional, como la Ley PNR, que obliga a esas compañías y a esos operadores a realizar tal transferencia constituye una «medida legislativa» en virtud del artículo 23, apartado 1, letra d), del RGPD y debe, en consecuencia, cumplir los requisitos establecidos en esta disposición.[34]

54. En tercer lugar, por lo que respecta a los tratamientos de los datos PNR efectuados *por la UIP y las autoridades nacionales competentes*, como se desprende de los razonamientos anteriores, la aplicabilidad del RGPD depende de las finalidades que esos tratamientos pretenden lograr.

55. Así, en primer término, los tratamientos de datos PNR llevados a cabo por la UIP y por las autoridades nacionales competentes en relación con los fines enumerados el artículo 8, apartado 1, puntos 1 a 3 y 5, de la Ley PNR[35] quedan excluidos del ámbito de aplicación del RGPD en la medida en que, como parece ser el caso, dichos fines están entre aquellos a los que se refiere la reserva establecida en el artículo 2, apartado 2, letra d), del RGPD. La protección de los datos de las personas afectadas por tales tratamientos está regulada por el Derecho nacional, sin perjuicio de la aplicación de la Directiva Policía[36] y, en el marco de su ámbito de aplicación, por la Directiva PNR.

30 Véase, en el mismo sentido, la sentencia Privacy International, apartado 47.

31 C-207/16, en lo sucesivo, «sentencia Ministerio Fiscal», EU:C:2018:788, apartado 34.

32 Véanse, por analogía, las sentencias Tele2 Sverige, apartados 72 a 74, y Ministerio fiscal, apartado 34. Estas sentencias versaban sobre la interpretación del artículo 15, apartado 1, primera frase, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37), que establece una reserva análoga a la del artículo 23, apartado 1, letras a) a d), RGPD.

33 En el contexto de dicha Directiva, estaba justificado referirse al artículo 15, apartado 1, de la Directiva 2002/58, a la vista de la redacción de la reserva prevista en su artículo 1, apartado 3, que se refiere, de forma general, a las «actividades del Estado en materia penal».

34 Véase, por analogía, la sentencia Privacy International, apartados 38 y 39.

35 Se trata de los tratamientos regulados en los capítulos 7 a 10 y 12 de la Ley PNR.

36 Véanse, en este sentido, las sentencias La Quadrature du Net, apartado 103, y Privacy International, apartado 48.

56. En segundo término, lo mismo ocurre con los tratamientos de los datos PNR efectuados por la UIP y por los servicios de seguridad e inteligencia en el marco del seguimiento de las actividades mencionadas en las disposiciones de la loi organique des services de renseignement et de sécurité (Ley Orgánica relativa a los Servicios de Inteligencia y Seguridad) enumeradas en el artículo 8, apartado 1, punto 4, de la Ley PNR, en la medida en que respondan a los fines enunciados en el artículo 2, apartado 2, letra d), del RGPD, extremo cuya apreciación corresponde al órgano jurisdiccional remitente.

57. El Gobierno belga sostiene que los tratamientos llevados a cabo con arreglo al artículo 8, apartado 1, punto 4, de la Ley PNR están, en cualquier caso, cubiertos por la reserva establecida en el artículo 2, apartado 2, letra a), del RGPD y la establecida en el artículo 2, apartado 3, letra a), de la Directiva Policía, dado que los servicios de seguridad e inteligencia no son actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.

58. A este respecto, al mismo tiempo que subrayo que el Tribunal de Justicia no conoce ahora de una cuestión prejudicial relativa a la interpretación de dichas disposiciones, debo señalar, en primer lugar, que el Tribunal de Justicia ya ha afirmado que una normativa nacional que impone obligaciones de tratamiento a operadores privados está sujeta a las disposiciones del Derecho de la Unión en materia de protección de datos personales, incluso cuando va dirigida a proteger la seguridad nacional.[37] De ello se infiere que, en principio, la transferencia de los datos PNR, impuesta por la Ley PNR a los transportistas y a los operadores de viajes, está comprendida en el ámbito de aplicación del RGPD, incluso cuando se efectúa a efectos del artículo 8, apartado 1, punto 4, de dicha ley.

59. A continuación, debo señalar que, si bien el considerando 16 del RGPD enuncia que este no se aplica a las «actividades relativas a la seguridad nacional» y el considerando 14 de la Directiva Policía precisa que «no deben considerarse comprendidas en el ámbito de aplicación de [dicha] Directiva las actividades relacionadas con la seguridad nacional, las actividades de los servicios o unidades que traten cuestiones de seguridad nacional», los criterios en función de los cuales un tratamiento de datos personales efectuado por una autoridad, una unidad o un servicio público de un Estado miembro está incluido en el ámbito de aplicación de uno u otro acto de Derecho de la Unión que regulan la protección de los datos de las personas afectadas en relación con tales tratamientos o se sitúa fuera del ámbito de aplicación de ese Derecho responden a una lógica vinculada tanto a las funciones encomendadas a esa autoridad, unidad o servicio, como a las finalidades de tal tratamiento. Así, el Tribunal de Justicia ha establecido que «debe considerarse que el artículo 2, apartado 2, letra a), del RGPD, interpretado a la luz del considerando 16 de dicho Reglamento, tiene como único objeto excluir del ámbito de aplicación del mencionado Reglamento los tratamientos de datos personales efectuados por autoridades estatales en el marco de una actividad dirigida a preservar la seguridad nacional o una actividad que pueda incluirse en la misma categoría, de modo que el mero hecho de que una actividad sea propia del Estado o de una autoridad pública no basta para que dicha excepción sea automáticamente aplicable a tal actividad».[38] El Tribunal de Justicia también ha precisado que «las actividades cuya finalidad es preservar la seguridad nacional a las que se refiere el artículo 2, apartado 2, letra a), del RGPD cubren, en particular […], las que tienen por objeto proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad».[39] De ello resulta que, en el supuesto de que un Estado miembro encargue a sus servicios de seguridad y de inteligencia funciones en los

37 Véase, en particular, la sentencia La Quadrature du Net.

38 Véase la sentencia de 22 de junio de 2021, Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504), apartado 66.

39 Véase la sentencia de 22 de junio de 2021, Latvijas Republikas Saeima (Puntos por infracciones de tráfico) (C-439/19, EU:C:2021:504).

ámbitos enumerados en el artículo 3, punto 7, letra a), de la Directiva Policía, los tratamientos de datos efectuados por esos servicios para el desempeño de esas funciones estarían comprendidos en el ámbito de aplicación de dicha Directiva y también, en su caso, de la Directiva PNR. Con carácter más general, debo indicar que el Tribunal de Justicia ha declarado reiteradamente, al interpretar el artículo 4 TUE, apartado 2, en el que se basa, entre otros, el Gobierno belga, que el mero hecho de que se haya adoptado una medida nacional con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho,[40] con lo que se muestra reticente a una exclusión automática y en bloque del ámbito de aplicación del Derecho de la Unión de las actividades de los Estados miembros relacionadas con la protección de la seguridad nacional.

60. En tercer término, según el parecer de todas las partes interesadas que han presentado observaciones, a excepción del Gobierno francés, debe considerarse que a los tratamientos de los datos PNR efectuados por las autoridades competentes belgas con los fines enunciados en el artículo 8, apartado 2, de la Ley PNR, a saber «mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal»[41] no les alcanza la reserva establecida en el artículo 2, apartado 2, letra d), del RGPD, ni otra reserva prevista en dicho artículo y, por lo tanto, están comprendido en el ámbito de aplicación del referido Reglamento. Contrariamente a lo que alega el Gobierno francés, dichos tratamientos no pueden regirse por la Directiva PNR, cuyo artículo 1, apartado 2, establece que «los datos PNR obtenidos con arreglo a la presente Directiva podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves» ni, en principio, por la Directiva Policía, que, con arreglo a su artículo 1, apartado 1, solo se aplica al tratamiento de los datos personales por parte de las autoridades competentes «con 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 contra la seguridad pública». Como resulta de la resolución de remisión, el artículo 8, apartado 2, de la Ley PNR y el capítulo 11 de dicha Ley, que recoge las disposiciones en materia de tratamiento de los datos PNR a efectos de mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal y que prevé, con tal fin, la transmisión de estos datos por parte de la UIP, en particular, a los servicios de policía encargados del control de fronteras, van dirigidos a transponer al Derecho belga la Directiva API y la Directiva 2010/65. Pues bien, ambas Directivas obligan a las autoridades competentes, en relación con los tratamientos que contemplan, al cumplimiento de lo dispuesto en la Directiva 95/46.[42] Contrariamente a lo que sostiene el Gobierno francés, debe entenderse que la remisión a las normas protectoras de dicha Directiva abarca cualquier tratamiento de datos personales efectuado con arreglo a la Directiva API y a la Directiva 2010/65. El hecho de que la Directiva API sea anterior a la entrada en vigor de la Decisión Marco 2008/977 es irrelevante por cuanto dicha Decisión Marco, al igual que la Directiva Policía que la sustituyó, solo afecta a los tratamientos de datos de carácter personal a que se refiere el artículo 3, apartado 1, de la Directiva API, efectuados por las autoridades competentes a efectos policiales.[43]

40 Véase la sentencia La Quadrature du Net, apartado 99 y jurisprudencia citada.

41 Los requisitos de estos tratamientos de datos figuran en el capítulo 11 de la Ley PNR.

42 Véanse los considerandos 8, 9 y 12, y el artículo 6 de la Directiva API, y el artículo 8, apartado 2, de la Directiva 2010/65.

43 La utilización de información previa sobre los pasajeros (en lo sucesivo, «datos API») por servicios policiales está expresamente prevista en el artículo 6, apartado 1, último párrafo, de la Directiva API.

61. Sobre la base del conjunto de consideraciones que preceden, sugiero al Tribunal de Justicia que conteste a la primera cuestión prejudicial que el artículo 23 del RGPD, en relación con el artículo 2, apartado 2, letra d), de dicho Reglamento, debe interpretarse en el sentido de que:

– Se aplica a una normativa nacional que transpone la Directiva PNR en la medida en que esa normativa regule los tratamientos de los datos PNR efectuados por los transportistas y por otros operadores económicos, incluida la transmisión de datos PNR a las UIP, prevista en el artículo 8 de dicha Directiva.

– No se aplica a una normativa nacional que transpone la Directiva PNR en la medida en que esta regule los tratamientos de datos efectuados con los fines establecidos en el artículo 1, apartado 2, de dicha Directiva por parte de las autoridades nacionales competentes, incluidas las UIP y, en su caso, los servicios de seguridad e información del Estado miembro interesado.

– Se aplica a una normativa nacional que transpone la Directiva API y la Directiva 2010/65 a efectos de mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal.

B. Sobre las cuestiones prejudiciales segunda, tercera, cuarta, sexta y octava

62. Mediante sus cuestiones prejudiciales segunda, tercera, cuarta y sexta, la Cour constitutionnelle (Tribunal Constitucional) interroga el Tribunal de Justicia acerca de la validez de la Directiva PNR en relación con los artículos 7, 8 y del artículo 52, apartado 1, de la Carta. Aunque la octava cuestión prejudicial está redactada en términos de cuestión interpretativa, también va dirigida, en esencia, a recabar el pronunciamiento del Tribunal de Justicia sobre la validez de dicha Directiva.

63. Estas cuestiones prejudiciales se refieren a los distintos elementos del sistema de tratamiento de los datos PNR instaurado por la Directiva PNR y solicitan, respecto de cada uno de esos elementos, una evaluación de si se cumplen los requisitos a los que se supedita la legalidad de las limitaciones introducidas en relación con el ejercicio de los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta. Así las cuestiones prejudiciales segunda y tercera se refieren al catálogo de datos PNR que figura en el anexo I, la cuarta guarda relación con la definición del concepto de «pasajero» a que se refiere el artículo 3, punto 4), de la Directiva PNR, la sexta trata de la utilización de los datos PNR a efectos de la evaluación previa prevista en su artículo 6 y la octava se refiere al período de conservación de los datos PNR establecido en el artículo 12, apartado 1, de la Directiva mencionada.

1. Sobre los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta

64. El artículo 7 de la Carta garantiza a toda persona el derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. En cuanto al artículo 8, apartado 1, de la Carta, reconoce explícitamente a toda persona el derecho a la protección de los datos de carácter personal que la conciernan. Según reiterada jurisprudencia, estos derechos, que atañen a toda información relativa a una persona física identificada o identificable, están estrechamente relacionados, pues el acceso a los datos personales de una persona física para su conservación o

su utilización afecta al derecho de dicha persona al respeto de la vida privada. [44]

65. Sin embargo, los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad. [45] Así, el artículo 8, apartado 2, de la Carta autoriza el tratamiento de los datos de carácter personal si se cumplen ciertos requisitos. Esta disposición establece que los datos de carácter personal se tratarán «de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley».

66. Cualquier limitación que se introduzca en el derecho a la protección de los datos personales, así como el derecho a la vida privada, deberá asimismo cumplir lo prescrito en el artículo 52, apartado 1, de la Carta. De esta manera, tal limitación deberá ser establecida por la ley, respetar el contenido esencial de dichos derechos y, dentro del respeto del principio de proporcionalidad, ser necesaria y responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

67. La apreciación de una medida que limite los mencionados derechos debe tener en cuenta asimismo la importancia de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta y la que presentan los objetivos de protección de la seguridad nacional y de lucha contra la delincuencia grave al contribuir a la protección de los derechos y de las libertades de terceros. [46] En este sentido, el artículo 6 de la Carta establece el derecho de todas las personas no solo a la libertad, sino también a la seguridad. [47]

68. Por otra parte, el artículo 52, apartado 3, de la Carta pretende garantizar la coherencia necesaria entre los derechos que esta consagra y los derechos correspondientes garantizados por el CEDH, que procede tener en cuenta como nivel mínimo de protección. [48] El derecho al respeto de la vida privada y familiar, consagrado en el artículo 7 de la Carta, se corresponde con el garantizado en el artículo 8 del CEDH y, por consiguiente, debe atribuírsele el mismo sentido y el mismo alcance. [49] De la jurisprudencia del Tribunal Europeo de Derechos Humanos (en lo sucesivo, «TEDH») se desprende que una injerencia en los derechos garantizados en dicho artículo solo puede justificarse, a la luz del apartado 2 de dicho artículo, si está prevista por la ley, si persigue uno o varios fines legítimos enumerados en dicho apartado y si es necesaria, en una sociedad democrática, para alcanzar ese o esos fines. [50] La medida tiene que ser compatible con la preeminencia del Derecho, expresamente mencionada en el preámbulo del CEDH e inherente al objeto y al fin de su artículo 8. [51]

44 Véase, en este sentido, en particular, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 170 y jurisprudencia citada.

45 Véase, en particular, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 172 y jurisprudencia citada.

46 Véase, en este sentido, la sentencia La Quadrature du Net, apartado 122.

47 Véase la sentencia La Quadrature du Net, apartado 123.

48 Véase la sentencia La Quadrature du Net, apartado 124 y jurisprudencia citada.

49 Véase la sentencia de 18 de junio de 2020, Comisión/Hungría (Transparencia asociativa) (C-78/18, EU:C:2020:476), apartado 122 y jurisprudencia citada.

50 Véanse, en particular, TEDH, sentencia de 4 de diciembre de 2015, Roman Zakharov c. Rusia (CE:ECHR:2015:1204JUD004714306), § 227; de 18 de mayo de 2010, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905), § 130, y de 25 de mayo de 2021, Centrum för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD003525208), § 246.

51 Véase TEDH, sentencia de 4 de diciembre de 2015, Roman Zakharov c. Rusia, (CE:ECHR:2015:1204JUD004714306), § 228; de 4 de mayo de 2000, Rotaru c. Rumanía (CE:ECHR:2000:0504JUD002834195), § 52; de 4 de diciembre de 2008, S. y Marper c. Reino Unido (CE:ECHR:2008:1204JUD003056204), § 95; de 18 de mayo de 2021, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905), § 151, y de 25 de mayo de 2021, Centrüm för Rättvisa c. Suecia (CE:ECHR:2021:0525JUD003525208), § 246.

69. Estos principios son los que deben servir de guía para examinar las cuestiones prejudiciales sobre la apreciación de validez planteadas por la Cour constitutionnelle (Tribunal Constitucional).

2. Sobre la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta

70. El Tribunal de Justicia ya ha declarado que aquellas disposiciones que impongan o permitan la comunicación de datos personales de personas físicas a un tercero, como una autoridad pública, deben calificarse, a falta de consentimiento de tales personas físicas y cualquiera que sea el uso posterior que se haga de los datos en cuestión, de injerencia en su vida privada y, por tanto, de limitación al derecho fundamental garantizado en el artículo 7 de la Carta, sin perjuicio de su posible justificación.[52] Así ocurre incluso a falta de circunstancias que permitan calificar esta injerencia de «grave» y sin que sea relevante que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia.[53] El acceso de las autoridades públicas a esta información constituye, del mismo modo, una injerencia en el derecho fundamental a la protección de los datos de carácter personal garantizado en el artículo 8 de la Carta, pues constituye un tratamiento de datos de carácter personal.[54] Asimismo, constituye en sí misma una injerencia en los derechos garantizados por los artículos 7 y 8 de la Carta la conservación, durante un determinado período, de datos relativos a la vida privada de una persona.[55]

71. El Tribunal de Justicia también ha declarado que los datos PNR, como los enumerados en el anexo I, incluyen información sobre personas físicas identificadas, a saber, los pasajeros aéreos afectados, y que, en consecuencia, los distintos tratamientos de los que estos datos pueden ser objeto afectan al derecho fundamental al respeto de la vida privada, garantizado en el artículo 7 de la Carta. El artículo 8 de la Carta es también aplicable a los tratamientos, que, en consecuencia, deben cumplir necesariamente los requisitos de protección de los datos previstos en el referido artículo.[56]

72. Así, los tratamientos de los datos PNR permitidos por la Directiva PNR y, en particular, en relación con lo que reviste un interés a efectos del presente asunto, la transferencia de esos datos por parte de las compañías aéreas a las UIP, su utilización por parte de dichas unidades, su transferencia posterior a autoridades nacionales competentes, en el sentido del artículo 7 de la citada Directiva, así como su conservación constituyen otras tantas injerencias en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta.

73. En lo tocante a la gravedad de esas injerencias, procede señalar, en primer lugar, que la Directiva PNR prevé la transferencia *sistemática* y *continua* a las UIP de los datos PNR de todo pasajero aéreo, según se define en el artículo 3, punto 4, de dicha Directiva, que tome un vuelo «exterior de la UE», en el sentido del artículo 3, punto 2, de esta. Esta transferencia supone un

52 Véase, entre otras, la sentencia de 18 de junio de 2020, Comisión/Hungría (Transparencia asociativa) (C-78/18, EU:C:2020:476), apartados 124 y 126 y jurisprudencia citada; véase también TEDH, sentencia de 4 de mayo de 2000, Rotaru c. Rumanía (CE:ECHR:2000:0504JUD002834195), § 48; de 26 de marzo de 1987, Leander c. Suecia (CE:ECHR:1987:0326JUD000924881), § 46, y de 29 de junio de 2006, Weber y Saravia c. Alemania (CE:ECHR:2006:0629DEC005493400), § 79.

53 Véase, entre otras, la sentencia Ministerio Fiscal, apartado 51 y jurisprudencia citada.

54 Véanse, entre otras, la sentencia de 18 de junio de 2020, Comisión/Hungría (Transparencia asociativa) (C-78/18, EU:C:2020:476), apartado 126, así como la sentencia Ministerio Fiscal, apartado 51 y jurisprudencia citada.

55 Véase la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, en lo sucesivo, «sentencia Digital Rights», EU:C:2014:238), apartado 34.

56 Véase el Dictamen 1/15, apartados 121 a 123.

acceso general, por parte de las UIP, a todos los datos PNR comunicados.[57] Contrariamente a lo que alegan algunos Estados miembros en el presente procedimiento, no obsta a esta apreciación el hecho de que, debido al tratamiento automatizado de que son objeto esos datos, las UIP solo tengan acceso concreto a los datos cuyo análisis haya dado un resultado positivo. En efecto, de una parte, hasta la fecha, esta circunstancia no ha impedido que el Tribunal de Justicia afirme, en el contexto de sistemas de tratamiento automatizado de datos personales recogidos o conservados «en bruto» parecidos, el carácter general del acceso de las autoridades públicas afectadas a esos datos. De otra parte, la mera puesta a disposición de las autoridades públicas de datos personales con vistas a su tratamiento y conservación por parte de estas supone un acceso, *a priori*, general y completo de estas a dichos datos y una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal.

74. En segundo lugar, conforme al artículo 2, apartado 1, de la Directiva PNR, los Estados miembros pueden decidir aplicar dicha Directiva a los vuelos «interiores de la UE», en el sentido de su artículo 3, punto 3. A tal respecto, debo señalar, por una parte, que la Directiva PNR no se limita a dotar a los Estados miembros de la facultad de extender su aplicación a los vuelos interiores de la UE, sino que también determina los requisitos, tanto formales como materiales, que regulan el ejercicio de esa facultad[58] y precisa que, cuando esta solo se ejerza respecto de determinados vuelos interiores de la UE, la elección de tales vuelos deberá realizarse teniendo en cuenta los objetivos perseguidos por dicha Directiva.[59] Por otra parte, la Directiva PNR prevé las consecuencias del ejercicio de dicha facultad, estableciendo en su artículo 2, apartado 2, que, en caso de que un Estado miembro decida aplicar dicha Directiva a los vuelos interiores de la UE, todas las disposiciones de esta «se aplicarán a los vuelos interiores de la UE de igual modo que si se tratara de vuelos al exterior de la UE, y a los datos PNR de vuelos interiores de la UE de igual modo que si se tratara de datos PNR de vuelos al exterior de la UE».

75. En estas circunstancias, mi opinión es que, contrariamente a lo alegado por un cierto número de los Gobiernos que han presentado observaciones en el presente procedimiento, aunque la aplicación de la Directiva PNR a los vuelos interiores de la UE depende de la decisión de los Estados miembros, cuando estos la adoptan, la Directiva PNR constituye la base legal de las injerencias en los derechos al respeto de la vida privada y a la protección de los datos de carácter personal relacionadas con la transferencia, el tratamiento y la conservación de los datos PNR en relación con dichos vuelos.

57 Véase, por analogía, la sentencia Privacy International, apartados 79 y 80 y jurisprudencia citada.

58 Véase el artículo 2, apartados 1 a 3, de la Directiva PNR.

59 Véase el artículo 2, apartado 3, de la Directiva PNR.

76. Pues bien, con excepción del Reino de Dinamarca, que no está sometido a dicha Directiva,[60] casi todos los Estados miembros aplican el régimen fijado por esta para los vuelos «interiores de la UE».[61] De ello se sigue que este régimen se aplica a todos los vuelos que entran y salen de la Unión, así como a prácticamente todos los vuelos realizados dentro de la Unión.

77. En tercer lugar, en cuanto a los datos PNR que deben transferirse, el anexo I enumera diecinueve categorías referidas a datos biográficos,[62] detalles del viaje aéreo[63] y otros datos recogidos en el contexto del contrato de transporte aéreo, como el número de teléfono, la dirección de correo electrónico, los datos de pago, la agencia de viajes o el operador de viajes, la información relativa al equipaje, así como observaciones generales.[64] Pues bien, como señala el Tribunal de Justicia en el apartado 128 del Dictamen 1/15, al pronunciarse sobre las categorías que figuran en el anexo del proyecto de Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (en lo sucesivo, «proyecto de Acuerdo PNR Canadá-UE»), formuladas de forma muy parecida a las del anexo I, «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».

78. En cuarto lugar, a tenor del artículo 6 de la Directiva PNR, los datos transferidos por las compañías aéreas van destinados a ser analizados por las UIP por medios automatizados y ello *de forma sistemática*, es decir, con independencia de la cuestión de si existe el menor indicio de que las personas afectadas puedan estar implicadas en delitos de terrorismo o en delitos graves. Más en particular, en el marco de la evaluación previa de los pasajeros prevista en el artículo 6, apartado 2, letra a), de dicha Directiva, y de conformidad con el apartado 3 de este artículo, los datos mencionados pueden comprobarse cotejándolos con bases de datos «pertinentes» [artículo 6, apartado 3, letra a)] y tratarse con arreglo a criterios predeterminados [artículo 6, apartado 3, letra b)]. Pues bien, el primer tipo de tratamiento puede proporcionar información adicional sobre la vida privada de las personas afectadas[65] y, en función de las bases de datos utilizadas para el cotejo, puede incluso hacer posible que se trace un *perfil preciso* de dichas personas. En estas circunstancias, la objeción formulada por varios Gobiernos de que la Directiva PNR únicamente permite el acceso a un conjunto de datos personales relativamente limitado no refleja adecuadamente el alcance potencial de las injerencias que esta Directiva implica en los derechos

60 De conformidad con los artículos 1 y 2 del Protocolo (n.º 22) sobre la posición de Dinamarca, dado que dicho Estado miembro no participa en la adopción de la Directiva PNR, no queda vinculada por la misma ni sujeta a su aplicación (véase el considerando 40 de dicha Directiva). No obstante, resulta de las observaciones escritas presentadas por el Gobierno danés que el Reino de Dinamarca adoptó, en 2018, una ley sobre la recogida, la utilización y la conservación de los datos PNR, cuyas disposiciones concuerdan en gran parte con las de la Directiva PNR. En cuanto a Irlanda, a tenor del considerando 39 de la Directiva PNR, dicho Estado miembro notificó, de conformidad con el artículo 3 del Protocolo (n.º 21) sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al TUE y al TFUE, su deseo de participar en la adopción y aplicación de dicha Directiva.

61 La Comisión ha publicado una lista actualizada de los Estados miembros que han optado por la aplicación de la Directiva [PNR] a los vuelos interiores de la UE, según establece el artículo 2 de la Directiva [PNR] (DO 2020, C 358, p. 7), corregida en septiembre de 2021 con el añadido de Eslovenia y la supresión de la referencia al Reino Unido (DO 2021, C 360, p. 8). Irlanda y Austria no figuran en esa lista. El Informe de la Comisión al Parlamento Europeo y al Consejo sobre la revisión de la Directiva [PNR], de 24 de julio de 2020 [COM(2020) 305 final, p. 11 (en lo sucesivo, «Informe de la Comisión de 2020»)] menciona que todos los Estados miembros, excepto uno, han ampliado la recogida de datos PNR a los vuelos interiores de la UE.

62 Véanse, en particular, los puntos 4) y 18) del anexo I relativos a los nombres y apellidos, sexo, fecha de nacimiento, nacionalidad y documentos de identidad del pasajero.

63 Véanse, en particular, los puntos 2), 3), 7), 13) y 18) del anexo I de la Directiva PNR, que mencionan, en particular, el número de vuelo, los aeropuertos de salida y de llegada, así como las fechas y horas de salida y de llegada.

64 Véanse los puntos 5), 6), 9), 12) y 16) del anexo I.

65 Véase, en este sentido, el Dictamen 1/15, apartado 131.

fundamentales protegidos por los artículos 7 y 8 de la Carta, desde el punto de vista de la extensión de los datos a los que dicha Directiva puede permitir acceder. En cuanto al segundo tipo de tratamiento de datos, contemplado en el artículo 6, apartado 3, letra b), de la Directiva PNR, deseo recordar que, en los apartados 169 y 172 del Dictamen 1/15, el Tribunal de Justicia subrayó que el presentar un cierto margen de error es algo inherente a cualquier tipo de análisis basado en criterios predeterminados, especialmente, el presentar un cierto número de resultados «falsos positivos». Según los datos cifrados contenidos en el documento de trabajo de los servicios de la Comisión [66] (en lo sucesivo, «documento de trabajo de 2020») anexo al Informe de la Comisión de 2020, el número de casos de resultados positivos que, tras una revisión individualizada con arreglo al artículo 6, apartado 5, de la Directiva PNR, resultan ser erróneos es bastante considerable y, a lo largo de los años 2018 y 2019, fue de, al menos, cinco de cada seis personas identificadas. [67]

79. En quinto lugar, de conformidad con el artículo 12, apartado 1, de la Directiva PNR, los datos PNR se conservan en una base de datos 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. La Directiva PNR permite, por lo tanto, disponer de información sobre la vida privada de los pasajeros aéreos durante un período particularmente largo. [68] Por otra parte, dado que la transferencia de los datos PNR afecta prácticamente a todos los vuelos con origen y con destino a la Unión, así como dentro de esta, y que el avión se ha convertido en un medio de transporte más bien habitual, una parte significativa de los pasajeros aéreos podrían encontrarse con que sus datos personales se conservan de forma prácticamente permanente por el mero hecho de desplazarse en avión al menos dos veces cada cinco años.

80. Por último, en un plano más general, la Directiva PNR establece medidas que, consideradas en su conjunto, van dirigidas a implantar, a escala de la Unión, un sistema de vigilancia «no selectiva», es decir, que no se pone en funcionamiento en razón de una sospecha sobre una o varias personas específicas, «masiva», al ejercerse sobre los datos personales de un gran número de individuos, [69] que abarca una misma categoría de personas en su totalidad [70] y «proactiva», en la medida en que no solo va dirigida a investigar amenazas conocidas, sino también, a localizar o identificar peligros desconocidos hasta el momento. [71] Tales medidas dan lugar, por su propia naturaleza, a graves injerencias en los derechos fundamentales protegidos por los artículos 7 y 8 de la Carta, [72] relacionadas, en particular, con su finalidad preventiva y predictiva, que requiere la evaluación de datos de carácter personal relativos a amplios segmentos de la población, siendo su

66 SWD(2020)128 final.

67 El documento de trabajo de 2020 (p. 28 y nota a pie de página 55) menciona un porcentaje de resultados positivos del 0,59 % en 2019, de los cuales solo el 0,11 % fueron objeto una transferencia a las autoridades competentes. En el año 2018, los porcentajes correspondientes fueron del 0,25 % y del 0,04 %, respectivamente.

68 Véase el Dictamen 1/15, apartado 132.

69 Antes de la crisis sanitaria, el sistema establecido por la Directiva PNR podía abarcar hasta mil millones de pasajeros al año, datos accesibles en https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=fr.

70 A saber, cualquier persona que encaje en el concepto de «pasajero», según se define en el artículo 3, punto 4, de la Directiva PNR, y que tome un «vuelo exterior de la UE» y, *de facto*, un «vuelo interior de la UE».

71 En un estudio emitido por la Comisión Europea por la Democracia a través del Derecho (Comisión de Venecia) en 2015, se considera que tales medidas corresponden al concepto de «vigilancia estratégica» y que siguen una «tendencia general» a hacer uso de una «vigilancia proactiva» de la población; véase el estudio *Actualización del Informe de 2007 sobre el control democrático de los servicios de seguridad e Informe sobre el control democrático de las agencias de recogida de información de origen electromagnético*, adoptado por la Comisión de Venecia durante su 102.ª sesión plenaria (Venecia, 20 y 21 de marzo de 2015), https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f, punto 61.

72 En cuanto al artículo 8 del CEDH, véase TEDH, sentencia de 25 de mayo de 2021, Big Brother Watch y otros c. Reino Unido (CE:ECHR:2021:0525JUD005817013) (en lo sucesivo, «sentencia Big Brother Watch»), § 325, sobre medidas de intervención masiva, en la que el TEDH afirma que la intensidad de la injerencia en el ejercicio del derecho al respecto de la vida privada de tales medidas aumenta a medida que se van franqueando las distintas etapas del proceso, a saber, la intervención y la retención inicial de las comunicaciones y de los datos vinculados a las mismas, el tratamiento automatizado mediante la aplicación de selectores, el examen realizado por analistas y la subsiguiente retención de los datos, así como el uso del «producto final».

fin el de «identificar» a las personas que, en función del resultado de dicha evaluación, deberían quedar sujetas a un examen más exhaustivo por parte de las autoridades competentes.[73] Por otra parte, el recurso cada vez más generalizado, con fines de prevención de ciertos delitos graves, al tratamiento de grandes cantidades de datos personales de distinta índole recogidos «en bruto», así como su cruce y su tratamiento combinado, producen un «efecto acumulativo» que amplifica la gravedad de las restricciones a los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal y tiene el riesgo de favorecer un proceso de deriva gradual hacia una «sociedad de vigilancia».[74]

81. Sobre la base del conjunto de consideraciones que anteceden, considero que la injerencia que implica la Directiva PNR en los derechos fundamentales protegidos por los artículos 7 y 8 de la Carta debe calificarse, cuando menos, de «grave».

82. Es bien cierto que, como sostiene, en particular, la Comisión, el conjunto de garantías y de salvaguardas establecidos por la Directiva PNR, especialmente para evitar una utilización abusiva de los datos PNR, puede reducir la intensidad o la gravedad de esas injerencias. No es menos cierto que todo régimen que prevea el acceso y el tratamiento de datos de carácter personal por parte de autoridades públicas presenta un nivel de gravedad, desde el punto de vista de la protección de los derechos fundamentales afectados, que es inherente a sus características objetivas. Este nivel de gravedad debe, a mi juicio, determinarse antes de proceder, en el marco de la apreciación de la proporcionalidad de las mencionadas injerencias, a evaluar la suficiencia y adecuación de las garantías previstas por ese régimen. Tal es, en mi opinión, la forma en que ha procedido hasta ahora el Tribunal de Justicia.

83. Para ser compatibles con la Carta, las injerencias que la Directiva PNR supone en los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal deben cumplir los requisitos enunciados en los puntos 65 y 66 de las presentes conclusiones, extremo que se examinará a continuación, ciñéndonos a los aspectos sometidos a la atención del Tribunal de Justicia por el órgano jurisdiccional remitente.

3. Sobre la justificación de la injerencia dimanante de la Directiva PNR

84. Mientras que la tercera cuestión prejudicial se refiere al cumplimiento del requisito establecido en el artículo 52, apartado 1, primera frase, de la Carta, con arreglo al cual toda injerencia en un derecho fundamental deberá ser «establecida por la ley», las cuestiones prejudiciales, segunda, cuarta, sexta y octava interrogan al Tribunal de Justicia, en particular, sobre el cumplimiento del principio de proporcionalidad, mencionado en la segunda frase de la referida disposición.

[73] Véanse, en este sentido, los considerandos 6 y 7 de la Directiva PNR; véase, para un análisis más profundo de la finalidad e implicaciones para la protección de la vida privada y de los datos personales, el informe titulado *Passenger Name Records (PNR), data mining and data protección: the need for strong safeguards*, preparado por Korff, D. con la contribución de Georges, M., https://rm.coe.int/16806a601b (en lo sucesivo, «Informe Korff»).

[74] Como se indica en el Informe Korff, «PNR is not an isolated issue, but a new symptom of a much wider disease».

a) Sobre el cumplimiento del requisito de que cualquier limitación al ejercicio de un derecho fundamental previsto por la Carta debe estar establecida por la ley

85. Según una jurisprudencia consolidada del Tribunal de Justicia,[75] inspirada en la jurisprudencia del TEDH,[76] el requisito de que cualquier limitación del ejercicio de un derecho fundamental deba ser «establecida por la ley» no solo se refiere al origen «legal» de la injerencia —que no se cuestiona en el presente asunto—, sino que también implica que la propia base legal que permita esta injerencia debe definir su alcance *de forma clara* y *precisa*. Al referirse a la «calidad de la ley» y, por ende, a la accesibilidad y previsibilidad de la medida de que se trate,[77] este segundo aspecto comprendido en la expresión «establecida por la ley», tanto en el sentido del artículo 52, apartado 1, de la Carta como en el del su artículo 8, apartado 2, y del artículo 8 del CEDH, no solo pretende garantizar el cumplimiento del principio de legalidad y una protección adecuada frente a la arbitrariedad,[78] sino que también obedece a una exigencia de seguridad jurídica. Esta exigencia también se afirma en el Dictamen de 19 de agosto de 2016 del Comité Consultivo del Convenio 108[79] 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»).[80]

86. Al adoptar la Directiva PNR, el propio legislador de la Unión llevó a cabo una limitación de los derechos consagrados en los artículos 7 y 8 de la Carta. Las injerencias en dichos derechos permitidas por la referida Directiva no pueden considerarse una consecuencia de la decisión de los Estados miembros,[81] pese al margen de apreciación del que han podido gozar estos últimos a la hora de transponerla al Derecho nacional, sino que encuentran su fundamento legal en la propia Directiva PNR. En estas circunstancias, incumbía al legislador de la Unión, para atenerse a la jurisprudencia recordada en el punto 85 de las presentes conclusiones y a las «exigencias elevadas» de protección de los derechos fundamentales contenidas, en particular, en la Carta y en el CEDH, a las que se refiere el considerando 15 de la Directiva PNR, establecer reglas claras y precisas que definieran tanto el alcance como la aplicación de las medidas que supongan tales injerencias.

75 Véanse, entre otras, las sentencias de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, EU:C:2020:559), apartado 175; de 8 de septiembre de 2020, Recorded Artists Actors Performers (C-265/19, EU:C:2020:677), apartado 86 y jurisprudencia citada, así como la sentencia Privacy international, apartado 65.

76 Véanse, entre otras, las sentencias del TEDH de 8 de junio de 2006, Lupsa c. Rumanía, (CE:ECHR:2006:0608JUD001033704), §§ 32 y 33, y de 15 de diciembre de 2020, Pişkìn c. Turquía (CE:ECHR:2020:1215JUD003339918), § 206; véase, asimismo, la sentencia Big Brother Watch, § 333. Sobre la necesidad de reconocer a la expresión «establecida por la ley» del artículo 52, apartado 1, de la Carta la misma interpretación que la realizada por el TEDH, véanse las conclusiones del Abogado General Wathelet presentadas en el asunto WebMindLicenses (C-419/14, EU:C:2015:606), puntos 134 a 143.

77 Véase, en último lugar, la sentencia Big Brother Watch, § 333.

78 Véase la sentencia de 17 de diciembre de 2015, WebMindLicenses (C-419/14, EU:C:2015:832), apartado 81; véase también TEDH, sentencia de 1 de julio de 2008, Liberty y otros c. Reino Unido (CE:ECHR:2008:0701JUD005824300), § 69, así como la sentencia Big Brother Watch, § 333.

79 Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptado en Estrasburgo el 28 de enero de 1981 y ratificado por los Estados miembros, más conocido como «Convenio 108». En 2018, se adoptó un Protocolo modificativo dirigido a su modernización. Mediante Decisión (UE) 2019/682 del Consejo, de 9 de abril de 2019 (DO 2019, L 115, p. 7), se autorizó a los Estados miembros a firmar, en interés de la Unión, el mencionado Protocolo modificativo, en la medida en que sus disposiciones entran en el ámbito de la competencia exclusiva de la Unión. En las siguientes conclusiones, me referiré también al texto del Convenio 108 modernizado, que, si bien no ha sido aún ratificado por todos los Estados miembros y no ha entrado todavía en vigor, prevé, como resulta de la Decisión 2019/682, garantías basadas en los mismos principios que los establecidos en el RGPD y en la Directiva Policía.

80 https://rm.coe.int/t-pd-2016-18rev-avis-pnr-fr/16807b6c09, pp. 3 y 5. El Informe explicativo que acompaña al Protocolo modificativo del Convenio 108 (en lo sucesivo, «Informe explicativo del Convenio 108 modernizado») también hace hincapié en el requisito de que la medida que establezca injerencias en los derechos al respeto de la vida privada y a la protección de los datos personales sea «accesible», «previsible», «suficientemente detallada» y «descrita con claridad»; véase el punto 91 de dicho Informe explicativo, https://rm.coe.int/informe-explicativo-de-convenio/1680968479.

81 Véase, *a contrario*, la sentencia de 3 de diciembre de 2019, República Checa/Parlamento y Consejo (C-482/17, EU:C:2019:1035), apartado 135.

87. Si, mediante su tercera cuestión prejudicial, el órgano jurisdiccional remitente se interroga específicamente sobre el cumplimiento de esta obligación en relación con los puntos 12 y 18 del anexo I, el examen de las cuestiones prejudiciales segunda, cuarta y sexta, mediante las cuales dicho órgano jurisdiccional plantea dudas en cuanto al carácter necesario de las injerencias que implica la Directiva PNR en los derechos fundamentales enunciados en los artículos 7 y 8 de la Carta, también requerirá pronunciarse sobre el carácter suficientemente claro y preciso de las disposiciones de la Directiva PNR que se han puesto en tela de juicio.

88. Aunque este análisis se refiera, como he señalado en el punto 85 de las presentes conclusiones, a la legalidad de la injerencia, en el sentido del artículo 52, apartado 1, primera frase, de la Carta, lo llevaré a cabo dentro del examen de su proporcionalidad, a que se refiere la segunda frase de dicho apartado, ateniéndome al enfoque seguido tanto por el Tribunal de Justicia como por el TEDH en asuntos en los que se examinan las medidas que tienen por objeto el tratamiento de datos personales. [82]

b) Sobre el respeto del contenido esencial de los derechos consagrados en los artículos 7 y 8 de la Carta

89. De acuerdo con el artículo 52, apartado 1, primera frase, de la Carta, cualquier restricción al ejercicio de los derechos fundamentales no solo debe fundamentarse en una base legal suficientemente precisa, sino también respetar el *contenido esencial* de dichos derechos.

90. Como se ha expuesto en el punto 66 de las presentes conclusiones, esta exigencia —que ha sido incorporada a las constituciones de diferentes Estados miembros, [83] y que, sin estar expresamente reconocida por el CEDH, está, sin embargo, muy arraigada en la jurisprudencia del TEDH— [84] aparece consagrada en el artículo 52, apartado 1, de la Carta. [85] Dicha exigencia, que fue reconocida por el Tribunal de Justicia mucho antes de ser codificada, [86] ha sido reiteradamente confirmada en la jurisprudencia de los órganos jurisdiccionales de la Unión, incluso antes de la entrada en vigor del Tratado de Lisboa.

91. Se desprende, en particular, de la sentencia de 6 de octubre de 2015, Schrems, [87] que el hecho de que un acto de la Unión no respete el contenido esencial de un derecho fundamental da lugar, *automáticamente*, a la nulidad o invalidez de ese acto, sin que sea preciso realizar una ponderación de los intereses en juego. De esta manera, el Tribunal de Justicia reconoce que todo derecho fundamental presenta un «núcleo duro», que garantiza a toda persona una esfera de libertad al abrigo de cualquier injerencia de parte de los poderes públicos y que no puede someterse a limitaciones, [88] ya que, de lo contrario, se cuestionarían los principios democráticos, del Estado de Derecho y del respeto a la dignidad humana que subyacen en la protección de los derechos fundamentales. Por lo demás, tanto de la redacción del artículo 52, apartado 1, de la Carta como de la jurisprudencia del Tribunal de Justicia y, especialmente, de la sentencia Schrems I se

82 Véase, entre otras, la sentencia La Quadrature du Net, apartado 132 y jurisprudencia citada; véase también TEDH, sentencia Big Brother Watch, § 334.

83 Véase, al respecto, Tridimas, T., y Gentile, G.: «The essence of Rights: an unreliable Boundary?», *German Law Journal*, 2019, p. 796; Lenaerts, K.: «Limits on limitations: The Essence of Fundamental Rights in the EU», *German Law Journal*, 2019, 20, p. 779 y sig.

84 A partir de TEDH, sentencia de 24 de octubre de 1979, Winterwerp c. Países Bajos, (CE:ECHR:1979:1024JUD000630173), § 60.

85 Véanse las Explicaciones sobre la Carta de los Derechos Fundamentales (DO 2007, C 303, p. 17, en particular «Explicación relativa al artículo 52», p. 32; en lo sucesivo, «Explicaciones sobre la Carta»).

86 Véanse, ya en este sentido, en particular, las sentencias de 14 de mayo de 1974, Nold/Comisión (4/73, EU:C:1974:51), apartado 14, y de 13 de diciembre de 1979, Hauer (44/79, EU:C:1979:290), apartado 23.

87 C-362/14, en lo sucesivo, sentencia «Schrems I», EU:C:2015:650, apartados 94 a 98.

88 Véase Lenaerts, K., *op. cit.*, p. 781; Tridimas, T., y Gentile, G., *op. cit.*, p. 803.

desprende que la apreciación relativa a la existencia de una injerencia en el contenido esencial del derecho fundamental de que se trate debe realizarse antes y con independencia de la evaluación de la proporcionalidad de la medida cuestionada. En otros términos, se trata de un test dotado de su propia autonomía.

92. Dicho esto, la delimitación de lo que constituye el «contenido esencial» y, por lo tanto, intocable, de un derecho fundamental susceptible de ser limitado en su ejercicio es una operación extremadamente compleja. Si, para cumplir su función, debería poder definirse este concepto en términos absolutos, habida cuenta de las características esenciales del derecho fundamental de que se trata, de los intereses subjetivos y objetivos que pretende proteger y, más en general, de su función en una sociedad democrática basada en el respeto de la dignidad humana, [89] en la práctica, tal operación resulta prácticamente imposible, al menos, si no se tienen en cuenta los criterios que suelen utilizarse en el examen de la proporcionalidad de la injerencia en el derecho de que se trate, tales como la gravedad de esta injerencia, su amplitud o dimensión temporal y, en consecuencia, si no se tienen en cuenta las especificidades del caso de que se trate.

93. Por lo que respecta, en particular, al derecho fundamental al respeto de la vida privada, es preciso tener en cuenta no solo la importancia que reviste, para la salud mental y física de cualquier individuo, para su bienestar, su autonomía, su realización personal y su capacidad de entablar y cultivar relaciones sociales, el hecho de disponer de una esfera privada en la que desarrollar lo que lleva dentro de sí, sino también la función que desempeña tal derecho para preservar otros derechos y libertades, tales como, en particular, las libertades de pensamiento, de conciencia, de religión, de expresión, de información, cuyo disfrute pleno supone el reconocimiento de una esfera de intimidad. Más en general, debe tenerse en cuenta que la función que cumple el respeto del derecho a la vida privada en una sociedad democrática. [90] Parece que, al apreciar la existencia de una lesión del contenido esencial de este derecho el Tribunal de Justicia tiene en cuenta tanto la *intensidad* como la *extensión* de la injerencia, lo cual lleva a considerar que tal menoscabo se define más cuantitativamente que cualitativamente. Así, de una parte, en la sentencia Digital Rights, el Tribunal de Justicia consideró, en esencia, que la obligación de conservar datos impuesta por la Directiva 2006/24/CE [91] no alcanzaba tal nivel de gravedad que tuviera un impacto en el contenido esencial del derecho al respecto de la vida privada, dado que no permitía «conocer el contenido de las comunicaciones electrónicas como tal». [92] De otra parte, en el Dictamen 1/15, el Tribunal de Justicia consideró, en esencia, que una limitación restringida a únicamente determinados aspectos de la vida privada de las personas afectadas no podía originar una injerencia en el contenido esencial de ese derecho fundamental. [93]

89 Las explicaciones sobre la Carta reconocen expresamente que «la dignidad de la persona humana forma parte de la esencia de los derechos inscritos en la […] Carta» y que «no podrá atentarse contra ella, incluso en el caso de limitación de un derecho».

90 A este respecto, me remito a las consideraciones contenidas en el voto en parte concordante común a los Jueces Lemmens, Vehabović y Bošniak en la sentencia Big Brother Watch, §§ 3 a 10.

91 Directiva del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58 (DO 2006, L 105, p. 54).

92 Véase la sentencia Digital Rights, apartado 39; véase, asimismo, en cuanto a la Directiva 2002/58, la sentencia Tele2 Sverige, apartado 101.

93 Véase el Dictamen 1/15, apartado 150.

94. Por lo que atañe al derecho fundamental a la protección de los datos de carácter personal, el Tribunal de Justicia parece considerar que el contenido esencial de dicho derecho queda a salvo cuando la medida que establece la injerencia circunscribe los fines del tratamiento y prevé normas que garanticen la seguridad de los datos en cuestión, en particular, contra la destrucción accidental o ilícita, pérdida accidental o alteración. [94]

95. En el presente asunto, aunque el órgano jurisdiccional remitente no se ha referido expresamente al requisito de respetar el contenido esencial de los derechos consagrados en los artículos 7 y 8 de la Carta, la cuestión del respeto de ese requisito subyace, a mi juicio, en las cuestiones prejudiciales cuarta a sexta. Por esta razón, sugiero al Tribunal de Justicia que la aborde.

96. En este aspecto, deseo recordar que en el apartado 150 del Dictamen 1/15, al tiempo que se reconocía que los datos PNR «pued[en], en su caso, revelar información muy precisa sobre la vida privada de una persona» [95] y que esta información puede desvelar, directa o indirectamente, datos sensibles de la persona afectada, [96] el Tribunal de Justicia concluyó, sin embargo, en relación con el proyecto de Acuerdo PNR Canadá-UE, que, dado que «la naturaleza de esa información se limita[ba] a determinados aspectos de esa vida privada, relativos en particular a los viajes aéreos entre Canadá y la Unión», la vulneración del derecho fundamental al respeto de la vida privada no podía afectar al contenido esencial de dicho derecho.

97. Pues bien, dejando de lado el hecho de que los datos PNR a que se refiere el proyecto de Acuerdo PNR Canadá-UE debían transferirse a un tercer Estado y que su posterior tratamiento correspondía a las autoridades de ese tercero Estado en el territorio de este, las injerencias en el derecho fundamental al respeto de la vida privada que resultan del mencionado proyecto de Acuerdo y las establecidas por la Directiva PNR coinciden, en gran parte, en su naturaleza. Este es el caso, en particular, de los datos PNR a que se refiere, del carácter sistemático y generalizado de la transmisión y del tratamiento de estos datos, del carácter automático de este tratamiento, así como de la conservación de estos datos. En cambio, lo que diferencia a esos dos asuntos es, por así decirlo, el «ámbito geográfico» de dichas injerencias. En efecto, como he señalado en el punto 77 de las presentes conclusiones, los tratamientos de datos de que se trata en el presente asunto no se limitan a las conexiones aéreas con un solo tercer país, como era el caso en el Dictamen 1/15, sino que abarcan prácticamente todos los vuelos que entran y que salen de la Unión y efectuados dentro de esta. De ello se sigue que, en comparación con el proyecto de Acuerdo PNR Canadá-UE, la Directiva PNR obliga al tratamiento sistemático de un número sensiblemente más importante de pasajeros aéreos que se desplazan por avión en el interior y al exterior de la Unión. Además, debido al incremento del volumen de los datos tratados y de la frecuencia con la que se recogen, parece que su tratamiento puede proporcionar informaciones a la vez más precisas y de mayor amplitud sobre la vida privada de las personas afectadas (hábitos de viajes, relaciones personales, situaciones económicas, etc.).

98. No es menos cierto que, como ocurría en el Dictamen 1/15, estas informaciones, consideradas aisladamente, solo se refieren a algunos aspectos de la vida privada relacionados con viajes aéreos. Pues bien, habida cuenta de la necesidad de definir el concepto de «contenido esencial» de los derechos fundamentales de forma restrictiva para que este conserve su función de bastión frente a los ataques a la propia sustancia de estos derechos, considero que la conclusión a la que llegó el Tribunal de Justicia en el apartado 150 del Dictamen 1/15 puede extrapolarse el presente asunto.

94 Véase en este sentido, en particular, la sentencia Digital Rights, apartado 40.

95 Véase, en este sentido, el Dictamen 1/15, apartado 128.

96 Véase el Dictamen 1/15, apartados 164 y 165.

99. En el Dictamen 1/15, el Tribunal de Justicia también descartó una vulneración del contenido esencial del derecho a la protección de los datos de carácter personal.[97] Considero que esta conclusión puede también extrapolarse a las circunstancias del presente asunto. En efecto, como ocurría con el proyecto de Acuerdo PNR Canadá-UE, la Directiva PNR acota, en su artículo 1, apartado 2, las finalidades del tratamiento de los datos PNR. Por otra parte, esta Directiva, al igual que los demás actos de la Unión a los que esta se remite, en particular, el RGPD y la Directiva Policía, contiene disposiciones específicas destinadas a garantizar, en particular, la seguridad, la confidencialidad y la integridad de esos datos y a protegerlos frente a los accesos y los tratamientos ilegales. Aunque no puede considerarse que una normativa como la que establece la Directiva PNR afecte al contenido esencial de los derechos fundamentales protegidos por los artículos 7 y 8 de la Carta, no es menos cierto que tal normativa debe estar sometida a un control de proporcionalidad estricto y riguroso.

c) Sobre el cumplimiento del requisito de que la injerencia debe favorecer el interés general

100. La Directiva PNR pretende, en particular, garantizar la seguridad interior de la Unión y proteger la vida y la seguridad de los ciudadanos a través de una transferencia de los datos PNR a las autoridades competentes de los Estados miembros con vistas a su utilización en el marco de la lucha contra el terrorismo y la delincuencia grave.[98]

101. Más concretamente, según el artículo 1, apartado 2, de la Directiva PNR, en relación con sus considerandos 6 y 7 y con la propuesta de la Comisión que condujo a la adopción de esta Directiva (en lo sucesivo, «propuesta de Directiva PNR»),[99] en relación con este objetivo, las autoridades represivas[100] utilizan los datos PNR de diferentes maneras. Primero, estos datos se utilizan con objeto de identificar personas implicadas o sospechosas de estar implicadas en delitos de terrorismo y delitos graves ya cometidos, de reunir pruebas y, en su caso, de descubrir a los cómplices de los delincuentes y desmantelar redes delictivas (utilización en «modo reactivo»). Segundo, los datos PNR pueden evaluarse antes de la llegada o salida de los pasajeros para prevenir la comisión de un delito e identificar a personas antes no sospechosas de estar implicadas en delitos de terrorismo o en delitos graves y que, a la vista del resultado del análisis de sus datos PNR, deban ser objeto de investigación adicional por parte de las autoridades policiales (utilización en «modo real»). Por último, los datos PNR se utilizan a efectos de definir criterios de evaluación que puedan luego aplicarse a la hora de apreciar el riesgo que representan los pasajeros antes de su llegada y antes de su salida (uso en «modo proactivo»). Con ese uso proactivo de los datos PNR, los servicios represivos pueden dar respuesta a la amenaza que suponen los delitos graves y el terrorismo desde una perspectiva distinta del tratamiento de otras categorías de datos personales.[101]

102. De la jurisprudencia del Tribunal de Justicia se desprende que el objetivo de protección de la seguridad pública, que abarca, en particular, la prevención, investigación, descubrimiento y persecución tanto de delitos de terrorismo como de delitos graves, constituye un objetivo de

97 Véase el Dictamen 1/15, apartado 150.

98 Véanse, en particular, considerandos 5, 6, 15 y 22 de la Directiva PNR.

99 Propuesta de la Comisión de 2 de febrero de 2011, relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves [COM(2011) 32 final, p. 4].

100 Por razones de simplificación, en las presentes conclusiones, utilizaré las expresiones «servicios represivos» o «autoridades represivas» para indicar, con carácter general, cualquier autoridad investida de autoridad en los ámbitos de la detección, prevención, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave cubiertos por la Directiva PNR.

101 Véase el considerando 7 de la Directiva PNR. Véase también la propuesta de Directiva PNR, p. 5.

interés general de la Unión, en el sentido del artículo 52, apartado 1, de la Carta que puede justificar injerencias, incluso graves, en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta. [102]

103. El Tribunal de Justicia también ha reconocido que los objetivos de protección de la seguridad pública y de lucha contra los delitos graves contribuyen a la protección de los derechos y libertades de los demás. [103] De esta forma, por lo que se refiere a la ponderación equilibrada de esos objetivos con los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, [104] es preciso tener también en cuenta la importancia de los derechos consagrados en los artículos 3, 4, 6 y 7 de la Carta. En este sentido, si bien, en la sentencia La Quadrature du Net, el Tribunal de Justicia consideró que el artículo 6 de la Carta «no puede interpretarse en el sentido de que obliga a los poderes públicos a adoptar medidas específicas para sancionar determinados delitos», [105] en cambio, por lo que respecta, específicamente, a la lucha efectiva contra los delitos perpetrados, en particular, contra los menores y otras personas vulnerables, subrayó que tanto del artículo 7 de la Carta como de los artículos 3 y 4 de esta (en lo tocante a la protección de la integridad física y psíquica de la persona y a la prohibición de la tortura y de los tratos inhumanos o degradantes) pueden resultar obligaciones positivas que incumban a los poderes públicos, con miras a la adopción de medidas jurídicas dirigidas a proteger la vida privada y familiar. [106]

104. Por último, el Tribunal de Justicia consideró que la importancia del objetivo de protección de la de la *seguridad nacional* supera a la de los objetivos de combatir la delincuencia en general, incluso grave, y de protección de la seguridad pública y que, por lo tanto, puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar esos otros objetivos. [107] Dado que las actividades terroristas pueden constituir amenazas para la seguridad nacional de los Estados miembros, el sistema establecido por la Directiva PNR, en la medida en que sirve de instrumento de lucha contra tales actividades, participa en el objetivo de protección de la seguridad nacional de los Estados miembros.

d) Sobre el respeto del principio de proporcionalidad

105. Conforme al artículo 52, apartado 1, segunda frase, de la Carta, dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones al ejercicio de un derecho fundamental reconocido por esta 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.

106. A este respecto, procede recordar que, según jurisprudencia reiterada del Tribunal de Justicia, el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos. [108]

102 Véase, en este sentido, el Dictamen 1/15 y la sentencia de 2 de marzo de 2021, Prokuratuur (Condiciones de acceso a los datos relativos a las comunicaciones electrónicas) (C-746/18, en lo sucesivo, «sentencia Prokuratuur», EU:C:2021:152), apartado 33 y jurisprudencia citada.

103 Véase, en este sentido, el Dictamen 1/15, apartado 149 y jurisprudencia citada, así como la sentencia La Quadrature du Net.

104 Véase, a continuación, un análisis relativo a la proporcionalidad de la injerencia.

105 Véase la sentencia la Quadrature du Net, apartado 125.

106 Véase la sentencia La Quadrature du Net, apartado 126 y jurisprudencia citada.

107 Véase la sentencia La Quadrature du Net, apartado 136.

108 Véase la sentencia Digital Rights, apartado 46 y jurisprudencia citada.

107. Conforme a la jurisprudencia reiterada del Tribunal de Justicia de Justicia, la protección del derecho fundamental a la intimidad a escala de la Unión exige que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de *lo estrictamente necesario*. Además, no puede perseguirse un objetivo de interés general sin tener en cuenta que debe conciliarse con los derechos fundamentales afectados por la medida, efectuando una ponderación equilibrada entre, por una parte, el objetivo de interés general y, por otra parte, los intereses y derechos de que se trate.[109] Más concretamente, la proporcionalidad de una limitación de los derechos consagrados en los artículos 7 y 8 de la Carta debe apreciarse determinando la gravedad de la injerencia que supone esa limitación y comprobando que la importancia del objetivo de interés general perseguido por dicha limitación guarde relación con tal gravedad.[110]

108. Según la jurisprudencia del Tribunal de Justicia, para cumplir el requisito de proporcionalidad, la Directiva PNR, como base legal que conlleva las injerencias en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta descritas en los puntos 70 a 83 de las presentes conclusiones, debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las medidas que supongan tales injerencias e imponer unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso, así como frente a cualquier acceso o uso ilícito de dichos datos.[111] La necesidad de disponer de tales garantías reviste especial importancia cuando, como en este asunto, los datos personales se someten a un tratamiento automatizado y cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles.[112]

109. Por lo que se refiere al alcance del control jurisdiccional del cumplimiento de las exigencias que se derivan del principio de proporcionalidad, debido al importante papel que desempeña la protección de los datos de carácter personal en lo que respecta al derecho fundamental al respeto de la vida privada y a la injerencia en estos derechos que supone la Directiva PNR, la facultad de apreciación del legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto.[113]

1) Sobre la idoneidad de los tratamientos de los datos PNR a que se refiere la Directiva PNR en relación con el objetivo perseguido

110. En el apartado 153 del Dictamen 1/15, el Tribunal de Justicia afirmó, en relación con el proyecto de Acuerdo PNR Canadá-UE, que la transferencia de los datos del PNR a Canadá y los tratamientos posteriores de estos pueden considerarse idóneos para lograr el objetivo perseguido consistente en garantizar la protección y la seguridad públicas. No creo que esta idoneidad,

109 Véase el Dictamen 1/15, apartado 140, así como la sentencia La Quadrature du Net, apartado 130, y jurisprudencia citada. La exigencia de que el tratamiento de los datos de carácter personal refleje, en cada etapa, un «equilibrio justo entre todos los intereses involucrados, ya sean públicos o privados, así como los derechos y las libertades en juego» aparece también enunciada en el artículo 5 del Convenio 108.

110 Véase, en este sentido, la sentencia Ministerio Fiscal, apartado 55 y jurisprudencia citada, así como las sentencias La Quadrature du Net, apartado 131, y Prokuratuur, apartado 32.

111 Véanse, en este sentido, las sentencias Digital Rights, apartado 54, y Schrems I, apartado 91, así como el Dictamen 1/15, apartado 141.

112 Véase el Dictamen 1/15, apartado 141 y jurisprudencia citada.

113 Véase, en este sentido, la sentencia Digital Rights, apartado 48.

reconocida desde hace mucho tiempo tanto a escala de la Unión como a escala mundial [114], pueda cuestionarse por lo que atañe a la recogida y al tratamiento posterior de los datos PNR en relación tanto con los vuelos exteriores de la UE como con los vuelos interiores de la UE. [115]

111. Dicho esto, la eficacia del sistema de tratamiento de los datos PNR establecido por la Directiva solo puede evaluarse *in concreto*, apreciando los resultados de su aplicación. [116] Desde esta óptica, es fundamental que esta eficacia sea objeto de una evaluación continua basada en datos estadísticos lo más precisos y fiables posible. [117] En este sentido, la Comisión debería realizar cada cierto tiempo una revisión similar a la que ya se prevé en el artículo 19 de la Directiva PNR.

2) Sobre el carácter estrictamente necesario de la injerencia

112. Aunque la Cour constitutionnelle (Tribunal Constitucional) no haya planteado expresamente dudas acerca de si Directiva PNR contiene reglas claras, precisas y limitadas a lo estrictamente necesario en cuanto la delimitación de los fines del tratamiento de los datos PNR, [118] el análisis de la proporcionalidad del sistema establecido por esa Directiva, solicitado por el órgano jurisdiccional remitente, no puede, a mi juicio, eludir esta cuestión. [119]

i) Sobre la delimitación de los fines del tratamiento de los datos PNR

113. Delimitar claramente los fines para los cuales se permite el acceso a datos personales por parte de las autoridades competentes y su utilización posterior por estas autoridades constituye una exigencia esencial de cualquier sistema de tratamiento de datos, especialmente, con fines represivos. Por otra parte, es necesario dar cumplimiento a esta exigencia para que el Tribunal de Justicia pueda apreciar la proporcionalidad de las medidas de que se trata aplicando el test de gravedad de la injerencia en relación con la importancia del objetivo perseguido establecido en su jurisprudencia. [120]

114. El Tribunal de Justicia ha subrayado la importancia de que los fines de las medidas que supongan limitaciones a los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales se delimiten con claridad, especialmente, en la sentencia Digital Rights, en la que declaró inválida la Directiva 2006/24. En el apartado 60 de dicha sentencia, el Tribunal de Justicia señaló que esta Directiva no fijaba «ningún criterio objetivo que permit[iera] delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a la magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, pu[dieran] considerarse suficientemente graves para justificar tal injerencia» y que, por el contrario, se limitaba a «remitir de manera general, en su artículo 1, apartado 1, a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro».

114 Véanse, en este sentido, los puntos 201 a 203 de las presentes conclusiones.

115 Me remito, a este respecto, a los datos contenidos en el documento de trabajo de 2020.

116 Véase, en este sentido, el Dictamen de 19 de agosto de 2016, p. 5.

117 Sobre la importancia de las estadísticas a efectos de la evaluación de la eficacia del sistema establecido por la Directiva PNR, véase, en particular, el Dictamen 1/2011 de 14 de junio de 2011, sobre la propuesta de Directiva PNR, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_FR.pdf, punto 2.1.2.1 (en lo sucesivo, «Dictamen 1/2011 de la FRA»).

118 En cambio, el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden, Alemania) plantea claramente esta cuestión en el asunto pendiente C-215/20.

119 Se dirigió a la Comisión una pregunta al efecto de que formulara por escrito sus observaciones sobre este tema. Las demás partes interesadas tuvieron ocasión de manifestarse al respecto sobre durante la vista.

120 Véase, el punto 107, *in fine*, de las presentes conclusiones.

115. El artículo 1, apartado 2, de la Directiva PNR enuncia un criterio general de limitación de las finalidades con arreglo al cual «los datos PNR obtenidos con arreglo a la presente Directiva podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves». Sin embargo, contrariamente a la Directiva 2006/24, la Directiva PNR no se limita a esta enunciación, sino que define, ella misma, en su artículo 3, puntos 8 y 9, tanto el concepto de «delitos de terrorismo» como el de «delitos graves», el primero, mediante una remisión a los artículos 1 a 4 de la Decisión marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (DO 2002, L 164, p. 3) [sustituida por la Directiva (UE) 2017/541],[121] y el segundo, por una parte, enumerando, en el anexo II, las categorías de delito que corresponden a ese concepto y, por otra parte, estableciendo un nivel de gravedad en función de la duración máxima de la pena privativa de libertad o de internamiento con que pueden castigarse tales delitos.

116. Aunque la remisión a las disposiciones pertinentes de la Directiva 2017/541 permite caracterizar de forma suficientemente clara y precisa los actos que pueden calificarse de delitos de terrorismo con arreglo al artículo 3, punto 8, de la Directiva PNR y apreciar la gravedad de los mismos a efectos de ponderar la importancia del objetivo de protección de la seguridad pública perseguido por esta última Directiva y la gravedad de la injerencia que supone en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, esta conclusión no se impone con la misma nitidez en relación con todos los delitos enumerados en el anexo II.

117. En el apartado 177 del Dictamen 1/15, el Tribunal de Justicia consideró que el proyecto de Acuerdo PNR Canadá-UE definía con claridad y precisión el grado de gravedad de los delitos a que se refiere el concepto de «delitos graves de carácter transnacional», exigiendo que tales delitos estén «castigados con una pena de privación de libertad no inferior a cuatro años o una pena más grave», remitiendo «a los delitos definidos por el Derecho canadiense» y enunciando «los diferentes supuestos en que un delito se considera de carácter transnacional».

118. En comparación con la normativa examinada por el Tribunal de Justicia en dicho dictamen, la Directiva PNR, primero, no tiene en cuenta, en la definición de los delitos a que se refiere, su carácter transnacional, segundo, establece un catálogo exhaustivo de delitos que, por su propia naturaleza, se consideran graves siempre que la pena máxima prevista para ellos alcance el mínimo previsto en el artículo 3, punto 9, de esta Directiva y, tercero, rebaja, en principio, el umbral de gravedad, adoptando un criterio basado en el nivel de la pena máxima y estableciendo ese nivel en tres años.

119. Por lo que atañe, en primer lugar, a la falta de un criterio de limitación basado en el carácter transnacional, bien es cierto que circunscribir el ámbito de aplicación material de la Directiva PNR únicamente a la delincuencia grave «transfronteriza» habría permitido cribar delitos que, por su naturaleza, podrían tener, al menos potencialmente, una relación objetiva con los viajes aéreos y, por lo tanto, con las categorías de datos recogidos y tratados con arreglo a la Directiva PNR.[122] Sin embargo, comparto, como principio, el punto de vista expresado por la Comisión con arreglo al

[121] Directiva del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo (DO 2017, L 88, p. 6).

[122] Deseo señalar a este respecto que, el concepto de «delito de carácter transnacional» tal y como se define, por ejemplo, en el proyecto de Acuerdo PNR Canadá-UE era suficientemente extenso para incluir también delitos cometidos en un solo país y cuyo autor «se enc[ontrara] en otro país o [tuviera] la intención de viajar a otro país»; véase el artículo 3, apartado 3, letra e), del proyecto de Acuerdo PNR Canadá-UE, cuya redacción figura en el apartado 30 del Dictamen 1/15. Asimismo, deseo señalar que, en su Dictamen 1/2011 (puntos 2.2.3.1 y 3.7), la FRA había sugerido limitar el sistema PNR de la Unión únicamente a los delitos transnacionales graves. En cambio, la propuesta de Directiva PNR contemplaba un tratamiento automatizado diferenciado para los delitos transnacionales y para aquellos que no revistieran este carácter (véase el artículo 4, apartado 2, letrado a), de esta propuesta).

cual, a diferencia de lo que ocurre en el contexto de un acuerdo internacional, la pertinencia y la necesidad de este criterio es menos evidente al tratarse de un dispositivo de lucha contra la delincuencia cuyo objetivo es proteger la seguridad interior de la Unión. Por otra parte, como sigue afirmando la Comisión, la ausencia de elementos transfronterizos no constituye un indicio que permita, por sí mismo, excluir la gravedad de una infracción.

120. En segundo lugar, por lo que se refiere al criterio que fija el umbral de gravedad de los delitos contemplados —que, a efectos de permitir una apreciación *ex ante* de esta gravedad, debe interpretarse en el sentido de que se refiere a la duración máxima de la pena privativa de libertad o del internamiento previsto por la ley y no aquella que pueda imponerse en un supuesto particular—, este criterio, aunque se base en el mínimo de la pena máxima y no en el mínimo de la pena mínima, no es en sí mismo inadecuado para determinar un nivel de gravedad suficiente para poder justificar la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que implican los tratamientos de datos previstos en la Directiva PNR. Sin embargo, es preciso, a mi juicio, interpretarlo como un criterio que determina un nivel de gravedad «mínimo». Así pues, si bien este criterio prohíbe a los Estados miembros considerar como «delitos graves» delitos contemplados en el anexo II para los cuales su Derecho penal establezca una pena de privación de libertad o una detención de una duración máxima inferior a tres años, no les obliga a reconocer automáticamente esta calificación a todos los delitos que pueden incluirse en el mencionado anexo II que puedan ser sancionados con una pena que alcance el umbral establecido en el artículo 3, punto 9, de la Directiva PNR, cuando, habida cuenta de las características específicas de su sistema penal, este reconocimiento conduciría a que se utilizara el régimen establecido por la Directiva PNR con fines de prevención, detección, investigación y enjuiciamiento de la delincuencia común, lo cual es contrario a las finalidades perseguidas por esta Directiva.

121. En tercer lugar, por lo que atañe al catálogo del anexo II, procede señalar, antes que nada, que la circunstancia de que la Directiva PNR enumere con carácter limitativo los delitos que responden a la definición de «delitos graves» constituye una garantía formal y sustantiva fundamental para garantizar la legalidad del sistema establecido por la Directiva PNR y la seguridad jurídica de los pasajeros. Sin embargo, es preciso observar que el mencionado catálogo incluye tanto delitos que, por su naturaleza, revisten un nivel de gravedad incuestionablemente —como, por ejemplo, la trata de seres humanos, la explotación sexual de los niños y la pornografía infantil, el tráfico ilícito de armas o de materias nucleares o radioactivas, el secuestro de aeronaves y buques, delitos incluidos en la jurisdicción de la Corte Penal Internacional, el homicidio voluntario, la violación, el secuestro, la detención ilegal y la toma de rehenes— [123] como delitos en

[123] Por otra parte, debo subrayar que una parte de los delitos mencionados en el anexo corresponden a ámbitos delictivos calificados como «de especial gravedad» por el artículo 83 TFUE, apartado 1, párrafo primero, y enumerados en el párrafo segundo del referido apartado. Se trata, en particular, de la trata de seres humanos, la explotación sexual de niños, el tráfico ilícito de drogas, el tráfico ilícito de armas, el blanqueo de capitales, la corrupción, la falsificación de medios de pago, la delincuencia informática y la delincuencia organizada. En varios de los ámbitos mencionados, el legislador de la Unión ha adoptado, con arreglo al artículo 83 TFUE, apartado 1, directivas por las que se establecen «normas mínimas relativas a la definición de las infracciones penales y de las sanciones»; véanse, en particular, la Directiva 2011/36/UE del Parlamento Europeo y del Consejo, de 5 de abril de 2011, relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas y por la que se sustituye la Decisión Marco 2002/629/JAI del Consejo (DO 2011, L 101, p. 1); la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo (DO 2011, L 335, p. 1); la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo (DO 2013, L 218, p. 8); la Directiva (UE) 2019/713 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión Marco 2001/413/JAI del Consejo (DO 2019, L 123, p. 18); la Directiva (UE) 2017/1371 del Parlamento Europeo y del Consejo, de 5 de julio de 2017, sobre la lucha contra el fraude que afecta a los intereses financieros de la Unión a través del Derecho penal (DO 2017, L 198, p. 29), y Directiva (UE) 2018/1673 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal (DO 2018, L 284, p. 22).

los que tal nivel de gravedad resulta menos evidente, como el fraude, la falsificación y la violación de derechos de propiedad intelectual o industrial de mercancías, la falsificación de documentos administrativos y el tráfico de documentos administrativos falsos, así como el tráfico de vehículos robados.[124] Por otra parte, entre los delitos incluidos en el anexo II, algunos tienen mayor tendencia que otros a revestir, por su propia naturaleza, carácter transnacional, como la trata de seres humanos, el tráfico ilícito de estupefacientes o de armas, la explotación sexual de niños, la ayuda a la entrada y residencia ilegales, el secuestro de aeronaves y también a tener relación con el transporte aéreo de pasajeros.

122. En cuanto al carácter suficientemente claro y preciso de las categorías que figuran en el anexo II, también aquí el nivel es muy variable. Así, aunque la lista contenida en ese anexo deba considerarse exhaustiva, varias de sus categorías son de carácter «abierto»[125] y otras remiten a conceptos genéricos, que pueden incluir un amplio número de delitos de gravedad variable, aunque siempre respetando el umbral máximo establecido en el artículo 3, punto 9, de la Directiva PNR.[126]

123. Sobre este particular, debo señalar, de una parte, que las directivas de armonización adoptadas en los ámbitos a que se refiere el artículo 83 TFUE, apartado 1, mencionadas en la nota 123 de las presentes conclusiones, aportan elementos pertinentes para poder identificar, cuando menos, algunos delitos graves que pueden encajar en las categorías correspondientes del anexo II. Así, en particular, la Directiva 2013/40 define, en sus artículos 3 a 8, diferentes infracciones penales que corresponden al concepto de «delitos informáticos/ciberdelincuencia» a que se refiere el punto 9 del referido anexo II, cuidándose, en cada caso, de excluir actos que constituyan «casos de menor gravedad».[127] De igual forma, la Directiva 2019/713 define algunas tipologías de delitos de fraude y la Directiva 2017/1371 define los elementos constitutivos de un «fraude contra los intereses financieros de la Unión». En este contexto, debe también mencionarse la Directiva 2008/99/CE, adoptada sobre la base del artículo 175 CE, apartado 1, relativa a la protección del medio ambiente mediante el Derecho penal,[128] que define, en su artículo 3, una serie de delitos medioambientales graves, que pueden incluirse en la categoría 10 del anexo II, incluidos los actos que pueden calificarse de «tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas», excluyendo cualquier actuación que tenga un impacto desdeñable sobre el bien protegido. Por último, debo recordar la Directiva 2002/90/CE,[129] que define la ayuda a la entrada, a la circulación y a la estancia irregulares, así como la Decisión marco 2002/946/JAI,[130] destinada a reforzar el marco penal para la represión de

124 No obstante, deseo señalar que todos los delitos mencionados en el anexo I, a excepción del «espionaje industrial», figuran en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO 2002, L 190, p. 1). Aunque no se los califique expresamente de graves, dan lugar a que, cuando alcanzan el mismo umbral de pena privativa de libertad prevista en el artículo 3, punto 9, de la Directiva PNR, a la entrega en virtud de una orden de detención europea, sin control de la doble tipificación de los hechos. La práctica totalidad de esos delitos, a excepción del «sabotaje», del «secuestro de aeronaves» y del «espionaje industrial», también figuran en el anexo I del Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo (DO 2018, L 295, p. 138), que enumera la lista de las «formas de delincuencia grave» para las que Eurojust es competente.

125 Se trata, en particular, de los puntos 7, 8, 10 y 16.

126 Así ocurre, por ejemplo, con el «fraude» (punto 7), la «corrupción» (punto 6), los «delitos informáticos/ciberdelincuencia» (punto 9) y los «delitos contra el medio ambiente» (punto 10). En el asunto pendiente C-215/20, el Verwaltungsgericht Wiesbaden (Tribunal de lo Contencioso-Administrativo de Wiesbaden) se interroga, en particular, sobre unos delitos de fraude.

127 Por otra parte, en su artículo 9, esta Directiva precisa la duración mínima de la sanción máxima de privación de libertad con la que deben sancionarse tales delitos, umbral que solo en determinadas circunstancias alcanza los tres años.

128 Directiva del Parlamento y del Consejo, de 19 de noviembre de 2008 (DO 2008, L 328, p. 28).

129 Directiva del Consejo, de 28 de noviembre de 2002, destinada a definir la ayuda a la entrada, a la circulación y a la estancia irregulares (DO 2002, L 328, p. 17).

130 Decisión marco del Consejo, de 28 de noviembre de 2002, destinada a reforzar el marco penal para la represión de la ayuda a la entrada, a la circulación y a la estancia irregulares (DO 2002, L 328, p. 1).

dichos delitos, la Decisión marco 2003/568/JAI,[131] que define las infracciones penales calificadas de «corrupción activa y pasiva en el sector privado», y la Decisión marco 2008/841/JAI,[132] que define las infracciones relativas a la participación en una organización delictiva.

124. Por otra parte, debo señalar que, como ha indicado con razón la Comisión, en ausencia de una armonización completa del Derecho penal material, no cabe reprochar al legislador de la Unión no haber precisado con mayor detalle los delitos mencionados en el anexo II. Así, a diferencia de lo que se señalará más adelante en las presentes conclusiones en relación con la lista de los datos PNR contenida en el anexo I, la transposición al Derecho interno del catálogo de delitos del anexo II requiere necesariamente que los Estados miembros definan, en función de las especificidades de sus sistemas penales nacionales, los delitos a los que puede referirse. Sin embargo, esta operación debe efectuarse respetando plenamente el criterio de que cualquier injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta debe limitarse a lo estrictamente necesario. De esta forma, no debe descartarse, en mi opinión, que, por ejemplo, los Estados miembros establezcan que la utilización de los datos PNR se limite, en relación con algunos delitos como, por ejemplo, los mencionados en los puntos 7, 16, 17, 18, 25 del anexo II, a los casos en que los delitos revistan un carácter transfronterizo o se cometan en el marco de una organización delictiva, o en que concurran en ellos ciertas circunstancias agravantes. Corresponderá a los órganos jurisdiccionales de los Estados miembros, bajo el control del Tribunal de Justicia, interpretar las disposiciones nacionales de transposición al Derecho interno del mencionado catálogo de una forma conforme tanto con la Directiva PNR como con la Carta, de manera que el tratamiento de los datos PNR siga limitado, para cada categoría, a los delitos que alcancen el nivel de gravedad requerido por dicha Directiva y a aquellos delitos para los que resulte pertinente tal tratamiento.[133]

125. Sin perjuicio de lo que se ha precisado en los puntos 120 y 124 de las presentes conclusiones, considero que el artículo 3, punto 9, de la Directiva PNR, así como el catálogo de delitos recogido en su anexo II cumplen los requisitos de claridad y de precisión y no sobrepasan los límites de lo estrictamente necesario.

126. Sin embargo, es preciso reconocer que la solución que se ilustra en el punto 124 de las presentes conclusiones no es enteramente satisfactoria. En efecto, por una parte, deja en manos de los Estados miembros un importante margen de discrecionalidad, de forma que el ámbito de aplicación material del tratamiento de los datos PNR puede variar sensiblemente de un Estado miembro a otro, comprometiendo también el objetivo de armonización perseguido por el legislador de la Unión.[134] Por otra parte, implica que el control de proporcionalidad en relación con un elemento fundamental del sistema, como es la limitación de los fines de este tratamiento, se ejerza *a posteriori* sobre las medidas nacionales de transposición, más que *a priori* sobre la propia Directiva PNR. En consecuencia, sería deseable que, en el supuesto de que el Tribunal de Justicia decida considerar, como se le sugiere, que el artículo 3, punto 9, de la Directiva PNR y también el catálogo de delitos contenido en su anexo II son conformes a los artículos 7, 8 y al artículo 52, apartado 1, de la Carta, llame la atención del legislador de la Unión sobre el carácter meramente provisional de esta apreciación y sobre el hecho de que requiere, por parte de dicho legislador, que compruebe, a la luz de la transposición que los Estados miembros han hecho de esta disposición y de dicho catálogo y con arreglo a los datos estadísticos a que se refiere el artículo 20 de la Directiva PNR, si es necesario: i) precisar con más detalle, restringiendo su

131 Decisión marco del Consejo, de 22 de julio de 2003, relativa a la lucha contra la delincuencia organizada (DO 2003, L 192, p. 54).

132 Decisión marco del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada (DO 2008, L 300, p. 42).

133 Véanse, en particular, considerandos 7 y 22 de la Directiva PNR.

134 Véase el considerando 35 de la Directiva PNR.

extensión, las categorías de delitos mencionados en dicho catálogo, ii) eliminar de este los delitos en relación con los cuales el tratamiento de los datos PNR resulte, o bien desproporcionado, o bien no pertinente, o ineficaz, y iii) elevar el umbral de gravedad de los delitos mencionados en el artículo 3, punto 9, de la Directiva PNR.[135] A este propósito, deseo subrayar que, si bien el artículo 19, apartado 2, letra b), de la Directiva PNR obliga a la Comisión a efectuar la revisión de todos los elementos de dicha Directiva, prestando especial atención «a la necesidad y la proporcionalidad de la recogida y del tratamiento de datos PNR para cada uno de los fines establecidos» en esta, ni el Informe de la Comisión de 2020 ni el documento de trabajo de 2020 que lo acompaña contienen, a mi juicio, un examen satisfactorio a tal respecto.

ii) Sobre las categorías de datos PNR mencionadas por la Directiva PNR (cuestiones prejudiciales segunda y tercera)

127. La Directiva PNR prevé la transmisión a las UIP de diecinueve categorías de datos PNR recogidos por las compañías aéreas a efectos de las reservas de vuelos. Estas categorías, enumeradas en el anexo I, corresponden a las que aparecen en los sistemas de reserva de las compañías aéreas y a las que se enumeran en el anexo I de las directrices sobre los datos del registro de nombres de los pasajeros aprobadas por la Organización de la Aviación Civil Internacional (OACI) en 2010[136] (en lo sucesivo, «directrices de la OACI»).

128. Mediante su segunda cuestión prejudicial, el órgano jurisdiccional remitente se pregunta acerca de la validez del anexo I a la luz de los artículos 7, 8, y del artículo 52, apartado 1, de la Carta, habida cuenta, por una parte, de la amplitud de los datos personales enumerados en dicho anexo —y, especialmente, de los datos API mencionados en el punto 18 de este, en la medida que van más allá de los datos enumerados en el artículo 3, apartado 2, de la Directiva API—, y, por otra parte, de la posibilidad de que esos datos, considerados conjuntamente, revelen datos sensibles y, en consecuencia, sobrepasen los límites de lo «estrictamente necesario». En cambio, mediante su tercera cuestión prejudicial —que, como ya he tenido ocasión de señalar, trata del cumplimiento del primero de los tres requisitos establecidos en el artículo 52, apartado 1, de la Carta, con arreglo al cual cualquier injerencia en un derecho fundamental deberá ser «establecida por la ley»—, la Cour constitutionnelle (Tribunal Constitucional) interroga al Tribunal de Justicia sobre la validez de los puntos 12 y 18 del anexo I, teniendo en cuenta, en particular, su carácter «abierto».

129. Dado que el examen que debe realizarse en el marco de la segunda cuestión prejudicial presupone el del carácter suficientemente claro y preciso de las categorías de datos personales mencionados en el anexo I, abordaré primero la tercera cuestión prejudicial.

– Sobre el carácter suficientemente claro y preciso de los puntos 12 y 18 del anexo I (tercera cuestión prejudicial)

130. Es preciso señalar, con carácter preliminar, que la amplitud y la gravedad de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta que implica una medida que introduce limitaciones en el ejercicio de tales derechos depende, ante todo, de la extensión y

135 Véanse, por analogía, las sentencias de 16 de diciembre de 2008, Arcelor Atlantique et Lorraine y otros (C-127/07, EU:C:2008:728), apartados 61 y 62, y de 17 de octubre de 2013, Schaible (C-101/12, EU:C:2013:661), apartados 91 y 94.

136 Véase el documento 9944, aprobado por el Secretario General de la OACI y publicado bajo su autoridad. Puede accederse a la versión de este documento en lengua española en https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_es.pdf. Con arreglo al punto 9.22 del anexo 9 (Facilitación) al Convenio sobre Aviación Civil Internacional, firmado en Chicago, el 7 de diciembre de 1944) (en lo sucesivo, «Convenio de Chicago»), los Estados contratantes que requieran datos PNR deberán ajustar sus necesidades en materia de datos y el tratamiento de estos datos, entre otros, a estas directrices.

de la naturaleza de los datos personales que son objeto del tratamiento. Por lo tanto, la identificación de tales datos constituye una operación fundamental que cualquier base legal por la que se introduzca tal medida debe efectuar imperativamente, del modo más claro y preciso que sea posible.

131. Esta exigencia fue reconocida, en relación con el tratamiento de los datos PNR, por el Dictamen 1/15. Al pronunciarse sobre las categorías que figuran en el anexo del proyecto de Acuerdo PNR Canadá-UE que contienen la enumeración de los datos PNR contemplados por el Acuerdo proyectado, el Tribunal de Justicia consideró, en particular, en el referido dictamen, que el recurso a categorías generales de información que no especifiquen suficientemente el alcance de la información que debe transferirse, así como la utilización de listas de ejemplos de datos, en las que no se establece limitación alguna en cuanto a la naturaleza y el alcance de la información que puede incluirse en la categoría de que se trate no cumplían los requisitos de claridad y de precisión.

132. Tales son los principios a la luz de los cuales procede examinar la tercera cuestión prejudicial.

133. En cuanto al punto 12 del anexo I, está redactado en los siguientes términos:

«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).»

134. Al referirse a «observaciones generales», este punto constituye, al igual que la categoría 17 del anexo del proyecto de Acuerdo PNR Canadá-UE, una categoría denominada «de texto libre», destinada a incluir toda la información recogida por las compañías aéreas en el marco de su actividad de prestación de servicios, además de las que las que se enumeran en otros puntos del anexo I. Pues bien, es preciso señalar, como lo hace el Tribunal de Justicia en el apartado 160 del Dictamen 1/15, que «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 […] PNR». Además, puesto que la precisión entre paréntesis incluida en la redacción del punto 12 del anexo I, relativa a la información sobre menores no acompañados únicamente se facilita a modo de ejemplo, como lo demuestra el empleo del término «incluida», este punto no establece limitación alguna en cuanto a la naturaleza y el alcance de la información que puede figurar en él. [137]

135. En estas circunstancias, no puede considerarse que el punto 12 del anexo I se esté delimitado con suficiente claridad y precisión.

136. Mientras que la Comisión y el Parlamento parecen compartir esta conclusión, los Estados miembros que han presentado observaciones sobre la tercera cuestión prejudicial y el Consejo se oponen a tal conclusión y lo hacen siguiendo unos argumentos que se solapan en gran medida.

[137] En el mismo sentido, véase el Dictamen 1/15, apartado 160.

137. En primer lugar, una primera serie de argumentos pretende, de forma general, cuestionar la posibilidad de extrapolar al presente asunto las conclusiones a las que llegó el Tribunal de Justicia en su Dictamen 1/15.

138. A este respecto, aun siendo consciente del diferente contexto que caracteriza los dos asuntos, me voy a limitar a señalar que la conclusión a la que llegó el Tribunal de Justicia en el apartado 160 del Dictamen 1/15 en relación con la categoría 17 del anexo del proyecto de Acuerdo PNR Canadá-UE se basaba en una interpretación exclusivamente semántica y estructural de esta categoría. Pues bien, esta interpretación puede extrapolarse perfectamente al punto 12 del anexo I, cuya redacción es, en su parte que no tiene carácter ilustrativo, idéntica a la de la mencionada categoría y presenta una estructura similar. Por otra parte, como se verá con mayor detalle a continuación, las dos disposiciones en cuestión se insertan en el mismo contexto normativo multilateral del que forman parte, en particular, las directrices de la OACI, a las que, por otra parte, se refiere expresamente el Tribunal de Justicia en el apartado 156 del Dictamen 1/15. En estas circunstancias no solamente nada se opone a que se siga, en relación con el punto 12 del anexo I, la misma interpretación que la que adoptó el Tribunal de Justicia en el apartado 160 del Dictamen 1/15 para la categoría 17 del anexo del proyecto de Acuerdo PNR Canadá-UE, sino que, además, nada justifica apartarse de ella.

139. En segundo lugar, un buen número de Estados miembros subraya que los distintos puntos del anexo I, incluido el punto 12, corresponden a las categorías del anexo I de las directrices de la OACI, que las compañías aéreas conocen bien y a las que pueden perfectamente dar un contenido preciso. Según dichos Estados miembros este punto 12 corresponde, en particular, a las dos últimas categorías del mencionado anexo, tituladas respectivamente «observaciones generales» y «Texto libre/campos de códigos en OSI [*Other Supplementary Information*], SSR [*Special Service Request*], SSI [*Special Service Information*], Observaciones/historial» y que se refieren a «información complementaria» o «del servicio solicitado». [138]

140. Sobre este extremo, he de señalar, antes que nada, que la correspondencia entre las categorías del anexo I del proyecto de Acuerdo PNR Canadá-UE, de una parte, y las categorías del anexo I de las directrices de la OACI, de otra parte, no impidió al Tribunal de Justicia declarar, en el Dictamen 1/15, que algunas de las categorías que figuraban en el anexo I del mencionado proyecto de Acuerdo no eran acordes con los requisitos de claridad y precisión que debe cumplir una medida que limita el ejercicio de derechos fundamentales. Además, debo señalar que una remisión, por lo demás no explícita, [139] a las directrices de la OACI, no permite, contrariamente a lo que parecen considerar algunos Estados miembros, precisar con mayor detalle la naturaleza y el alcance de informaciones a las que puede referirse en el punto 12 del anexo I. Al contrario, la lectura de tales directrices refuerza la conclusión de que una categoría de «texto libre», como el mencionado punto 12, incluye un número indefinido de datos de distinta naturaleza, además de los que figuran sistemáticamente en los PNR. [140]

141. En tercer lugar, algunos Gobiernos sostienen que incumbe a los Estados miembros, a través de medidas legislativas internas y dentro de los límites fijados por los artículos 7, 8, y el artículo 52, apartado 1, de la Carta, precisar las informaciones que pueden figurar en el punto 12 del

138 Véanse los puntos 2.1.2 y 2.1.5 de las directrices de la OACI.

139 La única referencia a las directrices de la OACI en la Directiva PNR aparece en su considerando 17 y afecta únicamente a los «formatos de datos admitidos para la transmisión de datos PNR por las compañías aéreas a los Estados miembros».

140 Así, el punto 2.1.5 de las mencionadas directrices menciona la «información complementaria» o «del servicio solicitado», que «puede referirse a necesidades dietéticas o médicas especiales, información sobre un "menor no acompañado", solicitudes de asistencia, etc.». El punto 2.1.6 precisa, por su parte, que el «campo de "observaciones generales"» puede también incluir «alguna información, como el diálogo o comunicación interna entre el personal de la línea aérea y los agentes que hacen las reservas».

anexo I. Consideran, en efecto, que corresponde a la propia naturaleza de una Directiva dejar a los Estados miembros un margen discrecional en cuanto a los medios necesarios para poner en obra las disposiciones que este anexo establece.

142. A este respecto, como ya ha expuesto en el punto 86 de las presentes conclusiones, considero que, cuando unas medidas que supongan injerencias en los derechos fundamentales consagrados por la Carta dimanen de un acto legislativo de la Unión, incumbe al legislador de la Unión fijar, cumpliendo los criterios de claridad y de precisión antes mencionados, así como el principio de proporcionalidad, el alcance exacto de estas injerencias. De ello se sigue que, cuando el instrumento elegido por ese legislador es una directiva, no cabe, a mi juicio, delegar en los Estados miembros la posibilidad de que, a la hora de su transposición a sus Derechos nacionales, determinen los elementos esenciales que definen el alcance de la injerencia, tales como, por lo que se refiere a limitaciones a los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, la naturaleza y el alcance de los datos de carácter personal sometidos a tratamiento.

143. En cuarto lugar, algunos Estados miembros señalan que debe entenderse que el punto 12 del anexo I se refiere únicamente a la información relacionada con la prestación del transporte. Interpretado de esa manera, este punto sería, en opinión de esos Estados miembros, compatible con los artículos 7, 8 y el artículo 52, apartado 1, de la Carta.

144. Este argumento tampoco me convence. Antes que nada, las informaciones que pueden figurar en una categoría de «observaciones generales» y en los códigos OSI, SSI y SSR. son de carácter muy heterogéneo (necesidades dietéticas y médicas especiales o alimentos preferidos, solicitudes de asistencia, información sobre un menor no acompañado, etc.) [141] y todas guardan relación con la prestación del transporte, puesto que su finalidad es, en particular, que el transportista aéreo pueda adaptar esta prestación a las exigencias de cada pasajero. En consecuencia, un criterio interpretativo basado en la pertinencia de la información en relación con la prestación de transporte no permitiría precisar con mayor detalle el alcance de este punto 12. Además, debo mencionar que el Tribunal de Justicia, al tiempo que utilizó, en el apartado 159 del Dictamen 1/15, este criterio con objeto de interpretar de una forma acorde con los requisitos de claridad y de precisión una categoría diferente del anexo del proyecto de Acuerdo PNR Canadá-UE, descartó, sin embargo, hacer lo mismo en relación con la categoría 17 del mencionado anexo, que se corresponde con el punto 12 del anexo I.

145. En quinto lugar, algunos Estados miembros han puesto de relieve la circunstancia de que las informaciones a las que puede referirse el punto 12 del anexo I son facilitadas a los transportistas aéreos por los propios pasajeros, a los que se informa debidamente de la posterior transmisión de estos datos a las autoridades públicas. La idea que subyace a este argumento es, en mi opinión, la existencia de una especie de consentimiento implícito, por parte del pasajero afectado, a que los datos que facilita a las compañías aéreas se transfieran, a continuación, a las autoridades públicas.

146. A este respecto, el Tribunal de Justicia ya ha tenido ocasión de precisar que no puede existir «consentimiento» cuando el interesado no puede oponerse con libertad al tratamiento de sus datos personales. [142] Pues bien, en relación con una gran parte de la información que puede figurar en el punto 12 del anexo I, el pasajero afectado no tiene verdaderamente la posibilidad de elegir, sino que está obligado a facilitar dicha información para poder obtener la prestación de

[141] Véanse los puntos 2.1.5 y 2.1.6 de las directrices de la OACI.

[142] Véase la sentencia de 17 de octubre de 2013, Schwarz (C-291/12, EU:C:2013:670), apartado 32, relativa al supuesto del solicitante de pasaporte obligado a someterse a la toma de sus impresiones dactilares para poder disponer de un documento que le permita efectuar desplazamientos a terceros países.

transporte. Así ocurre, en particular, con las personas discapacitadas o con movilidad reducida, o con las personas que tienen necesidades médicas o con los menores no acompañados. Por otra parte, deseo recordar que, en los puntos 142 y 143 del Dictamen 1/15, el Tribunal de Justicia afirmó con claridad que, dado que los tratamientos de los datos PNR por parte de las autoridades públicas persiguen una finalidad diferente de aquellas para la que dichos datos son recogidos por las compañías aéreas, no puede considerarse que estén basados en ninguna forma de consentimiento que presten los pasajeros para su recogida.

147. Por último, la mayoría de los Estados miembros alegan que los tratamientos de datos previstos por la Directiva PNR van acompañados de numerosas garantías, entre ellas, en lo que atañe a la transmisión de datos a las UIP, la obligación de estas últimas de suprimir los datos no incluidos en el anexo I y aquellos datos que puedan revelar el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona.

148. Sobre este extremo, debo comenzar señalando que opino que la apreciación del carácter suficientemente claro y preciso de las normas que definen el alcance y la naturaleza de los datos que pueden ser objeto de transmisión a las autoridades públicas, apreciación que, al ir dirigida a garantizar que una medida que suponga injerencias en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta respete los principios de legalidad y de seguridad jurídica, debe efectuarse sin tener en cuenta las garantías que acompañan a los tratamientos a los que las mencionadas autoridades someterán tales datos, pues tales garantías solo pueden tenerse en cuenta al examinar la proporcionalidad de la medida de que se trate. Precisamente, así procedió el Tribunal de Justicia, en los apartados 155 a 163 del Dictamen 1/15, en su apreciación de las categorías del proyecto de Acuerdo PNR Canadá-UE. Añadiré, con carácter más general, que debería prestarse una atención particular a la necesidad de mantener una clara distinción entre las distintas fases que integran el examen de una medida que suponga injerencias en los derechos fundamentales, pues una confusión entre estas distintas fases va siempre en detrimento de su efectiva protección.

149. Dicho esto, me limitaré ahora a señalar, por una parte, que la obligación que incumbe a las UIP, con arreglo al artículo 6, apartado 1, de la Directiva PNR, de suprimir aquellos datos que no sean los enumerados en el anexo I solo tiene utilidad si ese anexo contiene un catálogo claro y cerrado de los datos que se transfieren. Lo mismo ocurre en relación con la obligación de las UIP, con arreglo al artículo 13, apartado 4, de la Directiva PNR, de suprimir los datos denominados «sensibles».[143] En efecto, una definición excesivamente vaga, imprecisa o abierta de la información que debe transmitirse incrementa tanto las probabilidades de que esos datos sean objeto de transferencia indirectamente como el riesgo de que no sean inmediatamente identificados y suprimidos. En otros términos, las garantías antes mencionadas solo pueden cumplir su cometido de manera eficaz si las normas que definen la naturaleza y el alcance de los datos PNR que las compañías aéreas deben transmitir a las UIP son suficientemente claras y precisas y si la lista de estos datos presenta un carácter cerrado y taxativo.

150. Atendiendo al conjunto de consideraciones que anteceden, y como ya he adelantado en el punto 135 de las presentes conclusiones, considero que el punto 12 del anexo I, en la parte en que incluye las «observaciones generales» entre los datos que las compañías aéreas deben

[143] Volveré a referirme a esta categoría más adelante en estas conclusiones.

transferir a las UIP con arreglo a la Directiva PNR, no cumple los requisitos de claridad y de precisión establecidos en el artículo 52, apartado 1, de la Carta, tal y como lo interpreta el Tribunal de Justicia, [144] y que, en consecuencia, debería declararse inválido en esa medida.

151. En sus observaciones escritas, la Comisión y el Parlamento han sugerido al Tribunal de Justicia que se incline más bien por hacer uso de una «interpretación conforme» del punto 12 del anexo I, entendiéndolo en el sentido de que solo se refiere a la información sobre los menores expresamente mencionada en el mismo dentro del paréntesis. Debo reconocer que me cuesta un poco considerar que semejante interpretación se ajuste a los límites de una mera interpretación conforme. Es bien cierto que, según un principio general de interpretación, todo acto de la Unión debe interpretarse, en la medida de lo posible, de un modo que no cuestione su validez y de conformidad con el conjunto del Derecho primario y, en particular, con las disposiciones de la Carta. [145] Es igual de cierto que, por lo que atañe a la Directiva PNR, la posibilidad de esa interpretación aparece favorecida por la insistencia, entre otros, de un buen número de considerandos de dicha Directiva en el respeto pleno de los derechos fundamentales, del derecho al respeto de la vida privada, así como del principio de proporcionalidad. [146] Sin embargo, también es de reiterada jurisprudencia que solo se admite una interpretación conforme cuando un texto de Derecho derivado de la Unión es susceptible de varias interpretaciones y que es posible, en consecuencia, dar preferencia a aquella que hace que la disposición se ajuste al Derecho primario y no a la que conduce a considerarla incompatible con él. [147]

152. Pues bien, el punto 12 del anexo I no puede, a mi juicio, interpretarse de la manera que sugieren la Comisión y el Parlamento, salvo que se haga de él una lectura «*contra legem*». En efecto, este punto se refiere, como he explicado más arriba, a una amplia categoría de datos de distinta índole, que no cabe identificar *a priori*, de la cual los datos sobre los menores solo son una subcategoría. Entender que este punto se refiere únicamente a esta subcategoría no solo equivaldría a ignorar una parte de su texto, sino que también subvertiría el orden lógico del enunciado que este punto contiene. Tal operación, que consiste, en esencia, en eliminar la parte del texto del punto 12 del anexo I que se considere no conforme con los requisitos de claridad y de precisión, solo puede efectuarse, a mi juicio, declarándolo parcialmente nulo.

153. Por lo que se refiere a la parte restante del punto 12 del anexo I, que enumera una serie de datos relativos a los menores no acompañados, considero que responde a los requisitos de claridad y de precisión siempre que se interprete en el sentido de que solo comprende la información sobre los menores no acompañados directamente relacionada con el vuelo y expresamente contemplada en dicho punto.

144 La FRA se expresó en este sentido en su Dictamen 1/2011, p. 13. En su Dictamen de 25 de marzo de 2011 sobre la propuesta de Directiva PNR, (https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_es.pdf), punto 47 (en lo sucesivo, «Dictamen de 25 de marzo de 2011»), el CEPD propuso excluir la categoría «observaciones generales» de la lista del anexo I.

145 Véanse, en particular, las sentencias de 19 de noviembre de 2009, Sturgeon y otros (C-402/07 y C-432/07, EU:C:2009:716), apartado 47 y jurisprudencia citada; de 19 de septiembre de 2013, Reexamen Comisión/Strack (C-579/12 RX-II, EU:C:2013:570), apartado 40, y de 14 de mayo de 2019, M y otros (Revocación del estatuto de refugiado) (C-391/16, C-77/17 y C-78/17, EU:C:2019:403), apartado 77 y jurisprudencia citada.

146 Véanse, en particular, considerandos 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 y 37 de la Directiva PNR.

147 Véanse las sentencias de 26 de junio de 2007, Ordre des barreaux francophones et germanophone y otros (C-305/05, EU:C:2007:383), apartado 28, y de 14 de mayo de 2019, M y otros (Revocación del estatuto de refugiado) (C-391/16, C-77/17 y C-78/17, EU:C:2019:403), apartado 77.

154. En lo tocante al punto 18 del anexo I, está redactado en los siguientes términos:

«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).»

155. La estructura que presenta este punto es análoga a la del punto 12 del anexo I. También menciona una categoría general de datos, a saber, la información anticipada sobre los pasajeros (*Advance Passenger Information-API*), seguida, entre paréntesis, de una lista de datos que se consideran incluidos en esta categoría general, la cual se facilita meramente a modo de ejemplo, como demuestra la utilización de la expresión, «incluidos».

156. No obstante, contrariamente al punto 12 del anexo I, el punto 18 de este anexo remite a una categoría de datos más fáciles de identificar tanto en lo relativo a su naturaleza como en relación con su alcance. En efecto, del considerando 4 de la Directiva PNR se desprende que, cuando esta menciona dicha categoría de datos, se refiere a la información que, con arreglo a la Directiva API —a la que este considerando remite expresamente—, es transmitida por las compañías aéreas a las autoridades nacionales competentes con objeto de mejorar los controles fronterizos y combatir la inmigración ilegal. Estos datos se enumeran en el artículo 3, apartado 2, de esta última Directiva.

157. Asimismo, según el considerando 9[148] de la Directiva PNR, el artículo 3, apartado 2, de la Directiva API y la lista de carácter ilustrativo contenida en el punto 18 del anexo I, los datos API mencionados en ese punto son, por una parte, datos biográficos que permiten verificar la identidad del pasajero aéreo y, por otra parte, datos relativos al vuelo reservado. Más precisamente, en lo que afecta a la primera categoría, la de los datos biográficos, las informaciones enumeradas en el artículo 3, apartado 2, de la Directiva API y en el punto 18 del anexo I abarcan datos, generados en el embarque, que pueden extraerse de la parte de lectura mecánica del pasaporte (u otro documento de viaje).[149]

158. Así, el punto 18 del anexo I, interpretado a la luz de los considerandos 4 y 9 de la Directiva PNR, identifica, en principio, con suficiente claridad y precisión, cuando menos, la naturaleza de los datos a que se refiere.

148 A los efectos que ahora importan, el considerando 9 establece que «utilizar los datos PNR junto con los datos API representa un valor añadido para ayudar a los Estados miembros a verificar la identidad de una persona, reforzando así el valor policial de ese resultado y reduciendo al mínimo el riesgo de realizar controles e investigaciones de personas inocentes».

149 En este sentido, véase asimismo la propuesta de Directiva PNR, p. 7, punto 1. Estos mismos datos figuran en las directrices sobre información anticipada sobre viajeros (RPCV) elaboradas por la Organización Mundial de Aduanas (OMD), la Asociación de Transporte Aéreo Internacional (IATA) y la OACI, http://www.wcoomd.org/~/media/wco/public/fr/pdf/topics/facilitation/instruments-and-tools/tools/api-guidelines-and-pnr-doc/api-guidelines-_f.pdf?db=web) [(en lo sucesivo «directrices RPCV»), punto 8.1.5, letra a)], como «elementos principales de datos que pueden figurar en la zona mecánicamente legible de los documentos de viaje oficiales».

159. En cuanto a su alcance, es preciso señalar, por una parte, que el artículo 3, apartado 2, de la Directiva API también está redactado de forma «abierta», pues la lista de datos que enumera aparece precedida de la expresión «la información contendrá» [150] y, por otra parte, que, en la categoría de los datos API, tal y como la definen los instrumentos multilaterales de armonización en la materia, también figuran datos que no son ni los mencionados en la Directiva API ni los que se mencionan en el punto 18 del anexo I. [151]

160. En estas circunstancias, para que el punto 18 del anexo I se ajuste a los requisitos de claridad y precisión exigidos a las bases legales que supongan injerencias en los derechos contemplados en los artículos 7 y 8 de la Carta, es preciso interpretarlo en el sentido de que solo comprende los datos API que se enumeran expresamente en ese punto y en el artículo 3, apartado 2, de la Directiva API y que hayan sido recopilados por las compañías aéreas en el transcurso normal de su actividad. [152]

161. En este momento, es oportuno pasar revista rápidamente a los demás puntos del anexo I que, habida cuenta de su redacción, presentan también un carácter «abierto» o no son suficientemente precisos, a pesar de que el órgano jurisdiccional remitente no haya interrogado expresamente al Tribunal de Justicia respecto de estos. [153]

162. Por lo que se refiere, en primer lugar, al punto 5 del anexo I, que menciona «dirección y datos de contacto (número de teléfono, dirección de correo electrónico)», si bien debe considerarse que únicamente se refiere a los datos de contacto expresamente indicados entre paréntesis y que presenta, por ello, un carácter exhaustivo, tal punto no precisa, como era el caso de la categoría correspondiente del proyecto de Acuerdo PNR Canadá-UE, [154] si tales datos de contacto se refieren únicamente al viajero o a terceros que hayan efectuado la reserva del vuelo para el pasajero aéreo, a aquellos terceros por medio de los cuales pueda entrarse en contacto con el pasajero aéreo o a aquellos terceros que deban ser informados en caso de urgencia. [155] Habida cuenta de que si se interpretara que el punto 5 del anexo I también se refiere a las categorías de terceros antes mencionados, la injerencia que implica la Directiva PNR se extendería a otras personas, distintas de los pasajeros aéreos en el sentido del artículo 3, punto 4, de la Directiva PNR, sugiero al Tribunal de Justicia que, en defecto de datos precisos que permitan considerar que la obtención sistemática y generalizada de los datos de contacto de esos terceros constituye un elemento estrictamente necesario para la eficacia del sistema de tratamiento de los datos PNR instituido por esta Directiva, interprete el mencionado punto en el sentido de que solo se refiere a los datos de contacto expresamente mencionados en él y referidos al pasajero aéreo en cuyo nombre se ha hecho la reserva. Ciertamente, la Directiva PNR no excluye que puedan también

150 El artículo 3, apartado 2, de la Directiva API está redactado en los siguientes términos: «La información contendrá: el número y el 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, el lugar inicial de embarque». Deseo subrayar que, en su Programa de trabajo para 2022, COM(2021) 645 final, p. 9, la Comisión ha contemplado una actualización de la Directiva API. En septiembre de 2020, había publicado una evaluación de esta Directiva como base de la futura revisión de la esta, SWD(2020), 174 final (en lo sucesivo, «documento de trabajo de 2020 sobre la Directiva API»). En el mencionado documento, la Comisión subraya, en particular, el hecho de que la lista de datos contenida en el artículo 3, apartado 2, de la Directiva API no es conforme con las normas internacionales sobre los datos API, en particular, por no incluir todos los datos que figuran en la parte legible mecánicamente de los documentos de identidad (véase, en particular, p. 48).

151 Véanse las directrices RPCV, punto 8.1.5, letras b) y c).

152 En el apartado 161 del Dictamen 1/15, se hace una interpretación análoga de la categoría correspondiente del proyecto de Acuerdo PNR Canadá-UE.

153 Debo señalar que, en la actualidad, el Tribunal de Justicia conoce de una serie de cuestiones prejudiciales que tratan específicamente del carácter suficientemente preciso de varios puntos del anexo I, especialmente de los puntos 4, 8, 12, 18 (véase el asunto pendiente C-215/20).

154 Véase el Dictamen 1/15, apartado 158.

155 Debo señalar que las informaciones relativas a la agencia o al operador de viajes ya están mencionadas en el punto 5 del anexo I.

transferirse a las UIP datos personales de otras personas distintas de los pasajeros aéreos.[156] Sin embargo, es esencial que se indiquen, de forma clara y expresa, como se hace en relación con los operadores de viajes mencionados en el anexo I, punto 9, o con los tutores de los menores que viajan solos, mencionados en el punto 12 del mencionado anexo, los supuestos en los que cabe esta posibilidad. En efecto, solo si se cumple este requisito puede considerarse que, en la decisión de incluir tales datos entre los que deben transferirse a las UIP, se han ponderado los diferentes intereses en juego, en el sentido del considerando 15 de la Directiva PNR, y que los terceros afectados pueden ser informados adecuadamente del tratamiento de sus datos personales.

163. Por otra parte, por lo que se refiere al punto 6 del anexo I, referido a «todos los datos de pago, incluida la dirección de facturación», como declaró el Tribunal de Justicia en el apartado 159 del Dictamen 1/15, en relación con la categoría correspondiente del anexo al proyecto de Acuerdo PNR Canadá-UE, para que se cumplan los requisitos de claridad y de precisión, debe interpretarse que este punto «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». En consecuencia, esta información no puede incluir, por ejemplo, la relativa a los medios de pago de otros servicios no directamente relacionados con el vuelo, como el alquiler de un vehículo a la llegada.[157]

164. En cuanto al punto 8, relativo a la «información sobre viajeros asiduos», según la definición que recogen las normas de la OACI, se trata del número de cuenta y de la categoría de este tipo de pasajero.[158] Interpretado en este sentido, este punto cumple los requisitos de claridad y de precisión.

165. En cuanto al punto 10 del anexo I, que se refiere a la «situación del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva» y al punto 13 del mismo anexo, relativo a la «información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (*Automatic Ticket Fare Quote*)», pese a su redacción abierta, estos puntos se refieren únicamente a información muy precisa y claramente identificable, directamente relacionada con el vuelo. Lo mismo cabe decir del punto 14 del anexo I, relativo a los «datos del asiento, incluido el número» y del punto 16 de dicho anexo, que menciona «toda la información relativa al equipaje».

– *Sobre el alcance de los datos enumerados en el anexo I (segunda cuestión prejudicial)*

166. Entre los elementos que el Tribunal de Justicia tiene en cuenta para apreciar el carácter proporcionado de una medida que suponga injerencias en los derechos consagrados en los artículos 7 y 8 de la Carta figura el carácter adecuado, pertinente y no excesivo de los datos personales tratados (principio de «minimización de los datos»).[159] La jurisprudencia del TEDH establece el mismo criterio,[160] preconizado por el Convenio 108.[161]

156 Véase la definición de los datos PNR en el artículo 3, punto 5, de la Directiva PNR.

157 En este sentido, véanse, asimismo, las conclusiones presentadas por el Abogado General Mengozzi en el Dictamen 1/15 (Acuerdo PNR UE-Canadá), EU:C:2016:656, punto 218.

158 Véase la categoría correspondiente del apéndice I de las directrices de la OACI.

159 En este sentido, véase especialmente la sentencia Digital Rights, apartado 57. Sobre la exigencia de que las categorías de datos contemplada por una medida de acceso se limiten a lo estrictamente necesario para el objetivo perseguido, véase, en último lugar, la sentencia Prokuratuur, apartado 38. El artículo 5, apartado 1, letra c), del RGPD y el artículo 4, apartado 1, letra c), de la Directiva Policía establecen, entre otros, el principio de minimización de los datos.

160 Véase, en particular, TEDH, sentencia de 18 de abril de 2013, M. K. c. Francia (CE:ECHR:2013:0418JUD001952209), §35.

161 Véase el Informe explicativo del Convenio 108 de 1981 (https://rm.coe.int/16800ca471), artículo 5, punto 40, así como el Informe explicativo sobre el Convenio 108 modernizado, artículo 5, punto 51.

167. Del considerando 15 de la Directiva PNR resulta que la lista de datos PNR que deba obtener una UIP se elabora con el objetivo de reflejar las legítimas necesidades de las autoridades públicas en materia de lucha contra el terrorismo y los delitos graves y, al mismo tiempo, de proteger los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal, aplicando «exigencias elevadas», conforme a la Carta, al Convenio 108 y al CEDH. El mismo considerando precisa que los datos PNR solo deberían contener, en particular, la información detallada sobre las reservas e itinerarios de viaje que permita a las autoridades competentes identificar a los pasajeros por vía aérea que representan una amenaza para la seguridad interior.

168. En primer lugar, por lo que atañe al carácter adecuado y pertinente de los datos PNR que figuran en el anexo I, los diferentes puntos de este anexo, incluidos los puntos 5, 6, 8 y 18, según la interpretación que sugiero, [162] y el punto 12, a excepción de la parte que sugiero que se declare inválida, [163] solo mencionan datos que aportan información directamente relacionada con los viajes aéreos que están incluidos en el ámbito de aplicación de la Directiva PNR. Estos datos guardan, asimismo, una relación objetiva con los fines perseguidos por la mencionada Directiva. Más en particular, los datos API pueden utilizarse, en particular, en «modo reactivo» para identificar a una persona ya conocida por los servicios represivos, por ejemplo, por el hecho de que se sospeche que está involucrada en delitos de terrorismo o en delitos graves ya cometidos o que está a punto de cometer tal delito, mientras que los datos PNR pueden utilizarse más bien en «modo real o proactivo» para identificar amenazas que proceden de personas aún desconocidas para los servicios represivos.

169. Por lo que se refiere, en segundo lugar, al alcance de los datos PNR enumerados en el anexo I, estos datos, incluidos los que figuran en los puntos 5, 6, 8, 12 y 18 del referido anexo, según la interpretación que propongo en los puntos 134 a 164 de las presentes conclusiones, no resultan excesivos, habida cuenta, por una parte, de la importancia del objetivo de seguridad pública perseguido por la Directiva PNR y, por otra parte, de la capacidad del régimen establecido por dicha Directiva para perseguir tal objetivo.

170. En particular, por lo que se refiere a los datos API sobre los cuales se interroga, en particular, el órgano jurisdiccional remitente, debo señalar que, por lo general, estos datos, de carácter biográfico y relativos al viaje que se realiza, solo permiten obtener informaciones limitadas sobre la vida privada de los pasajeros afectados. Por otra parte, si bien es cierto que en el punto 18 del anexo I se contempla información que no se encuentra entre los datos que expresamente menciona el artículo 3, apartado 2, de la Directiva API, esta información, relativa a la identidad del pasajero aéreo (sexo), al documento de viaje utilizado (país de expedición, fecha de expiración de cualquier documento de identidad) y también al vuelo tomado (compañía aérea, número de vuelo, fecha y aeropuerto de salida y de llegada), se solapa parcialmente o puede extraerse de los datos PNR mencionados en otros puntos del anexo I, por ejemplo, los puntos 3, 7 y 13. Además, en la medida en que se refieren a datos biográficos o a los documentos de viaje utilizados, tales informaciones pueden ayudar a los servicios represivos a comprobar la identidad de una persona, reduciendo así, como se indica en el considerando 9 de la Directiva PNR, el riesgo de realizar controles injustificados e investigaciones de personas inocentes. Por último, debe subrayarse que el mero hecho de que el punto 18 del anexo I incluya datos adicionales en relación con los que figuran en el artículo 3, apartado 2, de la Directiva API no puede llevar automáticamente a afirmar el carácter excesivo de esos datos, dado que dicha Directiva y la Directiva PNR persiguen objetivos diferentes.

[162] Véanse los puntos 154 a 158 y 162 a 164 de las presentes conclusiones.

[163] Véanse los puntos 133 a 153 de las presentes conclusiones.

171. En cuanto a los datos relativos a los menores no acompañados enumerados en el punto 12 del anexo I, estos datos se refieren a una categoría vulnerable de personas que gozan de una protección particular, incluso en lo tocante al respeto de su vida privada y a la protección de sus datos personales.[164] No es menos cierto que una limitación a estos derechos puede resultar necesaria, especialmente para proteger a los niños de delitos graves de los que pueden ser víctimas, tales como la trata, la explotación sexual de niños o el secuestro de niños. En consecuencia, no cabe considerar *a priori* que el punto 12 del anexo I, al exigir la transferencia de un mayor número de datos personales en lo que se refiere a los menores no acompañados, sobrepase lo estrictamente necesario.

172. Si bien es cierto que los datos personales que las compañías aéreas deben transmitir a las UIP con arreglo a la Directiva PNR responden, a mi juicio, a los requisitos de adecuación y de pertinencia y que su alcance no sobrepasa lo estrictamente necesario para el funcionamiento del régimen instituido por esta Directiva, no es menos cierto que esta transmisión afecta a un número significativo de datos personales de distintos tipos en relación con cada pasajero afectado y a un número extremadamente elevado de tales datos personales, en términos absolutos. En estas circunstancias, es primordial que esta transferencia vaya acompañada de suficientes garantías dirigidas, por una parte, a velar por que solo se transfieran los datos expresamente mencionados y, por otra parte, a garantizar la seguridad y la confidencialidad de los datos transferidos.

173. En este aspecto, es preciso señalar, de una parte, que el legislador de la Unión ha previsto, en primer lugar, una serie de garantías que permiten limitar las categorías de datos PNR a cuyo acceso se autoriza a los servicios represivos y garantizar que este acceso permanezca limitado únicamente a aquellos datos cuyo tratamiento se considere necesario a los efectos de los objetivos que persigue la Directiva PNR. De esta manera, en primer lugar, y sin perjuicio de las consideraciones desarrolladas en el marco de la respuesta a la tercera cuestión prejudicial, esta Directiva enumera, de manera taxativa y precisa, los datos que pueden ser transmitidos a las UIP. En segundo lugar, la Directiva PNR indica expresamente que solo pueden ser objeto de transmisión a las UIP los datos contenidos en esa lista, que es el resultado de una ponderación entre los distintos intereses y exigencias mencionados en el considerando 15 de esta Directiva, (artículo 6, apartado 1, de la Directiva PNR). En tercer lugar, dicha Directiva precisa que, si los datos PNR transmitidos 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» (artículo 6, apartado 1, de la Directiva PNR). En cuarto lugar, dicha Directiva establece que los datos PNR mencionados en el anexo I solo pueden ser objeto de transmisión en la medida en que ya los hayan recopilado las compañías aéreas en el transcurso normal de su actividad (artículo 8, apartado 1, y considerando 8, de la Directiva PNR), lo cual implica que no todos los datos que figuran en el anexo I son sistemáticamente accesibles para las UIP, sino solo aquellos que constan en el sistema de reserva del operador interesado. En quinto lugar, el artículo 8, apartado 1, de la Directiva PNR obliga a los transportistas aéreos a utilizar el método de transmisión «enviar» para transmitir los datos PNR a las bases de datos de las UIP. Este método, recomendado por las directrices de la OACI,[165] implica que los propios transportistas transmiten los datos PNR a las bases de datos de las UIP. En comparación con el método «extraer», que permite a las autoridades competentes tener acceso a los sistemas de los operadores de aeronaves y extraer de sus bases de datos una copia de los datos necesarios, el método «enviar» ofrece más garantías, al conferir al transportista aéreo la función de guardián y controlador de los datos PNR. Por último,

[164] El derecho del niño al que se respete su vida privada está consagrado, en particular, en el artículo 16 de la Convención de Nueva York sobre los Derechos del Niño, adoptada el 20 de noviembre de 1989 y que entró en vigor el 2 de septiembre de 1990.

[165] Véase el punto 2.7.3 de las directrices de la OACI.

ateniéndose a las directrices de la OACI y al concepto de «ventanilla única», [166] la Directiva PNR prevé que la transferencia de los datos PNR se haga por conducto de un solo organismo, la UIP, que actúa bajo la supervisión del responsable mencionado en el artículo 5 de la reiterada Directiva, y, sobre todo, bajo la autoridad nacional de control a que se refiere el artículo 15 de dicha Directiva.

174. Por otra parte, la Directiva PNR contempla un cierto número de garantías dirigidas a preservar la *seguridad* de los datos PNR. Remito, a este respecto, al artículo 13, apartado 2, de dicha Directiva, en virtud del cual los artículos 28 y 29 de la Directiva Policía sobre la confidencialidad del tratamiento y la seguridad de los datos son aplicables a cualquier tratamiento de datos personales realizado con arreglo a la Directiva PNR y al apartado 3 de ese mismo artículo, que, por lo que respecta al tratamiento de los datos PNR por las compañías aéreas, recuerda las obligaciones que incumben a estas últimas, en virtud del RGPD, especialmente en lo relativo a las medidas técnicas y de organización adecuadas para proteger la seguridad y la confidencialidad de esos datos. [167]

175. Por último, procede señalar que la Directiva PNR reconoce, en sus considerandos 29 y 37, el derecho de los pasajeros a recibir «información precisa, de fácil acceso y comprensión», entre otras cosas, sobre la recogida de los datos PNR, solicitando a los Estados miembros que se aseguren de que se respeta ese derecho. Aunque este reconocimiento no se traduzca, en el texto de la Directiva PNR, en una disposición con valor vinculante, deseo recordar, como lo he hecho al examinar la primera cuestión prejudicial, que las disposiciones del RGPD son de aplicación a la transmisión de los datos PNR a las UIP. Así pues, las compañías aéreas están obligadas, en el marco de esta transmisión, a ajustarse, entre otros, a los artículos 13 y 14 del RGPD, que prevén el derecho de información de las personas afectadas por un tratamiento de datos personales. Si bien es cierto que sería preciso que, al transponer la Directiva PNR, los Estados miembros establecieran expresamente el derecho a la información de los pasajeros aéreos, tal y como lo reconocen los considerandos 29 y 37 de dicha Directiva, se excluye, en cualquier caso, que puedan limitar el alcance de los artículos 13 y 14 del RGPD, amparándose en el artículo 23, apartado 1, del referido Reglamento, por ser algo contrario al espíritu de la referida Directiva. Pues bien, para ser efectivo, tal derecho debe referirse también a las categorías de datos PNR que son objeto de transferencia.

176. Habida cuenta del conjunto de consideraciones precedentes, considero que, sin perjuicio de las limitaciones sugeridas y de las precisiones que se han hecho en el marco de la tercera cuestión prejudicial, los datos PNR cuyo tratamiento está contemplado en la Directiva PNR son pertinentes, adecuados y no excesivos a la vista de las finalidades perseguidas por esta Directiva y que su alcance no sobrepasa lo estrictamente necesario para llevar a cabo estas finalidades.

– *Sobre los datos sensibles*

177. La Directiva PNR prohíbe, con carácter general, cualquier tratamiento de «datos sensibles». [168]

166 Véase el punto 2.7.4 de las directrices de la OACI.

167 Precisamente, el requisito de garantizar la seguridad y la fiabilidad de la transmisión de los datos a las UIP se menciona en el artículo 16, apartado 1, de la Directiva PNR, relativo a los medios electrónicos utilizados para esta transmisión, y ha sido uno de los criterios a los que se ha atenido la Comisión a efectos de la adopción, exigida en el apartado 3 del dicho artículo, de los protocolos comunes y de los formatos que deberán utilizar las compañías aéreas para dicha transmisión; véase la Decisión de Ejecución (UE) 2017/759 de la Comisión, de 28 de abril de 2017, relativa a los protocolos comunes y los formatos de datos que deberán utilizar las compañías aéreas para la transmisión de los datos PNR a las Unidades de Información sobre Pasajeros (DO 2017, L 113, p. 48).

168 Véase el considerando 37 de la Directiva PNR.

178. Aunque esta Directiva no contiene una definición del concepto de «datos sensibles», de su artículo 13, apartado 4, se desprende que incluye, cuando menos, los «datos PNR que revele[n] el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud, la vida sexual o la orientación sexual de una persona». [169] En el apartado 165 del Dictamen 1/15, el Tribunal de Justicia precisó que cualquier medida que se base en la premisa de que una o varias de estas características «podrían, por sí solas y con independencia del comportamiento individual del viajero afectado, ser pertinentes en atención a la finalidad de los tratamientos de datos del PNR […] vulneraría los derechos garantizados en los artículos 7 y 8 de la Carta, en relación con el artículo 21 de esta». Por lo tanto, al prohibir cualquier tratamiento de los datos mencionados en su artículo 13, apartado 4, la Directiva PNR respeta los límites impuestos por el Tribunal de Justicia a la utilización de estas categorías de datos en el marco de un sistema de tratamiento de los datos PNR, tanto si pertenece al Derecho nacional, al Derecho de la Unión o a un acuerdo internacional celebrado por la Unión.

179. La prohibición general de tratamiento de datos sensibles establecida por la Directiva PNR incluye también su *recogida*. Así, como señala expresamente el considerando 15 de dicha Directiva, las diecinueve categorías que figuran en el anexo I no se basan en los datos PNR mencionados en su artículo 13, apartado 4.

180. Aunque ninguna de estas categorías se refiere expresamente a esos datos, estos últimos pueden encajar, en particular, en la categoría «Observaciones generales», mencionada en el punto 12 del anexo I, que constituye un «campo abierto», capaz de abarcar, como ya he tenido ocasión de señalar al examinar la tercera cuestión prejudicial, un número indefinido de informaciones de distinta índole. Existe, en efecto, un riesgo concreto, como señaló, por otra parte, el Tribunal de Justicia en el apartado 164 del Dictamen 1/15, de que informaciones que se enmarcan en esa categoría, referidas, por ejemplo, a preferencias dietéticas, a peticiones de asistencia, a precios especiales para ciertas categorías de personas o de asociaciones, revelen de forma directa, datos sensibles en el sentido del artículo 13, apartado 4, de la Directiva PNR, relativos, en particular, a las convicciones religiosas de los pasajeros de que se trate, a su estado de salud o a su pertenencia a un sindicato o a un partido político.

181. Pues bien, dado que el tratamiento de estos datos está excluido, de todas formas, por la Directiva PNR, su transmisión por parte de las compañías aéreas no solo sobrepasa manifiestamente lo estrictamente necesario, sino que, además, carece de cualquier utilidad. En este aspecto, debe señalarse que el hecho de que las UIP estén obligadas, en cualquier caso, conforme al artículo 13, apartado 4, segunda frase, de la Directiva PNR, a suprimir inmediatamente los datos PNR que revelen alguna de las informaciones enumeradas en la primera frase de dicho apartado no permite autorizar ni justificar una transmisión de tales datos, [170] pues la prohibición de su tratamiento dictada por esta Directiva debe entrar en juego a partir de la primera fase del tratamiento de los datos PNR. De esta manera, la obligación de supresión de los datos sensibles no es más que una garantía adicional prevista por dicha Directiva para el supuesto de que, de forma excepcional, tales datos se transmitan a las UIP por error.

[169] Las categorías de datos personales enumerados en el artículo 13, apartado 4, de la Directiva PNR están todas comprendidas en las que corresponden al concepto de «categorías especiales de datos personales» a que se refiere el artículo 9, apartado 1, del RGPD.

[170] En este sentido, considero que no son pertinentes las alegaciones formuladas por varios Estados miembros que han presentado observaciones sobre la segunda cuestión prejudicial basadas en la existencia de medios técnicos que permiten suprimir con facilidad los datos sensibles transferidos por las compañías aéreas.

182. Por lo demás, deseo señalar, como lo hizo el Sr. Abogado General Mengozzi en el punto 222 de sus conclusiones en el Dictamen 1/15,[171] que, dado que las informaciones que corresponden a las categorías de «texto libre» —como la categoría «Observaciones generales» a que se refiere el punto 12 del anexo I— que pueden contener datos sensibles, en virtud del artículo 13, apartado 4, de la Directiva PNR, únicamente se comunican por los pasajeros de manera facultativa, es poco probable que personas implicadas en delitos de terrorismo o en delitos graves efectúen esta comunicación espontánea, de modo que cabe concebir que la transmisión sistemática de estos datos solo puede afectar, en su mayor parte, a personas que hayan solicitado beneficiarse de un servicio adicional, las cuales no presentan, en realidad, ningún interés para los servicios represivos.[172]

183. Al examinar la tercera cuestión prejudicial, he llegado a la conclusión de que el punto 12 del anexo I, en la medida en que se refiere a la categoría «Observaciones generales», no cumple los requisitos de claridad y de precisión exigidos en el artículo 52, apartado 1, primera frase, de la Carta. Por los motivos que acabo de exponer, considero que incluir esta categoría en las categorías de datos que son objeto de una transmisión sistemática a las UIP, sin facilitar ninguna precisión en cuanto a la información a la que puede referirse, tampoco se ajusta al criterio de necesidad previsto en el artículo 52, apartado 1, segunda frase, de la Carta, según la interpretación que recibe del Tribunal de Justicia.[173]

184. Dicho esto, excluir las categorías denominadas de «texto libre» de la lista de los datos PNR que se transfieren a las autoridades estatales en el marco de un sistema de tratamiento de los datos PNR no basta para suprimir el riesgo de que, a pesar de ello, se pongan a disposición de estas autoridades datos sensibles. En efecto, no solo es posible inferir directamente esos datos de informaciones comprendidas en tales categorías, sino también que tales datos puedan presumirse o manifestarse a través de información recogida en categorías «codificadas». Así pues, por poner un ejemplo, el nombre del pasajero aéreo puede proporcionar indicaciones o, cuando menos, permitir establecer hipótesis sobre el origen étnico o sobre la pertenencia religiosa del pasajero interesado. Lo mismo ocurre con la nacionalidad. Estos datos no se prestan, en principio, a ser excluidos de la lista de los datos PNR que se transfieren ni a que las autoridades autorizadas para su recepción los supriman. En consecuencia, para evitar el riesgo de estigmatizar, sobre la base de características protegidas, a un gran número de individuos de los que, sin embargo, no se sospecha ningún delito, se necesita un sistema de tratamiento de los datos PNR que prevea garantías suficientes que permitan excluir, en cada fase del tratamiento de los datos recogidos, que ese tratamiento pueda tener en cuenta, directa o indirectamente, tales características, por ejemplo, utilizando selectores basados en esas características durante el análisis automatizado. Volveré sobre este tema más adelante.

185. Sobre la base del conjunto de todas las consideraciones anteriores y sin perjuicio de la conclusión a la que he llegado en el punto 183, considero que la Directiva PNR establece, en la fase de transferencia de los datos PNR a las UIP, suficientes garantías para la protección de los datos sensibles.

171 Conclusiones del Abogado General Mengozzi presentadas en el Dictamen 1/15 (Acuerdo PNR UE-Canadá), EU:C:2016:656.

172 Quisiera señalar que, incluso las directrices de la OACI, al tiempo que no excluyen que los datos sensibles que puedan extraerse de las categorías de «texto libre» pueden ser pertinentes para determinar el riesgo que pueda representar un pasajero, recomiendan, sin embargo, a los Estados contratantes hacer lo necesario para que se tengan en cuenta únicamente si hay indicaciones concretas que requieren el uso de esos datos para los fines perseguidos por sus normativas PNR.

173 Deseo recordar que esta exclusión fue sugerida por el CEPD en su Dictamen de 25 de marzo de 2011, apartado 47.

iii) Sobre el concepto de «pasajero» (cuarta cuestión prejudicial)

186. Mediante su cuarta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si el sistema establecido por la Directiva PNR, al permitir la transferencia y el tratamiento generalizados de los datos PNR de toda persona que encaje en el concepto de «pasajero», en el sentido del artículo 3, punto 4, de dicha Directiva, al margen de cualquier elemento objetivo que permita considerar que la persona afectada puede suponer un riesgo para la seguridad pública, es compatible con los artículos 7, 8, y con el artículo 52, apartado 1, de la Carta. Se interroga, en particular, sobre la posibilidad de extrapolar al sistema de tratamiento de datos personales instaurado por la Directiva PNR la jurisprudencia del Tribunal de Justicia en materia de conservación y de acceso a los datos en el sector de las comunicaciones electrónicas.

187. En dicha jurisprudencia, por lo que se refiere a aquello que reviste interés para el presente procedimiento, el Tribunal de Justicia ha llegado a la conclusión de que una normativa que prevea, con vistas a luchar contra la delincuencia grave, la *conservación* preventiva generalizada e indiferenciada de los datos de tráfico relativos a las comunicaciones electrónicas y los datos de localización,[174] con objeto de que las autoridades represivas puedan a acceder a estos, sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo que se persiga, no puede, en principio, considerarse justificada en una sociedad democrática.[175] El Tribunal de Justicia también se ha pronunciado en este sentido en relación con una normativa nacional que, con el fin de luchar contra el terrorismo, preveía el *análisis automatizado de la totalidad de esos datos* por medio de un filtrado efectuado por los proveedores de servicios de comunicaciones electrónicas a solicitud de las autoridades nacionales competentes y en función de los parámetros establecidos por estas.[176] Según el Tribunal de Justicia, tales medidas solo pueden justificarse en aquellas situaciones en las que el Estado miembro afectado se enfrenta a una amenaza grave para la seguridad nacional que resulta real y actual o previsible y cuando la decisión que establezca su aplicación sea objeto de un control efectivo bien por un órgano jurisdiccional, bien por una entidad administrativa independiente.[177] Además, según el Tribunal de Justicia, la utilización de estas medidas en tales situaciones debe limitarse temporalmente a lo estrictamente necesario y no puede tener en ningún caso carácter sistemático.[178]

188. Por otra parte, debo señalar que, si bien en esta jurisprudencia el Tribunal de Justicia no ha llegado a afirmar expresamente, como en la sentencia Schrems I, la existencia de una lesión al contenido esencial del derecho al respeto de la vida privada, sin embargo, ha considerado que las medidas en cuestión alcanzaban un nivel de gravedad de la injerencia tal que, salvo en el caso limitado de amenazas específicas a seguridad nacional de un Estado miembro, era simplemente

174 Se trata de datos que pueden dar información acerca de las comunicaciones efectuadas por un usuario de un medio de comunicación electrónica o sobre la localización de los equipos terminales que utiliza.

175 Véanse, en este sentido, las sentencias La Quadrature du Net, apartados 141 a 145, y Tele2 Sverige, apartados 105 y 106, pronunciadas en interpretación del artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y el artículo 52, apartado 1, de la Carta, así como la sentencia Digital Rights, apartados 57 y 58, en la que el Tribunal de Justicia declaró inválida la Directiva 2006/24.

176 Véase la sentencia La Quadrature du Net, apartado 177.

177 Véase la sentencia La Quadrature du Net, apartados 134 a 139 y 177. Según el Tribunal de Justicia, la responsabilidad que incumbe a los Estados miembros en materia de seguridad nacional «corresponde al interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas»; véanse las sentencias La Quadrature du Net, apartado 135, y Privacy International, apartado 74.

178 Véase la sentencia La Quadrature du Net, apartados 138 y 178.

imposible considerar que se limitaran a lo estrictamente necesario y que fueran, por ello, conformes a la Carta,[179] con independencia de las garantías que puedan preverse contra los riesgos de abuso y de acceso ilícito a los datos de que se trate.[180]

189. Ya he tenido ocasión de señalar que una normativa como la establecida por la Directiva PNR comparte con medidas del mismo tipo que las que ha examinado el Tribunal de Justicia en la jurisprudencia recordada en los puntos anteriores de las presentes conclusiones un cierto número de elementos comunes que le confieren un carácter particularmente intrusivo. Así, dicha Directiva instituye un sistema generalizado e indiferenciado de recogida y de análisis automatizados de los datos personales de una parte significativa de la población que se aplica de forma general al conjunto de personas que responden al concepto de «pasajeros» que figura en el artículo 3, punto 4, de la referida Directiva y, en consecuencia, también a las personas respecto de las que no existen indicios que sugieran que sus comportamientos podrían guardar relación, incluso indirecta o remota, con actividades terroristas o de delincuencia grave. En tales circunstancias, el órgano jurisdiccional remitente se pregunta si esta jurisprudencia es extrapolable a un sistema de tratamiento de los datos PNR como el establecido por la Directiva PNR.

190. Sobre este extremo, debo señalar que, en el Dictamen 1/15, cuando examinó, en los apartados 186 a 189 de este, el ámbito de aplicación *ratione personae* del proyecto de Acuerdo PNR Canadá-UE, el Tribunal de Justicia evitó establecer paralelismos entre las medidas dirigidas a la conservación y al acceso generalizado e indiferenciado al contenido de las comunicaciones electrónicas, a los datos relativos al tráfico y a los datos de localización, por una parte, y la transferencia de los datos PNR y su tratamiento automatizado en el marco de la evaluación previa de los pasajeros mencionados en dicho Acuerdo, por otra parte. Sin embargo, en la época en que se emitió este dictamen, existía ya una jurisprudencia muy asentada —confirmada, tan solo unos meses antes de que se emitiera, por la sentencia Tele2 Sverige, a la que se refiere el órgano jurisdiccional remitente—, en la que se consideró que, salvo en situaciones específicas y puntuales,[181] estas medidas eran incompatibles con la Carta.[182] Las sentencias más recientes del Tribunal de Justicia en este ámbito y especialmente la sentencia La Quadrature du Net siguen la estela de esta jurisprudencia, perfilándola y, en algunos aspectos, matizándola.

191. En los apartados mencionados del Dictamen 1/15, el Tribunal de Justicia consideró explícitamente que no se evidenciaba que el Acuerdo PNR Canadá-UE sobrepasara los límites de lo estrictamente necesario por el hecho de permitir la *transferencia* y el *tratamiento automatizado*, a efectos de su evaluación previa, de los datos PNR de la totalidad de los pasajeros aéreos a Canadá y ello a pesar de que se contemplaba que tales transferencia y tratamiento se realizaran «con independencia de cualquier elemento objetivo que permit[iera] considerar que los pasajeros pu[dieran] presentar un riesgo para la seguridad pública en Canadá».[183] En el apartado 187 de este dictamen, el Tribunal de Justicia llega a afirmar que «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

179 Véase, en particular, la sentencia La Quadrature du Net, apartados 141 a 145.

180 Véase la sentencia La Quadrature du Net, apartados 115 y 116; véanse, asimismo, las conclusiones del Abogado General Campos Sanchéz-Bordona presentadas en los asuntos acumulados SpaceNet y Telekom Deutschland (C-793/19 y C-794/19, EU:C:2021:939), puntos 74 y 75.

181 Véase la sentencia Tele2 Sverige, apartado 119.

182 Véase, en este sentido, la sentencia Tele2 Sverige, apartados 103 a 107 y 119 y jurisprudencia citada.

183 Véase el Dictamen 1/15, apartados 186 y 187.

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». [184]

192. Por lo tanto, al menos en lo que atañe a la transferencia generalizada e indiferenciada de los datos PNR, el Tribunal de Justicia se ha desmarcado del enfoque más riguroso que había adoptado en materia de conservación y acceso a los metadatos.

193. Si bien es innegable que, en su razonamiento, el Tribunal de Justicia tuvo en cuenta, como así resulta, especialmente, de los apartados 152 y 188 del Dictamen 1/15, de una parte, el hecho comprobado de que el tratamiento automatizado de los datos PNR facilita los controles de seguridad, especialmente en las fronteras, y, de otra parte, el hecho de que, con arreglo al Convenio de Chicago, los pasajeros aéreos que deseen entrar en el territorio de un Estado parte en dicho Convenio están obligados a someterse a los controles y a cumplir los requisitos de entrada y de salida prescritos por ese Estado, incluida la comprobación de sus datos PNR, considero que existen otras razones que abogan por esta diversidad de enfoques y, entre ellas, en primer lugar, la naturaleza de los datos tratados.

194. En numerosas ocasiones, el Tribunal de Justicia ha subrayado que no solo el contenido de las comunicaciones electrónicas, sino también los metadatos pueden revelar información sobre «un número considerable de aspectos de la vida privada de las personas de que se trate, incluida información de carácter sensible, como la orientación sexual, las opiniones políticas, las creencias religiosas, filosóficas, sociales u otras y el estado de salud»; que estos datos, considerados en su conjunto, «permiten extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los círculos sociales que frecuentan» y que estos datos proporcionan, en particular, medios para determinar «el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones de los datos». [185] Por otra parte, deseo recordar que las normativas examinadas hasta ahora por el Tribunal de Justicia, incluida la contenida en la Directiva 2006/24, no establecían ninguna excepción y se aplicaban también a las comunicaciones dirigidas a o procedentes de servicios de carácter social o religioso o de profesionales sujetos a obligaciones de secreto profesional. Por lo tanto, sin apreciar la existencia de una vulneración del contenido esencial del derecho al respeto de la vida privada, el Tribunal de Justicia ha afirmado, sin embargo, que, «habida cuenta del carácter sensible de la información que pueden proporcionar los datos de tráfico y de localización, la confidencialidad de estos es fundamental para el derecho al respeto de la vida privada». [186]

195. En cambio, si bien es cierto que, como he recordado en los puntos 77 y 98 de las presentes conclusiones, el Tribunal de Justicia reconoció, en el Dictamen 1/15, que los datos PNR pueden, en su caso, revelar información muy precisa sobre la vida privada de una persona, [187] el Tribunal

184 En las sentencias Digital Rights (apartado 59) y Tele2 Sverige (apartado 111), al igual que en la jurisprudencia posterior (véase, en particular, la sentencia La Quadrature du Net, apartados 143 a 150), el hecho de que la normativa en cuestión no se basara en «elementos objetivos» como los mencionados por el Tribunal de Justicia en el apartado 187 del Dictamen 1/15, que permitan dirigirse a un público cuyos datos puedan revelar una puedan presentar una relación, por lo menos indirecta, con delitos graves, contribuir de un modo u otro a la lucha contra la delincuencia grave, es precisamente lo que hace que esta normativa no sea proporcionada.

185 Véase la sentencia La Quadrature du Net, apartado 117 y jurisprudencia citada; véase también la sentencia Prokuratuur, apartado 36.

186 Sentencia La Quadrature du Net, apartado 142.

187 Véase el Dictamen 1/15, apartados 128 y 150.

de Justicia afirmó que la naturaleza de esa información se limita a determinados aspectos de esa vida privada, [188] lo cual hace que el acceso a tales datos sea menos intrusivo que el acceso al contenido de las comunicaciones, a los datos relativos al tráfico y a los datos de localización.

196. En segundo lugar, no solo la naturaleza de los datos PNR difiere de la de los datos relativos al tráfico y los datos de localización, sino que también difieren el número y la variedad de información que pueden revelar las distintas categorías de datos, pues la información contenida en los datos PNR está más limitada, tanto cuantitativa como cualitativamente. Esto depende no solo de que los sistemas de tratamiento generalizado e indiferenciado de los datos relativos a las comunicaciones electrónicas pueden afectar prácticamente a toda la población contemplada, mientras que los sistemas de tratamiento de los datos PNR se aplican un círculo de individuos más restringido, aunque significativo desde el punto de visa numérico, sino también de la frecuencia en la utilización de medios de comunicación electrónicos y de la multiplicidad de estos últimos. Por otra parte, la Directiva PNR prevé la recogida y el tratamiento de un número limitado de datos PNR exhaustivamente determinado, que excluye los datos comprendidos en las categorías enumeradas en el artículo 13, apartado 4, de dicha Directiva, de manera que puede ser, parcialmente, objeto de una apreciación anticipada, si no la cantidad, al menos, la sensibilidad de la información sobre la vida privada de los interesados que puede resultar de la recogida. [189] Pues bien, semejante limitación de la tipología de los datos que se contemplan, que permita excluir una gran parte de aquellos que puedan contener información sensible, solo es parcialmente posible por lo que se refiere a los datos del tráfico y a los datos de localización, habida cuenta del número de usuarios y de los medios de comunicación afectados. [190]

197. En tercer lugar, cualquier tratamiento de los metadatos de las comunicaciones electrónicas no solo puede afectar a la esfera íntima de la vida de prácticamente toda la población, sino que interfiere en el ejercicio de otras libertades a través de las cuales se ejerce la participación de cada individuo en la vida social y democrática de un país [191] y supone el riesgo, entre otras cosas, de un efecto disuasorio sobre la libertad de expresión de los usuarios de medios de comunicaciones electrónicas, [192] que constituye «uno de los fundamentos esenciales de una sociedad democrática y pluralista» y forma parte de los valores en los que se basa la Unión. [193] Este aspecto es inherente a las medidas que tienen por objeto esas categorías de datos personales y no afecta, en principio, a los sistemas de tratamiento de los datos PNR.

198. En cuarto lugar, debido principalmente al número y a la variedad de información de carácter sensible que puede extraerse del contenido de las comunicaciones electrónicas, de los datos relativos al tráfico y de los datos de localización, existe un riesgo de arbitrariedad relacionado con el tratamiento de estos datos significativamente más elevado que el que se refiere a los sistemas de tratamiento de los datos PNR.

199. Por el conjunto de razones que acabo de exponer, considero que el enfoque más estricto adoptado por el Tribunal de Justicia en el ámbito de las comunicaciones electrónicas no puede extrapolarse, en cuanto tal, a los sistemas de tratamiento de los datos PNR. El Tribunal de

188 Véase el Dictamen 1/15, apartado 150.

189 Sobre la dificultad de tal apreciación en relación con los metadatos, véase la sentencia Prokuratuur, apartado 40.

190 El legislador alemán hizo un esfuerzo en este sentido en la normativa que es objeto de los asuntos acumulados C-793/19 y C-794/19, SpaceNet y Telekom Deutschland, en los que el Abogado General Campos Sánchez-Bordona ha presentado sus conclusiones (EU:C:2021:939), puntos 60 y 61.

191 A este respecto, me remito, al punto 93 de las presentes conclusiones.

192 Véase la sentencia La Quadrature du Net, apartado 118 y jurisprudencia citada.

193 Véase la sentencia Tele2 Sverige, apartado 93.

Justicia ya se expresó, cuando menos implícitamente, en ese sentido en el Dictamen 1/15, en el contexto de un Acuerdo internacional que instaura un sistema de este tipo a efectos de la protección de la seguridad de un país tercero. Considero que la misma posición se justifica, con mayor motivo en relación con la Directiva PNR, cuyo objetivo es la protección de la seguridad interior de la Unión.

200. Dicho esto, es preciso señalar, al igual que hizo el Abogado General Mengozzi en el punto 216 de las conclusiones que presentó en el Dictamen 1/15,[194] que el interés mismo de los sistemas de tratamiento de los datos PNR, tanto si se adoptan de forma unilateral como si son objeto de un acuerdo internacional, consiste precisamente en garantizar la transmisión masiva de datos que permitan a las autoridades competentes identificar, con la ayuda de herramientas de tratamiento automatizado y de escenarios o criterios de evaluación preestablecidos, a individuos, desconocidos por los servicios represivos, pero que parezcan revestir un «interés» o un riesgo para la seguridad pública y que puedan, por lo tanto, ser sometidos posteriormente a controles individuales más exhaustivos. La exigencia de una «sospecha razonable» afirmada en la jurisprudencia del TEDH sobre las interceptaciones selectivas practicadas en el marco de la investigación de un delito[195] y en la del Tribunal de Justicia sobre la conservación de los metadatos[196] es, por lo tanto, menos pertinente en el contexto de una transmisión y de un tratamiento de tal índole.[197] El objetivo, en particular, de prevención perseguido por tales normativas tampoco puede alcanzarse limitando su aplicación a una categoría determinada de individuos, como, por cierto, afirmó el Tribunal de Justicia en los apartados del Dictamen 1/15 recordados en el punto 191 de las presentes conclusiones, de manera que el alcance de la Directiva PNR garantiza la realización eficaz de este objetivo.[198]

201. También debe subrayarse que la Comisión ha puesto de relieve, en reiteradas ocasiones, la importancia estratégica del tratamiento de los datos PNR como instrumento fundamental de la respuesta común de la Unión al terrorismo y a los delitos graves y como componente de primer orden de la Unión de la Seguridad.[199] En el marco de un «enfoque integral» para la lucha contra el terrorismo, el papel desempeñado por los sistemas de tratamiento de los datos PNR también ha tenido el reconocimiento del Consejo de seguridad de Naciones Unidas, que, en su Resolución 2396 (2017),[200] obliga a los Estados miembros de las Naciones Unidas a que «desarrollen la capacidad de reunir, procesar y analizar los datos [PNR] y se aseguren de que todas sus autoridades nacionales competentes utilicen y compartan esos datos, respetando plenamente los

194 Conclusiones del Abogado General Mengozzi presentadas en el Dictamen 1/15 (Acuerdo PNR UE-Canadá, EU:C:2016:656.

195 Véase, en particular, TEDH, sentencia de 4 de diciembre de 2015, Roman Zakharov c. Rusia (CE:ECHR:2015:1204JUD004714306), § 260.

196 Véanse las sentencias La Quadrature du Net, apartados 146 a 151, y Tele2 Sverige, apartado 119.

197 En este sentido, en relación con las medidas de interceptación masiva, véase la sentencia Big Brother Watch, § 348.

198 Véase, por analogía, la sentencia de 3 de octubre de 2019, A y otros (C-70/18, EU:C:2019:823), apartado 61.

199 Véase, recientemente, la Comunicación de la Comisión sobre la Estrategia de la UE para la Unión de la Seguridad [COM(2020) 605 final, p. 28] y la Comunicación de la Comisión: Agenda de lucha contra el terrorismo de la UE: anticipar, prevenir, proteger y responder [COM(2020) 795 final, p. 15 y ss.].

200 Resolución de 21 de diciembre de 2017 [en lo sucesivo, «Resolución 2396 (2017)»], https://undocs.org/es/S/RES/2396(2017).

derechos humanos y las libertades fundamentales, con el fin de prevenir, detectar e investigar los delitos de terrorismo y los viajes conexos».[201] Esta obligación se reafirma en la Resolución 2482/2019, en lo relativo al terrorismo y a la delincuencia transnacional grave.[202]

202. En este contexto, la adopción de un sistema de tratamiento de los datos PNR armonizado a escala de la Unión, tanto en relación con los vuelos exteriores de la UE como, para los Estados que recurren al artículo 2 de la Directiva PNR, con los vuelos interiores de la UE, permite garantizar que el tratamiento de estos datos se produzca dentro del cumplimiento del alto nivel de protección de los derechos consagrados en los artículos 7 y 8 de la Carta, fijado por dicha Directiva, y proporciona un sistema jurídico de referencia para la negociación de acuerdos internacionales sobre tratamiento y transferencia de los datos PNR.[203]

203. Por otra parte, si bien es cierto que el sistema instaurado por la Directiva PNR contempla de forma no diferenciada a todos los pasajeros aéreos, como con razón ha subrayado, en particular, el Parlamento en sus observaciones escritas y como también subraya el Consejo de Seguridad de las Naciones Unidas en la Resolución 2396 (2017), que evoca el riesgo concreto de que pueda utilizarse la aviación civil con fines terroristas, a la vez como medio de transporte y como objetivo,[204] existe una relación objetiva entre el transporte aéreo y las amenazas para la seguridad pública asociadas, en particular, al terrorismo y, cuando menos, a ciertas formas de delincuencia grave como, en particular, el tráfico de droga o la trata de seres humanos, que tienen, por lo demás, un componente transfronterizo muy significativo.

204. Por último, es preciso destacar que, como han alegado el Parlamento, el Consejo y varios de los Estados miembros que han presentado observaciones escritas, cuando entran o salen de la Unión, los pasajeros aéreos tienen la obligación de someterse a controles de seguridad.[205] La transferencia y el tratamiento de los datos PNR antes de su llegada o antes de su salida facilita y acelera esos controles, como también ha señalado el Tribunal de Justicia en el Dictamen 1/15, permitiendo a los servicios represivos concentrarse en los pasajeros respecto de los cuales disponen de elementos fácticos que señalen un riesgo real para la seguridad.[206]

205. Por último, en lo que atañe, en particular, a la extensión del sistema de la Directiva PNR a los vuelos interiores de la UE, si bien, *a priori*, no cabe excluir completamente que se produzca un impacto en la libertad de circulación de los ciudadanos de la Unión, consagrada, en particular, en

201 Véase la Resolución 2396 (2017), punto 12; en ese mismo punto 12, el Consejo de Seguridad de las Naciones Unidas «insta a la OACI a que colabore con sus Estados miembros con miras a establecer una norma para la reunión, el uso, el procesamiento y la protección de los datos PNR». A raíz de esa invitación, el 23 de junio de 2020, la OACI aprobó la enmienda n.º 28 del anexo 9 del Convenio de Chicago que, como ya se ha señalado, establece normas internacionales en materia de facilitación y cuyo capítulo 9, sección D, trata específicamente de los PNR. El 12 de enero de 2021, la Comisión adoptó una propuesta de Decisión del Consejo relativa a la posición que debe adoptarse, en nombre de la Unión, en [la OACI] en relación con dicha enmienda [COM(2021) 16 final].

202 Resolución de 19 de julio de 2019, punto 15, c), https://undocs.org/es/S/RES/2482(2019).

203 En la actualidad, existen dos acuerdos internacionales celebrados por la Unión, respectivamente, con Australia [Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de [datos PNR] por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia (DO 2012, L 186, p. 4)], y con los Estados Unidos de América [Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de [datos PNR] al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (DO 2012, L 215, p. 5)]. Actualmente se están evaluando conjuntamente estos dos acuerdos, con vistas a la celebración de nuevos acuerdos. El 18 de febrero de 2020, el Consejo autorizó también a la Comisión a entablar negociaciones con Japón.

204 Véase la Resolución 2396 (2017), p. 4.

205 Incluidas las personas que gozan del derecho de libre circulación con arreglo al Derecho de la Unión; véase el Reglamento (UE) 2017/458 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, por el que se modifica el Reglamento (UE) 2016/399 en lo relativo al refuerzo de los controles mediante la comprobación en las bases de datos pertinentes en las fronteras exteriores (DO 2017, L 74, p. 7).

206 En este sentido, véase, asimismo, el Dictamen 1/15, apartado 187. Véase también la Comunicación de la Comisión sobre el enfoque global de las transferencias de datos [PNR] a los terceros países [COM(2010) 492 final, p. 6, punto 2.2].

el artículo 45 de la Carta, considero que la injerencia en la vida privada que supone la Directiva PNR, aunque grave, no es tal que conlleve, en sí misma, un efecto disuasorio en el ejercicio de esta libertad, pues el público puede percibir el tratamiento de datos PNR como una medida necesaria para garantizar la seguridad de los viajes por vía aérea.[207] Así y todo, la posibilidad de tal efecto disuasorio debe ser objeto de una evaluación y de una monitorización continuos.

206. Sin embargo, para atenerse al criterio jurisprudencial recordado en los puntos 107 y 108 de las presentes conclusiones, la Directiva PNR no puede limitarse a exigir que el acceso y el tratamiento automatizado de los datos PNR del conjunto de los pasajeros aéreos responda a la finalidad perseguida, sino que debe también establecer, y ello de forma clara y precisa, los requisitos materiales y procedimentales que regulen este acceso y este tratamiento, así como la posterior utilización de esos datos,[208] y establecer garantías adecuadas en cada etapa del proceso. Ya he mencionado, al examinar la segunda cuestión prejudicial, las garantías que acompañan la transferencia de los datos PNR a las UIP. En el marco del examen de la sexta cuestión prejudicial, pasaré revista a las garantías que lleva aparejadas, más concretamente, el tratamiento automatizado de estos datos y también, al examinar la octava cuestión prejudicial, las que están relacionadas con su conservación.

207. Antes de continuar este examen, deseo subrayar la importancia capital que reviste, en el marco del sistema de garantías instaurado por la Directiva PNR, el control ejercido por la autoridad independiente a que se refiere el artículo 15 de la referida Directiva. Con arreglo a este artículo, todo tratamiento de datos previsto por dicha Directiva está sujeto a la vigilancia de una autoridad de control independiente, dotada de las facultades de verificar la licitud de ese tratamiento, de realizar investigaciones, inspecciones y auditorías, y de conocer de las reclamaciones presentadas por cualquier interesado. Semejante control, ejercido por un sujeto externo encargado de defender intereses potencialmente en conflicto con los que persiguen aquellos que efectúan los tratamientos de los datos PNR, al que se encomienda que vele por el respeto del conjunto de limitaciones y salvaguardas que acompañan estos tratamientos, constituye una garantía esencial, expresamente mencionada en el artículo 8, apartado 3, de la Carta, cuya eficacia, en términos de protección de los derechos fundamentales afectados, es incluso superior al sistema de vías de recurso puesto a disposición de los particulares. Por esta razón, considero fundamental que el Tribunal de Justicia haga una interpretación extensiva del alcance de las facultades de vigilancia establecidas en el artículo 15 de la Directiva PNR y que, cuando transpongan esta Directiva a su Derecho interno, los Estados miembros reconozcan a su autoridad nacional de control todo este abanico de facultades, dotándola de los medios materiales y personales necesarios para desempeñar su cometido.

208. Sobre la base del conjunto de consideraciones que preceden, considero que la Directiva PNR no sobrepasa los límites de lo estrictamente necesario al permitir la transferencia y el tratamiento automatizado de los datos de cualquier persona que encaje en el concepto de «pasajero» en el sentido del artículo 3, punto 4, de dicha Directiva.

207 De alguna manera, es lo que explica la Comisión en su propuesta de Directiva PNR, p. 3.

208 Véase, en este sentido, la sentencia Prokuratuur, apartado 49 y jurisprudencia citada.

iv) Sobre el carácter suficientemente claro, preciso y limitado a lo estrictamente necesario de la evaluación previa de los pasajeros (sexta cuestión prejudicial)

209. Mediante su sexta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si la evaluación previa a que se refiere el artículo 6 de la Directiva PNR es compatible con los artículos 7, 8 y con el artículo 52, apartado 1, de la Carta. Si bien la redacción de esta cuestión prejudicial se centra en el carácter sistemático y generalizado del tratamiento automatizado de los datos PNR de todos los pasajeros aéreos que esta evaluación previa implica, de los motivos de la resolución de remisión se desprende que la Cour constitutionnelle (Tribunal Constitucional) solicita al Tribunal de Justicia una apreciación más global del cumplimento de los requisitos de legalidad y de proporcionalidad en el contexto de ese tratamiento. A continuación, voy a realizar esta apreciación remitiéndome al mismo tiempo al análisis que he realizado al examinar la cuarta cuestión prejudicial en lo relativo al carácter no selectivo de dicho tratamiento automatizado.

210. El artículo 6, apartado 2, letra a), de la Directiva PNR prevé que las UIP lleven a cabo una evaluación previa de los pasajeros aéreos antes de su llegada o salida programada del Estado miembro. La finalidad de esta evaluación es identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes, «ante la posibilidad de que pudiera estar implicada en un delito de terrorismo o delito grave». Conforme al artículo 6, apartado 6, de la Directiva PNR, la UIP de un Estado miembro transmitirá los datos PNR de las personas identificadas en el marco de esta evaluación o los resultados del tratamiento de esos datos PNR a las autoridades competentes pertinentes a que hace referencia el artículo 7 de la referida Directiva, de ese mismo Estado miembro para su «ulterior examen».

211. A tenor del artículo 6, apartado 3, de la Directiva PNR, la evaluación previa a que se refiere el apartado 2, letra a), de dicho artículo se realiza comparando los datos PNR con bases de datos «pertinentes» [artículo 6, apartado 3, letra a)] o tratándolos con arreglo a criterios determinados [artículo 6, apartado 3, letra b)].

212. Antes de abordar el examen de cada uno de estos dos tipos de tratamiento de datos, deseo indicar que no se deduce claramente de la redacción del artículo 6, apartado 3, antes mencionado, si los Estados miembros están obligados a establecer que la evaluación previa de los pasajeros se realice procediendo de manera sistemática y en todos los casos tanto a uno como al otro análisis automatizado o si, como parece corroborar la utilización del verbo «poder» y de la conjunción disyuntiva «o», los Estados miembros pueden organizar sus sistemas de manera que, por ejemplo, el examen contemplado en el apartado 3, letra b, del mencionado artículo 6 quede reservado para unos casos concretos. Sobre esta cuestión, debo precisar que la propuesta de Directiva PNR establecía que dicho examen se llevara a cabo únicamente en el marco de lucha contra los delitos graves transfronterizos. [209]

213. Al igual que la Comisión, considero que se deduce, en particular, de la estructura de la Directiva PNR que los Estados miembros están obligados a prever dos tipos de tratamientos automatizados, por razones que también tienen que ver con la exigencia de garantizar la aplicación más uniforme posible del sistema de tratamiento de los datos PNR de la Unión. Sin embargo, ello no implica que los Estados miembros no estén autorizados —e incluso obligados, con objeto de garantizar que el tratamiento de datos que requiera la evaluación previa realizada con arreglo al artículo 6, apartado 2, letra a), de la Directiva PNR se limite a lo estrictamente

[209] Véase el artículo 4, apartado 2, letra a), de la propuesta de Directiva PNR.

necesario— a limitar el análisis con arreglo al artículo 6, apartado 3, letra b), de la Directiva PNR, en función de los resultados, entendidos en términos de eficacia, en relación con cada uno de los delitos mencionados por dicha Directiva y a reservarlo, en su caso, únicamente para algunos de estos delitos. Aboga por este enfoque el considerando 7 de la Directiva PNR, a cuyo tenor, «para garantizar que el tratamiento de datos se limite a lo necesario, el establecimiento y la aplicación de criterios de evaluación debe limitarse a los delitos de terrorismo y a la delincuencia grave para las que es pertinente el uso de esos criterios».

– Sobre la comparación con bases de datos en el sentido del artículo 6, apartado 3, letra a), de la Directiva PNR

214. La primera vertiente de la evaluación previa que realizan las UIP en virtud del artículo 6, apartado 2, letra a), de la Directiva PNR implica, con arreglo al apartado 3, letra a), del referido artículo, comparar los datos PNR (*data matching*) con bases de datos, con objeto de buscar posibles resultados positivos (*hits*). Estos hits deben ser verificados por las UIP, con arreglo al artículo 6, apartado 5, de la Directiva PNR, y, en su caso, plasmarse en un formato comparativo (en *match*) antes de comunicarse a las autoridades competentes.

215. Como ha reconocido el Tribunal de Justicia en el apartado 172 del Dictamen 1/15, el alcance de la injerencia que suponen estos tipos de análisis automatizados en los derechos consagrados en los artículos 7 y 8 de la Carta depende fundamentalmente de las bases de datos en que se apoyen aquellos. Por consiguiente, es fundamental que las disposiciones que establezcan tales tratamientos de datos identifiquen de forma suficientemente clara y precisa las bases de datos con las que se autoriza el cotejo de los datos objeto de tratamiento.

216. A tenor del artículo 6, apartado 3, letra a), de la Directiva PNR, las UIP realizan una comparación de los datos PNR con «bases de datos pertinentes» [210] en relación con los objetivos perseguidos por dicha Directiva. Esta disposición también menciona una categoría específica de bases de datos, a saber, las bases de datos sobre «personas u objetos buscados o bajo alerta», a las que, por lo tanto, el legislador de la Unión ha querido dar expresamente la calificación de «pertinentes» a efectos de dicha disposición.

217. Dejando aparte esta precisión, el concepto de «bases de datos pertinentes» tampoco se explicita mucho más. En particular, no se indica si, para poder considerarse «pertinentes», las bases de datos utilizadas a efectos del cotejo de los datos PNR deben estar gestionadas por autoridades represivas o, más en general, por cualquier autoridad pública, o si simplemente tales autoridades deben poder acceder a dichas bases directa o indirectamente. La naturaleza de los datos que tales bases pueden contener y su relación con los objetivos perseguidos por la Directiva PNR tampoco son objeto de mayores precisiones. [211] Por otra parte, de la redacción del artículo 6, apartado 3, letra a), de la Directiva PNR se infiere que pueden calificarse como «bases de datos

[210] Si, bien en su versión en lengua francesa, el artículo 6, apartado 3, letra a), se refiere a «bases de données utiles» (bases de datos útiles), en la mayor parte de las demás versiones lingüísticas esta disposición se refiere a «bases de datos pertinentes»: véanse, en particular, las versiones en lengua española («pertinentes»), alemana («massgeblich»), inglesa («relevant»), italiana («pertinenti»), neerlandesa («relevant») y portuguesa («relevante»).

[211] Tal y como está redactado, parece que el artículo 6, apartado 3, letra a), de la Directiva PNR permite análisis en forma de exploración de datos mediante cotejo con datos muy variados, siempre que tal exploración se oriente a la persecución de los objetivos mencionados en esta Directiva. En relación con los riesgos relacionados con el *data mining* en materia de datos PNR, véase el Informe Korff, p. 77. En su Dictamen de 25 de marzo de 2011, apartado 18, el CEPD denunció con fuerza la falta de precisión y de previsibilidad de la identificación de las bases de datos con las que pueden compararse los datos PNR.

pertinentes» las bases de datos tanto nacionales y de la Unión como internacionales, lo cual amplía aún más la lista de las bases de datos a las que potencialmente se refiere e incrementa el carácter abierto de este concepto. [212]

218. En estas circunstancias, con arreglo al principio general de interpretación recordado en el punto 151 de las presentes conclusiones, corresponde al Tribunal de Justicia interpretar, en la medida de lo posible, el artículo 6, apartado 3, letra a), de la Directiva PNR y, en particular, el concepto de «bases de datos pertinentes» de acuerdo con los requisitos de claridad y de precisión establecidos en la Carta. Asimismo, dado que la mencionada disposición se refiere a una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, debe interpretarse de forma restrictiva y teniendo en cuenta la exigencia de garantizar un alto nivel de protección de esos derechos fundamentales, según enuncia, en particular, el considerando 15 de la Directiva PNR. Asimismo, dicha disposición debe interpretarse a la luz del principio de limitación de las finalidades para las que pueden tratarse los datos PNR enunciado en el artículo 1, apartado 2, de la Directiva PNR.

219. Habida cuenta de estos criterios, procede, en mi opinión, interpretar el concepto de «bases de datos pertinentes» en el sentido de que solo se refiere a las bases de datos nacionales gestionadas por las autoridades competentes con arreglo al artículo 7, apartado 1, de la Directiva PNR y a las bases de datos de la Unión e internacionales directamente explotadas por esas autoridades en el marco de su cometido. Además, las mencionadas bases de datos deben tener una relación directa y estrecha con los fines de lucha contra el terrorismo y la delincuencia grave perseguidos por la Directiva PNR, lo cual implica que hayan sido desarrolladas para esos fines. Según esta interpretación, dicho concepto se refiere esencialmente, si no exclusivamente, a las bases de datos sobre personas u objetos buscados o bajo alerta, expresamente mencionadas en el artículo 6, apartado 3, letra a), de la Directiva PNR.

220. Con carácter general, se excluyen del concepto de «bases de datos pertinentes» las bases de datos gestionadas o explotadas por los servicios de inteligencia de los Estados miembros, salvo que cumplan estrictamente el requisito de tener una relación estrecha con los objetivos perseguidos por la Directiva PNR y que el Estado miembro en cuestión reconozca a sus servicios de inteligencia competencias específicas en el ámbito represivo. [213]

221. La interpretación que más arriba se propone se ajusta a las recomendaciones formuladas por el Tribunal de Justicia en el apartado 172 del Dictamen 1/15.

222. No obstante, aunque se interprete de ese modo, el artículo 6, apartado 3, letra a), de la Directiva PNR no permite identificar con suficiente precisión las bases de datos que los Estados miembros van a utilizar para su cotejo con los datos PNR y no puede considerarse que responda a los requisitos que se desprenden del artículo 52, apartado 1, de la Carta, según la interpretación que le da el Tribunal de Justicia. En consecuencia, este precepto debe interpretarse en el sentido de que obliga a los Estados miembros a que, al transponer a su Derecho nacional la Directiva

[212] El carácter vago y abierto de la redacción del artículo 6, apartado 3, letra a), de la Directiva PNR se traduce en una transposición al Derecho nacional muy diversa, que va desde una interpretación estricta del concepto de «bases de datos pertinentes», que limita el análisis contemplado a la mera comparación con las bases de datos expresamente mencionadas en dicha disposición (como es el caso de la República Federal de Alemania, según resulta de las observaciones presentadas por su Gobierno ante el Tribunal de Justicia) a una interpretación más amplia que abarca cualquier base de datos disponible o accesible para las autoridades competentes en el marco de su cometido (en este sentido está redactado, en particular, el artículo 24, apartado 1, punto 1), de la Ley PNR.

[213] Según mi criterio, un Estado miembro no deberá, en ningún caso, considerarse obligado, en virtud del artículo 6, apartado 3, letra a), de la Directiva PNR, a autorizar a su UIP a comparar sistemáticamente los datos PNR con «bases de datos pertinentes», en el sentido de esta disposición, gestionadas por sus servicios de inteligencia.

PNR, publiquen una lista de esas bases de datos y la mantengan al día. Por otra parte, sería deseable que se redactara, a escala de la Unión, una lista de las bases de datos «pertinentes», en el sentido del artículo 6, apartado 3, letra a), de la Directiva PNR, gestionadas por la Unión en colaboración con los Estados miembros, y de las bases de datos internacionales, con objeto de uniformar la práctica de los Estados miembros en esta materia.

– *Sobre el tratamiento de los datos PNR con arreglo a criterios predeterminados*

223. La segunda vertiente de la evaluación previa consiste, con arreglo al artículo 6, apartado 2, letra a), de la Directiva PNR, en un análisis automatizado en función de unos criterios predeterminados. Al realizar dicho análisis, los datos PNR se tratan, fundamentalmente, con fines predictivos, mediante la aplicación de algoritmos que pueden permitir «identificar» a los pasajeros que podrían estar implicados en delitos de terrorismo o en delincuencia grave. En este contexto, la UIP realiza fundamentalmente una actividad de elaboración de perfiles. [214] Dado que puede tener consecuencias importantes para los individuos identificados por el algoritmo, [215] tal tratamiento requiere una regulación precisa en lo relativo tanto a la forma en que debe realizarse como a las garantías que deben acompañarlo. En efecto, como señaló el Tribunal de Justicia en el apartado 172 del Dictamen 1/15, el alcance de la injerencia que suponen estos tipos de análisis en los derechos consagrados en los artículos 7 y 8 de la Carta depende fundamentalmente de los modelos y criterios preestablecidos.

224. A este respecto, deseo señalar, en primer lugar, que el artículo 6, apartado 4, segunda frase, de la Directiva PNR precisa que los criterios predeterminados de conformidad con los cuales se efectúa la evaluación previa contemplada en el artículo 6, apartado 3, letra b), de esa misma Directiva deben ser «orientados, proporcionados y específicos». El primero de estos requisitos tiene que ver con el objetivo perseguido por la evaluación previa prevista en el apartado 2, letra a), de ese artículo, a saber, identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes, y responde así a la necesidad, subrayada por el Tribunal de Justicia en el Dictamen 1/15, de que los criterios utilizados logren «seleccionar» individuos sobre los que podría recaer una «sospecha razonable» de participación en actividades terroristas o delitos graves. [216] Esta «selección» implica la aplicación de criterios de evaluación abstractos o, por utilizar una expresión que figura en la Recomendación de 2021 sobre la elaboración de perfiles, de

214 El artículo 3, punto 4, de la Directiva Policía define la «elaboración de perfiles» como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». La misma definición se encuentra en el artículo 4, punto 4, del RGPD y en el punto 1.1, letra c), del anexo a la Recomendación CM/Rec(2021)8, de 3 de noviembre de 2021, del Comité de Ministros del Consejo de Europa sobre la protección de los personas en relación con el tratamiento automatizado de datos de carácter personal en el contexto de la elaboración de perfiles, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148, (en lo sucesivo, «Recomendación de 2021 sobre la elaboración de perfiles»).

215 El punto 1.1, letra j, inciso i), del anexo de la Recomendación de 2021 sobre la elaboración de perfiles define como «tratamientos de elaboración de perfiles de alto riesgo», la «elaboración de perfiles cuyo funcionamiento acarrea efectos jurídicos o que suponen un impacto significativo para la persona interesada o para el grupo de personas identificado mediante el tratamiento de elaboración de perfiles».

216 Véase el Dictamen 1/15, apartado 272.

«perfiles» [217] por medio de los cuales se «filtran» los datos PNR con objeto de localizar a los pasajeros que respondan a los mismos y que, en consecuencia, podrían tener que someterse de nuevo a un control ulterior. En cambio, la Directiva PNR no autoriza la elaboración de perfiles individuales de todos los pasajeros aéreos cuyos datos se analizan, por ejemplo, asociando a cada uno de ellos una categoría de riesgo sobre una escala predeterminada, ya que, de lo contrario, se vulneraría el artículo 6, apartado 4, de dicha Directiva y se rebasarían los límites impuestos por el Tribunal de Justicia al tratamiento automatizado de los datos PNR en el Dictamen 1/15.

225. Con arreglo al artículo 6, apartado 4, segunda frase, los criterios predeterminados mencionados en el artículo 6, apartado 3, letra b), de la Directiva PNR deben, además, ser «específicos», [218] a saber, adecuados a la finalidad perseguida y pertinentes en relación con esta, además de «proporcionados», [219] es decir, que no sobrepasen los límites de esta finalidad. Para dar cumplimento a estos requisitos, en especial, «para garantizar que el tratamiento de datos PNR se limite a lo necesario», el considerando 7 de la Directiva PNR, como ya he subrayado, enuncia que el «establecimiento y la aplicación de criterios de evaluación debe limitarse a los delitos de terrorismo y a la delincuencia grave para las que es pertinente el uso de esos criterios».

226. Por último, tanto de la exposición de motivos y de las disposiciones de la Directiva PNR como de los requisitos establecidos por el Tribunal de Justicia en el Dictamen 1/15 se desprende que los criterios predeterminados a que se refiere el artículo 6, apartado 3, letra b), de la Directiva PNR han de ser también «fiables», [220] lo cual significa, de una parte, que deben elaborarse de forma que se minimice el riesgo de errores [221] y, de otra parte, que deben ser «actuales». [222] En este sentido, el artículo 6, apartado 4, tercera frase, de la Directiva PNR obliga a los Estados miembros a que se aseguren de que «las UIP establezcan esos criterios y los revisen periódicamente, en cooperación con las autoridades competentes mencionadas en el artículo 7». [223] Para garantizar la fiabilidad de estos criterios y limitar, tanto cuanto sea posible, los resultados falsos positivos es preciso, además, como ha reconocido la Comisión al contestar a una pregunta escrita formulada por el Tribunal de Justicia, que se elaboren de forma que tengan en cuenta tanto los elementos de cargo como los elementos de descargo.

227. En segundo lugar, la Directiva PNR prohíbe expresamente la elaboración de perfiles discriminatorios. Así, el artículo 6, apartado 4, primera frase, de esta Directiva prevé que la evaluación previa con los criterios predeterminados a que se refiere el apartado 3, letra b), de dicho artículo «se realizará de forma no discriminatoria». En este sentido, debe aclararse que, aunque la tercera frase de dicho artículo 6, apartado 4, afirma que los criterios «no se basarán en ningún caso en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona»,

217 A tenor del punto 1.1, letra d), del anexo de la Recomendación de 2021 sobre la elaboración de perfiles, el término «perfil» designa «un conjunto de datos atribuidos a una persona, que caracteriza a una categoría de personas o que está destinado a aplicase a una persona». Como explica el Informe sobre la evolución de la situación después de la adopción de la Recomendación (2010)13 sobre la elaboración de perfiles (https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b, p. 21), que precedió a la adopción de la Recomendación de 2021 sobre la elaboración de perfiles, el concepto de «perfil» conserva todo su sentido en sistemas que, como la Directiva PNR, distinguen las operaciones de creación de perfiles [véase, en particular, artículo 6, apartado 2, letra b), de esta Directiva] de las que los aplican, y hace posible la «transparencia de los criterios que se aplican en un segundo momento en la operación de elaboración de perfiles».

218 Véase el artículo 6, apartado 4, de la Directiva PNR, así como el Dictamen 1/15, apartado 172.

219 Véase el artículo 6, apartado 4, de la Directiva PNR.

220 Véase el Dictamen 1/15, apartado 172.

221 Véase el considerando 7 de la Directiva PNR.

222 Véase el Dictamen 1/15, apartado 174.

223 Este mismo requisito figura en el apartado 174 del Dictamen 1/15.

debe entenderse que la prohibición general de elaboración de perfiles discriminatorios abarca todos los motivos de discriminación mencionados en el artículo 21 de la Carta, incluso aquellos que no se mencionan expresamente. [224]

228. En tercer lugar, tanto del tenor del artículo 6, apartado 3, letra b), de la Directiva PNR como del sistema de garantías que acompaña al tratamiento automatizado de los datos PNR establecido por la Directiva PNR se desprende que el funcionamiento de los algoritmos utilizados para realizar el análisis al que se refiere esta disposición debe ser transparente y permitir la trazabilidad del resultado de su aplicación. Evidentemente, este requisito de transparencia no implica que deban hacerse públicos los «perfiles» utilizados. En cambio, requiere que se garantice que pueda identificarse la toma de decisión algorítmica. En efecto, por una parte, el requisito de que los criterios con arreglo a los cuales debe realizarse este análisis sean «predeterminados» excluye la posibilidad de que puedan modificarse sin intervención humana y se opone, en consecuencia, a la utilización de las tecnologías de inteligencia artificial llamadas *machine learning*, [225] las cuales, al mismo tiempo que pueden presentar un grado más elevado de precisión, son difíciles de interpretar, incluso por parte de los operadores que han efectuado el tratamiento automatizado. [226] De otra parte, para que sea efectiva la garantía prevista en el artículo 6, apartados 5 y 6, de la Directiva PNR, conforme a la cual se revisará individualmente, por medios no automatizado, todo resultado positivo que arroje el tratamiento automatizado de los datos PNR efectuado con arreglo al artículo 2, letra a), se requiere —por lo que respecta al análisis a que se refiere el artículo 6, apartado 3, letra b), de la Directiva PNR— que sea posible comprender la razón por la cual el programa ha alcanzado esa concordancia, lo cual no puede garantizarse, en particular, cuando se utilizan sistemas de autoaprendizaje. Lo mismo ocurre con el control de la licitud de dicho análisis, incluida la cuestión referida al carácter no discriminatorio de los resultados obtenidos, que incumbe al responsable de la protección de datos y a la autoridad nacional de control, en virtud del artículo 6, apartado 7, de la Directiva PNR, y del artículo 15, apartado 3, letra b), de dicha Directiva, respectivamente. La transparencia del funcionamiento de los algoritmos utilizados constituye también un requisito necesario para que los interesados puedan ejercer sus derechos de reclamación y su derecho a un recurso jurisdiccional efectivo.

– *Sobre las garantías que lleva aparejado el tratamiento automatizado de los datos PNR*

229. Ya he tenido ocasión de referirme a ciertas garantías que acompañan el tratamiento automatizado de los datos PNR en el marco de la evaluación previa prevista en el artículo 6, apartado 2, letra a), de la Directiva PNR y que responden a los requisitos establecidos por el Tribunal de Justicia en el Dictamen 1/15, a saber, la prohibición de tratamientos basados en criterios predeterminados discriminatorios (artículo 6, apartado 4, primera y cuarta frase, de la Directiva PNR; Dictamen 1/15, apartado 172), la actualización periódica de los criterios predeterminados con arreglo a los cuales debe efectuarse la evaluación previa a que se refiere el artículo 6, apartado 3, letra b), de dicha Directiva (artículo 6, apartado 4, tercera frase, de la Directiva PNR; Dictamen 1/15, apartado 174), la revisión por medios no automatizados de

224 Quisiera poner de relieve que el conjunto de motivos de discriminación mencionados en el artículo 21 de la Carta está reproducido en el considerando 20 de la Directiva PNR. La FRA propuso, en su dictamen, p. 8., que se siguiera la lista de motivos de discriminación recogida en el artículo 21 de la Carta.

225 A tenor del punto 1.1, letra g), del anexo de la Recomendación de 2021 sobre la elaboración de perfiles, la expresión «machine learning» designa «un tratamiento que hace uso de métodos particulares de inteligencia artificial basado en enfoques estadísticos para dotar a los ordenadores de la capacidad de "aprender" a partir de datos, es decir de mejorar su capacidad de resolver tareas sin estar programados expresamente para cada una».

226 En relación con los efectos de la opacidad de los sistemas algorítmicos en cuanto a la posibilidad de un control humano dirigido a prevenir efectos lesivos de dichos sistemas y sus repercusiones negativas en los derechos humanos, véase la Recomendación CM/Rec(2020)1 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre las repercusiones de los algoritmos en los derechos humanos.

cualquier resultado positivo que arroje el tratamiento automatizado de los datos PNR (artículo 6, apartados 5 y 6, de la Directiva PNR; Dictamen 1/15, apartado 173) y el control de la licitud de ese tratamiento por el responsable de la protección de datos y por la autoridad nacional de control [artículo 6, apartado 7, y artículo 15, apartado 3, letra b), de la Directiva PNR]. En este contexto, es primordial que el control efectuado por una autoridad independiente, como aquella a la que se refiere el artículo 15 de Directiva PNR, pueda, por una parte, versar sobre cualquier aspecto inherente al tratamiento automatizado de los datos PNR, incluida la identificación de las bases de datos utilizadas a efectos de la comparación en el sentido del artículo 6, apartado 3, letra a), de esta Directiva y la elaboración de los criterios predeterminados aplicados a los efectos del análisis realizado con arreglo al artículo 6, apartado 3, letra b), de dicha Directiva y, por otra parte, que pueda ejercerse tanto *a priori* como *a posteriori*.

230. Es preciso subrayar que las garantías antes mencionadas deben considerase aplicables de forma transversal a los dos tipos de análisis contemplados en el artículo 6, apartado 3, de la Directiva PNR y ello, a pesar de los términos en que están formuladas. De esta forma, si bien el artículo 6, apartado 4, primera frase, de esta Directiva recuerda la exigencia del respeto del principio de no discriminación únicamente en relación con la evaluación previa realizada con arreglo a criterios predeterminados, esta exigencia se impone en cualquier etapa del proceso de tratamiento de los datos PNR y, por lo tanto, también cuando estos datos se comparan con las bases de datos pertinentes al realizarse la evaluación previa prevista en el artículo 6, apartado 3, letra a), de la referida Directiva. Lo mismo cabe decir del requisito de que los criterios predeterminados utilizados al realizar el análisis a que se refiere el artículo 6, apartado 3, letra b), de la Directiva PNR deben ser fiables y estar actualizados, que ha de entenderse también referido a los datos contenidos en las bases de datos utilizadas a efectos de la comparación prevista en el artículo 6, apartado 3, letra a), de dicha Directiva. Sobre este particular, debo señalar, más en general, que todas las garantías aplicables a los tratamientos automatizados de datos personales establecidas en la Directiva Policía son también aplicables en el marco de la Directiva PNR, pues debe considerarse que los análisis automatizados realizados en el marco de esta Directiva están incluidos en el ámbito de aplicación de la Directiva Policía.

231. A las garantías enumeradas en el punto 229, se añade la prevista en el artículo 7, apartado 6, de la Directiva PNR, que viene a completar, por un lado, la prohibición de basar todo el proceso de decisión exclusivamente en los resultados del tratamiento automatizado de los datos PNR y, por otro lado, la prohibición de discriminación en el tratamiento y en la utilización de esos datos. Así, dicha disposición establece que «las autoridades competentes no adoptarán ninguna decisión que produzca efectos jurídicos adversos para una persona o que afecte significativamente a una persona únicamente en razón del tratamiento automatizado de datos PNR» y que «dichas decisiones no deberán basarse en la raza o el origen 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». Del mismo modo que he señalado en el punto 227 de las presentes conclusiones, en relación con el artículo 6, apartado 4, cuarta frase, de la Directiva PNR, es preciso completar este catálogo de motivos de discriminación añadiendo los que figuran en el artículo 21 de la Carta y que no se mencionan expresamente.

232. Por lo que se refiere a la seguridad de los datos PNR, el artículo 6, apartado 8, de la Directiva PNR establece que el almacenamiento, el tratamiento y análisis de estos datos por parte de la UIP se realizará exclusivamente en uno o varios lugares seguros, dentro del territorio de los Estados miembros.

– *Conclusión sobre la sexta cuestión prejudicial*

233. Habida cuenta del conjunto de consideraciones que preceden y sin perjuicio de las interpretaciones propuestas, en particular, en los puntos 213, 219, 220, 222, 227, 228, 230 y 231 de las presentes conclusiones, considero que el tratamiento automatizado de los datos PNR en el marco de la evaluación previa a que se refiere el artículo 6, apartado 2, letra a), de la Directiva PNR cumple los requisitos de claridad y de precisión y se limita a lo estrictamente necesario.

v) Sobre la conservación de los datos PNR (octava cuestión prejudicial)

234. Mediante su octava cuestión prejudicial, el órgano jurisdiccional remitente pregunta al Tribunal de Justicia si el artículo 12 de la Directiva PNR, en relación con los artículos 7, 8, y el artículo 52, apartado 1, de la Carta debe interpretarse en el sentido de que se opone a una normativa nacional que establece, con carácter general, un período de conservación de los datos PNR 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.

235. El artículo 12, apartado 1, de la Directiva PNR prevé que los datos PNR se conserven en una base de datos «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». Conforme al apartado 2 del citado artículo, al finalizar un «período inicial de conservación» [227] de una duración de seis meses, los datos PNR deberán ser despersonalizados mediante enmascaramiento de algunos datos que podrían servir para identificar directamente al interesado. A tenor del apartado 3 del citado artículo, al finalizar el período de seis meses, solo se permitirá la divulgación de los datos PNR completos, incluidos los elementos enmascarados, cuando se crea «razonablemente» que es necesario a los efectos establecidos en el artículo 6, apartado 2, letra b), de la Directiva PNR y cuando haya sido aprobada por una autoridad judicial u otra autoridad nacional competente con arreglo al Derecho nacional para verificar si se cumplen las condiciones para su divulgación. Por último, el apartado 4, del mismo artículo establece que, al finalizar el período de cinco años a que se refiere el apartado 1, los datos PNR serán suprimidos de modo permanente.

236. De lo anterior se infiere que la propia Directiva PNR establece el régimen de conservación de los datos PNR y determina la duración de esta conservación, fijándola en cinco años, [228] de forma que, en principio, los Estados miembros no tienen ningún margen discrecional en esta materia, como, por otra parte, ha confirmado la Comisión. En estas circunstancias, como ya he podido observar, la octava cuestión prejudicial, pese a estar formulada como cuestión de interpretación, invita, en realidad, al Tribunal de Justicia a pronunciarse sobre la compatibilidad de dicho régimen con la Carta.

237. Constituye un principio general en materia de protección de los datos personales que dichos datos no deben mantenerse de forma que se permita la identificación, directa o indirecta, de los interesados, durante más tiempo del necesario para los fines del tratamiento de los datos

[227] Esta definición figura en el considerando 25 de la Directiva PNR.

[228] Los términos del considerando 37 de la Directiva PNR, según el cual «[se] permite conservar los datos PNR durante un período *máximo de 5 años*, tras el cual los datos deberán suprimirse» (el subrayado es mío), no permiten, a mi juicio, cuestionar la clara redacción del artículo 12, apartado 1, de esta Directiva.

personales.[229] Por otra parte, según reiterada jurisprudencia, una normativa que establezca la conservación de los datos de carácter personal debe responder en todo caso a criterios objetivos y ha de existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr.[230]

238. En el Dictamen 1/15, el Tribunal de Justicia consideró, en relación con los datos recogidos a la entrada de Canadá, que la relación necesaria entre los datos PNR y el objetivo perseguido por el proyecto de Acuerdo PNR Canadá-UE existía en relación con todos los pasajeros aéreos mientras se encontraran en el territorio de ese país tercero.[231] En cambio, en lo que se refiere a los pasajeros aéreos que hayan abandonado Canadá y respecto de los cuales no se haya identificado un riesgo en materia de terrorismo o de delincuencia grave de carácter transnacional a su llegada a ese país tercero ni hasta su partida de dicho país, el Tribunal de Justicia consideró que no parecía que existiera tal relación, siquiera indirecta, que justificara la conservación de sus datos PNR.[232] No obstante, consideró que esta conservación podía ser admisible «en la medida en que se identifi[caran], en casos particulares, elementos objetivos que permit[ieran] considerar que determinados pasajeros aéreos podrían, incluso después de su partida de Canadá, presentar un riesgo en términos de lucha contra el terrorismo y la delincuencia grave de carácter transnacional».[233]

239. Si se aplican los principios establecidos por el Tribunal de Justicia en el Dictamen 1/15 al contexto de la Directiva PNR, ello implica que los datos PNR de los vuelos exteriores de la UE recogidos a la entrada de la Unión y los datos PNR de los vuelos interiores de la UE recogidos a la entrada del Estado miembro de que se trate solo puedan conservarse, después de su análisis previo en el sentido del artículo 6, apartado 2, letra a), de la Directiva PNR, mientras los pasajeros afectados permanezcan en el territorio de la Unión o en el de dicho Estado miembro. Por lo que respecta a los datos PNR de los vuelos exteriores de la UE recogidos a la salida de la Unión y a los datos PNR de los vuelos interiores de la UE recogidos a la salida del Estado miembro afectado, estos datos solo podrían conservarse, en principio, después de la mencionada evaluación previa, en el caso de los pasajeros respecto de los cuales existan elementos objetivos que puedan revelar la existencia de un riesgo en términos de lucha contra el terrorismo y la delincuencia grave.[234]

240. Los Gobiernos y las instituciones que han presentado observaciones ante el Tribunal de Justicia se oponen de forma general a que se extrapolen al marco del presente asunto principios establecidos en el Dictamen 1/15 en materia de conservación de los datos PNR. En este sentido, no se excluye, ciertamente, que la circunstancia de que el Tribunal de Justicia tuviera que pronunciarse sobre una conservación de datos personales en el territorio de un país tercero pudo haber influido en el hecho de que recurriera a un criterio relacionado con la estancia de la persona de que se trataba «en el territorio de Canadá». Existe la misma posibilidad de que la aplicación de tal criterio en el contexto de la Directiva PNR pueda materializarse concretamente en una injerencia en los derechos al respeto de la vida privada y a la protección de los datos personales de una importancia potencialmente mayor para ciertas categorías de personas, en particular

229 Véase, en relación con el tratamiento de datos personales a efectos de detección, prevención, enjuiciamiento e investigación en materia de infracciones penales, la Directiva Policía, artículo 4, letra e), y considerando 26. Véase, más en general, el artículo 5, apartado 1, letra e), del RGPD y el artículo 5, apartado 4, letra e), del Convenio 108 modernizado.

230 Véanse las sentencias Schrems I, apartado 93; Tele2 Sverige, apartado 110; Dictamen 1/15, apartado 191, y la sentencia La Quadrature du Net, apartado 133.

231 Véase el Dictamen 1/15, apartado 197.

232 Véase el Dictamen 1/15, apartado 205.

233 Véase el Dictamen 1/15, apartado 207.

234 Se trataría aquí de una aplicación analógica de los apartados 187 y ss. del Dictamen 1/15, dado que este último solo se refería a la hipótesis de los datos PNR recogidos a la entrada en el territorio de Canadá.

aquellas que tienen su residencia permanente en la Unión y que se desplazan en el interior de esta o que regresan tras una estancia en el extranjero. Por último, es verdad que, en la práctica, dicho criterio podría resultar difícil de aplicar, al menos respecto a los vuelos interiores de la UE, como han subrayado algunos Estados miembros y el Consejo.

241. No es menos cierto que, aunque se desee descartar el criterio seguido por el Tribunal de Justicia en el Dictamen 1/15, una conservación del conjunto de los datos PNR de todos los pasajeros aéreos que no tenga en cuenta el resultado de la evaluación previa mencionada en el artículo 6, apartado 2, letra a), de la Directiva PNR y no realice ninguna distinción en función del riesgo en materia de terrorismo o de delincuencia con arreglo a criterios objetivos y verificables va en contra de la jurisprudencia reiterada del Tribunal de Justicia recordada en el punto 237 de las presentes conclusiones, que el Tribunal de Justicia quiso aplicar en el referido dictamen. Pues bien, las consideraciones expuestas en los puntos 201 a 203 de las presentes conclusiones al examinar la cuarta cuestión prejudicial, aunque permiten, a mi entender, justificar la transferencia generalizada e indiferenciada de los datos PNR, así como su tratamiento automatizado en el marco de la evaluación previa a que se refiere el artículo 6, apartado 2, letra a), de la Directiva PNR, no permiten por sí mismas, a mi juicio, justificar una retención generalizada e indiferenciada de esos datos, incluso después de tal evaluación.

242. Por otra parte, debo indicar que se aplica el mismo período de conservación de cinco años tanto en relación con la lucha contra el terrorismo como con la lucha contra la delincuencia grave y, en el marco de esta última finalidad, en relación con todos los delitos mencionados en el anexo II, sin excepción. Pues bien, como resulta de las consideraciones desarrolladas en el punto 121 de las presentes conclusiones, esta lista es especialmente extensa y abarca delitos con tipologías y gravedades diferentes. En este sentido, es preciso señalar que la justificación que esgrimen la práctica totalidad de los Estados miembros e instituciones que han presentado observaciones en el presente procedimiento en relación con la duración y la complejidad de las investigaciones solo se invoca concretamente en relación con los delitos de terrorismo y ciertos delitos de carácter eminentemente transnacional, como la trata de seres humanos o el tráfico ilícito de estupefacientes, al igual que, más en general, en relación con ciertas formas de delincuencia organizada. Debo recordar, por lo demás, que, en el Dictamen 1/15, el Tribunal de Justicia solo aceptó una justificación similar en relación con la conservación de los datos PNR de los pasajeros aéreos que presentan un riesgo objetivo en términos de lucha contra el terrorismo o los delitos graves de carácter transnacional, respecto de los cuales se consideró que una retención de los datos de cinco años no excedía los límites de lo estrictamente necesario.[235] En cambio, se consideró que esta justificación no servía para autorizar «un almacenamiento continuado de los datos del PNR de la totalidad de los pasajeros aéreos […] 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».[236]

243. Es bien cierto que, como ponen de relieve el Consejo, el Parlamento y la Comisión, así como todos Gobiernos que han presentado observaciones sobre la octava cuestión prejudicial, la Directiva PNR prevé garantías específicas tanto en lo relativo a la conservación de los datos PNR, que se enmascaran parcialmente al finalizar un plazo inicial de seis meses, como en relación con su utilización durante el período de retención, que está sujeta a condiciones estrictas. Sin embargo, debo señalar, en primer lugar, por una parte, que el proyecto de Acuerdo PNR Canadá-UE también contemplaba un sistema de despersonalización de los datos PNR mediante

235 Véase el Dictamen 1/15, apartado 209.

236 Véase el Dictamen 1/15, apartado 205.

enmascaramiento [237] y, por otra parte, que, si bien esta despersonalización, como subraya en particular el Comité Consultivo del Convenio 108, [238] puede atenuar los riesgos inducidos por un período prolongado de conservación de los datos, como un acceso abusivo a estos, los datos enmascarados siguen permitiendo la identificación de las personas y siguen siendo, por ello, datos de carácter personal cuya conservación también debe limitarse en el tiempo con el fin de prevenir una vigilancia permanente generalizada. En este aspecto, debo señalar que un período de conservación de cinco años implica que un importante número de pasajeros, en particular aquellos que se desplazan dentro de la Unión, pueden estar fichados de manera casi permanente. En segundo lugar, en relación con las restricciones a la utilización de los datos, debo señalar que la conservación de datos de carácter personal y el acceso a los mismos constituyen injerencias diferenciadas en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, que requieren estar justificadas de forma autónoma. Si bien la existencia de garantías estrictas en materia de acceso a los datos conservados permite apreciar de forma global el impacto de una medida de vigilancia en dichos derechos fundamentales, no es menos cierto que no permiten suprimir las injerencias que tienen que ver con una conservación generalizada de carácter prolongado.

244. Respecto del argumento de la Comisión que sostiene la necesidad de conservar los datos PNR de todos los pasajeros aéreos para permitir que las UIP cumplan su cometido, mencionado en el artículo 6, apartado 2, letra c), de la Directiva PNR, de actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), del mencionado artículo, debo señalar que, si bien reconozco que, como afirma la Comisión, la precisión de dichos criterios depende, en parte, de su comparación con comportamientos «normales», no es menos cierto que su elaboración debe llevarse a cabo sobre la base de comportamientos «delictivos». Este argumento, que, por otra parte, solo esgrime un limitado número de Estados miembros, no puede, a mi juicio, revestir la importancia decisiva que parece atribuirle la Comisión ni justificar, por sí mismo, una conservación generalizada de los datos PNR de todos los pasajeros aéreos, en un formato no anónimo.

245. Habida cuenta de las anteriores consideraciones, y con objeto de garantizar una interpretación del artículo 12, apartado 1, de la Directiva PNR que sea conforme a los artículos 7, 8, y el artículo 52, apartado 1, de la Carta, procede, en mi opinión, interpretar esta disposición en el sentido de que solo se permite la conservación de los datos PNR proporcionados por las compañías aéreas a la UIP en una base de datos 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, después de que se haya llevado a cabo la evaluación previa con arreglo al artículo 6, apartado 2, letra a), de esta Directiva, en la medida en que se establezca, con arreglo a criterios objetivos, una relación entre dichos datos y la lucha contra el terrorismo o la delincuencia grave. Una conservación generalizada e indiferenciada de los datos PNR en un formato no anonimizado solo puede justificarse, por analogía con lo afirmado por el Tribunal de Justicia en esa misma jurisprudencia, frente a una amenaza grave para la seguridad de los Estados miembros que resulte real y actual o previsible, relacionada, por ejemplo, con actividades terroristas, y a condición de que la duración de esta conservación se limite a lo estrictamente necesario.

[237] El proyecto de Acuerdo PNR Canadá-UE preveía el enmascaramiento de los nombres de todos los pasajeros treinta días después de su recepción por Canadá y el enmascaramiento de otros datos expresamente enumerados dos años después de esa recepción: véase el artículo 16, apartado 3, del proyecto de Acuerdo PNR Canadá-UE, examinado por el Tribunal de Justicia, y el Dictamen 1/15, apartado 30.

[238] Véase el Dictamen de 19 de agosto de 2016, p. 9.

246. La delimitación de la medida de conservación contemplada en el artículo 12, apartado 1, de la Directiva PNR puede basarse, por ejemplo, en una evaluación de riesgos o en la experiencia adquirida por las autoridades nacionales competentes, que permitan centrarse en ciertos enlaces aéreos, en esquemas de viajes definidos, en las agencias a través de las cuales se hacen las reservas o también en categorías de personas o de zonas geográficas determinadas, identificadas sobre la base de elementos objetivos y no discriminatorios, como ha declarado el Tribunal de Justicia en su jurisprudencia en materia de conservación de los metadatos de las comunicaciones electrónicas.[239] Por otra parte, por analogía con el Dictamen 1/15, la necesaria relación entre los datos PNR y el objetivo perseguido por la Directiva PNR debe considerarse establecida mientras los pasajeros se encuentren en la Unión (o en el Estado miembro de que se trate) o se dispongan a abandonarla. Lo mismo ocurre con los datos de los pasajeros que hayan dado lugar a un resultado positivo comprobado.

247. Par terminar con el examen de la octava cuestión prejudicial, deseo dedicar algunas reflexiones a las normas que regulan el acceso a los datos PNR y su utilización después de la evaluación previa, contemplada en el artículo 6, apartado 2, letra a), de la Directiva PNR, y antes de su despersonalización, al final del plazo inicial de conservación de seis meses establecido en el artículo 12, apartado 2, de la Directiva PNR.

248. Si se ponen en relación el artículo 6, apartado 2, letra b), y el artículo 12, apartado 3, de la Directiva PNR, se desprende que, durante dicho período inicial, es posible comunicar a las autoridades competentes datos PNR no despersonalizados o los resultados de su tratamiento con arreglo a la primera de dichas disposiciones, sin que se cumplan los requisitos establecidos en las letras a) y b) de la segunda.[240] En efecto, el artículo 6, apartado 2, letra b), de la Directiva PNR se limita a exigir que las peticiones de las autoridades competentes con vistas a ese tratamiento y a esa comunicación estén «debidamente razonadas» y tengan «suficiente base».

249. Según reiterada jurisprudencia recordada por el Tribunal de Justicia en el Dictamen 1/15, una normativa de la Unión no puede limitarse a exigir que el acceso por parte de una autoridad a datos personales legítimamente conservados responda a alguna de las finalidades de dicha normativa, sino que debe establecer también los requisitos materiales y procedimentales que regulen la referida utilización,[241] en particular, para proteger esos datos contra los riesgos de abusos.[242] En dicho dictamen, el Tribunal de Justicia declaró que utilización de los datos PNR previa comprobación de los mismos a la llegada de los pasajeros aéreos a Canadá y durante su estancia en ese país debe basarse en circunstancias nuevas que la justifiquen,[243] precisando que «cuando existan elementos objetivos que permitan considerar que los datos del PNR de uno o varios pasajeros aéreos podrían contribuir de modo efectivo al objetivo de lucha contra los delitos de terrorismo y los delitos graves de carácter transnacional, no parece que la utilización de tales datos exceda de lo estrictamente necesario».[244] Remitiendo por analogía al apartado 120 de la sentencia Tele2 Sverige, el Tribunal de Justicia consideró que, para garantizar en la práctica el pleno cumplimiento de estos requisitos, «es esencial que la utilización durante la estancia de los pasajeros aéreos en Canadá de los datos del PNR conservados se supedite, en principio, salvo en

239 Véase, en particular, la sentencia La Quadrature du Net, apartados 148 y 149.

240 Lo mismo ocurre con las solicitudes dirigidas por las UIP de otros Estados miembros de que suministren los datos PNR con arreglo al artículo 9, apartado 2, de la Directiva PNR.

241 Véase el Dictamen 1/15, apartado 192 y jurisprudencia citada. Más recientemente, véanse las sentencias Privacy international, apartado 77, y, por analogía, Prokuratuur, apartado 49 y jurisprudencia citada.

242 Véase el Dictamen 1/15, apartado 200.

243 Véase el Dictamen 1/15, apartado 200.

244 Véase el Dictamen 1/15, apartado 201.

casos de urgencia debidamente justificados, al control previo de un órgano judicial o de una entidad administrativa independiente, y que la decisión de ese órgano judicial o de esa entidad administrativa se adopte a raíz de una solicitud motivada de las autoridades competentes, presentada, en particular, en el marco de procedimientos de prevención, de descubrimiento o de acciones penales».[245] En consecuencia, el Tribunal de Justicia ha supeditado la posibilidad de utilizar los datos PNR conservados después de su verificación con ocasión de un viaje aéreo a un doble requisito, a la vez material —a saber, la existencia de motivos que justifiquen tal utilización — y procedimental —a saber, el control por parte de un órgano jurisdiccional o de una autoridad administrativa independiente—. La interpretación por la que ha optado el Tribunal de Justicia, lejos de ser «contextual», constituye la aplicación en materia de datos PNR de la jurisprudencia que dimana, en particular, de las sentencias Digital Rights y Tele2 Sverige.

250. Pues bien, el régimen establecido por la Directiva PNR durante los seis primeros meses conservación de los datos PNR, que autoriza, tras la evaluación previa a que se refiere el artículo 6, apartado 2, letra a), de la referida Directiva, la divulgación y el tratamiento, potencialmente reiterados, de los datos PNR sin garantías procedimentales adecuadas y sin normas materiales suficientemente claras y precisas que definan el objeto y las condiciones de estas injerencias no respeta los requisitos establecidos por el Tribunal de Justicia en el Dictamen 1/15. Es evidente que tampoco responde a la exigencia de que la utilización de los datos PNR se limite a lo estrictamente necesario.

251. En consecuencia, propongo al Tribunal de Justicia que interprete el artículo 6, apartado 2, letra b), de la Directiva PNR de forma que los tratamientos de datos con arreglo a la referida disposición que se realicen durante el período inicial de seis meses contemplado en el artículo 12, apartado 2, de esta Directiva respeten los requisitos establecidos por el Tribunal de Justicia en el Dictamen 1/15.

252. Por lo que se refiere al primer requisito, de carácter material, al que el Tribunal de Justicia ha supeditado la utilización ulterior de los datos PNR, considero que los conceptos de «razonablemente» en el sentido del artículo 12, apartado 3, letra a), de la Directiva PNR y de «suficiente base» según el tenor del artículo 6, apartado 2, letra b), de esta Directiva pueden interpretarse sin dificultad en el sentido de que las peticiones de las autoridades competentes a que se refieren dichas disposiciones deben poner de manifiesto «elementos objetivos que permitan considerar que los datos del PNR de uno o varios pasajeros aéreos podrían contribuir de modo efectivo al objetivo de lucha contra los delitos de terrorismo y los delitos graves […]».[246]

253. Por lo que se refiere al segundo requisito, de carácter procedimental, procede, a mi juicio, interpretar que el artículo 6, apartado 2, letra b), de la Directiva PNR, en relación con el artículo 12, apartado 3, de esta y a la luz de los artículos 7, 8, y del artículo 52, apartado 1, de la Carta, en el sentido de que el requisito de aprobación previa por parte de una autoridad judicial o de una autoridad administrativa independiente establecido en el artículo 12, apartado 3, letra b), de esta Directiva se aplica a cualquier tratamiento de datos PNR efectuado con arreglo al citado artículo 6, apartado 2, letra b).

245 Véase el Dictamen 1/15, apartado 202.

246 Véase, en este sentido, el Dictamen 1/15, apartado 201.

4. Conclusiones sobre las cuestiones prejudiciales segunda, tercera, cuarta, sexta y octava

254. Sobre la base del conjunto de consideraciones que preceden, propongo al Tribunal de Justicia que declare la invalidez del punto 12 del anexo I en la medida en que incluye las «observaciones generales» entre las categorías de datos PNR que las compañías aéreas están obligadas a transmitir, con arreglo al artículo 8 de la Directiva PNR, a las UIP y que declare que el examen de las cuestiones judiciales segunda, tercera, cuarta, sexta y octava no desvela otros elementos que puedan afectar a la validez de dicha Directiva, siempre que se interprete como se ha propuesto en los puntos 153, 160, 161 à 164, 219, 228, 239 y 251 de las presentes conclusiones.

255. A la luz de la respuesta que propongo para las cuestiones prejudiciales relativas a la validez de la Directiva PNR y prescindiendo de cualquier otra consideración, no cabe estimar la solicitud formulada, en particular, por el Consejo, de que se mantengan los efectos de la Directiva PNR en el caso en que el Tribunal de Justicia decida invalidar total o parcialmente la Directiva PNR en su conjunto.

C. Sobre la quinta cuestión prejudicial

256. Mediante su quinta cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si el artículo 6 de la Directiva PNR, en relación con los artículos 7, 8, y el artículo 52, apartado 1, de la Carta debe interpretarse en el sentido de que se opone a una normativa nacional que permite, como fin del tratamiento de los datos PNR el seguimiento de ciertas funciones de los servicios de inteligencia y de seguridad. De la resolución de remisión se desprende que tales funciones son las que lleva a cabo la sûreté de l'État (Servicio de Seguridad del Estado) y el service général du renseignement et de la sécurité (Servicio General de Inteligencia y Seguridad) en el marco de su cometido de protección de la seguridad nacional.

257. Como he señalado los puntos 113 y 114 de las presentes conclusiones, la limitación de los fines del tratamiento de datos de carácter personal es una garantía fundamental que debe respetarse con objeto de que las injerencias en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta no vayan más allá de lo necesario, en el sentido de la jurisprudencia del Tribunal de Justicia. También he precisado, por lo que respecta a las injerencias en esos derechos fundamentales contemplados en la Directiva PNR, que incumbía al legislador de la Unión, a efectos de respetar los principios de legalidad y de proporcionalidad mencionados, en particular, en el artículo 52, apartado 1, de la Carta, prever reglas claras y precisas que regulen el alcance y la aplicación de las medidas que supongan tales injerencias.

258. Pues bien, el artículo 1, apartado 2, de la Directiva PNR precisa que los datos PNR obtenidos con arreglo a esta «podrán tratarse únicamente con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves contemplados en el artículo 6, apartado 2, letras a), b) y c)» de la mencionada Directiva. Conforme a esta disposición, las UIP solo tratan los datos PNR para realizar una evaluación previa de los pasajeros aéreos [artículo 6, apartado 2, letra a)], responder a las peticiones puntuales de las autoridades competentes [artículo 6, apartado 2, letra b)] y actualizar o establecer nuevos criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3, letra b), del mencionado artículo 6 [artículo 6, apartado 2, letra a)]. En los tres casos, se recuerdan expresamente los objetivos señalados en el artículo 1, apartado 2, de la Directiva PNR en materia de lucha contra el terrorismo y los delitos graves.

259. Por lo demás, el artículo 7, apartado 4, de esta Directiva precisa que no solo el tratamiento de los datos PNR contemplado en su artículo 6, sino también su tratamiento posterior y el resultado de dicho tratamiento por las autoridades competentes de los Estados miembros deben efectuarse «únicamente con el fin específico de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves».

260. El carácter exhaustivo de la determinación de los objetivos perseguidos por la Directiva PNR resulta claramente de la redacción de su artículo 1, apartado 2, y lo corroboran, además de su artículo 6, apartado 2, y de su artículo 7, apartado 4, ya mencionados, varios artículos y considerandos de esta Directiva que vinculan sistemáticamente cada etapa del proceso de acceso, de tratamiento, de conservación y de intercambio de los datos PNR únicamente a estos objetivos específicos. [247]

261. Tanto de la redacción del artículo 1, apartado 2, de la Directiva PNR como de su interpretación a la luz de los principios de legalidad y de proporcionalidad, que obligan a limitar de forma exhaustiva las finalidades de las medidas que supongan injerencias en los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal, se desprende que cualquier extensión de las finalidades del tratamiento de los datos PNR más allá de los objetivos de seguridad expresamente mencionados en esta disposición es contraria a la Directiva PNR.

262. En mi opinión, esta prohibición de ampliar los objetivos perseguidos por la Directiva es especialmente válida en lo relativo a las funciones de seguridad y de inteligencia de los Estados miembros, incluso debido a la falta de transparencia que caracteriza su *modus operandi*. En esta cuestión, mi parecer concuerda con el de la Comisión, concretamente, en el sentido de que, por regla general, estos servicios no deberían tener acceso directo a los PNR. En este contexto, ya me parece censurable que las UIP nacionales puedan, como es el caso de la UIP belga, contar entre sus miembros a funcionarios adscritos a servicios de seguridad. [248]

263. Sobre la base de las consideraciones que anteceden, procede, a mi juicio, responder a la quinta cuestión prejudicial en el sentido de que la Directiva PNR y, en particular, su artículo 1, apartado 2, y su artículo 6 deben interpretarse en el sentido de que se opone a una normativa nacional que permite, como fin del tratamiento de los datos PNR, el seguimiento de determinadas actividades desempeñadas por los servicios de inteligencia y de seguridad, en la medida en que, para atender a esta finalidad, la UIP nacional se vea obligada a tratar dichos datos y/o a transferir tales datos o el resultado de su tratamiento a los servicios mencionados con fines que no sean los que se indican exhaustivamente en el artículo 1, apartado 2, de la referida Directiva, extremo cuya comprobación corresponde al juez nacional.

247 Véanse, en particular, artículo 4, artículo 7, apartados 1 y 2, artículo 9, apartado 2, artículo 10, apartado 2, artículo 12, apartado 4, de la Directiva PNR; véanse, en particular, los considerandos 6, 9, 10, 11, 15, 23, 25, 35 y 38 de dicha Directiva. Por otra parte, recuérdese que la propuesta de Directiva PNR precisaba, en su considerando 28, que «la presente Directiva no afecta a la posibilidad de que los Estados miembros establezcan, con arreglo a sus legislaciones nacionales, un mecanismo para recoger y tratar los datos PNR con finalidades distintas de las especificadas en la presente Directiva». Pues bien, esta precisión no ha sido recogida en el texto final de la Directiva PNR.

248 Sin embargo, el artículo 4, apartado 3, de la Directiva PNR admite esta posibilidad, al señalar que «el personal de la UIP podrá ser enviado en comisión de servicios por las autoridades competentes», al menos en la medida en que los servicios de inteligencia y de seguridad del Estado miembro de que se trate puedan calificarse de «autoridades competentes», en el sentido del artículo 7, apartado 2, de esta Directiva.

D. Sobre la séptima cuestión prejudicial

264. Mediante su séptima cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia, si el artículo 12, apartado 3, letra b), de la Directiva PNR debe interpretarse en el sentido de que la UIP constituye una «autoridad nacional competente», en sentido de la disposición mencionada, que puede permitir la divulgación de los datos PNR completos al finalizar el período inicial de seis meses desde la transmisión de dichos datos.

265. Deseo recordar que el artículo 12, apartado 2, de la Directiva PNR prevé que, al finalizar el plazo de seis meses, los datos PNR deben ser despersonalizados mediante enmascaramiento de ciertos elementos que podrían servir para identificar directamente al pasajero a que se refieren. Después de dicho plazo, la divulgación de tales datos completos solo se permitirá en las condiciones establecidas en el apartado 3 del citado artículo 12 y, en particular, cuando dicha divulgación haya sido aprobada previamente por una «autoridad judicial» [artículo 12, apartado 3, letra b), i)] u «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» [artículo 12, apartado 3, letra b), inciso ii)].

266. La mayoría de los Gobiernos que han presentado observaciones escritas en el presente procedimiento no se ha pronunciado sobre la séptima cuestión prejudicial. El Gobierno checo considera, al igual que la Comisión, que el artículo 12, apartado 3, de la Directiva PNR no puede interpretarse en el sentido de que la UIP pueda constituir una «autoridad nacional competente». En cambio, los Gobiernos belga,[249] irlandés, español, francés y chipriota se oponen a tal interpretación. Consideran, en esencia, que ninguna disposición de la Directiva PNR o del Derecho de la Unión obsta a que se designe la UIP entre las autoridades nacionales competentes, en el sentido del artículo 12, apartado 2, letra b), inciso ii), de dicha Directiva y que la UIP es, por naturaleza, una autoridad suficientemente independiente para dar los permisos de tratamiento de datos PNR.

267. Por mi parte, debo señalar, primero, que de la redacción del artículo 12, apartado 3, letra b), de la Directiva PNR y, especialmente, de la utilización de la conjunción «u», que une los dos casos previstos en los incisos i) y ii) de esta disposición, se deduce que el legislador de la Unión ha querido situar en el mismo plano el control ejercido por la autoridad nacional contemplada en el inciso ii) y el que realiza la autoridad judicial mencionada en el inciso i). De ello se sigue que la mencionada autoridad nacional debe presentar un grado de independencia y de imparcialidad tal que el control que ejerza pueda considerarse una alternativa comparable al control que puede llevar a cabo una autoridad judicial.[250]

268. Segundo, de los trabajos preparatorios de la Directiva PNR se desprende que, el legislador de la Unión, por una parte, no ha seguido la propuesta de la Comisión de encomendar al responsable de la UIP el cometido de permitir la divulgación de los datos PNR completos[251] y, por otra parte, ha

[249] En relación con las dudas expresadas por el Gobierno belga respecto a la competencia del Tribunal de Justicia para responder a la séptima cuestión prejudicial, debe señalarse que, a tenor de su redacción, el órgano jurisdiccional remitente interroga al Tribunal de Justicia sobre la interpretación del artículo 12, apartado 3, de la Directiva PNR y no sobre la compatibilidad de la legislación nacional con dicha disposición. En cualquier caso, según una reiterada jurisprudencia, el Tribunal de Justicia puede dar indicaciones a los órganos jurisdiccional para que puedan apreciar esta compatibilidad (véase, en particular, sentencia de 7 de septiembre de 2016, ANODE, C-121/15, EU:C:2016:637), apartado 54 y jurisprudencia citada.

[250] Véase, a este respecto, la sentencia de 5 de noviembre de 2019, Comisión/Polonia (Independencia de los tribunales ordinarios) (C-192/18, EU:C:2019:924), apartados 108 a 110.

[251] El artículo 9, apartado 2, cuarta frase, de la propuesta de Directiva PNR disponía que «el acceso a la totalidad de los datos PNR solo lo autorizará el Jefe de la Unidad de Información sobre Pasajeros».

alargado, estableciéndolo en seis meses, el plazo inicial de retención de estos datos propuesto dicha institución, que era de 30 días. En este contexto, caracterizado por buscar un equilibrio entre la duración del período de retención que precede a la despersonalización de los datos PNR y los requisitos a los que está sujeto su desenmascaramiento al finalizar ese período, se sitúa la decisión del legislador de la Unión de supeditar el acceso a los datos PNR completos a requisitos procedimentales más estrictos que los inicialmente previstos por la Comisión y de encomendar a una autoridad independiente el cometido de comprobar el cumplimiento de las condiciones para la divulgación.

269. Tercero, como con razón ha señalado la Comisión, de la estructura de la Directiva PNR se desprende que la razón de ser del procedimiento de aprobación mencionado en el artículo 12, apartado 3, de la Directiva PNR reside en atribuir a una entidad tercera imparcial la tarea de efectuar, en cada caso concreto, una ponderación de los datos de los interesados con la finalidad represiva perseguida por esta Directiva.

270. Cuarto, según la jurisprudencia del Tribunal de Justicia, una entidad encargada de efectuar el control previo requerido para autorizar el acceso de las autoridades nacionales competentes a datos personales legítimamente conservados debe disponer de todas las atribuciones y presentar todas las garantías necesarias para conciliar los diferentes intereses y derechos de que se trate. El Tribunal de Justicia también ha precisado que esa entidad debe gozar de un estatuto que le permita actuar en el ejercicio de sus funciones con objetividad e imparcialidad y, para ello, ha de estar a resguardo de toda influencia externa.[252] En particular, a la vista del requisito de independencia exigido, sobre todo en el ámbito penal, la autoridad que ejerce el control previo debe tener la condición de tercero respecto de la que solicita el acceso a los datos, de modo que no debe estar implicada en la realización de la investigación penal y debe mantener una posición neutral respecto de las partes del procedimiento penal.[253]

271. Pues bien, se impone constatar que la UIP no presenta todas las garantías de independencia e imparcialidad que debe satisfacer la autoridad encargada de efectuar el control previo del artículo 12, apartado 3, de la Directiva PNR. En efecto, las UIP están directamente vinculadas a las autoridades competentes en materia de prevención y detección de los delitos de terrorismo y de los delitos graves, así como de su investigación y enjuiciamiento. Con arreglo al artículo 4, apartado 1, de la Directiva PNR, esa autoridad es la propia UIP o una sucursal de esta. Por otra parte, el apartado 3 de este artículo prevé que el personal de la UIP podrá ser enviado en comisión de servicios por las autoridades competentes. Así ocurre, en particular, con la UIP belga, que, a tenor del artículo 14 de la Ley PNR, está integrada, entre otros, por miembros adscritos a los servicios de policía, de seguridad del Estado, de inteligencia y seguridad, y a la Administración General de Aduanas e Impuestos Especiales.

272. Ciertamente, de forma general, los miembros de la UIP deben ofrecer todas las garantías de integridad, competencia, transparencia e independencia, e incumbe a los Estados miembros velar, en su caso, por que, habida cuenta de los vínculos que los une con los cuerpos a los que pertenecen, estas garantías puedan respetarse de un modo concreto, en particular, con objeto de evitar que las autoridades competentes a cuya estructura pertenecen originariamente tengan acceso directo al banco de datos PNR y no solamente a los resultados de las consultas efectuadas por las UIP. No es menos cierto que el personal de la UIP enviado en comisión de servicios por las autoridades competentes, en el sentido del artículo 7, apartado 2, de la Directiva PNR, guarda

252 Sentencia Prokuratuur, apartados 52 y 53.

253 Sentencia Prokuratuur, apartados 53 y 54. En el mismo sentido, véase la sentencia Big Brother Watch, § 349 a 352.

inevitablemente un vínculo con el servicio del que procede durante el período de comisión de servicios, conservando su estatuto, aunque esté situado bajo la autoridad funcional y jerárquica del funcionario que dirija la UIP.

273. La conclusión de que la UIP no es una autoridad nacional en el sentido del artículo 12, apartado 3, letra b), inciso ii), de la Directiva PNR se ve corroborada, por otra parte, por el hecho de que, según dicha disposición, debe darse al responsable de la protección de datos de la UIP de que se trate «información» de la petición de divulgación y este debe realizar una «revisión *a posteriori*». En efecto, si la UIP estuviera habilitada, como «otra autoridad nacional», a aprobar una petición de divulgación con arreglo al artículo 12, apartado 3, de la Directiva PNR, el responsable de la protección de datos encargado, entre otras cosas, en virtud del artículo 5, apartado 1, de dicha Directiva, de aplicar las garantías oportunas que acompañan el tratamiento de los datos PNR, estaría informado de la solicitud de acceso en el momento en que se presentara, con lo que su control ser produciría necesariamente *a priori*. [254]

274. A la luz de las consideraciones que anteceden, propongo al Tribunal de Justicia que conteste a la séptima cuestión prejudicial que el artículo 12, apartado 3, letra b), de la Directiva PNR debe interpretarse en el sentido de que la UIP no constituye «otra autoridad nacional competente» en el sentido de la referida disposición.

E. Sobre la novena cuestión prejudicial

275. Mediante su novena cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia, por una parte, si la Directiva API es compatible con el artículo 3 TUE, apartado 2, y con el artículo 45 de la Carta en la medida en que se aplique a los vuelos interiores de la Unión y, por otra parte, si debe interpretarse dicha Directiva, en relación con el artículo 3 TUE, apartado 2, y con el artículo 45 de la Carta, en el sentido de que se opone a una normativa nacional que, 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 que puede implicar indirectamente un restablecimiento de los controles en las fronteras interiores.

276. De la resolución de remisión se desprende que esta cuestión prejudicial se inserta en el marco del examen del segundo motivo del recurso, formulado por la LDH con carácter subsidiario. Dicho motivo, basado en la vulneración del artículo 22 de la Constitución belga, en relación con el artículo 3 TUE, apartado 2, y con el artículo 45 de la Carta va dirigido contra el artículo 3, apartado 1, el artículo 8, apartado 2, y el capítulo 11, en particular, los artículos 28 a 31, de la Ley PNR. Mientras el primero de los artículos mencionados enuncia, en términos generales, el objeto de esta Ley, precisando que «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», el artículo 8, apartado 2, de dicha Ley establece que, «con arreglo a las condiciones establecidas en el capítulo 11 [de dicha Ley] 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». En el marco de esta finalidad, conforme al artículo 29, apartado 1, de la Ley PNR, los «datos de los pasajeros» mencionados en su artículo 9, apartado 1, punto 18 (a saber, los datos API mencionados en el punto 18 de la Directiva PNR), relativos a tres categorías de pasajeros, son los únicos que se transmitirán a los servicios de policía encargados del control de las fronteras y al

[254] El artículo 9, apartado 2, cuarta frase, de la propuesta de Directiva PNR disponía que «el acceso a la totalidad de los datos PNR solo lo autorizará el Jefe de la Unidad de Información sobre Pasajeros».

Office des étrangers (Oficina de Extranjería, Bélgica). Se trata de los «pasajeros que tengan previsto entrar o hayan entrado en el territorio por las fronteras exteriores de Bélgica», de los «pasajeros que tengan previsto salir o hayan salido del territorio por las fronteras exteriores de Bélgica» y de los «pasajeros que tengan previsto pasar o hayan pasado por una zona internacional de tránsito situada en Bélgica o se encuentren en dicha zona».[255] A tenor del artículo 29, apartado 3, de la Ley PNR, dichos datos se transmitirán por la UIP a los servicios de policía encargados del control de las fronteras y a la Oficina de Extranjería «inmediatamente después de su registro en el banco de datos de pasajeros» y se destruirán veinticuatro horas después de su transmisión. A tenor de esta disposición, transcurrido ese plazo, la Oficina de Extranjería puede también dirigir a la UIP una petición razonada dirigida a obtener el acceso a esos mismos datos cuando dicho acceso resulte necesario en el marco del ejercicio de sus funciones legales. En consecuencia, dada la finalidad perseguida por el tratamiento de datos a que se refieren los artículos 28 y 29 de la Ley PNR, la novena cuestión prejudicial se sale del marco legal de la Directiva PNR para entrar en el de la Directiva API. Por otra parte, se desprende, en particular, de los autos trasladados a la Secretaría del Tribunal de Justicia que el segundo motivo de la LDH se basa en una interpretación de las disposiciones del capítulo 11 de la Ley PNR según la cual estas también se aplican en caso de cruce de las fronteras interiores de Bélgica.

277. La primera parte de la novena cuestión prejudicial se basa en un presupuesto erróneo y no requiere, a mi juicio, una respuesta por parte del Tribunal de Justicia. En efecto, del artículo 3, apartado 1, en relación con el artículo 2, letras b) y d), de la Directiva API se desprende que esta Directiva solo obliga a las compañías aéreas a comunicar los datos API a las autoridades encargadas de los controles de personas en las fronteras exteriores en relación con los vuelos que llevan a los pasajeros hacia un paso autorizado para cruzar las fronteras exteriores de los Estados miembros con terceros países. De igual forma, el artículo 6, apartado 1, de la referida Directiva solo contempla el tratamiento de los datos API relativos a dichos vuelos. Por otra parte, si bien es cierto que la Directiva PNR ofrece a los Estados miembros la posibilidad de ampliar la obligación de transferir los datos API que se recojan también a las compañías aéreas que realizan vuelos interiores de la UE, esta ampliación debe entenderse sin perjuicio de la Directiva API.[256] En el marco de la Directiva PNR, los datos API transferidos solo serán tratados en el marco de los fines policiales previstos en esta Directiva. A la inversa, el considerando 34 de la Directiva PNR establece que esta se entiende sin perjuicio de las normas vigentes de la Unión sobre la forma en que se realizan los controles de fronteras y de las normas de la Unión que rigen la entrada y salida de su territorio y el artículo 6, apartado 9, segunda frase de esta Directiva estipula que cuando las evaluaciones que se hacen en virtud del apartado 2 de dicho artículo se efectúen en relación con los vuelos interiores de la UE entre Estados miembros a los que sea aplicable el Código de fronteras Schengen,[257] las consecuencias de tales evaluaciones se ajustarán a dicho Reglamento.

278. Reformular esta parte de la novena cuestión prejudicial, como sugiere con carácter subsidiario la Comisión, en el sentido de que vaya referida a la compatibilidad con las disposiciones del Tratado y de la Carta no de la Directiva API, sino de la Directiva PNR y, en particular, de su artículo 2, no solo implicaría modificar el acto en relación con el cual órgano jurisdiccional remitente ha solicitado la apreciación de validez, sino que significaría salir del

255 Ley PNR, artículo 29, apartados 1 y 2.

256 Véase el considerando 10 de la Directiva PNR.

257 Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen) (DO 2016, L 77, p. 1; en lo sucesivo, «Código de fronteras Schengen»).

marco legal en el que se sitúa esta cuestión prejudicial. En efecto, como he explicado, las disposiciones del capítulo 11 de la Ley PNR, contra las que se dirige el segundo motivo de recurso, transponen la Directiva API y no la Directiva PNR.

279. Para el supuesto de que Tribunal de Justicia realice tal reformulación, me ceñiré a las reflexiones que siguen, en particular, en relación con la cuestión de si la evaluación previa que se permite realizar a los Estados miembros de los datos PNR de los pasajeros de los vuelos interiores de la UE, a tenor de la facultad de que disponen con arreglo al artículo 2 de la Directiva PNR, puede considerarse equivalente al ejercicio de las «inspecciones fronterizas» en el sentido del artículo 23, letra a), del Código de fronteras Schengen.[258] En primer término, si bien la evaluación previa de los datos PNR no se produce «en el paso fronterizo» ni el «momento del cruce de la frontera», sino antes de ese momento, se efectúa «con motivo» del cruce inminente de las fronteras. En segundo término, conforme al artículo 2 de la Directiva PNR, se permite a los Estados miembros que puedan ampliar la evaluación previa de los datos PNR a que se refiere el artículo 6, apartado 2, letra a), de la Directiva PNR a los pasajeros de todos los vuelos interiores de la UE, con independencia del comportamiento de las personas en cuestión y de la concurrencia de circunstancias que revelen un riesgo de perturbación de la seguridad pública. Esta evaluación previa tiene además carácter sistemático. Pues bien, ni uno ni otro de esos elementos parece cumplir los indicios mencionados en el artículo 23, letra a), segunda frase, incisos ii), iii) y iv), del Código de fronteras Schengen.[259] En tercer término, por lo que respecta a los indicios mencionados en la letra a), segunda frase, incisos i) y iii), de dicho artículo, me pregunto si la evaluación previa con arreglo al artículo 6, apartado 2, letra a), de la Directiva PNR no se solapa, al menos en parte, con la finalidad de las inspecciones fronterizas efectuadas con arreglo al artículo 8, apartado 2, letra b), y apartado 3, letra a), inciso vi) y letra g), inciso iii), del Código de fronteras Schengen, en su versión modificada por el Reglamento (UE) 2017/458, y, sobre todo, si se distingue claramente, en cuanto a las formas, de esas inspecciones sistemáticas.[260] En este sentido, debo señalar que el artículo 8, apartado 2, *sexies*, y apartado 3, inciso i *bis*), de dicho Código precisan que tales inspecciones «podrán llevarse a cabo por anticipado basándose en datos de los pasajeros recibidos de conformidad con la Directiva [API] o con arreglo a otro derecho de la Unión o nacional». Dicho esto, es verdad que la finalidad de la Directiva PNR no es «garantizar *que pueda autorizarse* la entrada de personas en el territorio de los Estados miembros», o «impedir que las personas se sustraigan a dichas inspecciones», finalidades que el Tribunal de Justicia ha reconocido como objetivos del «control de fronteras» a tenor del Código de fronteras Schengen,[261] dado que dicha Directiva tiene una finalidad exclusivamente represiva. Además, el artículo 23 letra a), segunda frase, inciso ii), del mencionado Código prevé expresamente que el ejercicio de las competencias de policía no puede considerarse equivalente al ejercicio de inspecciones fronterizas cuando los controles estén destinados, en particular, a combatir la delincuencia transfronteriza.[262] Por último, el Tribunal de

258 El artículo 23, letra a), del Código de fronteras Schengen establece que el ejercicio de las competencias de policía no podrá considerarse equivalente al ejercicio de las inspecciones fronterizas cuando las medidas policiales «i) no tengan como objetivo el control de fronteras, ii) estén basadas en información y experiencia policiales de carácter general sobre posibles amenazas a la seguridad pública y estén destinadas, en particular, a combatir la delincuencia transfronteriza, iii) estén concebidas y se ejecuten de un modo claramente diferenciado de las inspecciones sistemáticas de personas en las fronteras exteriores, iv) se lleven a cabo sirviéndose de inspecciones aleatorias».

259 Véase, por analogía, la sentencia de 13 de diciembre de 2018, Touring Tours und Travel y Sociedad de transportes (C-412/17 y C-474/17, EU:C:2018:1005), apartado 61 y jurisprudencia citada, así como el auto de 4 de junio de 2020, FU (C-554/19, no publicado, EU:C:2020:439), apartados 49 a 56.

260 Sobre este extremo, debo señalar que, en el apartado 188 del Dictamen 1/15, el Tribunal de Justicia afirmó que «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».

261 Véase la sentencia de 13 de diciembre de 2018, Touring Tours und Travel y Sociedad de transportes (C-412/17 y C-474/17, EU:C:2018:1005), apartado 55 y jurisprudencia citada.

262 Véase, en este sentido, en particular, el auto de 4 de junio de 2020, FU (C-554/19, no publicado, EU:C:2020:439), apartado 46.

Justicia debería tener en cuenta, asimismo, en su apreciación, la circunstancia destacada, en particular, por la Comisión, de que el artículo 2 de la Directiva PNR únicamente autoriza a los Estados miembros a obligar a las compañías aéreas a transferir los datos PNR que han recopilado en el transcurso normal de su actividad y no contempla, por lo tanto, una obligación análoga a la establecida por la Directiva API para el cruce de las fronteras exteriores.

280. Por lo que se refiere a la segunda parte de la novena cuestión prejudicial, estimo, al igual que la Comisión, que debe entenderse que se refiere al cruce de las fronteras interiores y que pretende conseguir del Tribunal de Justicia unas aclaraciones que permitan al órgano jurisdiccional remitente apreciar la compatibilidad de las disposiciones del capítulo 11 de la Ley PNR con la abolición de los controles en las fronteras interiores de los Estados miembros en el espacio Schengen.

281. A este respecto, habida cuenta de los escasos elementos de que dispone el Tribunal de Justicia, me limitaré a señalar que las disposiciones del capítulo 11 de la Ley PNR solo pueden ser compatibles con el Derecho de la Unión y, en particular, con el artículo 67 TFUE, apartado 2, si se interpretan en el sentido de que se refieren únicamente a la transferencia y al tratamiento de los datos API de los pasajeros que cruzan las fronteras exteriores de Bélgica con países terceros.

282. En la medida en que el Tribunal de Justicia decida reformular la segunda parte de la novena cuestión prejudicial en el sentido de que versa sobre la interpretación de la Directiva PNR en relación con las disposiciones del capítulo 11 de la Ley PNR, me limitaré a señalar que el tratamiento de los datos API previsto en los artículos 28 y 29 de dicha Ley sigue el sistema instaurado por el legislador belga para transponer la Directiva PNR. Así, en primer lugar, los datos API que son objeto de tratamiento son los enumerados en el punto 12 del anexo I de esta Directiva y no solo los contenidos en la lista que figura en el artículo 3, apartado 2, de la Directiva API. En segundo lugar, con arreglo al artículo 29, apartado 1, de la Ley PNR, estos datos se transmitirán a los servicios de policía y a la Oficina de Extranjería por la UIP —que está encargada de recoger y tratar los datos PNR únicamente en el marco de los fines perseguidos por la Directiva PNR— y no directamente por las compañías aéreas, como prevé la Directiva API. Por otra parte, esta transmisión también se refiere a los datos de los pasajeros que pretenden salir o han salido del territorio belga, y sus destinatarios no son únicamente las autoridades encargadas de los controles en las fronteras exteriores, sino también la Oficina de Extranjería, que se encarga de la gestión de la población inmigrante y de combatir la inmigración ilegal. En tercer lugar, en virtud del artículo 29, apartado 4, párrafo segundo, de la Ley PNR, parece que la Oficina de Extranjería ostenta la facultad de dirigir a la UIP solicitudes de acceso a los datos API incluso después del tratamiento de esos datos con ocasión del cruce de las fronteras de los pasajeros de que se trate. En este sentido, esta Oficina se equipara, *de facto*, a una autoridad competente en el sentido del artículo 7 de la Directiva PNR, pese a no revestir tal naturaleza ni figurar en la lista de dichas autoridades comunicada a la Comisión por Bélgica. Pues bien, no cabe, a mi juicio, admitir esta confusión entre los sistemas establecidos por la Directiva API y por la Directiva PNR, pues incumple el principio de la limitación de los fines recogido en el artículo 1, apartado 2, de la Directiva PNR. [263]

283. Sobre la base del conjunto de consideraciones que preceden, propongo al Tribunal de Justicia que conteste a la novena cuestión prejudicial que el artículo 3, apartado 1, de la Directiva API, en virtud del cual los Estados miembros adoptarán las disposiciones necesarias para imponer a las compañías aéreas, la obligación de comunicar, a más tardar al término del embarque, cuando

[263] En su documento de trabajo de 2020 sobre la Directiva API (p. 20), la Comisión también subraya el carácter problemático de la superposición de los sistemas de tratamiento de los datos PNR y API a escala nacional.

lo soliciten las autoridades encargadas de los controles de personas en las fronteras exteriores, la información relativa a las personas a que se refiere el apartado 2 del citado artículo, en relación con el artículo 2, letras b) y d) de la referida Directiva, solo afecta a los pasajeros transportados hacia un paso autorizado para el cruce de las fronteras exteriores de los Estados miembros con países terceros. Una normativa nacional que, con la única finalidad de mejorar los controles en las fronteras y combatir la inmigración ilegal, extiende esta obligación a los datos de las personas que cruzan las fronteras interiores del Estado miembro de que se trate por avión o por otros medios de transporte sería contraria al artículo 67 TFUE, apartado 2, y al artículo 22 del Código de fronteras Schengen.

F. Sobre la décima cuestión prejudicial

284. Mediante su décima cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia si, en el caso de que tuviera que llegar a la conclusión de que Ley PNR incumple los artículos 7, 8, y el artículo 52, apartado 1, de la Carta, puede mantener provisionalmente los efectos de esta Ley con objeto de evitar la inseguridad jurídica y permitir que los datos recogidos y almacenados previamente puedan seguir utilizándose para los fines previstos por la Ley PNR.

285. El Tribunal de Justicia contestó a una cuestión prejudicial del mismo tenor en la sentencia La Quadrature du Net relativa al almacenamiento de los metadatos de las comunicaciones electrónicas, pronunciada después de que se planteara la presente cuestión prejudicial. En esta sentencia, el Tribunal de Justicia recordó, en primer lugar, la jurisprudencia en la que afirma que se estaría actuando en menoscabo de la primacía y de la aplicación uniforme del Derecho de la Unión si los órganos jurisdiccionales nacionales estuvieran facultados para otorgar primacía a las normas nacionales contrarias a este último ordenamiento, aunque fuera con carácter provisional. A continuación, recordó que, en la sentencia de 29 de julio de 2019, Inter-Environnement Wallonie y Bond Beter Leefmilieu Vlaanderen,[264] en un asunto en el que se estaba examinando la legalidad de medidas adoptadas incumpliendo la obligación establecida por el Derecho de la Unión de efectuar una evaluación previa de las repercusiones de un proyecto sobre el medio ambiente y sobre un lugar protegido, reconoció que un órgano jurisdiccional nacional puede, si el Derecho interno se lo permite, mantener excepcionalmente los efectos de dichas medidas cuando ese mantenimiento esté justificado por consideraciones imperiosas relacionadas con la necesidad de evitar una amenaza real y grave de corte del suministro eléctrico del Estado miembro afectado durante el tiempo estrictamente necesario para corregir la referida ilegalidad. No obstante, llegó a la conclusión de que, contrariamente al incumplimiento de una obligación procesal como la evaluación previa de las repercusiones de un proyecto en el ámbito específico de la protección del medio ambiente, la infracción de los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta no puede ser objeto de una regularización mediante un procedimiento comparable al previsto en la sentencia mencionada.[265] Considero que debe darse la misma respuesta la décima cuestión prejudicial en el presente procedimiento.

286. En la medida en que tanto el órgano jurisdiccional remitente como el Gobierno belga y la Comisión y el Consejo se interrogan sobre la cuestión de si el Derecho de la Unión se opone a un uso, en el marco de un proceso penal, de informaciones o de pruebas obtenidas utilizando los datos PNR recogidos, tratados y/o conservados de forma incompatible con el Derecho de la Unión, debo recordar que, en el apartado 222 de la sentencia La Quadrature du Net, el Tribunal

264 C-411/17, EU:C:2019:622, apartados 175, 176, 179 y 181.

265 Véase la sentencia La Quadrature du Net, apartados 217 a 219.

de Justicia precisó que, en el estado actual del Derecho de la Unión, incumbe en principio únicamente al Derecho nacional determinar las normas relativas a la admisibilidad y a la apreciación, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia grave, de la información y de las pruebas que se han obtenido mediante una conservación de datos contraria al Derecho de la Unión, sin perjuicio del cumplimiento de los principios de equivalencia y de efectividad. Por lo que se refiere a este último, el Tribunal de Justicia consideró que dicho principio exige al juez penal nacional que descarte las informaciones y las pruebas que se han obtenido a través de una conservación generalizada e indiferenciada de los datos de tráfico y de localización incompatible con el Derecho de la Unión, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos de delincuencia, cuando estas personas no estén en condiciones de comentar eficazmente tales informaciones y pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y pueden influir destacadamente en la apreciación de los hechos. Estos principios también pueden aplicarse *mutatis mutandis* a las circunstancias del procedimiento principal.

IV. Conclusión

287. Sobre la base del conjunto de consideraciones que preceden, propongo al Tribunal de Justicia que conteste a las cuestiones prejudiciales planteadas por la Cour constitutionnelle (Tribunal Constitucional, Bélgica) del siguiente modo:

«1) 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), en relación con el artículo 2, apartado 2, letra d), de dicho Reglamento, debe interpretarse en el sentido de que:

– Se aplica a una normativa nacional 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, en la medida en que esa normativa regula los tratamientos de los datos PNR efectuados por los transportistas aéreos y por otros operadores económicos, incluida la transmisión de datos PNR a las Unidades de Información sobre los Pasajeros (UIP) mencionadas en el artículo 4 dicha Directiva, prevista en el artículo 8 de dicha Directiva.

– No se aplica a una normativa nacional que transpone la Directiva 2016/681 en la medida en que esta regula los tratamientos de datos efectuados con los fines establecidos en el artículo 1, apartado 2, de dicha Directiva por parte de las autoridades nacionales competentes, incluidas las UIP y, en su caso, los servicios de seguridad e información del Estado miembro interesado.

– Se aplica a una normativa nacional que transpone 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, a efectos de mejorar los controles de personas en las fronteras exteriores y combatir la inmigración ilegal.

2) El punto 12 del anexo I de la Directiva 2016/681 es inválido en la medida en que incluye las "observaciones generales" entre las categorías de datos que las compañías aéreas deben transferir a las UIP con arreglo al artículo 8 de dicha Directiva.

3) El examen de las cuestiones prejudiciales segunda, tercera, cuarta, sexta y octava no ha puesto de relieve otros elementos que puedan afectar a la validez de la Directiva 2016/681.

4) El punto 12 del anexo I de la Directiva 2016/681, en la parte que no sea declarada inválida, debe interpretarse en el sentido de que incluye únicamente la información sobre los menores expresamente contemplada en el mismo y directamente relacionada con el vuelo.

5) El punto 18 del anexo I de la Directiva 2016/681 debe interpretarse en el sentido de que solo comprende la información anticipada sobre los pasajeros expresamente enumerada en ese punto y en el artículo 3, apartado 2, de la Directiva 2004/82 que haya sido recogida por las compañías aéreas en el transcurso normal de su actividad.

6) El concepto de "bases de datos pertinentes" a que se refiere el artículo 6, apartado 3, letra a), de la Directiva 2016/681 debe interpretarse en el sentido de que solo se refiere a las bases de datos nacionales gestionadas por las autoridades competentes con arreglo al artículo 7, apartado 1, de la dicha Directiva y a las bases de datos de la Unión e internacionales directamente explotadas por esas autoridades en el marco de su cometido. Las mencionadas bases de datos deben tener una relación directa y estrecha con los fines de lucha contra el terrorismo y la delincuencia grave perseguidos por dicha Directiva, lo cual implica que hayan sido desarrolladas para esos fines. Al transponer a su Derecho nacional la Directiva 2016/681, los Estados miembros deben publicar una lista de dichas bases de datos y mantenerla al día.

7) El artículo 6, apartado 3, letra b), de la Directiva 2016/681 debe interpretarse en el sentido de que se opone a que, en el marco del tratamiento automatizado previsto por dicha disposición, se utilicen sistemas algorítmicos que puedan conducir a una modificación sin intervención humana de los criterios predeterminados con arreglo a los cuales se ha efectuado el tratamiento, y que no permitan identificar de forma clara y transparente los motivos por los que el tratamiento ha arrojado un resultado positivo.

8) El artículo 12, apartado 1, de la Directiva 2016/681, interpretado de conformidad con los artículos 7, 8, y con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que solo se permite la conservación de los datos PNR proporcionados por las compañías aéreas a la UIP en una base de datos 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, después de que se haya llevado a cabo la evaluación previa con arreglo al artículo 6, apartado 2, letra a), de esta Directiva, en la medida en que se aprecie la existencia, con arreglo a criterios objetivos, de una relación entre dichos datos y la lucha contra el terrorismo o la delincuencia grave. Una conservación generalizada e indiferenciada de los datos PNR en un formato no anonimizado solo puede justificarse frente a una amenaza grave para la seguridad de los Estados miembros que resulte real y actual o previsible, relacionada, por ejemplo, con actividades terroristas, y a condición de que la duración de esta conservación se limite a lo estrictamente necesario.

9) El artículo 6, apartado 2, letra b), de la Directiva 2016/681 debe interpretarse en el sentido de que la comunicación de los datos PNR o del resultado del tratamiento de esos datos con arreglo a la referida disposición que se realicen durante el período inicial de seis meses contemplado en el artículo 12, apartado 2, de esta Directiva debe respetar los requisitos establecidos en el artículo 12, apartado 3, letra b), de dicha Directiva.

10) La Directiva 2016/681, y, en particular, su artículo 1, apartado 2, y su artículo 6, debe interpretarse en el sentido de que se opone a una normativa nacional que permite, como fin del tratamiento de los datos PNR, el seguimiento de determinadas actividades funciones desempeñadas por los servicios de inteligencia y de seguridad, en la medida en que, para atender a esta finalidad, la UIP nacional se vea obligada a tratar dichos datos y/o a transferir tales datos o el resultado de su tratamiento a los servicios mencionados con fines que no sean el que se indica exhaustivamente en el artículo 1, apartado 2, de la referida Directiva, extremo cuya comprobación corresponde al juez nacional.

11) El artículo 12, apartado 3, letra b), de la Directiva 2016/681 debe interpretarse en el sentido de que la UIP no constituye "otra autoridad nacional competente" en el sentido de la referida disposición.

12) El artículo 3, apartado 1, de la Directiva 2004/82, en virtud del cual los Estados miembros adoptarán las disposiciones necesarias para imponer a las compañías aéreas, la obligación de comunicar, a más tardar al término del embarque, cuando lo soliciten las autoridades encargadas de los controles de personas en las fronteras exteriores, la información relativa a las personas a que se refiere el apartado 2 del citado artículo, en relación con el artículo 2, letras b) y d) de la referida Directiva, solo afecta a los pasajeros transportados hacia un paso autorizado para el cruce de las fronteras exteriores de los Estados miembros con países terceros. Una normativa nacional que, con la única finalidad de mejorar los controles en las fronteras y combatir la inmigración ilegal, extienda esta obligación a los datos de las personas que cruzan las fronteras interiores del Estado miembro de que se trate por avión o por otros medios de transporte sería contraria al artículo 67 TFUE, apartado 2, y al artículo 22 del Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras (Código de fronteras Schengen).

13) Un órgano jurisdiccional nacional no puede aplicar una disposición de su Derecho nacional que lo autorice a limitar en el tiempo los efectos de una declaración de ilegalidad que le incumbe, en virtud de ese Derecho, referida a una legislación nacional que obliga a las compañías de transporte aéreo, terrestre y marítimo, así como a los operadores de viajes, con vistas a luchar contra el terrorismo y la delincuencia grave, a transferir los datos PNR y que prevé un tratamiento y una conservación generalizados e indiferenciados de esos datos incompatibles con los artículos 7, 8, y con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea. Con arreglo al principio de efectividad, el juez penal nacional debe descartar las informaciones y la pruebas que se hayan obtenido, en virtud de tal legislación incompatible con el Derecho de la Unión, en el marco de un proceso penal incoado contra personas sospechosas de haber cometido actos terroristas o delitos graves, cuando estas personas no estén en condiciones de comentar eficazmente tales informaciones y pruebas, que proceden de un ámbito que escapa al conocimiento de los jueces y pueden influir destacadamente en la apreciación de los hechos.»