



Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
GIOVANNI PITRUZZELLA
apresentadas em 27 de janeiro de 2022¹

Processo C-817/19

**Ligue des droits humains
contra
Conseil des ministres**

[pedido de decisão prejudicial apresentado pela Cour constitutionnelle (Tribunal Constitucional, Bélgica)]

«Reenvio prejudicial — Proteção dos dados pessoais — Tratamento dos dados dos registos de identificação dos passageiros (PNR) — Regulamento (UE) 2016/679 — Âmbito de aplicação — Diretiva (UE) 2016/681 — Validade — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.º, 8.º e 52.º, n.º 1»

Índice

I.	Introdução	3
II.	Quadro jurídico	4
	A. Direito da União	4
	1. Carta	4
	2. RGPD	5
	3. Diretiva PNR	5
	4. Outros atos de direito da União pertinentes	8
	B. Direito belga	8
	C. Litígio no processo principal, questões prejudiciais e tramitação do processo no Tribunal de Justiça	10

¹ Língua original: francês.

III. Análise	13
A. Quanto à primeira questão prejudicial	13
B. Quanto às segunda, terceira, quarta, sexta e oitava questões prejudiciais	20
1. Quanto aos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta	20
2. Quanto à ingerência nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta	21
3. Quanto à justificação da ingerência resultante da Diretiva PNR	26
a) Quanto ao cumprimento do requisito segundo o qual qualquer restrição ao exercício de um direito fundamental previsto na Carta deve ser previsto por lei ...	26
b) Quanto ao respeito pelo conteúdo essencial dos direitos enunciados nos artigos 7.º e 8.º da Carta	27
c) Quanto ao respeito do requisito segundo o qual a ingerência deve corresponder a um objetivo de interesse geral	30
d) Quanto ao respeito do princípio da proporcionalidade	31
1) Quanto à aptidão dos tratamentos dos dados PNR previstos na Diretiva PNR à luz do objetivo prosseguido	32
2) Quanto ao carácter estritamente necessário da ingerência	33
i) Quanto à delimitação das finalidades do tratamento dos dados PNR	33
ii) Quanto às categorias de dados PNR previstas na Diretiva PNR (segunda e terceira questões prejudiciais)	38
– Quanto ao carácter suficientemente claro e preciso dos pontos 12 e 18 do anexo I (terceira questão prejudicial)	38
– Quanto à extensão dos dados enumerados no anexo I (segunda questão prejudicial)	46
– Quanto aos dados sensíveis	49
iii) Quanto ao conceito de «passageiro» (quarta questão prejudicial)	51
iv) Quanto ao carácter suficientemente claro, preciso e limitado ao estritamente necessário da avaliação prévia dos passageiros (sexta questão prejudicial)	57
– Quanto à comparação com bases de dados na aceção do artigo 6.º, n.º 3, alínea a), da Diretiva PNR	59
– Quanto ao tratamento dos dados PNR à luz de critérios preestabelecidos	60

– Quanto às garantias que rodeiam o tratamento automatizado dos dados PNR	63
– Conclusão quanto à sexta questão prejudicial	64
v) Quanto à conservação dos dados PNR (oitava questão prejudicial)	64
2. Conclusões sobre as segunda, terceira, quarta, sexta e oitava questões prejudiciais	70
C. Quanto à quinta questão prejudicial	70
D. Quanto à sétima questão prejudicial	72
E. Quanto à nona questão prejudicial	74
F. Quanto à décima questão prejudicial	78
IV. Conclusão	79

I. Introdução

1. Com o presente pedido de decisão prejudicial, a Cour constitutionnelle (Tribunal Constitucional, Bélgica) submete ao Tribunal de Justiça uma série de dez questões prejudiciais respeitantes à interpretação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (a seguir «RGPD»)², bem como à validade e à interpretação da Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (a seguir «Diretiva PNR»)³ e da Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras (a seguir «Diretiva API»)⁴. Estas questões foram suscitadas no âmbito de um recurso interposto pela associação sem fins lucrativos Ligue des droits humains (LDH), em que é pedida a anulação total ou parcial da loi du 25 décembre 2016 relative au traitement des données des passagers (Lei de 25 de dezembro de 2016, relativa ao tratamento dos dados dos passageiros) (a seguir «Lei PNR»)⁵, que transpõe para o direito belga a Diretiva PNR bem como a Diretiva API.

2. As questões que o Tribunal de Justiça deverá decidir no presente processo inscrevem-se no âmbito de um dos principais dilemas do constitucionalismo liberal democrático contemporâneo: como deve ser definido o equilíbrio entre o indivíduo e a coletividade na era dos dados, quando as tecnologias digitais permitiram a recolha, a conservação, o tratamento e a análise de enormes massas de dados pessoais para fins preditivos? Os algoritmos, a análise dos *big data* e a inteligência artificial utilizados pelas autoridades públicas podem servir para promover e proteger os interesses fundamentais da sociedade com uma eficácia anteriormente inimaginável: da proteção da saúde pública à sustentabilidade ambiental, da luta contra o terrorismo à

² JO 2016, L 119, p. 1.

³ JO 2016, L 119, p. 132.

⁴ JO 2004, L 261, p. 24.

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

prevenção da criminalidade, em especial a criminalidade grave. Simultaneamente, a recolha indiferenciada de dados pessoais e a utilização das tecnologias digitais pelos poderes públicos podem dar origem a um pan-ótico digital, ou seja, um poder público que vê tudo sem ser visto. Um poder onisciente que pode controlar e prever os comportamentos de qualquer pessoa e tomar as medidas que se impõem, até ao resultado paradoxal, imaginado por Steven Spielberg no filme *Minority Report*, de retirar a liberdade, a título preventivo, ao autor de um crime que ainda não foi cometido. Como é sabido, em certos países, a sociedade prevalece sobre o indivíduo e a utilização dos dados pessoais permite legitimamente realizar uma vigilância de massas eficaz destinada a proteger interesses públicos considerados fundamentais. Inversamente, o constitucionalismo europeu — nacional e supranacional — atribuindo o lugar central ao indivíduo e às suas liberdades, coloca uma importante barreira ao aparecimento de uma sociedade de vigilância de massas, sobretudo após o reconhecimento dos direitos fundamentais à proteção da vida privada e à proteção dos dados pessoais. Contudo, em que medida pode esta barreira ser erigida sem lesar gravemente certos interesses fundamentais da sociedade — como os acima mencionados a título de exemplo — que podem, todavia, ter nexos constitucionais? Encontramo-nos no cerne da questão da relação entre indivíduo e coletividade na sociedade digital. Uma questão que necessita, por um lado, da procura e da aplicação de equilíbrios delicados entre os interesses da coletividade e os direitos dos indivíduos, partindo da importância absoluta que estes últimos têm no património constitucional europeu, e, por outro, do estabelecimento de garantias contra os abusos. Também aqui nos encontramos no âmbito da versão contemporânea de um tema clássico do constitucionalismo, pois, como afirmava de modo lapidar *O Federalista*, os homens não são anjos e é por isso que são necessários mecanismos jurídicos para limitar e controlar o poder público.

3. São estas as questões de ordem geral que se inscrevem no contexto das presentes conclusões, as quais só podem limitar-se a interpretar o direito da União, à luz da jurisprudência anterior do Tribunal de Justiça, utilizando técnicas bem assentes, entre as quais figura a interpretação conforme. É uma técnica a que se recorrerá frequentemente nas presentes conclusões, quando tal se afigure juridicamente possível, com o objetivo de encontrar o equilíbrio necessário, do ponto de vista constitucional, entre as finalidades públicas subjacentes ao sistema de transferência, de recolha e de tratamento dos dados dos registos de identificação dos passageiros (a seguir «dados PNR») e os direitos consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»).

I. Quadro jurídico

A. Direito da União

1. Carta

4. Nos termos do artigo 7.º da Carta, «[t]odas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações».

5. Nos termos do artigo 8.º da Carta:

«1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»

6. Em conformidade com o artigo 52.º, n.º 1, da Carta, «[q]ualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros».

2. RGPD

7. O artigo 2.º, n.º 2, alínea d), do RGPD exclui do âmbito de aplicação deste regulamento o tratamento de dados pessoais efetuado «pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública».

8. Nos termos do artigo 23.º, n.º 1, alínea d), do RGPD:

«O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:

[...]

d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.»

3. Diretiva PNR

9. Apresentarei a seguir apenas uma panorâmica sucinta do funcionamento do sistema instituído pela Diretiva PNR. No decurso da análise jurídica, serão apresentados mais pormenores sobre o conteúdo das disposições da Diretiva PNR pertinente para efeitos da resposta a dar às questões prejudiciais.

10. Em conformidade com o seu artigo 1.º, a Diretiva PNR, adotada com base no artigo 82.º, n.º 1, alínea d), TFUE e no artigo 87.º, n.º 2, alínea a), TFUE, organiza, ao nível da União Europeia, um sistema de transferência, pelas transportadoras aéreas, dos dados PNR de voos extra-UE⁶, bem como de recolha, de tratamento e de conservação destes dados pelas autoridades competentes dos Estados-Membros para fins de luta contra o terrorismo e a criminalidade grave.

11. Nos termos do artigo 3.º, ponto 5, desta diretiva, o «[r]egisto de identificação dos passageiros» ou «PNR» é um «registo das formalidades de viagem impostas a cada passageiro que contém as informações necessárias para permitir o tratamento e o controlo das reservas feitas pelas transportadoras aéreas participantes relativamente a cada viagem reservada por uma pessoa ou em seu nome, quer o registo conste dos sistemas de reserva, dos sistemas de controlo das partidas utilizado para efetuar o controlo dos passageiros embarcados nos voos, ou de sistemas equivalentes que ofereçam as mesmas funcionalidades».

12. O anexo I da Diretiva PNR (a seguir «anexo I») enumera os dados dos registos de identificação dos passageiros recolhidos pelas transportadoras aéreas, que são objeto de transferência na aceção e segundo as modalidades previstas no artigo 8.º desta diretiva.

13. O anexo II da Diretiva PNR (a seguir «anexo II») contém a lista das infrações que constituem «criminalidade grave» na aceção do artigo 3.º, ponto 9, desta diretiva.

14. O artigo 2.º da Diretiva PNR prevê a possibilidade de os Estados-Membros decidirem aplicar esta diretiva também aos «voos intra-UE»⁷ ou a alguns deles, considerados «necessários» a fim de prosseguir os objetivos da referida diretiva.

15. Nos termos do artigo 4.º, n.º 1, da Diretiva PNR, «[c]ada Estado-Membro cria ou designa uma autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave, ou cria ou designa uma secção de tal autoridade, para agir na qualidade da sua “unidade de informações de passageiros” (UIP)». Em conformidade com o n.º 2, alínea a), deste artigo 4.º, a UIP é responsável, nomeadamente, pela recolha dos dados PNR junto das transportadoras aéreas, pela conservação e pelo tratamento desses dados, bem como pela transferência desses dados ou dos resultados do seu tratamento às autoridades competentes referidas no artigo 7.º da Diretiva PNR. Nos termos do n.º 2 deste artigo 7.º, essas autoridades são «autoridades competentes para fins de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave»⁸.

⁶ Nos termos do artigo 3.º, ponto 2, da Diretiva PNR, um «voo extra-UE» é «um voo regular ou não regular efetuado por uma transportadora aérea a partir de um país terceiro e programado para aterrar no território de um Estado-Membro, ou a partir do território de um Estado-Membro e programado para aterrar num país terceiro, incluindo, em ambos os casos, os voos com escala no território de Estados-Membros ou de países terceiros».

⁷ Nos termos do artigo 3.º, ponto 3, da Diretiva PNR, constitui um «voo intra-UE» «um voo regular ou não regular efetuado por uma transportadora aérea a partir do território de um Estado-Membro, programado para aterrar no território de um ou mais Estados-Membros, sem escala no território de um país terceiro».

⁸ O artigo 7.º, n.º 1, da Diretiva PNR prevê que cada Estado-Membro adota uma lista das autoridades competentes habilitadas a solicitar às UIP ou a delas receber dados PNR ou o resultado do tratamento de tais dados, a fim de analisar mais minuciosamente essas informações ou de tomar medidas apropriadas para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Esta lista foi publicada pela Comissão em 2018 (JO 2018, C 194, p. 1; retificação JO 2020, C 366, p. 55).

16. Nos termos do artigo 6.º, n.º 1, segundo período, da Diretiva PNR, «[c]aso os dados PNR transferidos pelas transportadoras aéreas incluam dados distintos dos enumerados no anexo I, a UIP apaga imediata e definitivamente esses dados assim que os receber». O n.º 2 deste artigo tem a seguinte redação:

«2. A UIP procede ao tratamento dos dados PNR exclusivamente para os seguintes fins:

- a) Proceder a uma avaliação dos passageiros antes da sua chegada prevista ao Estado-Membro ou da sua partida prevista desse Estado-Membro, a fim de identificar as pessoas que, pelo facto de poderem estar implicadas numa infração terrorista ou numa forma de criminalidade grave, devem ser sujeitas a um controlo mais minucioso pelas autoridades competentes a que se refere o artigo 7.º e, se for caso disso, pela Europol, nos termos do artigo 10.º;
- b) Responder, caso a caso, aos pedidos devidamente fundamentados, baseados em motivos suficientes, apresentados pelas autoridades competentes, para fornecer e tratar dados PNR, em casos específicos, para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas ou da criminalidade grave, e para disponibilizar às autoridades competentes ou, se for caso disso, à Europol os resultados desse tratamento; e
- c) Analisar os dados PNR com o objetivo de atualizar ou criar novos critérios a utilizar nas avaliações realizadas nos termos do n.º 3, alínea b), a fim de identificar pessoas que possam estar implicadas em infrações terroristas ou em formas de criminalidade grave.»

17. O artigo 12.º da Diretiva PNR contém as disposições relativas à conservação dos dados PNR.

18. O artigo 5.º da Diretiva PNR prevê que cada UIP nomeia um responsável pela proteção de dados incumbido de controlar o tratamento dos dados PNR e de aplicar as salvaguardas relevantes. Além disso, cada Estado-Membro é obrigado, em conformidade com o artigo 15.º desta diretiva, a estabelecer que a autoridade nacional de controlo referida no artigo 25.º da Decisão-Quadro 2008/977/JAI⁹, substituída pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (a seguir «Diretiva Cooperação Policial»)¹⁰, seja responsável por monitorizar a aplicação, no seu território, das disposições adotadas por força da referida diretiva. Esta autoridade, que exerce as suas funções tendo em vista a proteção dos direitos fundamentais no âmbito do tratamento de dados pessoais¹¹, é encarregada, nomeadamente, por um lado, de analisar as reclamações apresentadas por qualquer titular de dados, investigar a questão e informar os titulares dos dados sobre os progressos e os resultados da reclamação num prazo razoável e, por outro, de verificar a legalidade do tratamento de dados, proceder a investigações, inspeções e auditorias nos termos do direito nacional, por sua própria iniciativa ou com base numa reclamação¹².

⁹ Decisão-Quadro do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO 2008, L 350, p. 60).

¹⁰ JO 2016, L 119, p. 89. O artigo 25.º da Decisão-Quadro 2008/977/JAI foi substituído pelo artigo 41.º da Diretiva Cooperação Policial.

¹¹ V. artigo 15.º, n.º 2, da Diretiva PNR.

¹² V. artigo 15.º, n.º 3, alíneas a) e b), da Diretiva PNR.

4. Outros atos de direito da União pertinentes

19. O quadro jurídico do presente processo é completado pela Diretiva API e pela Diretiva Cooperação Policial. Por razões de legibilidade das presentes conclusões, o conteúdo das disposições pertinentes destes atos será exposto na medida em que tal se revele necessário para o tratamento das questões que lhes dizem respeito ou, mais genericamente, para efeitos da análise jurídica.

B. Direito belga

20. Em conformidade com o artigo 22.º da Constituição belga, «[t]odas as pessoas têm direito ao respeito pela sua vida privada e familiar, exceto nos casos e nas condições estabelecidos por lei».

21. Nos termos do seu artigo 2.º, a Lei PNR transpõe a Diretiva API e a Diretiva PNR, bem como, parcialmente, a Diretiva 2010/65/UE¹³.

22. Em conformidade com o seu artigo 3.º, § 1, a Lei PNR «determina as obrigações das transportadoras e dos operadores de viagens relativas à transmissão de dados dos passageiros com destino, proveniência ou trânsito em território nacional». Nos termos do artigo 4.º, pontos 1 e 2, desta lei, entende-se por «transportadora» «qualquer pessoa singular ou coletiva que preste, a título profissional, serviços de transporte de pessoas por via aérea, marítima, ferroviária ou terrestre» e por «operador de viagens» «qualquer organizador ou intermediário de viagens na aceção da Lei de 16 de fevereiro de 1994, que regula o contrato de organização de viagens e o contrato de intermediação de viagens».

23. O artigo 8.º da Lei PNR dispõe:

«§ 1. Os dados dos passageiros são tratados para efeitos de:

1º Investigação e repressão, incluindo a execução de penas ou de medidas restritivas da liberdade, relativas às infrações previstas no artigo 90.º ter, § 2, [...] 7º, [...] 8º, [...] 11º, [...] 14º, [...] 17º, 18º, 19º e § 3, do Code d’Instruction criminelle (Código de Processo Penal);

2º Investigação e repressão, incluindo a execução de penas ou de medidas restritivas da liberdade, relativas às infrações previstas nos artigos 196.º, no que respeita às infrações de falsificação de documentos autênticos e públicos, 198.º, 199.º, 199.º bis, 207.º, 213.º, 375.º e 505.º do Code pénal (Código Penal);

3º Prevenção das perturbações graves da segurança pública no contexto da radicalização violenta, através do acompanhamento dos fenómenos e grupos, em conformidade com o artigo 44/5.º, § 1, 2.º e 3.º, e § 2, da loi du 5 août 1992 sur la fonction de police (Lei relativa à função de polícia, de 5 de agosto de 1992);

4º Acompanhamento das atividades referidas no artigo 7.º, 1º e 3º/l, e no artigo 11.º, § 1, 1º a 3º e 5º, da loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998)¹⁴;

¹³ Diretiva do Parlamento Europeu e do Conselho, de 20 de outubro de 2010, relativa às formalidades de declaração exigidas aos navios à chegada e/ou à partida dos portos dos Estados-Membros e que revoga a Diretiva 2002/6/CE (JO 2010, L 283, p. 1).

¹⁴ *Moniteur belge* de 18 de dezembro de 1998, p. 40312.

5° Investigação e repressão das infrações previstas no artigo 220.º, § 2, da loi générale sur les douanes et accises du 18 juillet 1977 (Lei geral em matéria aduaneira e de impostos especiais de consumo, de 18 de julho de 1977) e no artigo 45.º, n.º 3, da loi du 22 décembre 2009 relative au régime général d'accise (Lei relativa ao regime geral dos impostos especiais de consumo, de 22 de dezembro de 2009) [...]

§ 2. Nas condições previstas no capítulo 11, os dados dos passageiros são igualmente tratados a fim de melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal.»

24. O artigo 9.º da Lei PNR contém a lista dos dados que são objeto de transferência. Estes dados correspondem aos enumerados no anexo I.

25. Em conformidade com o artigo 18.º da Lei PNR, «os dados dos passageiros são conservados no banco de dados dos passageiros por um período máximo de cinco anos a contar do respetivo registo. Decorrido esse prazo, os dados dos passageiros são destruídos».

26. O artigo 19.º desta lei prevê que «[d]ecorrido o prazo de seis meses a contar do registo dos dados dos passageiros no banco de dados dos passageiros, todos os dados dos passageiros são anonimizados mediante mascaramento dos elementos de informação».

27. O artigo 24.º da Lei PNR prevê:

«§ 1. Os dados dos passageiros são tratados para efeitos de realização de uma avaliação prévia dos passageiros antes da sua chegada, da sua partida ou do seu trânsito previsto em território nacional, a fim de determinar as pessoas que devem ser submetidas a um exame mais aprofundado.

§ 2. No âmbito das finalidades previstas no artigo 8.º, § 1, 1.º, 4.º e 5.º, ou relativas às ameaças mencionadas nos artigos 8.º, 1.º, a), b), c), d), f), g) e 11.º, § 2, da loi du 30 novembre 1998 organique des services de renseignement et de sécurité (Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998) a avaliação prévia dos passageiros assenta numa correspondência positiva, resultante de uma correlação dos dados dos passageiros com:

1º os bancos de dados geridos pelos serviços competentes ou que estejam diretamente à sua disposição ou acessíveis no âmbito das suas funções ou com listas de pessoas elaboradas pelos serviços competentes no âmbito das suas funções.

2º os critérios de avaliação preestabelecidos pela UIP, referidos no artigo 25.º

§ 3 No âmbito das finalidades previstas no artigo 8.º, § 1, 3º, a avaliação prévia dos passageiros assenta numa correspondência positiva, resultante de uma correlação dos dados dos passageiros com os bancos de dados referidos no § 2, 1º[...].»

28. O artigo 25.º da Lei PNR reproduz o conteúdo do artigo 6.º, n.º 4, da Diretiva PNR.

29. O capítulo 11 da Lei PNR contém as disposições que regem o tratamento dos dados dos passageiros com vista à melhoria do controlo nas fronteiras e à luta contra a imigração ilegal. Estas disposições constituem a transposição da Diretiva API para o direito belga.

30. O artigo 44.º da Lei PNR prevê que a UIP designa um responsável pela proteção de dados no service public fédéral intérieur (Serviço Público Federal Interior). A supervisão da aplicação das disposições da Lei PNR é exercida pela Commission de la protection de la vie privée (Comissão para a proteção da vida privada).

31. O artigo 51.º da Lei PNR altera a Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998, inserindo um artigo 16.º/3 com a seguinte redação:

«§ 1. Os serviços de informações e de segurança podem, no interesse do exercício das suas funções, decidir, de forma devidamente fundamentada, aceder aos dados dos passageiros referidos no artigo 7.º da Lei [PNR].

§ 2. A decisão referida no § 1 é tomada pelo chefe do serviço e comunicada por escrito à Unidade de Informação dos passageiros referida no capítulo 7 da referida lei. A decisão é notificada ao Comité Permanente R com a respetiva fundamentação.

O Comité Permanente R proíbe os serviços de informações e de segurança de explorarem os dados recolhidos em condições que não respeitem os requisitos legais.

A decisão pode incidir sobre um conjunto de dados relativos a uma investigação de informações específica. Neste caso, a lista das consultas dos dados dos passageiros é comunicada mensalmente ao Comité Permanente R.»

C. Litígio no processo principal, questões prejudiciais e tramitação do processo no Tribunal de Justiça

32. Por petição enviada à Cour constitutionnelle (Tribunal Constitucional, Bélgica) em 24 de julho de 2017, a LDH interpôs um recurso de anulação total ou parcial da Lei PNR. Invocou dois fundamentos de recurso.

33. No primeiro fundamento, invocado a título principal e relativo à violação do artigo 22.º da Constituição belga, em conjugação com o artigo 23.º do RGPD, com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta bem como com o artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, assinada em Roma em 4 de novembro de 1950 (a seguir «CEDH»), a LDH considera que a lei impugnada não respeita o princípio da proporcionalidade quanto ao seu âmbito de aplicação e às categorias de dados abrangidos, aos tratamentos de dados que institui, às suas finalidades e ao prazo de conservação dos dados. Em especial, sustenta que a definição dos dados PNR é demasiado ampla e suscetível de conduzir à revelação de dados sensíveis, e que a definição do conceito de «passageiro» contida nessa lei permite um tratamento sistemático não direcionado dos dados de todos os passageiros em causa. Além disso, a LDH considera que a Lei PNR não define de forma suficientemente clara a natureza e as modalidades do método de *pre-screening* dos bancos de dados de passageiros bem como dos critérios que servem de «indicadores de ameaça». Por último, considera que a Lei PNR excede os limites do estritamente necessário, no sentido de que prossegue finalidades de tratamento dos dados PNR mais amplas do que as admitidas pela Diretiva PNR e que o prazo de cinco anos para a conservação dos dados PNR é desproporcionado. No segundo fundamento, invocado a título subsidiário e relativo à violação do artigo 22.º da Constituição belga, em conjugação o artigo 3.º, n.º 2, TUE e com o artigo 45.º da Carta, a LDH contesta as disposições do capítulo 11 da Lei PNR que transpõem a Diretiva API.

34. O Conselho de Ministros do Reino da Bélgica, enquanto interveniente na Cour constitutionnelle (Tribunal Constitucional, Bélgica), opõe-se ao recurso da LDH, contestando tanto a admissibilidade como a procedência dos dois fundamentos de recurso invocados.

35. A Cour constitutionnelle (Tribunal Constitucional, Bélgica), por seu lado, apresenta as seguintes considerações.

36. No que respeita ao primeiro fundamento, interroga-se, antes de mais, sobre a questão de saber se a definição dos dados PNR, que figura no anexo I, é suficientemente clara e precisa. A descrição de alguns destes dados reveste carácter exemplificativo e não exaustivo. Seguidamente, o referido órgão jurisdicional observa que a definição do conceito de «passageiro» que figura no artigo 3.º, ponto 4, da Diretiva PNR implica a recolha, a transferência, o tratamento e a conservação dos dados PNR de qualquer pessoa transportada ou que deva ser transportada e inscrita na lista de passageiros, independentemente da existência de motivos sérios para crer que a pessoa em causa cometeu uma infração ou está prestes a cometer uma infração, ou foi considerada culpada de uma infração. No que respeita aos tratamentos dos dados PNR, observa que estes últimos são sistematicamente objeto de uma avaliação prévia que implica o cruzamento dos dados PNR de todos os passageiros com bancos de dados ou critérios preestabelecidos, com vista a estabelecer correspondências. No entanto, a Cour constitutionnelle (Tribunal Constitucional, Bélgica) precisa que, embora os critérios devam ser específicos, fiáveis e não discriminatórios, parece-lhe tecnicamente impossível definir melhor os critérios preestabelecidos que servirão para a determinação de perfis de risco. No que respeita ao prazo de conservação dos dados PNR previsto no artigo 12.º, n.º 1, da Diretiva PNR, por força do qual os referidos dados podem ser conservados por um prazo de cinco anos, o órgão jurisdicional de reenvio considera que os dados PNR são conservados sem ter em conta a questão de saber se os passageiros em causa seriam ou não suscetíveis, no âmbito da avaliação prévia, de representar um risco para a segurança pública. Nestas circunstâncias, o órgão jurisdicional de reenvio interroga-se sobre a questão de saber se, atendendo à jurisprudência resultante, nomeadamente, do Acórdão de 21 de dezembro de 2016, *Tele2 Sverige e Watson e o.*¹⁵ e do Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017¹⁶, se pode considerar que o sistema de recolha, de transferência, de tratamento e de conservação dos dados PNR estabelecido pela Diretiva PNR não ultrapassa os limites do estritamente necessário. Neste contexto, esse órgão jurisdicional interroga-se igualmente sobre a questão de saber se a Diretiva PNR se opõe a uma regulamentação nacional, como a que resulta do artigo 8.º, n.º 1, ponto 4), da Lei PNR, que autoriza o tratamento dos dados PNR para uma finalidade diferente das previstas por esta diretiva. Por último, interroga-se sobre se a UIP pode ser considerada «outra autoridade nacional» suscetível, nos termos do artigo 12.º, n.º 3, alínea b), ii), da Diretiva PNR, de autorizar a divulgação dos dados PNR integrais após um prazo de seis meses. Quanto ao segundo fundamento, o órgão jurisdicional de reenvio observa que visa o artigo 3.º, n.º 1, o artigo 8.º, n.º 2, bem como os artigos 28.º a 31.º da Lei PNR, que regem a recolha e o tratamento dos dados dos passageiros para efeitos de combate à imigração ilegal e melhoria dos controlos nas fronteiras. Recordando que, segundo a primeira destas disposições, esta lei abrange os voos com destino ao território nacional, dele provenientes e transitando pelo mesmo, esse órgão jurisdicional precisa que o legislador nacional tinha incluído os voos «intra-UE» no âmbito de aplicação da referida lei, a fim de obter «um quadro mais completo dos passageiros que constituam uma potencial ameaça para a segurança [dentro da União] e nacional», baseando-se na faculdade prevista no artigo 2.º da Diretiva PNR, em conjugação com o seu considerando 10.

¹⁵ C-203/15 e C-698/15, a seguir «Acórdão *Tele2 Sverige*», EU:C:2016:970.

¹⁶ A seguir «Parecer 1/15», EU:C:2017:592.

37. Foi neste contexto que a Cour constitutionnelle (Supremo Tribunal, Bélgica) decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

- «1) Deve o artigo 23.º do [RGPD], em conjugação com o artigo 2.º, n.º 2, alínea d), deste regulamento, ser interpretado no sentido de que se aplica a uma legislação nacional como a Lei [PNR], que transpõe a Diretiva [PNR], bem como a Diretiva [API] e a Diretiva 2010/65?
- 2) O anexo I [...] é compatível com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], no sentido de que os dados que enumera são muito vastos — nomeadamente os dados referidos no ponto 18 [deste anexo I], que excedem os dados referidos no artigo 3.º, n.º 2, da Diretiva [API] — e de que, considerados conjuntamente, poderiam revelar dados sensíveis e violar, assim, os limites do “estritamente necessário”?
- 3) Os pontos 12 e 18 do anexo I [...] são compatíveis com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], na medida em que, tendo em conta os termos “designadamente” e “incluindo”, os dados a que se referem são mencionados a título exemplificativo, e não exaustivo, de modo que a exigência de precisão e de clareza das regras que implicam uma ingerência no direito ao respeito da vida privada e no direito à proteção dos dados pessoais não é respeitada?
- 4) O artigo 3.º, ponto 4, da Diretiva [PNR,] e o anexo I [...] são compatíveis com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], na medida em que o sistema de recolha, de transferência e de tratamento generalizados de dados dos passageiros que essas disposições instituem abrange qualquer pessoa que utilize o meio de transporte em causa, independentemente de qualquer elemento objetivo que permita considerar que essa pessoa é suscetível de representar um risco para a segurança pública?
- 5) Deve o artigo 6.º da Diretiva [PNR], em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que se opõe a uma legislação nacional como a lei impugnada, que admite como finalidade do tratamento dos dados “PNR” o acompanhamento das atividades visadas pelos serviços de informações e de segurança, integrando assim esta finalidade na prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave?
- 6) O artigo 6.º da Diretiva [PNR] é compatível com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], na medida em que a avaliação prévia que regula, através de uma correlação com bancos de dados e critérios preestabelecidos, se aplica de forma sistemática e generalizada aos dados dos passageiros, independentemente de qualquer elemento objetivo que permita considerar que esses passageiros são suscetíveis de representar um risco para a segurança pública?
- 7) Pode o conceito de “outra autoridade nacional competente” a que se refere o artigo 12.º, n.º 3, da Diretiva [PNR] ser interpretado no sentido de que abrange a UIP criada pela Lei [PNR], que pode, assim, autorizar o acesso aos dados PNR, decorrido o prazo de seis meses, no âmbito de investigações pontuais?
- 8) Deve o artigo 12.º da Diretiva [PNR], em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da [Carta], ser interpretado no sentido de que se opõe a uma legislação nacional como a lei impugnada, que prevê um prazo geral de conservação dos dados de cinco anos, sem distinguir se os passageiros em causa se revelam, no âmbito da avaliação prévia, suscetíveis ou não de representar um risco para a segurança pública?

- 9) a) A Diretiva [API] é compatível com o artigo 3.º, n.º 2, [TUE] e com o artigo 45.º da [Carta], na medida em que as obrigações que institui se aplicam aos voos no interior da [União]?
- b) Deve a Diretiva [API], em conjugação com o artigo 3.º, n.º 2, [TUE] e com o artigo 45.º da [Carta], ser interpretada no sentido de que se opõe a uma legislação nacional como a lei impugnada, que, para efeitos de combate à imigração ilegal e de melhoria dos controlos nas fronteiras, autoriza um sistema de recolha e de tratamento de dados dos passageiros “com destino, proveniência ou trânsito em território nacional”, o que pode implicar indiretamente o restabelecimento dos controlos nas fronteiras internas?
- 10) Se, com base nas respostas dadas às questões prejudiciais anteriores, concluir que a lei impugnada, que transpõe, designadamente, a Diretiva [PNR], viola uma ou mais das obrigações decorrentes das disposições mencionadas nestas questões, poderia a Cour constitutionnelle (Tribunal Constitucional) manter provisoriamente os efeitos da Lei [PNR], a fim de evitar uma insegurança jurídica e permitir que os dados recolhidos e conservados anteriormente possam ainda ser utilizados para os fins previstos [por esta] lei?»

38. Foram apresentadas observações escritas, nos termos do artigo 23.º do Estatuto do Tribunal de Justiça da União Europeia, pela LDH, pelos Governos belga, checo, dinamarquês, alemão, estónio, irlandês, espanhol, francês, cipriota, letão, neerlandês, austríaco, polaco e finlandês, bem como pelo Parlamento Europeu, pelo Conselho da União Europeia e pela Comissão Europeia. Em conformidade com o artigo 24.º do Estatuto do Tribunal de Justiça da União Europeia, a Comissão, a Autoridade Europeia para a Proteção de Dados (AEPD) e a Agência dos Direitos Fundamentais da União Europeia (FRA) foram convidadas a responder por escrito a perguntas colocadas pelo Tribunal de Justiça. Foi realizada uma audiência de alegações em 13 de julho de 2021.

II. Análise

A. Quanto à primeira questão prejudicial

39. Com a sua primeira questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se o artigo 2.º, n.º 2, alínea d), do RGPD deve ser interpretado no sentido de que este regulamento, nomeadamente o seu artigo 23.º, n.º 1, nos termos do qual o direito da União ou os direitos dos Estados-Membros podem limitar por medida legislativa, por razões exaustivamente enumeradas, o alcance das obrigações e dos direitos previstos pelo referido regulamento, é aplicável aos tratamentos de dados efetuados com base numa legislação nacional, como a Lei PNR, que transpõe para o direito interno a Diretiva PNR bem como a Diretiva API e a Diretiva 2010/65.

40. O artigo 2.º, n.º 2, do RGPD prevê exceções ao âmbito de aplicação deste regulamento, conforme definido, em termos muito amplos¹⁷, no seu artigo 2.º, n.º 1¹⁸. Enquanto derrogações à aplicação de uma regulamentação que rege o tratamento de dados pessoais suscetível de violar as liberdades fundamentais, essas exceções devem ser objeto de interpretação estrita¹⁹.

41. O artigo 2.º, n.º 2, alínea d), do RGPD contém, nomeadamente, uma cláusula de exclusão nos termos da qual este regulamento não se aplica ao tratamento de dados pessoais efetuado «pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública». Esta cláusula de exclusão baseia-se num duplo critério, subjetivo e objetivo. Ficam, assim, excluídos do âmbito de aplicação do referido regulamento os tratamentos de dados efetuados, em primeiro lugar, pelas «autoridades competentes» e, em segundo lugar, para os fins enumerados nesta disposição. Por conseguinte, há que apreciar os diferentes tipos de tratamento de dados abrangidos pela Lei PNR à luz deste duplo critério.

42. No que respeita, em primeiro lugar, aos tratamentos de dados efetuados pelas transportadoras (aéreas, ferroviárias, terrestres e marítimas) na UIP ou pelos operadores de viagens *para efeitos de prestação de serviços ou comerciais*, na medida em que sejam visados pela referida lei, continuam a ser regidos pelo RGPD, uma vez que nem a vertente subjetiva nem a vertente objetiva do critério de exclusão contido no artigo 2.º, n.º 2, alínea d), deste regulamento estão preenchidas.

43. No que respeita, em segundo lugar, *à transferência pelas transportadoras ou pelos operadores de viagem dos dados PNR para a UIP*, que constitui, em si, um «tratamento» na aceção do artigo 4.º, ponto 2, do RGPD²⁰, a sua inclusão no âmbito de aplicação deste regulamento é menos evidente.

44. Com efeito, por um lado, esta transferência não é efetuada por uma «autoridade competente», na aceção do artigo 3.º, ponto 7, da Diretiva Cooperação Policial, para o qual se deve remeter por analogia, na falta de definição deste conceito pelo RGPD²¹. Um operador económico, como uma empresa de transporte ou uma agência de viagens, ao qual incumbe apenas uma obrigação legal

¹⁷ V., neste sentido, Acórdão de 22 de junho de 2021, Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504, n.º 61).

¹⁸ Nos termos do artigo 2.º, n.º 1, do RGPD, «[o] presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados».

¹⁹ V. Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems (C-311/18, EU:C:2020:559, n.º 84), bem como Acórdão de 22 de junho de 2021, Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504, n.º 62).

²⁰ V., neste sentido, Acórdão de 6 de outubro de 2020, Privacy International (C-623/17, a seguir «Acórdão Privacy International», EU:C:2020:790, n.º 41 e jurisprudência referida). Nos termos do artigo 4.º, ponto 2, do RGPD, constitui «tratamento» «uma operação [...] [efetuada] sobre dados pessoais ou sobre conjuntos de dados pessoais [...] tais como [...] a divulgação por transmissão».

²¹ V., neste sentido, Acórdão de 22 de junho de 2021, Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504, n.º 69). Nos termos do artigo 3.º, ponto 7, alíneas a) e b), da Diretiva Cooperação Policial, uma «autoridade competente» é «a) [u]ma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou b) [q]ualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos» para esses mesmos efeitos.

de transferência de dados pessoais e ao qual não foi confiada qualquer prerrogativa de poder público²², não pode ser considerado um organismo ou entidade na aceção do referido artigo 3.º, ponto 7, alínea b)²³.

45. Por outro lado, a transferência dos dados PNR pelas empresas de transporte e pelos operadores de viagens é efetuada para cumprir uma obrigação imposta pela lei com o objetivo de permitir a prossecução dos fins enumerados no artigo 2.º, n.º 2, alínea d), do RGPD.

46. Ora, na minha opinião, resulta claramente da redação desta disposição que apenas os tratamentos que preencham simultaneamente a vertente subjetiva e a vertente objetiva do critério de exclusão nela enunciado estão situados fora do âmbito de aplicação do RGPD. A transferência dos dados PNR para a UIP imposta pela Lei PNR às empresas de transporte e aos operadores de viagens está, por conseguinte, abrangida por este regulamento.

47. No que respeita às disposições da Lei PNR que transpõem a Diretiva PNR, esta conclusão é corroborada pelo artigo 21.º, n.º 2, desta diretiva, que prevê que esta «não prejudica a aplicabilidade da Diretiva 95/46/CE²⁴ ao tratamento de dados pessoais pelas transportadoras aéreas». A leitura desta disposição que o Governo francês, nomeadamente, sugere, segundo a qual a mesma se limita a prever que as transportadoras continuam sujeitas às obrigações fixadas pelo RGPD para os tratamentos de dados que não sejam previstos pela Diretiva PNR, deve, na minha opinião, ser afastada. Com efeito, atendendo à sua redação, o alcance desta «cláusula de não prejuízo» é amplo e define-se unicamente por referência ao autor do tratamento, sem qualquer menção à finalidade do tratamento nem ao quadro em que este ocorre, se for efetuado no exercício da atividade comercial da transportadora aérea ou em execução de uma obrigação legal. Observo, além disso, que uma cláusula com o mesmo teor figura no artigo 13.º, n.º 3, da Diretiva PNR, que se refere especialmente às obrigações que incumbem às transportadoras aéreas por força do RGPD «de tomarem as medidas técnicas e organizativas adequadas para proteger a segurança e confidencialidade dos dados pessoais». Ora, esta disposição figura entre as que organizam a proteção dos dados pessoais tratados ao abrigo da Diretiva PNR e segue-se ao artigo 13.º, n.º 1, desta diretiva, que, de um modo geral, submete qualquer tratamento de dados efetuado em aplicação desta às disposições da Decisão-Quadro 2008/977 aí mencionadas. Contrariamente ao que sustenta o Governo francês, esta estrutura normativa permite, por um lado, ler o n.º 3 do referido artigo 13.º como uma cláusula que sujeita ao RGPD apenas o tratamento de dados previsto na Diretiva PNR que não seja efetuado por «autoridades competentes» na aceção da Diretiva Cooperação Policial e, por outro, entender a referência ao respeito das obrigações impostas pelo referido regulamento em matéria de segurança e de confidencialidade dos dados como uma forma de recordar as garantias que devem obrigatoriamente envolver a transferência dos dados PNR pelas transportadoras para as UIP.

²² Não resulta da decisão de reenvio nenhum indício nesse sentido.

²³ Esse operador também não poderia ser qualificado de «subcontratante» na aceção do artigo 4.º, ponto 8, do RGPD ou do artigo 3.º, ponto 9, da Diretiva Cooperação Policial, tratando-se antes do «responsável pelo tratamento», na aceção do artigo 4.º, ponto 7, segundo período, do RGPD. Nos termos do artigo 4.º, ponto 8, do RGPD e do artigo 3.º, ponto 9, da Diretiva Cooperação Policial, que são redigidos de forma idêntica, o «subcontratante» é a «pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes». Nos termos do artigo 4.º, ponto 7, primeiro período, do RGPD, o «responsável pelo tratamento», é «a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que [...] determina as finalidades e os meios de tratamento», o segundo período desta disposição precisa que «sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro».

²⁴ Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31). Esta diretiva foi revogada e substituída pelo RGPD, v. artigo 94.º deste regulamento.

48. A conclusão enunciada no n.º 46 das presentes conclusões não é posta em causa pelo considerando 19 do RGPD e pelo considerando 11 da Diretiva Cooperação Policial, a que se referem, nomeadamente, os Governos alemão, irlandês e francês para sustentar a natureza de *lex specialis* da Diretiva PNR. A este respeito, é decerto verdade que esta diretiva institui, para os tratamentos de dados pessoais por ela visados, um quadro de proteção autónomo desses dados em relação ao RGPD. No entanto, este quadro específico só se aplica aos tratamentos dos dados PNR efetuados pelas «autoridades competentes», na aceção do artigo 3.º, ponto 7, da Diretiva Cooperação Policial, entre as quais figuram, nomeadamente, as UIP, ao passo que a transferência dos dados PNR para as UIP continua sujeita ao quadro geral estabelecido pelo RGPD em aplicação, designadamente, da «cláusula de não prejuízo» prevista no artigo 21.º, n.º 2, da Diretiva PNR.

49. Em apoio da sua tese segundo a qual o RGPD não se aplica à transferência dos dados PNR para as UIP pelas transportadoras e pelos operadores de viagens, os Governos belga, irlandês, francês e cipriota remetem para o Acórdão de 30 de maio de 2006, Parlamento/Conselho e Comissão²⁵, no qual o Tribunal de Justiça declarou que a transferência dos dados PNR pelas transportadoras aéreas comunitárias para as autoridades dos Estados Unidos da América, no âmbito de um acordo negociado entre estes últimos e a Comunidade Europeia, constituía um tratamento de dados pessoais na aceção do artigo 3.º, n.º 2, da Diretiva 95/46²⁶, e não era, portanto, abrangida pelo âmbito de aplicação desta diretiva. Para chegar a esta conclusão, o Tribunal de Justiça teve em conta a *finalidade da transferência* bem como o facto de a mesma «[se integrar] num quadro instituído pelos poderes públicos», apesar de os dados serem recolhidos e transferidos por operadores privados²⁷.

50. A este respeito, basta observar que, no Acórdão de 6 de outubro de 2020, La Quadrature du Net e o.²⁸, o Tribunal de Justiça considerou, em substância, que o Acórdão Parlamento/Conselho não era transponível para o contexto do RGPD²⁹.

51. Por outro lado, no n.º 102 do Acórdão La Quadrature du Net³⁰, aplicando por analogia o raciocínio seguido nos Acórdãos Tele2 Sverige e de 2 de outubro de 2018, Ministerio Fiscal³¹, o Tribunal de Justiça afirmou que, «embora o [RGPD] precise, no seu artigo 2.º, n.º 2, alínea d), que não é aplicável aos tratamentos efetuados “pelas autoridades competentes” para fins, nomeadamente, de prevenção e de deteção de infrações penais, incluindo a salvaguarda e a

²⁵ C-317/04 e C-318/04, a seguir «Acórdão Parlamento/Conselho», EU:C:2006:346. Nos processos que deram origem a esse acórdão, o Parlamento tinha pedido, por um lado, a anulação da Decisão 2004/496/CE do Conselho, de 17 de maio de 2004, relativa à celebração de um acordo entre a Comunidade Europeia e os Estados Unidos da América sobre o tratamento e a transferência de dados contidos nos registos de identificação dos passageiros (PNR) por parte das transportadoras aéreas para o Serviço das Alfândegas e Proteção das Fronteiras do Departamento de Segurança Interna dos Estados Unidos (JO 2004, L 183, p. 83, e retificação JO 2005, L 255, p. 168) e, por outro, a anulação da Decisão 2004/535/CE da Comissão, de 14 de maio de 2004, sobre o nível de proteção adequado dos dados pessoais contidos nos Passenger Name Record transferidos para o Bureau of Customs and Border Protection dos Estados Unidos (JO 2004, L 235, p. 11).

²⁶ Nos termos do artigo 3.º, n.º 2, primeiro travessão, da Diretiva 95/46, esta diretiva não se aplicava ao tratamento de dados pessoais «efetuado no exercício de atividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objeto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as atividades do Estado no domínio do direito penal» (sublinhado meu).

²⁷ Quanto à «abordagem teleológica» e «contextual» do Tribunal de Justiça no Acórdão Parlamento/Conselho, v. Conclusões do advogado-geral M. Campos Sánchez-Bordona nos processos apensos La Quadrature du Net e o. (C-511/18 e C-512/18, EU:C:2020:6, n.ºs 47 e 62).

²⁸ C-511/18, C-512/18 e C-520/18, a seguir «Acórdão La Quadrature du Net», EU:C:2020:791.

²⁹ V. Acórdão La Quadrature du Net, n.ºs 100 a 102.

³⁰ V., no mesmo sentido, Acórdão Privacy International, n.º 47.

³¹ C-207/16, a seguir «Acórdão Ministerio Fiscal», EU:C:2018:788, n.º 34.

prevenção de ameaças à segurança pública, resulta do artigo 23.º, n.º 1, alíneas d) e h), do mesmo regulamento que os tratamentos de dados pessoais efetuados para esses mesmos fins por particulares estão abrangidos pelo seu âmbito de aplicação»³².

52. Pelas razões já expostas, estou convencido de que a conclusão de que a transferência dos dados PNR pelas empresas de transporte e pelos operadores de viagens para as UIP está abrangida pelo RGPD resulta já claramente da redação do artigo 2.º, n.º 2, alínea d), do RGPD, que se refere apenas aos tratamentos efetuados pelas «autoridades competentes», sem que seja necessário fazer referência à cláusula de limitação contida no artigo 23.º, n.º 1, do referido regulamento³³. No entanto, a afirmação contida no n.º 102 do Acórdão *La Quadrature du Net* constitui uma clara tomada de posição do Tribunal de Justiça a favor de tal conclusão.

53. Uma vez que a transferência dos dados PNR por empresas de transporte e operadores de viagens é abrangida pelo âmbito de aplicação do RGPD, uma legislação nacional, como a Lei PNR, que obriga essas empresas e esses operadores a proceder a tal transferência, constitui uma «medida legislativa» nos termos do artigo 23.º, n.º 1, alínea d), do RGPD e deve, portanto, preencher os requisitos previstos nesta disposição³⁴.

54. No que respeita, em terceiro lugar, aos tratamentos dos dados PNR efetuados *pela UIP e pelas autoridades nacionais competentes*, a aplicabilidade do RGPD depende, como resulta dos desenvolvimentos precedentes, das finalidades prosseguidas por esses tratamentos.

55. Assim, em primeiro lugar, os tratamentos de dados PNR efetuados pela UIP e pelas autoridades nacionais competentes para as finalidades enumeradas no artigo 8.º, § 1, pontos 1 a 3 e 5, da Lei PNR³⁵, estão excluídos do âmbito de aplicação do RGPD na medida em que, como parece ser o caso, as referidas finalidades se enquadram entre as abrangidas pela cláusula de exclusão inscrita no artigo 2.º, n.º 2, alínea d), do RGPD. A proteção dos dados das pessoas afetadas por esses tratamentos é abrangida pelo direito nacional, sem prejuízo da aplicação da Diretiva Cooperação Policial³⁶ e, no quadro do seu âmbito de aplicação, da Diretiva PNR.

56. O mesmo se aplica, em segundo lugar, aos tratamentos dos dados PNR efetuados pela UIP e pelos serviços de segurança e de informações no âmbito do acompanhamento das atividades previstas nas disposições da Lei Orgânica dos Serviços de Informações e de Segurança enumeradas no artigo 8.º, § 1, ponto 4, da Lei PNR, na medida em que correspondam às finalidades enunciadas no artigo 2.º, n.º 2, alínea d), do RGPD, o que cabe ao órgão jurisdicional de reenvio apreciar.

³² V., por analogia, Acórdãos *Tele2 Sverige*, n.ºs 72 a 74, e *Ministerio fiscal*, n.º 34. Esses acórdãos tinham por objeto a interpretação do artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO 2002, L 201, p. 37), que prevê uma cláusula de limitação análoga à contida no artigo 23.º, n.º 1, alíneas a) a d), do RGPD.

³³ Uma referência ao artigo 15.º, n.º 1, da Diretiva 2002/58 era justificada no contexto desta diretiva, tendo em conta a redação da cláusula de exclusão prevista no seu artigo 1.º, n.º 3, que se refere, de maneira geral, às «atividades do Estado em matéria de direito penal».

³⁴ V., por analogia, Acórdão *Privacy International*, n.ºs 38 e 39.

³⁵ São os tratamentos regidos pelos capítulos 7 a 10 e 12 da Lei PNR.

³⁶ V., neste sentido, Acórdãos *La Quadrature du Net*, n.º 103, e *Privacy International*, n.º 48.

57. O Governo belga sustenta que os tratamentos efetuados nos termos do artigo 8.º, § 1, ponto 4, da Lei PNR estão, em qualquer caso, abrangidos pela cláusula de exclusão prevista no artigo 2.º, n.º 2, alínea a), do RGPD, bem como pela prevista no artigo 2.º, n.º 3, alínea a), da Diretiva Cooperação Policial, uma vez que as atividades dos serviços de segurança e de informações não estão abrangidas pelo âmbito de aplicação do direito da União.

58. A este respeito, embora sublinhando que não foi submetida ao Tribunal de Justiça uma questão relativa à interpretação destas disposições, observo, antes de mais, que o Tribunal de Justiça já afirmou que uma regulamentação nacional que impõe obrigações de tratamento a operadores privados está abrangida pelas disposições do direito da União em matéria de proteção de dados pessoais, mesmo quando visa a proteção da segurança nacional³⁷. Daqui resulta que a transferência dos dados PNR imposta pela Lei PNR às transportadoras e aos operadores de viagens está, em princípio, abrangida pelo RGPD, mesmo quando é efetuada para os fins do artigo 8.º, § 1, ponto 4, desta lei.

59. Seguidamente, observo que, embora o considerando 16 do RGPD enuncie que este não se aplica às «atividades [...] que se prendem com a segurança nacional» e o considerando 14 da Diretiva Cooperação Policial precise que «não deverão ser consideradas atividades abrangidas [por esta] diretiva as atividades relacionadas com a segurança nacional e as atividades das agências ou unidades que se dedicam a questões de segurança nacional [...]», os critérios com base nos quais um tratamento de dados pessoais efetuado por uma autoridade, um serviço público ou uma agência pública de um Estado-Membro é abrangido pelo âmbito de aplicação de um dos atos do direito da União que organizam a proteção das pessoas em causa relativamente a tais tratamentos, ou se situa fora do âmbito de aplicação deste direito, obedecem a uma lógica associada tanto às funções atribuídas a essa autoridade, a esse serviço ou essa agência como às finalidades do referido tratamento. Assim, o Tribunal de Justiça declarou que o artigo 2.º, n.º 2, alínea a), do RGPD, lido à luz do considerando 16 deste regulamento «tem por único objetivo excluir do âmbito de aplicação do referido regulamento os tratamentos de dados pessoais efetuados pelas autoridades estatais no âmbito de uma atividade que visa preservar a segurança nacional ou de uma atividade que pode ser classificada na mesma categoria, pelo que o simples facto de uma atividade ser própria do Estado ou de uma autoridade pública não é suficiente para que essa exceção seja automaticamente aplicável a tal atividade»³⁸. O Tribunal de Justiça precisou igualmente que «[a]s atividades que têm por finalidade preservar a segurança nacional, referidas no artigo 2.º, n.º 2, alínea a), do RGPD, abrangem em especial [...] as que têm por objeto proteger as funções essenciais do Estado e os interesses fundamentais da sociedade»³⁹. Daqui resulta que, no caso de um Estado-Membro encarregar os seus serviços de segurança e de informações de missões nos domínios enumerados no artigo 3.º, ponto 7, alínea a), da Diretiva Cooperação Policial, os tratamentos de dados efetuados por estes serviços para o cumprimento dessas missões estariam abrangidos pelo âmbito de aplicação desta diretiva bem como, sendo caso disso, da Diretiva PNR. Mais genericamente, observo que o Tribunal de Justiça declarou reiteradamente, no âmbito da interpretação do artigo 4.º, n.º 2, TUE, no qual se apoia, nomeadamente, o Governo belga, que o simples facto de uma medida nacional ter sido adotada para efeitos da proteção da segurança nacional não pode implicar a inaplicabilidade do direito da União e dispensar os Estados-Membros do respeito necessário desse direito⁴⁰, mostrando-se assim reticente a uma exclusão automática e em bloco do âmbito de aplicação do direito da União das atividades dos Estados-Membros relacionadas com a proteção da segurança nacional.

³⁷ V., nomeadamente, Acórdão La Quadrature du Net.

³⁸ V. Acórdão de 22 de junho de 2021, *Latvijas Republikas Saeima* (Pontos de penalização) (C-439/19, EU:C:2021:504, n.º 66).

³⁹ V. Acórdão de 22 de junho de 2021, *Latvijas Republikas Saeima* (Pontos de penalização) (C-439/19, EU:C:2021:504).

⁴⁰ V. Acórdão *La Quadrature du Net*, n.º 99 e jurisprudência referida.

60. Em terceiro lugar, em conformidade com a opinião de todos os interessados que apresentaram observações, com exceção do Governo francês, há que considerar que os tratamentos dos dados PNR efetuados pelas autoridades competentes belgas para as finalidades enunciadas no artigo 8.º, § 2, da Lei PNR, a saber, «melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal»⁴¹ não estão abrangidos pela cláusula de exclusão contida no artigo 2.º, n.º 2, alínea d), do RGPD, nem por outra causa de exclusão prevista nesse artigo e estão, por conseguinte, abrangidos pelo âmbito de aplicação deste regulamento. Contrariamente ao que sustenta o Governo francês, os referidos tratamentos não podem ser regidos pela Diretiva PNR, cujo artigo 1.º, n.º 2, prevê que «[o]s dados PNR recolhidos nos termos da presente diretiva só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave» nem, em princípio, pela Diretiva Cooperação Policial que, em conformidade com o seu artigo 1.º, n.º 1, se aplica apenas aos tratamentos de dados pessoais pelas autoridades competentes «para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública». Como resulta da decisão de reenvio, o artigo 8.º, § 2, da Lei PNR e o capítulo 11 desta lei, que contém as disposições que regem o tratamento dos dados PNR com vista a melhorar o controlo nas fronteiras e combater a imigração ilegal, e que prevê, para esse efeito, a transferência destes dados pela UIP, nomeadamente para os serviços policiais responsáveis pelo controlo das fronteiras, visam transpor para o direito belga a Diretiva API e a Diretiva 2010/65. Ora, estas duas diretivas impõem às autoridades competentes, quanto aos tratamentos que preveem, o respeito das disposições da Diretiva 95/46⁴². Ao contrário do que sustenta o Governo francês, a remissão para as regras de proteção desta diretiva deve ser entendida no sentido de abranger qualquer tratamento de dados pessoais efetuado com base na Diretiva API e na Diretiva 2010/65. O facto de a Diretiva API ser anterior à entrada em vigor da Decisão-Quadro 2008/977 não é pertinente a este respeito, uma vez que esta decisão-quadro, bem como a Diretiva Cooperação Policial que a substituiu, apenas dizem respeito aos tratamentos de dados pessoais previstos no artigo 3.º, n.º 1, da Diretiva API, efetuados pelas autoridades competentes para efeitos de aplicação da lei⁴³.

61. Com base em todas as considerações precedentes, proponho ao Tribunal de Justiça que responda à primeira questão prejudicial que o artigo 23.º do RGPD, em conjugação com o artigo 2.º, n.º 2, alínea d), deste regulamento, deve ser interpretado no sentido de que:

- é aplicável a uma legislação nacional que transpõe a Diretiva PNR, na medida em que essa legislação regule os tratamentos dos dados PNR efetuados pelas transportadoras e por outros operadores económicos, incluindo a transferência de dados PNR para as UIP, prevista no artigo 8.º da referida diretiva;
- não é aplicável a uma legislação nacional que transpõe a Diretiva PNR, na medida em que regule os tratamentos de dados efetuados, para as finalidades previstas no artigo 1.º, n.º 2, desta diretiva, pelas autoridades competentes, incluindo as UIP e, se for caso disso, os serviços de segurança e de informações do Estado-Membro em causa;
- é aplicável a uma legislação nacional que transpõe a Diretiva API e a Diretiva 2010/65 com vista a melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal.

⁴¹ As condições que rodeiam esses tratamentos de dados estão previstas no capítulo 11 da Lei PNR.

⁴² V. considerandos 8, 9 e 12, e artigo 6.º da Diretiva API e artigo 8.º, n.º 2, da Diretiva 2010/65.

⁴³ A utilização das informações prévias sobre os passageiros (a seguir «dados API») por serviços responsáveis pela aplicação da lei está expressamente prevista no artigo 6.º, n.º 1, último parágrafo, da Diretiva API.

B. Quanto às segunda, terceira, quarta, sexta e oitava questões prejudiciais

62. Com as segunda, terceira, quarta e sexta questões prejudiciais, a Cour constitutionnelle (Tribunal Constitucional, Bélgica) interroga o Tribunal de Justiça sobre a validade da Diretiva PNR à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta. A oitava questão prejudicial, embora redigida como uma questão de interpretação, pretende também, em substância, que o Tribunal de Justiça se pronuncie sobre a validade desta diretiva.

63. Estas questões dizem respeito aos diferentes elementos do sistema de tratamento dos dados PNR estabelecido pela Diretiva PNR e pedem, relativamente a cada um desses elementos, uma avaliação do cumprimento dos requisitos a que está sujeita a legalidade das restrições impostas ao exercício dos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta. Assim, a segunda e a terceira questão prejudicial respeitam à lista dos dados PNR que figura no anexo I, a quarta diz respeito à definição do conceito de «passageiro» que figura no artigo 3.º, ponto 4, da Diretiva PNR, a sexta diz respeito à utilização dos dados PNR para efeitos da avaliação prévia nos termos do artigo 6.º desta diretiva e a oitava diz respeito ao prazo de conservação dos dados PNR previsto no artigo 12.º, n.º 1, da referida Diretiva.

1. Quanto aos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta

64. O artigo 7.º da Carta garante a todas as pessoas o direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Quanto ao artigo 8.º, n.º 1, da Carta, este reconhece expressamente a todas as pessoas o direito à proteção dos dados de caráter pessoal que lhes digam respeito. Segundo jurisprudência constante, estes direitos, que dizem respeito a todas as informações relativas a uma pessoa singular identificada ou identificável, estão estreitamente ligados, uma vez que o acesso a dados pessoais de uma pessoa singular, com vista à sua conservação ou à sua utilização, afeta o direito dessa pessoa ao respeito pela vida privada⁴⁴.

65. Os direitos consagrados nos artigos 7.º e 8.º da Carta não são, contudo, prerrogativas absolutas, mas devem ser tomados em consideração de acordo com a sua função na sociedade⁴⁵. Assim, o artigo 8.º, n.º 2, da Carta autoriza o tratamento de dados de caráter pessoal se estiverem preenchidos determinados requisitos. Esta disposição prevê que os dados de caráter pessoal devem ser objeto de um tratamento «leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei».

66. Qualquer restrição imposta ao direito à proteção de dados pessoais, bem como ao direito à vida privada, deve, além disso, respeitar o disposto no artigo 52.º, n.º 1, da Carta. Assim, tal restrição deve ser prevista por lei, respeitar o conteúdo essencial dos referidos direitos e, na observância do princípio da proporcionalidade, ser necessária e corresponder efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

⁴⁴ V., neste sentido, nomeadamente, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems (C-311/18, EU:C:2020:559, n.º 170 e jurisprudência referida).

⁴⁵ V., nomeadamente, Acórdão de 16 de julho de 2020, Facebook Ireland e Schrems (C-311/18, EU:C:2020:559, n.º 172 e jurisprudência referida).

67. A apreciação de uma medida que limite os referidos direitos deve ter igualmente em conta a importância dos direitos consagrados nos artigos 3.º, 4.º, 6.º e 7.º da Carta e a importância dos objetivos de proteção da segurança nacional e de luta contra a criminalidade grave, contribuindo para a proteção dos direitos e liberdades de terceiros⁴⁶. A este respeito, o artigo 6.º da Carta consagra o direito de qualquer pessoa não apenas à liberdade mas também à segurança⁴⁷.

68. Por outro lado, o artigo 52.º, n.º 3, da Carta visa assegurar a coerência necessária entre os direitos contidos nesta última e os direitos correspondentes garantidos pela CEDH, que devem ser tidos em conta enquanto limiar de proteção mínima⁴⁸. O direito ao respeito pela vida privada e familiar, consagrado no artigo 7.º da Carta, corresponde ao direito garantido no artigo 8.º da CEDH e deve, por conseguinte, ser-lhe reconhecido o mesmo sentido e alcance⁴⁹. Decorre da jurisprudência do Tribunal Europeu dos Direitos do Homem (a seguir «TEDH») que uma ingerência nos direitos garantidos neste artigo só pode ser justificada à luz do n.º 2 do referido artigo se for prevista por lei, visar um ou mais dos fins legítimos enumerados neste número e for necessária, numa sociedade democrática, para atingir esse ou esses fins⁵⁰. A medida deve igualmente ser compatível com o primado do direito, expressamente mencionado no preâmbulo da CEDH, e inerente ao objeto e fim do artigo 8.º desta⁵¹.

69. É à luz destes princípios que há que examinar as questões de apreciação da validade submetidas pela Cour constitutionnelle (Tribunal Constitucional, Bélgica).

2. Quanto à ingerência nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta

70. O Tribunal de Justiça já declarou que disposições que impõem ou permitem a comunicação de dados pessoais de pessoas singulares a terceiros, como uma autoridade pública, devem, na falta de consentimento dessas pessoas singulares e independentemente da utilização posterior dos dados em causa, ser qualificadas de ingerências na sua vida privada e, por conseguinte, de restrições ao direito fundamental garantido no artigo 7.º da Carta, sem prejuízo da sua eventual justificação⁵². Assim é, mesmo na falta de circunstâncias que permitam qualificar tal ingerência de «grave» e sem que seja relevante que as informações relativas à vida privada em questão sejam ou não sensíveis, ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência⁵³. O acesso das autoridades públicas a tais informações constitui igualmente uma ingerência no direito fundamental à proteção dos dados pessoais, garantido pelo

⁴⁶ V., neste sentido, Acórdão La Quadrature du Net, n.º 122.

⁴⁷ V. Acórdão La Quadrature du Net, n.º 123.

⁴⁸ V. Acórdão La Quadrature du Net, n.º 124 e jurisprudência referida.

⁴⁹ V. Acórdão de 18 de junho de 2020, Comissão/Hungria (Transparência associativa) (C-78/18, EU:C:2020:476, n.º 122 e jurisprudência referida).

⁵⁰ V., nomeadamente, TEDH, 4 de dezembro de 2015, Roman Zakharov c. Rússia (CE:ECHR:2015:1204JUD004714306, § 227); TEDH, 18 de maio de 2010, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905, § 130), e TEDH, 25 de maio de 2021, Centrum för Rättvisa c. Suécia (CE:ECHR:2021:0525JUD003525208, § 246).

⁵¹ V. TEDH, 4 de dezembro de 2015, Roman Zakharov c. Rússia (CE:ECHR:2015:1204JUD004714306, § 228); TEDH, 4 de maio de 2000, Rotaru c. Roménia (CE:ECHR:2000:0504JUD002834195, § 52); TEDH, 4 de dezembro de 2008, S. e Marper c. Reino Unido (CE:ECHR:2008:1204JUD003056204, § 95); TEDH, 18 de maio de 2021, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905, § 151), e TEDH, 25 de maio de 2021, Centrum för Rättvisa c. Suécia (CE:ECHR:2021:0525JUD003525208, § 246).

⁵² V., entre outros, Acórdão de 18 de junho de 2020, Comissão/Hungria (C-78/18, ECLI:EU:C:2020:476, n.ºs 124 e 126, bem como jurisprudência referida); v., igualmente, TEDH, 4 de maio de 2000, Rotaru c. Roménia (CE:ECHR:2000:0504JUD002834195, § 48); TEDH, 26 de março de 1987, Leander c. Suécia (CE:ECHR:1987:0326JUD000924881, § 46), e TEDH, 29 de junho de 2006, Weber e Saravia c. Alemanha (CE:ECHR:2006:0629DEC005493400, § 79).

⁵³ V., entre outros, Acórdão Ministerio Fiscal, n.º 51 e jurisprudência referida.

artigo 8.º da Carta, uma vez que constitui um tratamento de dados pessoais⁵⁴. De igual modo, a conservação, durante um determinado período, dos dados relativos à vida privada de uma pessoa constitui, em si mesma, uma ingerência nos direitos garantidos pelos artigos 7.º e 8.º da Carta⁵⁵.

71. O Tribunal de Justiça já declarou também que os dados PNR, como os enumerados no anexo I, incluem informações sobre pessoas singulares identificadas, a saber, os passageiros aéreos em causa, e que, por conseguinte, os diferentes tratamentos de que estes podem ser objeto afetam o direito fundamental ao respeito pela vida privada, garantido no artigo 7.º da Carta. Estes tratamentos estão igualmente abrangidos pelo artigo 8.º da Carta e devem, assim, necessariamente, respeitar os requisitos da proteção de dados previstos neste artigo⁵⁶.

72. Assim, os tratamentos dos dados PNR que a Diretiva PNR permite, nomeadamente, na medida em que é relevante para efeitos do presente processo, a transferência desses dados pelas transportadoras aéreas para as UIP, a sua utilização por estas unidades, a sua posterior transferência para autoridades nacionais competentes na aceção do artigo 7.º desta diretiva, bem como a sua conservação, constituem igualmente ingerências nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta.

73. No que respeita à gravidade destas ingerências, há que observar, em primeiro lugar, que a Diretiva PNR prevê a transferência *sistemática e contínua* para as UIP dos dados PNR de qualquer passageiro aéreo, conforme definido no artigo 3.º, ponto 4, desta diretiva, que viaje num voo «extra-UE», na aceção do artigo 3.º, n.º 2, da mesma. Tal transferência implica um acesso geral por parte das UIP a todos os dados PNR fornecidos⁵⁷. Ao contrário do que alegam certos Estados-Membros no presente processo, esta conclusão não é colocada em causa pela circunstância de os dados serem sujeitos a um tratamento automatizado, pelo que as UIP só terão concretamente acesso aos dados cuja análise tenha gerado um resultado positivo. Com efeito, por um lado, essa circunstância não impediu, até à data, o Tribunal de Justiça de afirmar, no âmbito de sistemas semelhantes de tratamento automatizado de dados pessoais recolhidos ou conservados «a granel», o caráter geral do acesso das autoridades públicas em causa a esses dados. Por outro lado, a simples colocação à disposição das autoridades públicas de dados pessoais com vista ao seu tratamento e à sua conservação por essas autoridades comporta um acesso *a priori* geral e completo dessas autoridades a tais dados e uma ingerência nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais.

74. Em segundo lugar, em conformidade com o artigo 2.º, n.º 1, da Diretiva PNR, os Estados-Membros podem decidir aplicar esta diretiva aos voos «intra-UE», na aceção do artigo 3.º, ponto 3, da mesma. A este respeito, observo, por um lado, que a Diretiva PNR não se limita a prever a faculdade dos Estados-Membros de alargarem a sua aplicação aos voos intra-UE, mas determina igualmente os requisitos, tanto formais como materiais, que regem o exercício desta faculdade⁵⁸ e precisa que, quando a mesma é exercida apenas quanto a voos intra-UE selecionados, a seleção desses voos deve ser efetuada tendo em conta os objetivos prosseguidos pela referida diretiva⁵⁹. Por outro lado, a Diretiva PNR estabelece as consequências do exercício

⁵⁴ V., entre outros, Acórdão de 18 de junho de 2020, Comissão/Hungria (C-78/18, EU:C:2020:476, n.º 126), bem como Acórdão Ministério Fiscal, n.º 51 e jurisprudência referida.

⁵⁵ V. Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, a seguir «Acórdão Digital Rights», EU:C:2014:238, n.º 34).

⁵⁶ V. Parecer 1/15, n.ºs 121 a 123.

⁵⁷ V., por analogia, Acórdão Privacy Internacional, n.ºs 79 e 80 bem como jurisprudência referida.

⁵⁸ V. artigo 2.º, n.ºs 1 a 3, da Diretiva PNR.

⁵⁹ V. artigo 2.º, n.º 3, da Diretiva PNR.

dessa faculdade, prevendo, no seu artigo 2.º, n.º 2, que, quando um Estado-Membro decide aplicar esta diretiva aos voos intra-UE, todas as disposições da mesma «são aplicáveis aos voos intra-UE como se se tratasse de voos extra-UE e aos dados PNR respeitantes aos voos intra-UE como se se tratassem de dados referentes a voos extra-UE».

75. Nestas circunstâncias, sou da opinião, contrariamente ao que alegaram alguns governos que apresentaram observações no presente processo, que, embora a aplicação da Diretiva PNR aos voos intra-UE dependa da opção dos Estados-Membros, a base legal das ingerências nos direitos ao respeito pela vida privada e à proteção dos dados pessoais associados à transferência, ao tratamento e à conservação dos dados PNR relativos a esses voos é constituída, quando essa opção é exercida, pela Diretiva PNR.

76. Ora, com exceção do Reino da Dinamarca, que não está sujeito a esta diretiva⁶⁰, quase todos os Estados-Membros aplicam o regime por ela estabelecido aos voos «intra-UE»⁶¹. Daqui decorre que este regime se aplica a todos os voos que entram e saem da União, bem como a praticamente todos os voos operados dentro da União.

77. Em terceiro lugar, no que respeita aos dados PNR a transferir, o anexo I enumera 19 rubricas, respeitantes aos dados biográficos⁶², aos pormenores da viagem aérea⁶³ e a outros dados recolhidos no contexto do contrato de transporte aéreo, como o número de telefone, o endereço eletrónico, os meios de pagamento, a agência ou o agente de viagens, as informações relativas às bagagens bem como observações gerais⁶⁴. Ora, como o Tribunal de Justiça indicou no n.º 128 do Parecer 1/15, ao pronunciar-se sobre as rubricas que figuram no anexo I do Projeto de Acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros (a seguir «Projeto de Acordo PNR Canadá-UE»), formuladas em grande medida em termos análogos aos do anexo I, «ainda que certos dados PNR, considerados isoladamente, não pareçam suscetíveis de revelar informações importantes sobre a vida privada das pessoas em causa, não deixa de ser verdade que, considerados conjuntamente, os referidos dados podem revelar, entre outros, um itinerário de viagem completo, hábitos de viagem, relações existentes entre duas ou mais pessoas e informações sobre a situação financeira dos passageiros aéreos, os seus hábitos alimentares ou o seu estado de saúde, podendo até fornecer informações sensíveis sobre esses passageiros».

⁶⁰ Nos termos dos artigos 1.º e 2.º do Protocolo (n.º 22) relativo à posição da Dinamarca, uma vez que este Estado-Membro não participa na adoção da Diretiva PNR, não fica a ela vinculado nem sujeito à sua aplicação (v. considerando 40 desta diretiva). Resulta, no entanto, das observações escritas apresentadas pelo Governo dinamarquês que o Reino da Dinamarca adotou, em 2018, uma lei relativa à recolha, à utilização e à conservação dos dados PNR, cujas disposições correspondem em grande medida às da Diretiva PNR. Quanto à Irlanda, resulta do considerando 39 da Diretiva PNR que este Estado-Membro, nos termos do artigo 3.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, notificou a sua intenção de participar na adoção e na aplicação desta diretiva.

⁶¹ A Comissão publicou uma lista atualizada dos Estados-Membros que decidiram aplicar a Diretiva PNR aos voos intra-UE conforme referido no artigo 2.º da Diretiva [PNR] (JO 2020, C 358, p. 7), retificada em setembro de 2021 com a inclusão da Eslovénia e a supressão da referência ao Reino Unido (JO 2021, C 360, p. 8). A Irlanda e a Áustria não figuram nesta lista. O Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre o reexame da Diretiva [PNR], de 24 de julho de 2020, [COM(2020)305 final, p. 11 (a seguir «Relatório da Comissão de 2020»)] menciona que todos os Estados-Membros, exceto um, alargaram a recolha de dados PNR aos voos intra-UE.

⁶² V., nomeadamente, pontos 4) e 18) do anexo I relativos aos nomes, ao sexo, à data de nascimento, à nacionalidade e aos documentos de identidade do passageiro.

⁶³ V., nomeadamente, pontos 2), 3), 7), 13) e 18) do anexo I da Diretiva PNR que mencionam, designadamente, o número de voo, os aeroportos de partida e de chegada, bem como as datas e horas de partida e de chegada.

⁶⁴ V. pontos 5), 6), 9), 12) e 16) do anexo I.

78. Em quarto lugar, nos termos do artigo 6.º da Diretiva PNR, os dados transferidos pelas transportadoras aéreas destinam-se a ser analisados pelas UIP por meios automatizados e *de modo sistemático*, ou seja, independentemente da questão de saber se existe a menor indicação de que as pessoas em causa podem estar implicadas em infrações de terrorismo ou em formas de criminalidade grave. Mais especificamente, no âmbito da avaliação prévia dos passageiros prevista no artigo 6.º, n.º 2, alínea a), desta diretiva, e em conformidade com o n.º 3 deste artigo, os referidos dados podem ser verificados por cruzamento com as bases de dados «relevantes» [artigo 6.º, n.º 3, alínea a)] e tratados de acordo com critérios preestabelecidos [artigo 6.º, n.º 3, alínea b)]. Ora, o primeiro tipo de tratamento é suscetível de fornecer informações adicionais sobre a vida privada das pessoas em causa⁶⁵ e, em função das bases de dados utilizadas para o cruzamento, pode até permitir traçar um *perfil preciso* dessas pessoas. Nestas circunstâncias, a objeção levantada por vários governos, segundo a qual a Diretiva PNR só permite o acesso a um conjunto de dados pessoais relativamente limitado, não reflete adequadamente a extensão potencial das ingerências que esta diretiva comporta nos direitos fundamentais protegidos pelos artigos 7.º e 8.º da Carta, do ponto de vista da extensão dos dados a que é suscetível de permitir o acesso. No que respeita ao segundo tipo de tratamento de dados, previsto no artigo 6.º, n.º 3, alínea b), da Diretiva PNR, recorro que, nos n.ºs 169 e 172 do Parecer 1/15, o Tribunal de Justiça sublinhou que é inerente a qualquer tipo de análise baseada em critérios preestabelecidos que apresente uma certa taxa de erro, nomeadamente um certo número de resultados «falsos positivos». Segundo os dados quantificados contidos no documento de trabalho dos serviços da Comissão⁶⁶ (a seguir «Documento de trabalho de 2020») anexo ao Relatório da Comissão de 2020, o número de casos de resultados positivos que, na sequência da verificação individual prevista no artigo 6.º, n.º 5, da Diretiva PNR, se revelaram errados é bastante significativo e ascendia, durante os anos de 2018 e 2019, a pelo menos cinco de seis pessoas identificadas⁶⁷.

79. Em quinto lugar, nos termos do artigo 12.º, n.º 1, da Diretiva PNR, os dados PNR são conservados numa base de dados por um prazo de cinco anos contados a partir da sua transferência para a UIP do Estado-Membro em cujo território o voo aterre ou de cujo território descole. A Diretiva PNR permite, portanto, dispor de informações sobre a vida privada dos passageiros aéreos durante um período particularmente longo⁶⁸. Por outro lado, uma vez que a transferência dos dados PNR diz respeito à quase totalidade dos voos operados com partida e chegada na União e no interior desta, e que o avião se tornou um meio de transporte bastante comum, uma parte significativa de passageiros aéreos poderia ter os seus dados pessoais conservados de modo praticamente permanente, pelo simples facto de se deslocarem de avião pelo menos duas vezes de cinco em cinco anos.

80. Por último, mais genericamente, a Diretiva PNR prevê medidas que, consideradas globalmente, visam estabelecer, ao nível da União, um sistema de vigilância «não direcionada», a saber, que não é ativada em função de uma suspeita que incida sobre uma ou várias pessoas específicas, «maciça», ao ser exercida sobre dados pessoais de um grande número de pessoas⁶⁹, abrangendo a totalidade de uma mesma categoria de pessoas⁷⁰ e «pró-ativa», na medida em que

⁶⁵ V., neste sentido, Parecer 1/15, n.º 131.

⁶⁶ SWD(2020)128 final.

⁶⁷ O Documento de trabalho de 2020 (p. 28 e nota de rodapé 55) menciona uma taxa de resultados positivos de 0,59 % quanto ao ano de 2019, dos quais apenas 0,11 % foram objeto de transferência para as autoridades competentes. Quanto ao ano de 2018, as percentagens correspondentes eram, respetivamente, de 0,25 % e de 0,04 %.

⁶⁸ V. Parecer 1/15, n.º 132.

⁶⁹ O sistema estabelecido pela Diretiva PNR era suscetível de abranger, antes da crise sanitária, até mil milhões de passageiros por ano, dados acessíveis em <https://ec.europa.eu/eurostat/databrowser/view/ttr00012/default/table?lang=fr>.

⁷⁰ A saber, qualquer pessoa que corresponda ao conceito de «passageiro», conforme definido no artigo 3.º, ponto 4, da Diretiva PNR e que viaje num «voo extra-UE», bem como, de facto, num «voo intra-UE».

visa investigar não só ameaças conhecidas, como também encontrar ou identificar perigos até então desconhecidos⁷¹. Tais medidas dão origem, pela sua própria natureza, a ingerências graves nos direitos fundamentais protegidos pelos artigos 7.º e 8.º da Carta⁷², associadas, nomeadamente, à sua finalidade preventiva e preditiva, que exige a avaliação de dados pessoais relativos a grandes segmentos da população, com o objetivo de «identificar» as pessoas que, em função dos resultados dessa avaliação, devem ser sujeitas a um controlo mais minucioso por parte das autoridades competentes⁷³. Por outro lado, o recurso cada vez mais generalizado, para fins de prevenção da criminalidade grave, ao tratamento de grandes quantidades de dados pessoais de diversa natureza recolhidos «a granel», bem como a sua correlação e o seu tratamento conjugado, geram um «efeito cumulativo» que amplia a gravidade das restrições aos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, com o risco de favorecer um processo de deslizamento gradual para uma «sociedade de vigilância»⁷⁴.

81. Com base em todas as considerações precedentes, considero que a ingerência que a Diretiva PNR comporta nos direitos fundamentais protegidos pelos artigos 7.º e 8.º da Carta deve, pelo menos, ser qualificada de «grave».

82. É verdade que, como sustenta, em especial, a Comissão, o conjunto de garantias e salvaguardas que a Diretiva PNR prevê, nomeadamente para evitar uma utilização abusiva dos dados PNR, é suscetível de reduzir a intensidade ou a gravidade dessas ingerências. Mas não é menos verdade que qualquer regime que preveja o acesso e o tratamento de dados pessoais por parte de autoridades públicas apresenta um nível de gravidade, do ponto de vista da proteção dos direitos fundamentais afetados, que é inerente às suas características objetivas. Este nível de gravidade deve, na minha opinião, ser determinado antes de se proceder, no âmbito da apreciação da proporcionalidade das referidas ingerências, à avaliação do caráter suficiente e adequado das garantias que este regime prevê. Parece-me que é assim que o Tribunal de Justiça tem procedido até à data.

83. Para serem compatíveis com a Carta, as ingerências que a Diretiva PNR comporta nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais devem satisfazer os requisitos enunciados nos n.ºs 65 e 66 das presentes conclusões, o que será examinado seguidamente, dentro dos limites dos aspetos que foram submetidos à apreciação do Tribunal de Justiça pelo órgão jurisdicional de reenvio.

⁷¹ Num estudo adotado pela Comissão Europeia para a Democracia através do Direito (Comissão de Veneza) em 2015, considera-se que tais medidas são abrangidas pelo conceito de «vigilância estratégica» e seguem uma «tendência geral» para recorrer a uma «vigilância proativa» da população; v. o estudo *Mise à jour du rapport de 2007 sur le contrôle démocratique des services de sécurité et rapport sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique*, adotado pela Comissão de Veneza na sua 102.ª sessão plenária (Veneza, 20 e 21 de março de 2015), [https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD\(2015\)006-f](https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)006-f), ponto 61.

⁷² No que respeita ao artigo 8.º da CEDH, v. Acórdão TEDH, 25 de maio de 2021, *Big Brother Watch e o. c. Reino Unido* (CE:ECHR:2021:0525JUD005817013, § 325, a seguir «Acórdão Big Brother Watch») relativo às medidas de interceção em massa, em que o TEDH afirma que a intensidade da ingerência dessas medidas no exercício do direito ao respeito pela vida privada aumenta à medida que são ultrapassadas as diferentes etapas do processo, a saber, a interceção e a conservação inicial das comunicações e dos dados associados, o tratamento automatizado através da aplicação de seletores, o exame por analistas e a subsequente conservação dos dados bem como a utilização do «produto final».

⁷³ V., neste sentido, considerando 6 e 7 da Diretiva PNR; para uma análise aprofundada da finalidade e das implicações para a proteção da vida privada e dos dados pessoais, v. relatório intitulado *Passenger Name Records (PNR), data mining and data protection: the need for strong safeguards*, elaborado por Korff, D., com o contributo de Georges, M., <https://rm.coe.int/16806a601b> (a seguir «Relatório Korff»).

⁷⁴ Como se indica no Relatório Korff, «PNR is not an isolated issue, but a new symptom of a much wider disease».

3. Quanto à justificação da ingerência resultante da Diretiva PNR

84. Enquanto a terceira questão prejudicial tem por objeto o cumprimento do requisito previsto no artigo 52.º, n.º 1, primeiro período, da Carta, segundo o qual qualquer ingerência num direito fundamental deve ser «prevista por lei», as segunda, quarta, sexta e oitava questões prejudiciais interrogam o Tribunal de Justiça, nomeadamente, sobre o respeito pelo princípio da proporcionalidade, referido no segundo período desta disposição.

a) Quanto ao cumprimento do requisito segundo o qual qualquer restrição ao exercício de um direito fundamental previsto na Carta deve ser previsto por lei

85. Segundo jurisprudência assente do Tribunal de Justiça⁷⁵, inspirada na jurisprudência do TEDH⁷⁶, o requisito segundo o qual qualquer restrição ao exercício de um direito fundamental deve ser «prevista por lei» não visa unicamente a origem «legal» da ingerência – que não está em causa no presente processo – mas implica também que a base legal que permite essa ingerência deve definir ela própria, de maneira *clara e precisa*, o alcance da mesma. Prendendo-se com a «qualidade da lei» e, portanto, com a acessibilidade e a previsibilidade da medida em causa⁷⁷, esta segunda vertente da expressão «prevista por lei», na aceção tanto do artigo 52.º, n.º 1, da Carta como do seu artigo 8.º, n.º 2, e do artigo 8.º da CEDH, não visa apenas assegurar o respeito pelo princípio da legalidade e uma proteção adequada contra a arbitrariedade⁷⁸, mas obedece igualmente a um imperativo de segurança jurídica. Este requisito é também afirmado no Parecer de 19 de agosto de 2016 do Comité Consultivo da Convenção 108⁷⁹ sobre as implicações, em matéria de proteção de dados, do tratamento dos dados dos passageiros (a seguir «Parecer de 19 de agosto de 2016»)⁸⁰.

86. Ao adotar a Diretiva PNR, o próprio legislador da União procedeu à limitação dos direitos consagrados nos artigos 7.º e 8.º da Carta. As ingerências que esta diretiva permite nos referidos direitos não podem, portanto, ser consideradas consequência da escolha dos Estados-Membros⁸¹, apesar da margem de apreciação de que estes últimos beneficiaram no momento da sua

⁷⁵ V., entre outros, Acórdãos de 16 de julho de 2020, Facebook Ireland e Schrems (C-311/18, EU:C:2020:559, n.º 175), de 8 de setembro de 2020, Recorded Artists Actors Performers (C-265/19, EU:C:2020:677, n.º 86 e jurisprudência referida), bem como Acórdão Privacy International, n.º 65.

⁷⁶ V., entre outros, Acórdãos do TEDH de 8 de junho de 2006, Lupsa c. Roménia (CE:ECHR:2006:0608JUD001033704, §§ 32 e 33), e de 15 de dezembro de 2020, Pişkin c. Turquia (CE:ECHR:2020:1215JUD003339918, § 206); v., igualmente, Acórdão Big Brother Watch, § 333. Quanto à necessidade de reconhecer à expressão «prevista por lei» no artigo 52.º, n.º 1, da Carta a mesma interpretação que a adotada pelo TEDH, v. Conclusões do advogado-geral M. Wathelet no processo WebMindLicenses (C-419/14, EU:C:2015:606, n.ºs 134 a 143).

⁷⁷ V., mais recentemente, Acórdão Big Brother Watch, § 333.

⁷⁸ V. Acórdão de 17 de dezembro de 2015, WebMindLicenses (C-419/14, EU:C:2015:832, n.º 81); v., igualmente, TEDH, 1 de julho de 2008, Liberty e o. c. Reino Unido (CE:ECHR:2008:0701JUD005824300, § 69), bem como Acórdão Big Brother Watch, § 333.

⁷⁹ Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, adotada em Estrasburgo, em 28 de janeiro de 1981, e ratificada por todos os Estados-Membros, mais conhecida por «Convenção 108». Em 2018, foi elaborado um protocolo de alteração desta convenção, com vista à sua modernização. Através da Decisão (UE) 2019/682 do Conselho, de 9 de abril de 2019 (JO 2019, L 115, p. 7), os Estados-Membros foram autorizados a assinar, no interesse da União, o referido protocolo de alteração na medida em que as suas disposições são da competência exclusiva da União. No seguimento das presentes conclusões, referir-me-ei igualmente ao texto da Convenção 108 modernizada, que, embora não tenha ainda sido ratificada por todos os Estados-Membros e ainda não tenha entrado em vigor, prevê, como resulta da Decisão 2019/682, garantias baseadas nos mesmos princípios que os referidos no RGPD e na Diretiva Cooperação Policial.

⁸⁰ <https://rm.coe.int/t-pd-2016-18rev-avis-pnr-fr/16807b6c09>, pp. 3 e 5. O relatório explicativo que acompanha o protocolo de alteração da Convenção 108 (a seguir «Relatório explicativo sobre a Convenção 108 modernizada») destaca também o requisito de que a medida que prevê ingerências nos direitos ao respeito pela vida privada e à proteção dos dados pessoais seja «acessível», «previsível», «suficientemente detalhada» e «claramente formulada», v. n.º 91 desse relatório explicativo, <https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726>.

⁸¹ V., *a contrario sensu*, Acórdão de 3 de dezembro de 2019, República Checa/Parlamento e Conselho (C-482/17, EU:C:2019:1035, n.º 135).

transposição para o direito nacional, mas têm como base legal a própria Diretiva PNR. Nestas condições, incumbia ao legislador da União, a fim de dar cumprimento à jurisprudência recordada no n.º 85 das presentes conclusões, bem como às «normas exigentes» de proteção dos direitos fundamentais contidas, nomeadamente, na Carta e na CEDH, a que se refere o considerando 15 da Diretiva PNR, estabelecer regras claras e precisas que definissem tanto o alcance como a aplicação das medidas que comportam as referidas ingerências.

87. Embora com a sua terceira questão prejudicial o órgão jurisdicional de reenvio se interrogue especificamente sobre o respeito desta obrigação relativamente aos pontos 12 e 18 do anexo I, o exame das segunda, quarta e sexta questões prejudiciais, através das quais este órgão jurisdicional suscita dúvidas quanto à necessidade das ingerências que a Diretiva PNR comporta nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta, exige igualmente que se tome posição sobre o carácter suficientemente claro e preciso das disposições da Diretiva PNR colocadas em causa.

88. Embora esta análise diga respeito, como expus no n.º 85 das presentes conclusões, à legalidade da ingerência, na aceção do artigo 52.º, n.º 1, primeiro período, da Carta, procederei à mesma no âmbito do exame da sua proporcionalidade, a que se refere o segundo período deste número, em conformidade com a abordagem seguida tanto pelo Tribunal de Justiça como pelo TEDH nos processos em que estão em causa medidas que têm por objeto o tratamento de dados pessoais⁸².

b) Quanto ao respeito pelo conteúdo essencial dos direitos enunciados nos artigos 7.º e 8.º da Carta

89. Em conformidade com o artigo 52.º, n.º 1, primeiro período, da Carta, qualquer restrição ao exercício dos direitos fundamentais deve não só assentar numa base legal suficientemente precisa como também respeitar o *conteúdo essencial* desses direitos.

90. Como já expus no n.º 66 das presentes conclusões, este requisito — que se encontra incorporado nas constituições de vários Estados-Membros⁸³, e que, embora não esteja expressamente reconhecido na CEDH, está todavia bem assente na jurisprudência do TEDH⁸⁴ — está inscrito no artigo 52.º, n.º 1, da Carta⁸⁵. Reconhecido pelo Tribunal de Justiça muito antes da sua codificação⁸⁶, este requisito foi constantemente reafirmado na jurisprudência dos órgãos jurisdicionais da União, mesmo após a entrada em vigor do Tratado de Lisboa.

91. Resulta, nomeadamente, do Acórdão de 6 de outubro de 2015, Schrems⁸⁷, que o desrespeito pelo conteúdo essencial de um direito fundamental por um ato da União implica *automaticamente* a nulidade ou a invalidade deste, sem que seja necessário proceder a uma ponderação dos interesses em jogo. O Tribunal de Justiça reconhece, assim, que todos os direitos fundamentais têm um «núcleo duro», garantindo a qualquer pessoa uma esfera de liberdade ao

⁸² V., entre outros, Acórdão La Quadrature du Net, n.º 132 e jurisprudência referida; V., igualmente, TEDH, Acórdão Big Brother Watch, § 334.

⁸³ V., a este respeito, Tridimas, T., 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, pp. 779 e segs.

⁸⁴ A partir do Acórdão do TEDH de 24 de outubro de 1979, Winterwerp c. Países Baixos (CE:ECHR:1979:1024JUD000630173, § 60).

⁸⁵ Ver Anotações relativas à Carta dos Direitos Fundamentais (JO 2007, C 303, p. 17, em especial «Anotação *ad* artigo 52.º», p. 32, a seguir «Anotações relativas à Carta»).

⁸⁶ V., já neste sentido, nomeadamente, Acórdãos de 14 de maio de 1974, Nold/Comissão (4/73, EU:C:1974:51, n.º 14), e de 13 de dezembro de 1979, Hauer (44/79, EU:C:1979:290, n.º 23).

⁸⁷ C-362/14, a seguir Acórdão «Schrems I», EU:C:2015:650, n.ºs 94 a 98.

abrigo de qualquer ingerência pelos poderes públicos e que não pode sofrer limitações⁸⁸, sob pena de colocar em questão os princípios democráticos, do Estado de direito e do respeito pela dignidade humana subjacentes à proteção dos direitos fundamentais. Por outro lado, resulta tanto da redação do artigo 52.º, n.º 1, da Carta como da jurisprudência do Tribunal de Justiça, nomeadamente do Acórdão Schrems I, que a apreciação relativa à existência de uma ingerência no conteúdo essencial do direito fundamental em causa deve ser efetuada antes e independentemente da avaliação da proporcionalidade da medida impugnada. Trata-se, por outras palavras, de um teste dotado da sua própria autonomia.

92. No entanto, determinar o que constitui o «conteúdo essencial» e, por conseguinte, intocável de um direito fundamental suscetível de ser limitado no seu exercício é uma operação extremamente complexa. Embora, para cumprir a sua função, este conceito devesse poder ser definido em termos absolutos, atendendo às características essenciais do direito fundamental em causa, aos interesses subjetivos e objetivos que visa proteger e, mais genericamente, à sua função numa sociedade democrática baseada no respeito pela dignidade humana⁸⁹, na prática, tal operação revela-se quase impossível, pelo menos sem ter em conta critérios que são habitualmente utilizados no exame da proporcionalidade da ingerência no direito em causa, como a gravidade dessa ingerência, a sua extensão ou a sua dimensão temporal e, portanto, sem ter em conta as especificidades de cada caso concreto.

93. No que toca, nomeadamente, ao direito fundamental ao respeito pela vida privada, há que ter em conta não só a importância que reveste, para a saúde mental e física de qualquer pessoa, o seu bem-estar, a sua autonomia, o seu desenvolvimento pessoal, a sua capacidade de construir e de cultivar relações sociais, o facto de dispor de uma esfera privada dentro da qual possa desenvolver a sua interioridade pessoal, mas também o papel que esse direito desempenha para preservar outros direitos e liberdades, como, nomeadamente, as liberdades de pensamento, de consciência, de religião, de expressão, de informação, cujo pleno gozo pressupõe o reconhecimento de uma esfera de intimidade. Mais genericamente, há que tomar em conta a função que o respeito pelo direito à vida privada desempenha numa sociedade democrática⁹⁰. O Tribunal de Justiça parece apreciar a existência de uma violação do conteúdo essencial deste direito tomando em consideração tanto a *intensidade* como a *extensão* da ingerência, o que leva a considerar que tal violação é definida de forma mais quantitativa do que qualitativa. Assim, por um lado, no Acórdão Digital Rights, o Tribunal de Justiça considerou, em substância, que a obrigação de conservação dos dados imposta pela Diretiva 2006/24/CE⁹¹ não atingia um nível de gravidade tal que afetasse o conteúdo essencial do direito ao respeito pela vida privada, uma vez que não permitia «tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal»⁹². Por outro lado, no Parecer 1/15, o Tribunal de Justiça considerou, em substância, que uma limitação que abrangia apenas certos aspetos da vida privada das pessoas em causa não podia dar origem a uma ingerência no conteúdo essencial deste direito fundamental⁹³.

⁸⁸ V. Lenaerts, K., op. cit., p. 781; Tridimas, T., Gentile, G., op. cit., p. 803.

⁸⁹ As Anotações relativas à Carta reconhecem expressamente que «a dignidade do ser humano faz parte da essência dos direitos [...] consignados [na Carta]» e que «[n]ão pode, pois, ser lesada, mesmo nos casos em que um determinado direito seja objeto de restrições».

⁹⁰ Remeto, a este respeito, para as considerações contidas na opinião conjunta parcialmente concordante dos juízes Lemmens, Vehabović e Bošniak no Acórdão Big Brother Watch, §§ 3 a 10.

⁹¹ Diretiva do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO 2006, L 105, p. 54).

⁹² V. Acórdão Digital Rights, n.º 39; v., igualmente, quanto à Diretiva 2002/58, Acórdão Tele2 Sverige, n.º 101.

⁹³ V. Parecer 1/15, n.º 150.

94. Quanto ao direito fundamental à proteção dos dados pessoais, o Tribunal de Justiça parece considerar que o conteúdo essencial deste direito é preservado quando a medida que estabelece a ingerência circunscreve as finalidades do tratamento e prevê regras que garantem a segurança dos dados em causa, nomeadamente contra a destruição acidental ou ilícita, a perda ou a alteração acidental⁹⁴.

95. No presente processo, embora o órgão jurisdicional de reenvio não tenha evocado explicitamente o requisito do respeito pelo conteúdo essencial dos direitos enunciados nos artigos 7.º e 8.º da Carta, a questão do respeito deste requisito está, na minha opinião, subjacente à quarta e à sexta questão prejudicial. É por esta razão que sugiro ao Tribunal de Justiça que a aborde.

96. A este respeito, recordo que, no n.º 150 do Parecer 1/15, embora reconhecendo que os dados PNR «[podem], se for caso disso, revelar informações muito precisas sobre a vida privada de uma pessoa»⁹⁵, e que estas informações podem expor, direta ou indiretamente, dados sensíveis da pessoa em causa⁹⁶, o Tribunal de Justiça concluiu, todavia, no que respeita ao Projeto de Acordo PNR Canadá-UE, que, uma vez que a «natureza destas informações [estava] limitada a certos aspetos dessa vida privada, relativos, em particular, às viagens aéreas entre o Canadá e a União», a violação do direito fundamental ao respeito pela vida privada não era suscetível de afetar o conteúdo essencial do referido direito.

97. Ora, abstraindo da circunstância de os dados PNR visados pelo Projeto de Acordo PNR Canadá-UE deverem ser transferidos para um Estado terceiro e de o seu tratamento posterior dever ser efetuado pelas autoridades desse Estado terceiro no seu território, as ingerências no direito fundamental ao respeito pela vida privada resultantes do referido projeto de acordo e as previstas pela Diretiva PNR são em grande medida coincidentes quanto à natureza. É o caso, nomeadamente, dos dados PNR visados, do caráter sistemático e generalizado da transferência e do tratamento desses dados, da sua natureza automatizada e da conservação dos referidos dados. Em contrapartida, o que distingue os dois processos é, por assim dizer, a «cobertura geográfica» destas ingerências. Com efeito, como indiquei no n.º 77 das presentes conclusões, os tratamentos dos dados em causa no presente processo não se limitam às ligações aéreas com um único país terceiro, como era o caso no Parecer 1/15, mas dizem respeito a praticamente todos os voos que entram e saem da União, e operados no seu interior. Daqui resulta que, em comparação com o Projeto de Acordo PNR Canadá-UE, a Diretiva PNR impõe o tratamento sistemático dos dados de um número consideravelmente mais elevado de passageiros aéreos, que se deslocam de avião no interior e no exterior da União. Além disso, atendendo ao aumento do volume dos dados tratados e à frequência com que são recolhidos, o seu tratamento é provavelmente suscetível de fornecer informações simultaneamente mais precisas e mais amplas sobre a vida privada das pessoas em causa (hábitos de viagem, relações pessoais, situações financeiras, etc.).

98. Todavia, tal como no Parecer 1/15, estas informações, consideradas isoladamente, apenas dizem respeito a certos aspetos da vida privada, ligados às viagens aéreas. Ora, tendo em conta a necessidade de definir o conceito de «conteúdo essencial» dos direitos fundamentais de modo restritivo, para que este mantenha a sua função de bastião contra os ataques à própria substância destes direitos, considero que a conclusão a que o Tribunal de Justiça chegou no n.º 150 do Parecer 1/15 pode ser transposta para o presente processo.

⁹⁴ V. neste sentido, nomeadamente, Acórdão Digital Rights, n.º 40.

⁹⁵ V., neste mesmo sentido, Parecer 1/15, n.º 128.

⁹⁶ V. Parecer 1/15, n.ºs 164 e 165.

99. No Parecer 1/15, o Tribunal de Justiça excluiu também a violação do conteúdo essencial do direito à proteção dos dados pessoais⁹⁷. Na minha opinião, esta conclusão é igualmente transponível para as circunstâncias do presente processo. Com efeito, precisamente como o Projeto de Acordo PNR Canadá-UE, a Diretiva PNR circunscreve, no seu artigo 1.º, n.º 2, as finalidades do tratamento dos dados PNR. Por outro lado, esta diretiva, bem como os outros atos da União para os quais remete, nomeadamente o RGPD e a Diretiva Cooperação Policial, contém disposições específicas destinadas a garantir, em especial, a segurança, a confidencialidade e a integridade desses dados, bem como a protegê-los contra os acessos e os tratamentos ilegais. Embora não se possa considerar que uma regulamentação como a prevista pela Diretiva PNR afeta o conteúdo essencial dos direitos fundamentais protegidos pelos artigos 7.º e 8.º da Carta, tal regulamentação deve, contudo, ser sujeita a uma fiscalização estrita e rigorosa quanto à sua proporcionalidade.

c) Quanto ao respeito do requisito segundo o qual a ingerência deve corresponder a um objetivo de interesse geral

100. A Diretiva PNR visa, nomeadamente, garantir a segurança interna e proteger a vida e a segurança das pessoas através de uma transferência dos dados PNR para as autoridades competentes dos Estados-Membros, com vista à sua utilização no âmbito da luta contra o terrorismo e a criminalidade grave⁹⁸.

101. Mais especificamente, resulta do artigo 1.º, n.º 2, da Diretiva PNR, em conjugação com os seus considerandos 6 e 7, bem como da proposta da Comissão que conduziu à adoção desta diretiva (a seguir «Proposta de Diretiva PNR»)⁹⁹, que, no âmbito desse objetivo, os dados PNR são utilizados pelas autoridades responsáveis pela aplicação da lei¹⁰⁰ de diferentes formas. Em primeiro lugar, esses dados são utilizados para identificar pessoas implicadas ou suspeitas de estarem implicadas em infrações terroristas e formas de criminalidade grave que já tenham sido cometidas, para recolher provas bem como, se for caso disso, encontrar os cúmplices de criminosos e desmantelar redes criminosas (utilização de «forma reativa»). Em segundo lugar, os dados PNR podem ser avaliados antes da chegada ou da partida dos passageiros para prevenir a prática de um crime e identificar pessoas que não eram anteriormente suspeitas de participação em infrações terroristas ou formas de criminalidade grave e que, com base no resultado dessa avaliação, devam ser sujeitas a um controlo mais minucioso por parte das autoridades de aplicação da lei (utilização «em tempo real»). Por último, os dados PNR são utilizados para definir critérios de avaliação que poderão seguidamente ser aplicados na apreciação do risco que representam os passageiros antes da sua chegada e antes da sua partida (utilização de «forma proativa»). Essa utilização proativa dos dados PNR deve permitir aos serviços responsáveis pela aplicação da lei fazer face à ameaça que representam a grande criminalidade e o terrorismo numa perspetiva diferente da do tratamento de outras categorias de dados pessoais¹⁰¹.

⁹⁷ V. Parecer 1/15, n.º 150.

⁹⁸ V., nomeadamente, considerandos 5, 6, 15 e 22 da Diretiva PNR.

⁹⁹ Proposta da Comissão, de 2 de fevereiro de 2011, relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave [COM(2011) 32 final, p. 4].

¹⁰⁰ Por razões de simplificação, utilizarei, nas presentes conclusões, as expressões «serviços responsáveis pela aplicação da lei» ou «autoridades responsáveis pela aplicação da lei» para indicar, de maneira geral, qualquer autoridade investida de poderes nos domínios da deteção, prevenção, repressão ou investigação em matéria de terrorismo ou de criminalidade grave, abrangidos pela Diretiva PNR.

¹⁰¹ V. considerando 7 da Diretiva PNR. V., igualmente, Proposta de Diretiva PNR, p. 5.

102. Resulta da jurisprudência do Tribunal de Justiça que o objetivo de proteção da segurança pública, que abrange, nomeadamente, a prevenção, a investigação, a deteção e a perseguição tanto de infrações terroristas como de infrações penais que se enquadram na criminalidade grave, constitui um objetivo de interesse geral da União, na aceção do artigo 52.º, n.º 1, da Carta, suscetível de justificar ingerências, ainda que graves, nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta¹⁰².

103. O Tribunal de Justiça reconheceu igualmente que os objetivos de proteção da segurança pública e de luta contra a criminalidade grave contribuem para a proteção dos direitos e liberdades de terceiros¹⁰³. Assim, no que respeita à ponderação equilibrada entre estes objetivos e os direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta¹⁰⁴, há que tomar igualmente em conta a importância dos direitos consagrados nos artigos 3.º, 4.º, 6.º e 7.º da Carta. A este respeito, embora, no Acórdão *La Quadrature du Net*, o Tribunal de Justiça tenha considerado que o artigo 6.º da Carta «não pode ser interpretado no sentido de que impõe aos poderes públicos a obrigação de adotarem medidas específicas para [exercerem a] ação penal contra determinadas infrações penais»¹⁰⁵, em contrapartida, no que diz respeito, em particular, à luta efetiva contra as infrações penais de que são vítimas, nomeadamente, menores e outras pessoas vulneráveis, sublinhou que obrigações positivas que incumbem ao poderes públicos podem resultar tanto do artigo 7.º da Carta, tendo em vista a adoção de medidas jurídicas destinadas a proteger a vida privada e familiar, como dos seus artigos 3.º e 4.º, relativos à proteção da integridade física e psíquica das pessoas e à proibição da tortura e dos tratos desumanos e degradantes¹⁰⁶.

104. Por último, o Tribunal de Justiça considerou que a importância do objetivo de salvaguarda da *segurança nacional* ultrapassa a dos objetivos de luta contra a criminalidade em geral, incluindo grave, bem como de salvaguarda da segurança pública e que é, por conseguinte, suscetível de justificar medidas que incluem ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar¹⁰⁷. Uma vez que as atividades de terrorismo são suscetíveis de constituir ameaças à segurança nacional dos Estados-Membros, o sistema instituído pela Diretiva PNR, na medida em que constitui um instrumento de luta contra tais atividades, contribui para o objetivo de salvaguarda da segurança nacional dos Estados-Membros.

d) Quanto ao respeito do princípio da proporcionalidade

105. Em conformidade com o artigo 52.º, n.º 1, segundo período, da Carta, na observância do princípio da proporcionalidade, só podem ser introduzidas restrições ao exercício de um direito fundamental reconhecido pela mesma se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros.

¹⁰² V., neste sentido, Parecer 1/15, bem como Acórdão de 2 de março de 2021, *Prokuratuur* (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, a seguir «Acórdão *Prokuratuur*», EU:C:2021:152, n.º 33 e jurisprudência referida).

¹⁰³ V., neste sentido, Parecer 1/15, n.º 149 e jurisprudência referida, bem como Acórdão *La Quadrature du Net*.

¹⁰⁴ V. a análise que se segue sobre a proporcionalidade da ingerência.

¹⁰⁵ V. Acórdão *La Quadrature du Net*, n.º 125.

¹⁰⁶ V. Acórdão *La Quadrature du Net*, n.º 126 e jurisprudência referida.

¹⁰⁷ V. Acórdão *La Quadrature du Net*, n.º 136.

106. A este propósito, cabe recordar que o princípio da proporcionalidade exige, segundo jurisprudência constante do Tribunal de Justiça, que os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos¹⁰⁸.

107. Em conformidade com a jurisprudência constante do Tribunal de Justiça, a proteção do direito fundamental ao respeito pela vida privada ao nível da União exige que as derrogações à proteção dos dados pessoais e as restrições à mesma operem na medida do *estritamente necessário*. Além disso, um objetivo de interesse geral não pode ser prosseguido sem se ter em conta o facto de que deve ser conciliado com os direitos fundamentais abrangidos pela medida, mediante uma ponderação equilibrada entre o objetivo e os interesses e direitos em causa¹⁰⁹. Mais especificamente, a proporcionalidade de uma limitação aos direitos consagrados nos artigos 7.º e 8.º da Carta deve ser apreciada medindo a gravidade da ingerência que essa limitação comporta e verificando se a importância do objetivo de interesse geral prosseguido por essa limitação tem relação com a gravidade dessa ingerência¹¹⁰.

108. Resulta da jurisprudência do Tribunal de Justiça que, para satisfazer o requisito da proporcionalidade, a Diretiva PNR, enquanto base legal que comporta as ingerências nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta descritas nos n.ºs 70 a 83 das presentes conclusões, deve prever regras claras e precisas que regulem o âmbito e a aplicação das medidas que comportem tais ingerências e impor requisitos mínimos, de modo a que as pessoas cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso e utilização ilícitos dos mesmos¹¹¹. A necessidade de dispor de tais garantias é ainda mais importante quando, como no caso em apreço, os dados pessoais são sujeitos a um tratamento automatizado e quando está em jogo a proteção desta categoria específica de dados pessoais que são os dados sensíveis¹¹².

109. No que toca ao alcance da fiscalização jurisdicional do respeito dos requisitos que decorrem do princípio da proporcionalidade, tendo em conta o importante papel desempenhado pela proteção dos dados pessoais à luz do direito fundamental ao respeito pela vida privada e a ingerência neste direito que a Diretiva PNR comporta, o poder de apreciação do legislador da União fica reduzido, pelo que essa fiscalização deve ser estrita¹¹³.

1) Quanto à aptidão dos tratamentos dos dados PNR previstos na Diretiva PNR à luz do objetivo prosseguido

110. No n.º 153 do Parecer 1/15, o Tribunal de Justiça afirmou, no que respeita ao Projeto de Acordo PNR Canadá-UE, que a transferência dos dados PNR para o Canadá e os tratamentos posteriores dos mesmos podem ser considerados aptos a garantir a realização do objetivo relativo à salvaguarda da proteção e da segurança do público. Não me parece que esta aptidão, reconhecida

¹⁰⁸ V. Acórdão Digital Rights, n.º 46 e jurisprudência referida.

¹⁰⁹ V. Parecer 1/15, n.º 140, bem como Acórdão La Quadrature du Net, n.º 130 e jurisprudência referida. O requisito segundo o qual o tratamento de dados pessoais deve refletir, em cada fase, um «justo equilíbrio entre todos os interesses presentes, sejam eles públicos ou privados, bem como os direitos e liberdades em jogo» é igualmente enunciado no artigo 5.º da Convenção 108.

¹¹⁰ V., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, n.º 55 e jurisprudência referida), bem como Acórdãos La Quadrature du Net, n.º 131, e Prokuratuur, n.º 32.

¹¹¹ V., neste sentido, Acórdãos Digital Rights, n.º 54, e Schrems I, n.º 91, bem como Parecer 1/15, n.º 141.

¹¹² V. Parecer 1/15, n.º 141 e jurisprudência referida.

¹¹³ V., neste sentido, Acórdão Digital Rights, n.º 48.

desde há muito tempo tanto a nível da União como a nível mundial¹¹⁴, possa ser posta em causa quanto à recolha e ao tratamento posterior dos dados PNR no que respeita tanto aos voos extra-UE como aos voos intra-UE¹¹⁵.

111. No entanto, a eficácia do sistema de tratamento dos dados PNR estabelecido pela diretiva só pode ser avaliada em concreto, apreciando os resultados da sua aplicação¹¹⁶. Nesta perspetiva, é essencial que essa eficácia seja objeto de uma avaliação contínua com base em dados estatísticos o mais precisos e fiáveis possível¹¹⁷. A este respeito, a Comissão deveria, com intervalos regulares, proceder a um reexame análogo ao já previsto no artigo 19.º da Diretiva PNR.

2) Quanto ao caráter estritamente necessário da ingerência

112. Embora a Cour constitutionnelle (Tribunal Constitucional, Bélgica) não tenha suscitado explicitamente dúvidas quanto ao facto de a Diretiva PNR conter regras claras, precisas e limitadas ao estritamente necessário no que respeita à delimitação das finalidades do tratamento dos dados PNR¹¹⁸, a análise da proporcionalidade do sistema previsto por esta diretiva, solicitada pelo órgão jurisdicional de reenvio, não pode, na minha opinião, deixar de abordar esta questão¹¹⁹.

i) Quanto à delimitação das finalidades do tratamento dos dados PNR

113. Uma clara delimitação das finalidades para as quais é permitido o acesso a dados pessoais pelas autoridades competentes, bem como a sua posterior utilização pelas mesmas, constitui um requisito essencial de qualquer sistema de tratamento de dados, nomeadamente para fins de aplicação da lei. A satisfação deste requisito é, por outro lado, necessária para permitir ao Tribunal de Justiça apreciar a proporcionalidade das medidas em causa, aplicando o critério, estabelecido na sua jurisprudência, da gravidade da ingerência relativamente à importância do objetivo prosseguido¹²⁰.

114. O Tribunal de Justiça sublinhou a importância de uma delimitação clara das finalidades das medidas que comportam limitações aos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, nomeadamente no Acórdão Digital Rights, no qual declarou inválida a Diretiva 2006/24. No n.º 60 desse acórdão, o Tribunal de Justiça observou que esta diretiva não previa «critérios objetivos que [permitissem] delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas suficientemente graves, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, para justificar tal ingerência» e que se limitava, pelo contrário, «a remeter, no seu artigo 1.º, n.º 1, de forma genérica, para as infrações graves tal como definidas no direito nacional de cada Estado-Membro».

¹¹⁴ V., neste sentido, n.ºs 201 a 203 das presentes conclusões.

¹¹⁵ Remeto, a este respeito, para os dados contidos no Documento de trabalho de 2020.

¹¹⁶ V., neste sentido, Parecer de 19 de agosto de 2016, p. 5.

¹¹⁷ Quanto à importância das estatísticas para efeitos da avaliação da eficácia do sistema estabelecido pela Diretiva PNR, v., nomeadamente, Parecer 1/2011, de 14 de junho de 2011, sobre a Proposta de Diretiva PNR, https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_FR.pdf, ponto 2.1.2.1 (a seguir «Parecer 1/2011 da FRA»).

¹¹⁸ Esta questão é, em contrapartida, claramente colocada pelo Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha), no processo pendente C-215/20.

¹¹⁹ A Comissão foi convidada a apresentar as suas observações a este respeito no âmbito de uma pergunta para resposta escrita. Os outros interessados tiveram a oportunidade de se pronunciar na audiência.

¹²⁰ V. n.º 107, *in fine*, das presentes conclusões.

115. O artigo 1.º, n.º 2, da Diretiva PNR enuncia um critério geral de limitação das finalidades segundo o qual «[o]s dados PNR recolhidos nos termos da presente diretiva só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave». Todavia, ao contrário da Diretiva 2006/24, a Diretiva PNR não se limita a tal enunciação, mas define ela própria, no seu artigo 3.º, pontos 8 e 9, tanto o conceito de «infrações terroristas» como o de «criminalidade grave», o primeiro por remissão para os artigos 1.º a 4.º da Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO 2002, L 164, p. 3) (substituída pela Diretiva 2017/541)¹²¹, e o segundo, por um lado, enumerando no anexo II as categorias de infrações penais que correspondem a este conceito e, por outro, estabelecendo um limiar de gravidade em termos de duração máxima da pena de prisão ou da medida de segurança de que tais infrações são passíveis.

116. Embora a remissão para as disposições pertinentes da Diretiva 2017/541 permita caracterizar, de forma suficientemente clara e precisa, os atos suscetíveis de serem qualificados de infrações terroristas nos termos do artigo 3.º, ponto 8, da Diretiva PNR e apreciar a sua gravidade para efeitos da ponderação da importância do objetivo de proteção da segurança pública prosseguido por esta diretiva e da gravidade da ingerência que esta comporta nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta, a mesma conclusão não se impõe com igual evidência no que respeita a todas as infrações enumeradas no anexo II.

117. No n.º 177 do Parecer 1/15, o Tribunal de Justiça considerou que o Projeto de Acordo PNR Canadá-UE definia com clareza e precisão o grau de gravidade das infrações abrangidas pelo conceito de «criminalidade transnacional grave», impondo que estas infrações fossem «puníveis com penas privativas de liberdade com uma duração de, pelo menos, quatro anos ou por penas mais graves», remetendo para as «infrações definidas pela legislação canadiana» e enunciando «os diferentes casos em que uma infração é considerada transnacional».

118. Relativamente à regulamentação examinada pelo Tribunal de Justiça nesse parecer, a Diretiva PNR, em primeiro lugar, não tem em conta, na definição das infrações visadas, o seu caráter transnacional, em segundo lugar, prevê uma lista exaustiva de infrações que, pela sua natureza, são consideradas abrangidas pela criminalidade grave, desde que atinjam o mínimo de pena máxima previsto no artigo 3.º, ponto 9, desta diretiva, em terceiro lugar, baixa, em princípio, o limiar de gravidade, adotando um critério baseado no nível da pena máxima e fixando esse limiar em três anos.

119. No que respeita, em primeiro lugar, à inexistência de um critério de limitação baseado no caráter transnacional, é decerto verdade que a delimitação do âmbito de aplicação material da Diretiva PNR de modo a abranger apenas a criminalidade «transfronteiriça» grave teria permitido visar infrações suscetíveis, pela sua natureza, de apresentarem, pelo menos potencialmente, uma relação objetiva com as viagens aéreas e, por conseguinte, com as categoria de dados recolhidos e tratados em aplicação da Diretiva PNR¹²². Todavia, partilho, em princípio, da posição expressa pela Comissão, segundo a qual, diferentemente do que se passa no contexto

¹²¹ Diretiva do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho (JO 2017, L 88, p. 6).

¹²² Observo, a este respeito, que o conceito de «crime de natureza transnacional», conforme definido, por exemplo, no Projeto de Acordo PNR Canadá-UE, é suficientemente amplo para incluir igualmente infrações cometidas num único país e se o autor «estiver noutro país ou tencionar viajar para outro país»; v. artigo 3.º, n.º 3, alínea e), do Projeto de Acordo PNR Canadá-UE, cujo texto é reproduzido no n.º 30 do Parecer 1/15. Observo igualmente que, no seu Parecer 1/2011 (pontos 2.2.3.1 e 3.7), a FRA tinha sugerido a limitação do sistema PNR da União apenas às infrações transnacionais graves. A Proposta de Diretiva PNR previa, em contrapartida, um tratamento automatizado diferenciado para as infrações transnacionais e para as que não tinham esse caráter (v. artigo 4.º, n.º 2, alínea a), desta proposta).

de um acordo internacional, a pertinência e a necessidade de tal critério é menos evidente quando se trata de um dispositivo de luta contra a criminalidade cujo objetivo consiste em proteger a segurança interna da União. Por outro lado, como afirma ainda a Comissão, a inexistência de elementos transfronteiriços não é, em si, um indício que permita excluir a gravidade de uma infração.

120. No que respeita, em segundo lugar, ao critério que fixa o limiar de gravidade das infrações visadas – que, para permitir uma apreciação *ex ante* dessa gravidade, deve ser interpretado no sentido de que se refere à duração máxima da pena de prisão ou da medida de segurança prevista por lei, e não à que é suscetível de ser concretamente aplicada num caso particular – este critério, embora se baseie no mínimo de pena máxima e não no mínimo de pena mínima, não é, por si só, inapto para identificar um nível suficiente de gravidade suscetível de justificar a ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que comportam os tratamentos de dados previstos pela Diretiva PNR. No entanto, na minha opinião, este critério deve ser interpretado como um critério que identifica um nível de gravidade «mínimo». Assim, embora tal critério proíba os Estados-Membros de considerarem «criminalidade grave» as infrações enumeradas no anexo II para as quais o seu direito penal nacional preveja uma pena de prisão ou medida de segurança de duração máxima inferior a três anos, não os obriga, em contrapartida, a reconhecer automaticamente essa qualificação a todas as infrações suscetíveis de serem incluídas no referido anexo II que sejam passíveis de uma pena que atinja o limiar previsto no artigo 3.º, ponto 9, da Diretiva PNR, quando, tendo em conta as especificidades do seu sistema penal, esse reconhecimento resultasse numa utilização do regime previsto pela Diretiva PNR para efeitos de prevenção, deteção, investigação e repressão de formas de criminalidade comum, contrária às finalidades prosseguidas por esta diretiva.

121. No que respeita, em terceiro lugar, à lista do anexo II, importa, antes de mais, salientar que a circunstância de a Diretiva PNR enumerar taxativamente as infrações abrangidas pela definição de «criminalidade grave» constitui uma garantia formal e substancial fundamental para assegurar a legalidade do sistema estabelecido pela Diretiva PNR e a segurança jurídica dos passageiros. Há que constatar, todavia, que a referida lista inclui tanto infrações que, pela sua natureza, revestem um nível de gravidade incontestavelmente elevado — como, por exemplo, o tráfico de seres humanos, a exploração sexual de crianças e pedopornografia, o tráfico de armas, ou de materiais nucleares ou radioativos, o desvio de avião ou navio, os crimes abrangidos pela jurisdição do Tribunal Penal Internacional, o homicídio voluntário, a violação, o rapto, o sequestro e a tomada de reféns¹²³ — como infrações quanto às quais esse nível de gravidade se revela menos evidente, como a fraude, a contrafação e piratagem de produtos, a falsificação de documentos

¹²³ Saliento, por outro lado, que uma parte das infrações referidas no anexo II se inscreve em domínios de criminalidade qualificada de «particularmente grave» pelo artigo 83.º, n.º 1, primeiro parágrafo, TFUE e enumerados no segundo parágrafo deste número. Trata-se, nomeadamente, do tráfico de seres humanos, da exploração sexual das crianças, do tráfico de droga, do tráfico de armas, do branqueamento de capitais, da corrupção, da contrafação de meios de pagamento, da criminalidade informática e da criminalidade organizada. Em vários destes domínios, o legislador da União adotou, com base no artigo 83.º, n.º 1, TFUE, diretivas que estabelecem «regras mínimas relativas à definição das infrações penais e das sanções»; v., nomeadamente, a Diretiva 2011/36/UE do Parlamento Europeu e do Conselho, de 5 de abril de 2011, relativa à prevenção e luta contra o tráfico de seres humanos e à proteção das vítimas, e que substitui a Decisão-Quadro 2002/629/JAI do Conselho (JO 2011, L 101, p. 1); a Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO 2011, L 335, p. 1); a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO 2013, L 218, p. 8); a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho (JO 2019, L 123, p. 18); a Diretiva (UE) 2017/1371 do Parlamento Europeu e do Conselho, de 5 de julho de 2017, relativa à luta contra a fraude lesiva dos interesses financeiros da União através do direito penal (JO 2017, L 198, p. 29), e a Diretiva (UE) 2018/1673 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativa ao combate ao branqueamento de capitais através do direito penal (JO 2018, L 284, p. 22).

administrativos e respetivo tráfico, bem como o tráfico de veículos roubados¹²⁴. Por outro lado, entre as infrações incluídas no anexo II, algumas são mais suscetíveis do que outras de revestirem, pela sua própria natureza, caráter transnacional, como o tráfico de seres humanos, o tráfico de estupefacientes ou de armas, a exploração sexual de crianças, o auxílio à entrada e à permanência irregulares, o desvio de avião, e de apresentarem também uma relação com o transporte aéreo de passageiros.

122. Quanto ao caráter suficientemente claro e preciso das rubricas que figuram no anexo II, o nível é, também neste caso, muito variável. Assim, embora a lista contida nesse anexo deva ser considerada exaustiva, várias das suas rubricas têm caráter «aberto»¹²⁵ e outras remetem para conceitos genéricos, suscetíveis de incluírem um número muito amplo de infrações de gravidade variável, embora sempre dentro do limite do limiar máximo previsto no artigo 3.º, ponto 9, da Diretiva PNR¹²⁶.

123. A este respeito, observo, por um lado, que as diretivas de harmonização adotadas nos domínios a que se refere o artigo 83.º, n.º 1, TFUE, mencionadas na nota 123 das presentes conclusões, fornecem elementos pertinentes que permitem identificar pelo menos algumas das infrações penais graves suscetíveis de ser abrangidas pelas rubricas correspondentes do anexo II. Assim, nomeadamente, a Diretiva 2013/40 define, nos seus artigos 3.º a 8.º, diferentes infrações penais abrangidas pelo conceito de «criminalidade informática/cibercrime» previsto no ponto 9 do referido anexo II, tendo o cuidado, em cada um dos casos, de excluir os atos que não «se revistam de alguma gravidade»¹²⁷. Do mesmo modo, a Diretiva 2019/713 define certos tipos de infrações fraudulentas, e a Diretiva 2017/1371 define os elementos que constituem uma «fraude contra os interesses financeiros da União». Neste contexto, importa mencionar igualmente a Diretiva 2008/99/CE, adotada com base no artigo 175.º, n.º 1, CE, relativa à proteção do ambiente através do direito penal¹²⁸, que define, no seu artigo 3.º, uma série de infrações ambientais graves, suscetíveis de serem incluídas na rubrica 10 do anexo II, incluindo os atos qualificáveis de «tráfico de espécies animais ameaçadas e de espécies e variedades vegetais ameaçadas», excluindo todos os atos que tenham impacto negligenciável sobre o bem protegido. Recordarei, por último, a Diretiva 2002/90/CE¹²⁹, que define o auxílio à entrada, ao trânsito e à residência irregulares, bem como a Decisão-Quadro 2002/946/JAI¹³⁰, relativa ao reforço do quadro penal para a prevenção dessas

¹²⁴ Saliento, todavia, que todas as infrações referidas no anexo I, com exceção da «espionagem industrial», figuram no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO 2002, L 190, p. 1). Embora não sejam explicitamente qualificadas de graves, determinam, todavia, quando atingem o mesmo limiar de pena privativa de liberdade previsto no artigo 3.º, ponto 9, da Diretiva PNR, a entrega com base num mandado de detenção europeu, sem controlo da dupla incriminação do facto. Quase todas as referidas infrações, com exceção da «sabotagem», do «desvio de avião» e da «espionagem industrial», figuram igualmente no anexo I do Regulamento (UE) 2018/1727 do Parlamento Europeu e do Conselho, de 14 de novembro de 2018, que cria a Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust), e que substitui e revoga a Decisão 2002/187/JAI do Conselho (JO 2018, L 295, p. 138), que enumera a lista das «formas graves de criminalidade» que são da competência da Eurojust.

¹²⁵ Trata-se, nomeadamente, dos pontos 7, 8, 10 e 16.

¹²⁶ É o caso, por exemplo, da «fraude» (ponto 7), da «corrupção» (ponto 6), da «criminalidade informática/cibercrime» (ponto 9) e dos «crimes contra o ambiente» (ponto 10). É especialmente a respeito das infrações fraudulentas que o Verwaltungsgericht Wiesbaden (Tribunal Administrativo de Wiesbaden, Alemanha) se interroga no processo pendente C-215/20.

¹²⁷ Esta diretiva precisa, aliás, no seu artigo 9.º, a duração mínima da pena de prisão máxima de que as referidas infrações devem ser passíveis, limiar que só em determinadas circunstâncias atinge os três anos.

¹²⁸ Diretiva do Parlamento e do Conselho, de 19 de novembro de 2008 (JO 2008, L 328, p. 28).

¹²⁹ Diretiva do Conselho, de 28 de novembro de 2002, relativa à definição do auxílio à entrada, ao trânsito e à residência irregulares (JO 2002, L 328, p. 17).

¹³⁰ Decisão-Quadro do Conselho, de 28 de novembro de 2002, relativa ao reforço do quadro penal para a prevenção do auxílio à entrada, ao trânsito e à residência irregulares (JO 2002, L 328, p. 1).

infrações, a Decisão-Quadro 2003/568/JAI¹³¹, que define as infrações penais qualificadas de «corrupção ativa e passiva no setor privado», e a Decisão-Quadro 2008/841/JAI¹³², que define as infrações relativas à participação em organização criminosa.

124. Por outro lado, saliento que, como a Comissão corretamente observou, na falta de harmonização completa do direito penal material, não se pode censurar o legislador da União por não ter precisado melhor as infrações referidas no anexo II. Assim, ao contrário de que será observado mais adiante nas presentes conclusões a respeito da lista dos dados PNR contida no anexo I, a transposição para ao direito interno da lista de infrações do anexo II exige necessariamente que os Estados-Membros definam, em função das especificidades dos seus sistemas penais nacionais, as infrações suscetíveis de serem visadas. Esta operação deve, contudo, ser efetuada respeitando plenamente o critério segundo o qual qualquer ingerência nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta deve ser limitada ao estritamente necessário. Assim, por exemplo, não se pode excluir, na minha opinião, que os Estados-Membros prevejam que a utilização dos dados PNR seja limitada, quanto a certas infrações, como, por exemplo, as referidas nos pontos 7, 16, 17, 18 e 25 do anexo II, aos casos em que essas infrações revistam caráter transfronteiriço, ou sejam cometidas no âmbito de uma organização criminosa, ou comportem certas circunstâncias agravantes. Caberá aos órgãos jurisdicionais dos Estados-Membros, sob a fiscalização do Tribunal de Justiça, interpretar as disposições nacionais que transpõem para o direito interno a referida lista em conformidade tanto com a Diretiva PNR como com a Carta, de modo a que o tratamento dos dados PNR continue, quanto a cada rubrica, limitado às infrações que atinjam o elevado nível de gravidade exigido por esta diretiva e às infrações para as quais esse tratamento se revele pertinente¹³³.

125. Sem prejuízo das precisões apresentadas nos n.ºs 120 e 124 das presentes conclusões, considero que o artigo 3.º, ponto 9, da Diretiva PNR, bem como a lista de infrações contida no seu anexo II, satisfazem os requisitos de clareza e de precisão e não ultrapassam os limites do estritamente necessário.

126. Há que reconhecer, todavia, que a solução ilustrada no n.º 124 das presentes conclusões não é completamente satisfatória. Com efeito, por um lado, deixa uma margem de apreciação importante aos Estados-Membros, pelo que o âmbito de aplicação material do tratamento dos dados PNR é suscetível de variar consideravelmente de um Estado-Membro para outro, comprometendo, assim, o objetivo de harmonização prosseguido pelo legislador da União¹³⁴. Por outro lado, implica que a fiscalização da proporcionalidade de um elemento essencial do sistema, como a limitação das finalidades desse tratamento, seja exercida *ex post* sobre as medidas nacionais de transposição, em vez de ser exercida *ex ante* sobre a própria Diretiva PNR. Por conseguinte, seria desejável que, na hipótese de o Tribunal de Justiça decidir, como sugiro, considerar o artigo 3.º, ponto 9, da Diretiva PNR, bem como a lista de infrações contida no seu anexo II, conformes com os artigos 7.º, 8.º, e 52.º, n.º 1, da Carta, o Tribunal de Justiça chamasse a atenção do legislador da União para o facto de essa apreciação ser apenas provisória e implicar que esse legislador verifique, à luz da transposição feita pelos Estados-Membros dessa disposição e dessa lista, e com base nos dados estatísticos a que se refere o artigo 20.º da Diretiva PNR, a necessidade de: i) precisar melhor, restringindo o seu alcance, as categorias de infrações previstas na referida lista, ii) eliminar da mesma as infrações relativamente às quais o tratamento dos dados PNR se revele quer desproporcionado, quer não pertinente ou ineficaz, e iii) aumentar o limiar de

¹³¹ Decisão-Quadro do Conselho, de 22 de julho de 2003, relativa ao combate à corrupção no setor privado (JO 2003, L 192, p. 54).

¹³² Decisão-Quadro do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada (JO 2008, L 300, p. 42).

¹³³ V., nomeadamente, considerando 7 e 22 da Diretiva PNR.

¹³⁴ V. considerando 35 da Diretiva PNR.

gravidade das infrações previstas no artigo 3.º, ponto 9, da Diretiva PNR¹³⁵. A este respeito, observo que, embora o artigo 19.º, n.º 2, alínea b), da Diretiva PNR obrigue a Comissão a proceder ao reexame de todos os elementos desta diretiva, dando especial atenção «à necessidade e proporcionalidade da recolha e do tratamento dos dados PNR para cada um dos fins fixados» na mesma, nem o Relatório da Comissão de 2020, nem o Documento de trabalho de 2020 que o acompanha, contêm, na minha opinião, uma análise satisfatória quanto a este aspeto.

ii) Quanto às categorias de dados PNR previstas na Diretiva PNR (segunda e terceira questões prejudiciais)

127. A Diretiva PNR prevê a transferência para as UIP de 19 categorias de dados PNR recolhidos pelas transportadoras aéreas para efeitos da reserva de voos. Estas categorias, enumeradas no anexo I, correspondem às que surgem nos sistemas de reserva das companhias aéreas e às enumeradas no anexo I das Orientações sobre os dados dos registos de identificação dos passageiros adotadas pela Organização da Aviação Civil Internacional (OACI) em 2010¹³⁶ (a seguir «Orientações da OACI»).

128. Com a sua segunda questão prejudicial, o órgão jurisdicional de reenvio interroga-se sobre a validade do anexo I à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, tendo em conta, por um lado, a amplitude dos dados pessoais enumerados nesse anexo — nomeadamente os dados API referidos no seu ponto 18, na medida em que ultrapassam os dados enumerados no artigo 3.º, n.º 2, da Diretiva API — e, por outro, a possibilidade de esses dados, considerados em conjunto, revelarem dados sensíveis e violarem, assim, os limites do «estritamente necessário». Com a sua terceira questão prejudicial — que tem por objeto, como já tive ocasião de sublinhar, o respeito do primeiro dos três requisitos previstos no artigo 52.º, n.º 1, da Carta, segundo o qual qualquer ingerência num direito fundamental deve ser «prevista por lei» — a Cour constitutionnelle (Tribunal Constitucional, Bélgica) interroga, em contrapartida, o Tribunal de Justiça sobre a validade dos pontos 12 e 18 do anexo I, tendo em conta, nomeadamente, o seu carácter «aberto».

129. Uma vez que o exame a efetuar no âmbito da segunda questão prejudicial pressupõe o exame do carácter suficientemente claro e preciso das categorias de dados pessoais referidas no anexo I, abordarei em primeiro lugar a terceira questão prejudicial.

– Quanto ao carácter suficientemente claro e preciso dos pontos 12 e 18 do anexo I (terceira questão prejudicial)

130. Importa observar, a título preliminar, que a amplitude e a gravidade da ingerência nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta que uma medida que introduz limitações ao exercício destes direitos comporta depende, antes de mais, da extensão e da natureza dos dados pessoais que são objeto do tratamento. A identificação destes dados constitui, portanto, uma operação essencial, que qualquer base legal que introduza tal medida deve obrigatoriamente efetuar da forma mais clara e precisa possível.

¹³⁵ V., por analogia, Acórdãos de 16 de dezembro de 2008, Arcelor Atlantique et Lorraine e o. (C-127/07, EU:C:2008:728, n.ºs 61 e 62), bem como de 17 de outubro de 2013, Schaible (C-101/12, EU:C:2013:661, n.ºs 91 e 94).

¹³⁶ Ver documento 9944, aprovado pelo Secretário-Geral da OACI e publicado sob a sua autoridade. A versão em língua francesa deste documento está disponível em https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_fr.pdf. Em conformidade com o ponto 9.22 do anexo 9 (Facilitação) da Convenção sobre a Aviação Civil Internacional, assinada em Chicago, em 7 de dezembro de 1944 (a seguir «Convenção de Chicago»), os Estados contratantes desta convenção que exigem os dados PNR são obrigados a alinhar as suas necessidades em matéria de dados e o tratamento desses dados, nomeadamente, com essas orientações.

131. Este requisito foi reconhecido, no que respeita ao tratamento dos dados PNR, pelo Parecer 1/15. Pronunciando-se sobre as rubricas que figuram no anexo do Projeto de Acordo PNR Canadá-UE, que contêm a enumeração dos dados PNR previstos pelo acordo projetado, o Tribunal de Justiça considerou nomeadamente, nesse parecer, que o recurso a categorias gerais de informações que não determinem suficientemente a extensão dos dados a transferir, bem como o recurso a listas exemplificativas de dados que não fixam nenhuma limitação quanto à natureza e à amplitude das informações suscetíveis de figurarem na rubrica em causa, não satisfaziam os requisitos de clareza e de precisão.

132. É à luz destes princípios que há que examinar a terceira questão prejudicial.

133. No que respeita ao ponto 12 do anexo I, a sua redação é a seguinte:

«Observações gerais (designadamente todas as informações disponíveis sobre menores não acompanhados com idade inferior a 18 anos, como nome e sexo do menor, idade, língua(s) falada(s), nome e contactos da pessoa que o acompanha no momento da partida e sua relação com o menor, nome e contactos da pessoa que o acompanha no momento da chegada e sua relação com o menor, agente presente na partida e na chegada).»

134. Na medida em que visa as «observações gerais», este ponto constitui, à semelhança da rubrica 17 do anexo do Projeto de Acordo PNR Canadá-UE, uma rubrica dita de «texto livre», destinada a incluir qualquer informação recolhida pelas transportadoras aéreas no âmbito da sua atividade de prestação de serviços, além das expressamente enumeradas nos outros pontos do anexo I. Ora, há que constatar, como o Tribunal de Justiça o fez no n.º 160 do Parecer 1/15, que uma rubrica deste tipo «não fornece nenhuma indicação sobre a natureza e a extensão das informações que devem ser transmitidas e parece até suscetível de englobar informações desprovidas de qualquer relação com a finalidade da transferência dos dados PNR». Além disso, uma vez que a especificação entre parênteses que figura na redação do ponto 12 do anexo I, relativa às informações sobre os menores não acompanhados, é fornecida apenas a título de exemplo, como demonstra a utilização do termo «designadamente», este ponto não fixa nenhuma limitação quanto à natureza e à extensão das informações que o mesmo poderá conter¹³⁷.

135. Nestas condições, não se pode considerar que o ponto 12 do anexo I esteja delimitado com clareza e precisão suficientes.

136. Embora a Comissão e o Parlamento pareçam partilhar desta conclusão, os Estados-Membros que apresentaram observações sobre a terceira questão prejudicial, bem como o Conselho, opõem-se à mesma, com base em argumentos que coincidem em grande medida.

137. Em primeiro lugar, uma primeira série de argumentos visa, de maneira geral, colocar em causa a possibilidade de transpor para o presente processo as conclusões a que o Tribunal de Justiça chegou no Parecer 1/15.

138. A este respeito, embora esteja consciente da diferença de contexto que caracteriza os dois processos, limitar-me-ei aqui a observar que a conclusão a que o Tribunal de Justiça chegou no n.º 160 do Parecer 1/15 no que respeita à rubrica 17 do anexo do Projeto de Acordo PNR Canadá-UE se baseava numa interpretação exclusivamente semântica e estrutural desta rubrica.

¹³⁷ V., no mesmo sentido, Parecer 1/15, n.º 160.

Ora, tal interpretação é perfeitamente transponível para o ponto 12 do anexo I, cuja redação é, na parte não exemplificativa, idêntica à da referida rubrica e apresenta uma estrutura análoga. Por outro lado, como se verá mais pormenorizadamente em seguida, ambas as regras em questão estão inseridas no mesmo contexto regulamentar multilateral, constituído, nomeadamente, pelas Orientações da OACI, às quais o Tribunal de Justiça, aliás, se referiu expressamente no n.º 156 do Parecer 1/15. Nestas condições, não só nada obsta a que se siga, no ponto 12 do anexo I, a mesma interpretação que a adotada pelo Tribunal de Justiça no n.º 160 do Parecer 1/15 para a rubrica 17 do anexo do Projeto de Acordo PNR Canadá-UE, como, sobretudo, nada justifica um afastamento dessa interpretação.

139. Em segundo lugar, muitos Estados-Membros sublinham que os diferentes pontos do anexo I, incluindo o ponto 12, correspondem às rubricas do anexo I das Orientações da OACI, que as transportadoras aéreas conhecem bem e às quais são perfeitamente capazes de atribuir um conteúdo preciso. Este ponto 12 corresponderia, nomeadamente, às duas últimas rubricas do referido anexo, intituladas, respetivamente, «observações gerais» e «texto livre/campos de código em OSI [Other Supplementary Information], SSR [Special Service Request], SSI [Special Service Information], Observações/históricos» e que visam «informações suplementares» ou «relativas a serviços pedidos»¹³⁸.

140. A este respeito, observo, antes de mais, que a correspondência entre as rubricas do anexo I do Projeto de Acordo PNR Canadá-UE, por um lado, e as rubricas do anexo I das Orientações da OACI, por outro, não impediu o Tribunal de Justiça de declarar, no Parecer 1/15, que algumas das rubricas constantes do anexo I do referido projeto de acordo não satisfaziam os requisitos de clareza e de precisão a que deve obedecer uma medida que limita o exercício de direitos fundamentais. Seguidamente, observo que uma remissão, que não é, de resto, explícita¹³⁹, para as Orientações da OACI não permite, contrariamente ao que certos Estados-Membros parecem considerar, precisar melhor a natureza e a extensão das informações suscetíveis de ser visadas pelo ponto 12 do anexo I. Pelo contrário, a leitura destas orientações reforça a conclusão de que uma rubrica «texto livre», como o referido ponto 12, inclui um número indefinido de informações de diversa natureza, além das que figuram automaticamente nos PNR¹⁴⁰.

141. Em terceiro lugar, alguns governos sustentam que incumbe aos Estados-Membros, através de medidas legislativas internas e respeitando os limites impostos pelos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, precisar as informações suscetíveis de figurarem no ponto 12 do anexo I. Com efeito, a própria natureza de uma diretiva implicaria que se deixasse aos Estados-Membros uma margem discricionária quanto aos meios necessários para aplicar as disposições que a mesma prevê.

142. A este respeito, como já expus no n.º 86 das presentes conclusões, sou de opinião que, quando as medidas que comportam ingerências nos direitos fundamentais estabelecidos pela Carta têm origem num ato legislativo da União, incumbe ao legislador da União fixar, respeitando os critérios de clareza e de precisão acima referidos, bem como o princípio da proporcionalidade, o alcance exato destas ingerências. Daqui decorre que, quando o instrumento escolhido por este legislador é uma diretiva, não pode, na minha opinião, delegar-se nos Estados-Membros, aquando da transposição da mesma para os seus direitos nacionais, a

¹³⁸ V. pontos 2.1.2 e 2.1.5 das Orientações da OACI.

¹³⁹ A única referência às Orientações da OACI na Diretiva PNR figura no seu considerando 17 e diz apenas respeito aos «formatos de dados reconhecidos para as transferências de dados PNR pelas transportadoras aéreas para os Estados-Membros».

¹⁴⁰ Assim, o ponto 2.1.5 das referidas orientações menciona «informações suplementares» ou «relativas a serviços pedidos», que podem incidir «sobre pedidos de assistência médica ou de refeições especiais, “menores que viajem sozinhos”, pedidos de assistência, etc.». O ponto 2.1.6 precisa, por sua vez, que o «campo “observações gerais”» pode igualmente conter «certas informações, como as correspondências ou comunicações internas entre o pessoal das companhias aéreas e os agentes de reserva».

determinação de elementos essenciais que definem o alcance da ingerência, como, no que respeita a limitações aos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta, a natureza e o alcance dos dados pessoais sujeitos a tratamento.

143. Em quarto lugar, alguns Estados-Membros observam que o ponto 12 do anexo I deve ser entendido no sentido de visar unicamente informações relacionadas com a prestação de transporte. Interpretado deste modo, este ponto seria compatível com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta.

144. Este argumento também não me convence. Com efeito, antes de mais, as informações que podem figurar numa rubrica «observações gerais» e nos códigos OSI, SSI e SSR são de natureza muito heterogénea (cuidados médicos, refeições especiais ou preferências alimentares, qualquer pedido de assistência, informações relativas aos menores que viajem sozinhos, etc.)¹⁴¹ e todas têm uma relação com a prestação de transporte na medida em que visam, nomeadamente, permitir que a transportadora aérea adapte essa prestação às exigências de cada passageiro. Um critério interpretativo baseado na pertinência da informação relativamente à prestação de transporte não permite, portanto, precisar melhor o alcance deste ponto 12. Seguidamente, observo que, embora tenha recorrido, no n.º 159 do Parecer 1/15, a este critério para interpretar de modo conforme com os requisitos de clareza e de precisão uma rubrica diferente do anexo do Projeto de Acordo PNR Canadá-UE, o Tribunal de Justiça excluiu, todavia, que pudesse proceder do mesmo modo no que respeita à rubrica 17 deste anexo, correspondente ao ponto 12 do anexo I.

145. Em quinto lugar, alguns Estados-Membros destacaram o facto de as informações suscetíveis de serem visadas pelo ponto 12 do anexo I serem voluntariamente prestadas às transportadoras aéreas pelos próprios passageiros, que são devidamente informados da transferência posterior desses dados para as autoridades públicas. Parece-me que a ideia subjacente a este argumento é a de que existe uma espécie de consentimento implícito por parte do passageiro em causa para que os dados que fornece às companhias aéreas sejam posteriormente transferidos para as autoridades públicas.

146. A este respeito, o Tribunal de Justiça teve já a oportunidade de precisar que não se pode tratar de um «consentimento» quando a pessoa em causa não se pode opor livremente ao tratamento dos seus dados pessoais¹⁴². Ora, quanto a uma grande parte das informações suscetíveis de figurarem no ponto 12 do anexo I, o passageiro em causa não dispõe de uma verdadeira opção, mas é obrigado a fornecê-las para poder beneficiar da prestação de transporte. É o caso, nomeadamente, das pessoas com deficiência ou mobilidade reduzida, ou das pessoas que necessitam de assistência médica ou, ainda, dos menores não acompanhados. Recordo, por outro lado, que, nos n.ºs 142 e 143 do Parecer 1/15, o Tribunal de Justiça afirmou claramente que não se pode considerar que os tratamentos dos dados PNR pelas autoridades públicas, que prosseguem uma finalidade diferente daquela para a qual esses dados são recolhidos pelas transportadoras aéreas, se baseiam numa qualquer forma de consentimento dado pelos passageiros com vista a essa recolha.

147. Por último, a maior parte dos Estados-Membros alega que os tratamentos de dados previstos na Diretiva PNR estão rodeados de numerosas garantias, entre as quais, no que respeita à transferência de dados para as UIP, a obrigação que incumbe a estas de apagarem os dados que

¹⁴¹ V. pontos 2.1.5 e 2.1.6 das Orientações da OACI.

¹⁴² V. Acórdão de 17 de outubro de 2013, Schwarz (C-291/12, EU:C:2013:670, n.º 32), relativo ao caso de um requerente de passaporte obrigado a submeter-se à recolha das suas impressões digitais a fim de poder dispor de um documento que lhe permitisse efetuar deslocações com destino a um país terceiro.

não figuram no anexo I bem como os dados suscetíveis de revelar a raça ou origem étnica da pessoa, as suas opiniões políticas, a sua religião ou as suas convicções filosóficas, filiação sindical, o seu estado de saúde, a sua vida sexual ou a sua orientação sexual.

148. A este respeito, diria desde já que, na minha opinião, a apreciação do carácter suficientemente claro e preciso das regras que definem a extensão e a natureza dos dados que podem ser objeto de transferência para as autoridades públicas, na medida em que visa assegurar que uma medida que comporta ingerências nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta respeita os princípios da legalidade e da segurança jurídica, deve ser efetuada sem ter em conta as garantias que rodeiam os tratamentos a que esses dados serão sujeitos por parte das referidas autoridades, só sendo estas garantias tomadas em consideração no âmbito do exame da proporcionalidade da medida em causa. Foi, aliás, desta forma que o Tribunal de Justiça procedeu, nos n.ºs 155 a 163 do Parecer 1/15, à apreciação das rubricas do Projeto de Acordo PNR Canadá-UE. Acrescento, mais genericamente, que se deve prestar especial atenção à necessidade de manter uma clara distinção entre as diferentes fases do exame de uma medida que comporta ingerências nos direitos fundamentais, uma vez que uma amálgama destas diferentes fases será sempre, na minha opinião, em detrimento de uma proteção efetiva desses direitos.

149. Dito isto, limito-me aqui a salientar, por um lado, que a obrigação que incumbe às UIP, em conformidade com o artigo 6.º, n.º 1, da Diretiva PNR, de apagarem os dados que não os enumerados no anexo I só tem utilidade se este anexo contiver uma lista clara e fechada de dados a transferir. O mesmo se aplica à obrigação que incumbe às UIP, em conformidade com o artigo 13.º, n.º 4, da Diretiva PNR, de apagarem os dados ditos «sensíveis»¹⁴³. Com efeito, uma definição demasiado vaga, imprecisa ou aberta das informações que devem ser transmitidas aumenta tanto a probabilidade de tais dados serem indiretamente objeto de transferência como o risco de não serem imediatamente identificadas e apagadas. Por outras palavras, as garantias acima referidas só podem cumprir utilmente a sua função se as regras que definem a natureza e a extensão dos dados PNR que as transportadoras aéreas são chamadas a transferir para as UIP forem suficientemente claras e precisas e se a lista desses dados for de carácter fechado e exaustivo.

150. Com base em todas as considerações precedentes, e como já antecipei no n.º 135 das presentes conclusões, considero que o ponto 12 do anexo I, na parte em que inclui as «observações gerais» entre os dados que as transportadoras aéreas são obrigadas a transferir para as UIP em conformidade com a Diretiva PNR, não satisfaz os requisitos de clareza e de precisão exigidos pelo artigo 52.º, n.º 1, da Carta, conforme interpretado pelo Tribunal de Justiça¹⁴⁴, e deve, por conseguinte, nesta medida, ser declarado inválido.

151. Nas suas observações escritas, a Comissão e o Parlamento sugeriram ao Tribunal de Justiça que recorresse antes a uma «interpretação conforme» do ponto 12 do anexo I, lendo-o no sentido de que visa apenas as informações sobre os menores que aí são explicitamente mencionadas entre parênteses. Confesso que tenho alguma dificuldade em considerar que tal leitura respeita os limites de uma simples interpretação conforme. É decerto verdade que, segundo um princípio geral de interpretação, um ato da União deve ser interpretado, tanto quanto possível, de forma a não pôr em causa a sua validade e em conformidade com o direito primário no seu conjunto,

¹⁴³ Voltarei a esta categoria de dados mais adiante nas presentes conclusões.

¹⁴⁴ A FRA expressou-se neste sentido no seu Parecer 1/2011, p. 13. No seu parecer de 25 de março de 2011 sobre a Proposta de Diretiva PNR (https://edps.europa.eu/sites/edp/files/publication/11-03-25_pnr_en.pdf, ponto 47) (a seguir «Parecer da AEPD de 25 de março de 2011»), a AEPD propôs a exclusão da rubrica «Observações gerais» da lista do anexo I.

nomeadamente com as disposições da Carta¹⁴⁵. É igualmente verdade que, no que respeita à Diretiva PNR, a possibilidade desta interpretação afigura-se favorecida pela circunstância de muitos dos seus considerandos destacarem o pleno respeito dos direitos fundamentais, do direito ao respeito pela vida privada bem como do princípio da proporcionalidade¹⁴⁶. Todavia, é igualmente jurisprudência constante que uma interpretação conforme só é admissível se o texto de direito derivado da União for suscetível de mais do que uma interpretação e se, por conseguinte, for possível dar preferência àquela que torna a disposição conforme com o direito primário, em vez da que leva a declarar a sua incompatibilidade com este¹⁴⁷.

152. Ora, o ponto 12 do anexo I não é, na minha opinião, suscetível de ser interpretado como sugerem a Comissão e o Parlamento, a menos que dele se faça uma leitura «*contra legem*». Com efeito, este ponto visa, como expus atrás, uma categoria ampla de dados de diversas naturezas, não identificáveis *a priori*, relativamente à qual os dados sobre os menores constituem apenas uma subcategoria. Ler este ponto como se visasse apenas esta subcategoria não só equivaleria a ignorar uma parte do seu texto, como subverteria a ordem lógica do enunciado que este ponto contém. Essa operação, que consiste, em substância, em eliminar a parte da redação do ponto 12 do anexo I que seria considerada não conforme com os requisitos de clareza e de precisão, só pode ser efetuada, na minha opinião, declarando uma anulação parcial.

153. No que respeita à parte restante do ponto 12 do anexo I, que enumera uma série de dados relativos aos menores não acompanhados, sou de opinião de que preenche os requisitos de clareza e de precisão, desde que seja interpretada no sentido de que apenas abrange as informações relativas aos menores não acompanhados que tenham uma relação direta com o voo e que estejam expressamente previstas nesse ponto.

154. No que respeita ao ponto 18 do anexo I, a sua redação é a seguinte:

«Todas as informações prévias sobre os passageiros (dados API) que tenham sido recolhidas (incluindo, tipo e número de documento(s), país de emissão e termo de validade do(s) documento(s), nacionalidade, nome(s) e apelido(s), sexo, data de nascimento, companhia aérea, número de voo, data de partida, data de chegada, aeroporto de partida, aeroporto de chegada, hora de partida e hora de chegada).»

155. Este ponto apresenta uma estrutura análoga à do ponto 12 do anexo I. Menciona também uma categoria geral de dados, a saber, as informações prévias sobre os passageiros (Advance Passenger Information — API), seguida, entre parênteses, de uma lista de dados considerados incluídos nesta categoria geral, que é fornecida a título meramente exemplificativo, como demonstra o uso do termo «incluindo».

156. Todavia, ao contrário do ponto 12 do anexo I, o ponto 18 deste anexo remete para uma categoria de dados mais facilmente identificáveis no que respeita tanto à sua natureza como à sua extensão. Com efeito, resulta do considerando 4 da Diretiva PNR que, quando esta se refere a esta categoria de dados, visa as informações que, em conformidade com a Diretiva API, para a qual este

¹⁴⁵ V., nomeadamente, Acórdãos de 19 de novembro de 2009, *Sturgeon e o.* (C-402/07 e C-432/07, EU:C:2009:716, n.º 47 e jurisprudência referida); de 19 de setembro de 2013, *Reapreciação Comissão/Strack* (C-579/12 RX-II, EU:C:2013:570, n.º 40), bem como de 14 de maio de 2019, *M e o.* (Revogação do estatuto de refugiado) (C-391/16, C-77/17 e C-78/17, EU:C:2019:403, n.º 77 e jurisprudência referida).

¹⁴⁶ V., nomeadamente, considerandos 5, 7, 11, 15, 16, 20, 22, 23, 25, 27, 28, 31, 36 e 37 da Diretiva PNR.

¹⁴⁷ V. Acórdãos de 26 de junho de 2007, *Ordre des barreaux francophones et germanophone e o.* (C-305/05, EU:C:2007:383, n.º 28), bem como de 14 de maio de 2019, *M e o.* (Revogação do estatuto de refugiado) (C-391/16, C-77/17 e C-78/17, EU:C:2019:403, n.º 77).

considerando remete expressamente, são objeto de transmissão pelas transportadoras aéreas às autoridades nacionais competentes, a fim de melhorar os controlos nas fronteiras e de combater a imigração ilegal. Estes dados são enumerados no artigo 3.º, n.º 2, desta última diretiva.

157. Além disso, resulta do considerando 9¹⁴⁸ da Diretiva PNR bem como do artigo 3.º, n.º 2, da Diretiva API e da lista exemplificativa constante do ponto 18 do anexo I que os dados API visados pelo referido ponto são, por um lado, dados biográficos que permitem verificar a identidade do passageiro aéreo e, por outro, dados relativos ao voo reservado. No que respeita, mais precisamente, à primeira categoria, a dos dados biográficos, as informações enumeradas no artigo 3.º, n.º 2, da Diretiva API e no ponto 18 do anexo I abrangem dados, gerados no momento do registo, suscetíveis de serem recolhidos da zona de leitura ótica de um passaporte (ou outro documento de viagem)¹⁴⁹.

158. Assim, o ponto 18 do anexo I, interpretado à luz dos considerandos 4 e 9 da Diretiva PNR, identifica, em princípio, com suficiente clareza e precisão, pelo menos a natureza dos dados nele referidos.

159. No que respeita à sua extensão, há que observar, por um lado, que o artigo 3.º, n.º 2, da Diretiva API é também redigido de forma «aberta», sendo a lista de dados que enumera precedida da expressão «as informações acima referidas devem incluir»¹⁵⁰ e, por outro, que na categoria de dados API, conforme definida nos instrumentos multilaterais de harmonização nesta matéria, figuram igualmente dados diferentes dos visados tanto pela Diretiva API como pelo ponto 18 do anexo I¹⁵¹.

160. Nestas circunstâncias, para que o ponto 18 do anexo I satisfaça os requisitos de clareza e de precisão exigidos às bases legais que comportam ingerências nos artigos 7.º e 8.º da Carta, deve ser interpretado no sentido de que abrange apenas os dados API expressamente enumerados neste ponto bem como no artigo 3.º, n.º 2, da Diretiva API e que tenham sido recolhidos pelas transportadoras aéreas no exercício normal das suas atividades¹⁵².

¹⁴⁸ O considerando 9 prevê, na parte relevante para o presente processo, que «[a] utilização dos dados PNR em conjunto com os dados API contribui para ajudar os Estados-Membros a verificar a identidade dos indivíduos, reforçando, assim, a utilidade desse resultado para fins policiais e minimizando o risco de controlar e investigar pessoas inocentes».

¹⁴⁹ Neste sentido, v., igualmente, Proposta de Diretiva PNR, p. 7, ponto 1. Estes mesmos dados figuram nas orientações relativas às informações prévias respeitantes aos viajantes (IPRV) elaboradas pela Organização Mundial das Alfândegas (OMA), pela Associação do Transporte Aéreo Internacional (IATA) e pela 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 [(a seguir «Orientações IPRV»), ponto 8.1.5, alínea a)], como «principais elementos de dados suscetíveis de figurarem na zona de leitura ótica dos documentos de viagem oficiais».

¹⁵⁰ O artigo 3.º, n.º 2, da Diretiva API tem a seguinte redação: «As informações acima referidas devem incluir: o número e o tipo do documento de viagem utilizado, a nacionalidade, o nome completo, a data de nascimento, o ponto de passagem da fronteira à entrada no território dos Estados-Membros, o código do transporte, a hora de partida e de chegada do transporte, o número total de passageiros incluídos nesse transporte, o ponto inicial de embarque». Sublinho que, no seu Programa de trabalho para 2022, COM(2021) 645 final, p. 9, a Comissão previu uma atualização da Diretiva API. Em setembro de 2020, publicou uma avaliação desta diretiva que constitui a base para a sua futura revisão, SWD(2020) 174 final (a seguir «Documento de trabalho de 2020 sobre a Diretiva API»). No referido documento, a Comissão sublinha, nomeadamente, o facto de a lista de dados contida no artigo 3.º, n.º 2, da Diretiva API não estar em conformidade com as normas internacionais sobre os dados API, nomeadamente na medida em que não inclui todos os dados que figuram na zona de leitura ótica dos documentos de identidade (v., nomeadamente, p. 48).

¹⁵¹ V. Orientações IPRV, pontos 8.1.5, alíneas b) e c).

¹⁵² Figura no n.º 161 do Parecer 1/15 uma interpretação análoga da rubrica correspondente do Projeto de Acordo PNR Canadá-UE.

161. Importa, nesta fase, analisar sucintamente os outros pontos do anexo I que, tendo em conta a sua redação, revestem igualmente carácter «aberto» ou que não são suficientemente precisos, apesar de o órgão jurisdicional de reenvio não ter questionado expressamente o Tribunal de Justiça a seu respeito¹⁵³.

162. No que se refere, antes de mais, ao ponto 5 do anexo I, que menciona «endereço e informações de contacto (número de telefone, endereço de correio eletrónico)», embora se deva considerar que visa apenas os contactos expressamente referidos entre parênteses e reveste, portanto, carácter exaustivo, não precisa, contudo, como era o caso da rubrica correspondente do Projeto de Acordo PNR Canadá-UE¹⁵⁴, se esses contactos se referem apenas ao viajante ou aos terceiros que efetuaram a reserva do voo para o passageiro aéreo, aos terceiros por intermédio dos quais um passageiro aéreo pode ser contactado ou ainda aos terceiros que devem ser informados em caso de emergência¹⁵⁵. Tendo em conta o facto de que interpretar o ponto 5 do anexo I no sentido de visar igualmente as categorias de terceiros acima referidas alargaria a ingerência que comporta a Diretiva PNR a outras pessoas, além dos passageiros aéreos na aceção do artigo 3.º, ponto 4, da Diretiva PNR, sugiro ao Tribunal de Justiça, na falta de dados precisos que permitam considerar que a aquisição sistemática e generalizada dos contactos desses terceiros constitui um elemento estritamente necessário para a eficácia do sistema de tratamento dos dados PNR instituído por esta diretiva, que interprete o referido ponto no sentido de que visa apenas os contactos que nele são expressamente mencionados e que dizem respeito ao passageiro aéreo em nome do qual a reserva é feita. É certo que a Diretiva PNR não exclui que possam também ser objeto de transferência para as UIP os dados pessoais de outras pessoas que não os passageiros aéreos¹⁵⁶. Todavia, é essencial que as hipóteses em que tal é possível sejam indicadas de forma clara e explícita, como é o caso dos agentes de viagens, mencionados no anexo I, ponto 9, ou das pessoas que acompanham menores que viajam sozinhos, referidos no ponto 12 deste anexo. Com efeito, é só no caso de este requisito estar preenchido que se pode considerar que a decisão de incluir esses dados entre os dados que devem ser transferidos para as UIP foi objeto de uma ponderação entre os diferentes interesses em jogo, na aceção do considerando 15 da Diretiva PNR, e que os terceiros em causa podem ser adequadamente informados do tratamento dos seus dados pessoais.

163. No que respeita, seguidamente, ao ponto 6 do anexo I, que visa «[t]odas as informações sobre as modalidades de pagamento, incluindo o endereço de faturação», à semelhança do que o Tribunal de Justiça declarou no n.º 159 do Parecer 1/15, a respeito da rubrica correspondente do anexo do Projeto de Acordo PNR Canadá-UE, para respeitar os requisitos de clareza e de precisão, este ponto deve ser interpretado no sentido de que «é apenas relativ[o] às informações sobre as modalidades de pagamento e a faturação do bilhete de avião, excluindo qualquer outra informação sem relação direta com o voo». Por conseguinte, essas informações não podem incluir, por exemplo, as relativas às modalidades de pagamento de outros serviços não diretamente relacionados com o voo, como o aluguer de um veículo à chegada¹⁵⁷.

¹⁵³ Observo que está atualmente submetida à apreciação do Tribunal de Justiça uma série de questões prejudiciais que têm especificamente por objeto o carácter suficientemente preciso de vários pontos do anexo I, nomeadamente dos pontos 4, 8, 12 e 18 (v. processo pendente C-215/20).

¹⁵⁴ V. Parecer 1/15, n.º 158.

¹⁵⁵ Observo que as informações relativas à agência ou ao agente de viagens já estão abrangidas pelo ponto 5 do anexo I.

¹⁵⁶ V. definição de dados PNR no artigo 3.º, n.º 5, da Diretiva PNR.

¹⁵⁷ Neste sentido, v., igualmente, Conclusões do advogado-geral P. Mengozzi no Parecer 1/15, [(Acordo PNR UE-Canadá), EU:C:2016:656], n.º 218.

164. Quanto ao ponto 8, relativo às «[i]nformações de passageiro frequente», é definido pelas normas da OACI no sentido de respeitar ao número de conta e ao estatuto do passageiro frequente¹⁵⁸. Interpretado neste sentido, este ponto satisfaz os requisitos de clareza e de precisão.

165. No que respeita ao ponto 10 do anexo I, relativo à «[s]ituação do passageiro, incluindo confirmações, situação do registo, não comparência ou passageiro de última hora sem reserva» e ao ponto 13 deste anexo, relativo às «[i]nformações sobre a emissão dos bilhetes, incluindo número do bilhete, data de emissão, bilhetes só de ida, dados ATFQ (Automatic Ticket Fare Quote)», apesar da sua redação aberta, estes pontos visam apenas informações muito precisas e claramente identificáveis, diretamente relacionadas com o voo. O mesmo se aplica ao ponto 14 do anexo I, que respeita ao «[n]úmero do lugar e outras informações relativas ao lugar» e ao ponto 16 desse anexo, que respeita a «[t]odas as informações relativas às bagagens».

– *Quanto à extensão dos dados enumerados no anexo I (segunda questão prejudicial)*

166. Entre os elementos que o Tribunal de Justiça tem em conta para apreciar o caráter proporcionado de uma medida que comporta ingerências nos direitos consagrados nos artigos 7.º e 8.º da Carta figura o caráter adequado, pertinente e não excessivo dos dados pessoais tratados (princípio da «minimização dos dados»)¹⁵⁹. O mesmo critério é previsto pela jurisprudência do TEDH¹⁶⁰ e preconizado pela Convenção 108¹⁶¹.

167. Resulta do considerando 15 da Diretiva PNR que a lista dos dados PNR a transmitir às UIP foi elaborada com o objetivo simultâneo de refletir as exigências legítimas das autoridades públicas em matéria de luta contra o terrorismo e a criminalidade grave e de salvaguardar os direitos fundamentais à privacidade e à proteção dos dados pessoais, através da aplicação de «normas exigentes», de acordo com a Carta, com Convenção 108 e com a CEDH. O mesmo considerando precisa que os dados PNR devem incluir apenas, nomeadamente, informações sobre as reservas e os itinerários do passageiro que permitam às autoridades competentes identificar os passageiros aéreos que representem uma ameaça para a segurança interna.

168. No que respeita, em primeiro lugar, ao caráter adequado e pertinente dos dados PNR que figuram no anexo I, os diferentes pontos deste anexo, incluindo os pontos 5, 6, 8 e 18, conforme proponho interpretá-los¹⁶², bem como o ponto 12, com exceção da parte que proponho seja declarada inválida¹⁶³, visam apenas dados que fornecem informações diretamente relacionadas com as viagens aéreas abrangidas pelo âmbito de aplicação da Diretiva PNR. Estes dados têm, além disso, uma ligação objetiva com as finalidades prosseguidas por esta diretiva. Mais especificamente, os dados API são suscetíveis de ser utilizados, nomeadamente, «de forma reativa», a fim de identificar uma pessoa já conhecida dos serviços responsáveis pela aplicação da lei, por exemplo, por ser suspeita de estar implicada em infrações terroristas ou em formas de criminalidade grave que já tenham sido cometidas, ou de estar prestes a cometer tal infração, ao

¹⁵⁸ V. rubrica correspondente do apêndice I às Orientações da OACI.

¹⁵⁹ V., nomeadamente, neste sentido, Acórdão Digital Rights, n.º 57. Quanto ao requisito de as categorias de dados visadas por uma medida de acesso serem limitadas ao estritamente necessário para o objetivo prosseguido, v., mais recentemente, Acórdão Prokuratuur, n.º 38. O princípio da minimização dos dados está previsto, nomeadamente, no artigo 5.º, n.º 1, alínea c) do RGPD e no artigo 4.º, n.º 1, alínea c), da Diretiva Cooperação Policial.

¹⁶⁰ V., nomeadamente, TEDH, 18 de abril de 2013, M. K. c. França (CE:ECHR:2013:0418JUD001952209, § 35).

¹⁶¹ V. Relatório Explicativo da Convenção 108 de 1981 (<https://rm.coe.int/16800ca471>), artigo 5.º, ponto 40, bem como Relatório Explicativo da Convenção 108 modernizada, artigo 5.º, ponto 51.

¹⁶² V. n.ºs 154 a 158 e 162 a 164 das presentes conclusões.

¹⁶³ V. n.ºs 133 a 153 das presentes conclusões.

passo que os dados PNR são suscetíveis de ser utilizados sobretudo em «tempo real ou de forma proativa», a fim de identificar ameaças provenientes de pessoas ainda não conhecidas dos serviços responsáveis pela aplicação da lei.

169. No que respeita, em segundo lugar, à extensão dos dados PNR enumerados no anexo I, estes dados, incluindo os que figuram nos pontos 5, 6, 8, 12 e 18 deste anexo, conforme proponho interpretá-los nos n.ºs 134 a 164 das presentes conclusões, não se afiguram excessivos, tendo em conta, por um lado, a importância do objetivo de segurança pública prosseguido pela Diretiva PNR e, por outro, a aptidão do regime instituído por esta diretiva para prosseguir tal objetivo.

170. No que se refere, nomeadamente, aos dados API, sobre os quais se interroga em especial o órgão jurisdicional de reenvio, observo que estes dados, de ordem biográfica e relativos ao trajeto percorrido, só permitem, regra geral, extrair informações limitadas sobre a vida privada dos passageiros em causa. Por outro lado, embora seja verdade que o ponto 18 do anexo I visa informações que não figuram entre as expressamente mencionadas no artigo 3.º, n.º 2, da Diretiva API, estas informações, relativas à identidade do passageiro aéreo (o sexo), ao documento de viagem utilizado (país de emissão, termo de validade de qualquer documento de identidade), ou ainda o voo utilizado (companhia aérea, número de voo, data e aeroporto de partida e chegada), sobrepõem-se parcialmente ou podem ser extraídas dos dados PNR constantes de outros pontos do anexo I, por exemplo os pontos 3, 7 e 13. Além disso, na medida em que respeitem a dados biográficos ou aos documentos de viagem utilizados, tais informações são suscetíveis de ajudar os serviços responsáveis pela aplicação da lei a verificar a identidade de uma pessoa e reduzem, assim, como é observado no considerando 9 da Diretiva PNR, o risco de sujeitar pessoas inocentes a controlos e investigações injustificados. Por último, importa sublinhar que o simples facto de o ponto 18 do anexo I incluir dados adicionais relativamente aos que figuram no artigo 3.º, n.º 2, da Diretiva API não pode levar automaticamente a declarar o carácter excessivo destes dados, na medida em que esta diretiva e a Diretiva PNR prosseguem objetivos diferentes.

171. Quanto aos dados relativos aos menores não acompanhados, enumerados no ponto 12 do anexo I, os mesmos visam uma categoria de pessoas vulneráveis que beneficiam de uma proteção particular, incluindo no que toca ao respeito pela sua vida privada e à proteção dos seus dados pessoais¹⁶⁴. Todavia, uma limitação destes direitos pode revelar-se necessária, nomeadamente para proteger as crianças contra formas de criminalidade grave de que podem ser vítimas, como o tráfico e a exploração sexual de crianças ou o rapto de crianças. Por conseguinte, não se pode considerar *a priori* que o ponto 12 do anexo I, na medida em que exige a transferência de um maior número de dados pessoais no que respeita aos menores não acompanhados, excede o estritamente necessário.

172. Embora os dados pessoais que as transportadoras aéreas são obrigadas a transmitir às UIP em conformidade com a Diretiva PNR satisfaçam, na minha opinião, os requisitos de adequação e de pertinência e a sua extensão não exceda o estritamente necessário para o funcionamento do regime instituído por esta diretiva, não deixa de ser verdade que essa transmissão diz respeito a um número significativo de dados pessoais de natureza variada quanto a cada passageiro em causa, bem como a um número extremamente elevado desses dados em termos absolutos. Nestas circunstâncias, é primordial que essa transferência seja rodeada de garantias suficientes destinadas, por um lado, a assegurar que só sejam transferidos os dados expressamente referidos e, por outro, a garantir a segurança e a confidencialidade dos dados transferidos.

¹⁶⁴ O direito da criança ao respeito da sua vida privada está consagrado, nomeadamente, no artigo 16.º da Convenção de Nova Iorque sobre os Direitos da Criança, adotada em 20 de novembro de 1989 e que entrou em vigor em 2 de setembro de 1990.

173. A este respeito, importa observar, por um lado, que o legislador da União previu, antes de mais, uma série de garantias que permitem limitar as categorias de dados PNR tornadas acessíveis aos serviços responsáveis pela aplicação da lei e assegurar que esse acesso se mantém circunscrito apenas aos dados cujo tratamento seja considerado necessário para os fins dos objetivos prosseguidos pela Diretiva PNR. Assim, em primeiro lugar, esta diretiva enumera, sem prejuízo das considerações desenvolvidas no âmbito da resposta à terceira questão prejudicial, de forma exaustiva e precisa os dados que podem ser transferidos para as UIP. Em segundo lugar, a Diretiva PNR indica expressamente que só os dados contidos nessa lista, que resulta de uma ponderação entre os diferentes interesses e exigências mencionados no considerando 15 desta diretiva, podem ser objeto de transferência para as UIP (artigo 6.º, n.º 1, da Diretiva PNR). Em terceiro lugar, esta diretiva precisa que, quando os dados PNR transferidos comportem dados distintos dos enumerados no anexo I, a UIP apaga «imediate e definitivamente esses dados assim que os receber» (artigo 6.º, n.º 1, da Diretiva PNR). Em quarto lugar, a referida diretiva prevê que os dados PNR referidos no anexo I só podem ser objeto de transferência na medida em que já tenham sido recolhidos pelas transportadoras aéreas no exercício normal das suas atividades (artigo 8.º, n.º 1, e considerando 8 da Diretiva PNR), o que implica que nem todos os dados que figuram no anexo I são sistematicamente acessíveis às UIP, sendo-o apenas os que figuram no sistema de reservas do operador em causa. Em quinto lugar, o artigo 8.º, n.º 1, da Diretiva PNR impõe às transportadoras aéreas que utilizem o método de transferência por exportação («push») para transmitirem os dados PNR às UIP. Este método, recomendado pelas Orientações da OACI¹⁶⁵, implica que as transportadoras transferem elas próprias os dados PNR para as bases de dados das UIP. Em comparação com o método de transferência por extração («pull»), que permite às autoridades competentes aceder aos sistemas dos operadores e extrair das suas bases de dados uma cópia dos dados exigidos, o método de transferência por exportação apresenta mais garantias, uma vez que confere à transportadora aérea em causa o papel de guardião e de controlador dos dados PNR. Por último, em conformidade com as Orientações da OACI e com o princípio do «balcão único»¹⁶⁶, a Diretiva PNR prevê que a transferência dos dados PNR seja efetuada por intermédio de um único organismo, a UIP, que atua sob a supervisão do responsável previsto no artigo 5.º desta diretiva e, sobretudo, sob a da autoridade nacional de controlo prevista no artigo 15.º da referida diretiva.

174. Por outro lado, a Diretiva PNR prevê um certo número de garantias destinadas a preservar a *segurança* dos dados PNR. Remeto, a este respeito, para o artigo 13.º, n.º 2, desta diretiva, que torna aplicável a todos os tratamentos de dados pessoais efetuados nos termos da mesma os artigos 28.º e 29.º da Diretiva Cooperação Policial, respeitantes à confidencialidade do tratamento e à segurança dos dados, bem como para o n.º 3 deste mesmo artigo que, no que respeita ao tratamento dos dados PNR pelas transportadoras aéreas, recorda as obrigações que incumbem a estas últimas por força do RGPD, nomeadamente no que toca às medidas técnicas e organizativas adequadas para proteger a segurança e confidencialidade desses dados¹⁶⁷.

175. Por último, há que sublinhar que a Diretiva PNR reconhece, nos seus considerandos 29 e 37, o direito dos passageiros a receberem «informações precisas, de fácil acesso e compreensão», nomeadamente, sobre a recolha de dados PNR, requerendo aos Estados-Membros que

¹⁶⁵ V. ponto 2.7.3 das Orientações da OACI.

¹⁶⁶ V. ponto 2.7.4 das Orientações da OACI.

¹⁶⁷ A exigência de garantir a segurança e a fiabilidade da transferência dos dados para as UIP é, aliás, recordada no artigo 16.º, n.º 1, da Diretiva PNR no que respeita aos meios eletrónicos utilizados para essa transferência e foi um dos critérios que a Comissão cumpriu para efeitos da adoção, exigida no n.º 3 deste artigo, dos protocolos comuns e dos formatos de dados que as transportadoras aéreas devem utilizar aquando da referida transferência; v. Decisão de Execução (UE) 2017/759 da Comissão, de 28 de abril de 2017, relativa aos protocolos comuns e aos formatos de dados que as transportadoras aéreas devem utilizar para transferir dados PNR para as unidades de informações de passageiros (JO 2017, L 113, p. 48).

asseguem o respeito desse direito. Embora este reconhecimento não se traduza, no texto da Diretiva PNR, por uma disposição com valor vinculativo, recorro que, como indiquei no exame da primeira questão prejudicial, as disposições do RGPD são aplicáveis à transferência dos dados PNR para as UIP. Por conseguinte, as transportadoras aéreas estão obrigadas, no âmbito dessa transferência, a respeitar, nomeadamente, os artigos 13.º e 14.º do RGPD, que prevê o direito à informação das pessoas cujos dados pessoais tenham sido objeto de tratamento. Embora fosse conveniente que, no âmbito da transposição da Diretiva PNR, os Estados-Membros previssem expressamente o direito à informação dos passageiros aéreos, conforme reconhecido pelos considerandos 29 e 37 desta diretiva, estão, em qualquer caso, impedidos, por tal ser contrário ao espírito da mesma, de limitar o alcance dos artigos 13.º e 14.º do RGPD em aplicação do artigo 23.º, n.º 1, deste regulamento. Ora, para ser efetivo, tal direito deve abranger igualmente as categorias de dados PNR que são objeto de transferência.

176. Tendo em conta todas as considerações precedentes, sou de opinião que os dados PNR cujo tratamento é previsto pela Diretiva PNR, sem prejuízo das limitações sugeridas e das precisões apresentadas no âmbito do exame da terceira questão prejudicial, são pertinentes, adequados e não excessivos, à luz das finalidades prosseguidas por esta diretiva, e que a sua extensão não ultrapassa o estritamente necessário para realização dessas finalidades.

– *Quanto aos dados sensíveis*

177. A Diretiva PNR proíbe, em termos gerais, qualquer tratamento de «dados sensíveis»¹⁶⁸.

178. Embora esta diretiva não contenha uma definição do conceito de «dados sensíveis», resulta do seu artigo 13.º, n.º 4, que o mesmo inclui, pelo menos, os «dados PNR que revelem a raça ou origem étnica da pessoa, as suas opiniões políticas, religião ou convicções filosóficas, filiação sindical[,] saúde, vida ou orientação sexual»¹⁶⁹. No n.º 165 do Parecer 1/15, o Tribunal de Justiça precisou que qualquer medida baseada no pressuposto de que uma ou várias dessas características «poderiam, em si mesmas e independentemente do comportamento individual do passageiro em causa, ser pertinentes à luz da finalidade dos tratamentos dos dados PNR [...] violaria os direitos garantidos pelos artigos 7.º e 8.º da Carta, conjugados com o seu artigo 21.º». Ao proibir qualquer tratamento dos dados previstos no seu artigo 13.º, n.º 4, a Diretiva PNR respeita, portanto, os limites impostos pelo Tribunal de Justiça à utilização destas categorias de dados no âmbito de um sistema de tratamento dos dados PNR, seja ele abrangido pelo direito nacional, pelo direito da União ou por um acordo internacional celebrado pela União.

179. A proibição geral de tratamento de dados sensíveis prevista na Diretiva PNR inclui igualmente a sua *recolha*. Assim, como indica expressamente o considerando 15 desta diretiva, as 19 rubricas que figuram no anexo I não se baseiam nos dados PNR referidos no artigo 13.º, n.º 4, da mesma.

180. Embora nenhuma destas rubricas vise explicitamente tais dados, estes últimos poderiam, todavia, ser abrangidos pela rubrica «Observações gerais», prevista no ponto 12 do anexo I, que constitui um «campo aberto», que pode abranger, como já tive ocasião de observar no âmbito do exame da terceira questão prejudicial, um número indefinido de informações de diversas naturezas. Com efeito, existe um risco concreto, como o Tribunal de Justiça observou, aliás, no

¹⁶⁸ V. considerando 37 da Diretiva PNR.

¹⁶⁹ As categorias de dados pessoais enumeradas no artigo 13.º, n.º 4, da Diretiva PNR estão, todas elas, incluídas nas categorias que correspondem ao conceito de «categorias especiais de dados pessoais» a que se refere o artigo 9.º, n.º 1, do RGPD.

n.º 164 do Parecer 1/15, de que as informações abrangidas pela referida rubrica, relativas, por exemplo, a preferências dietéticas, a pedidos de assistência, a pacotes de preços para certas categorias de pessoas ou de associações, revelem, de forma direta, dados sensíveis na aceção do artigo 13.º, n.º 4, da Diretiva PNR, relativos, nomeadamente, às convicções religiosas dos passageiros em causa, ao seu estado de saúde ou à sua filiação num sindicato ou num partido político.

181. Ora, uma vez que o tratamento destes dados está, de qualquer forma, excluído pela Diretiva PNR, a sua transferência pelas transportadoras aéreas não só excede manifestamente o que é estritamente necessário, como se revela também desprovida de qualquer utilidade. A este respeito, importa sublinhar que o facto de as UIP serem em qualquer caso obrigadas, em conformidade com o artigo 13.º, n.º 4, segundo período, da Diretiva PNR, a apagar imediatamente os dados PNR que revelem uma das informações enumeradas no primeiro período deste número não permite autorizar ou justificar uma transferência desses dados¹⁷⁰, uma vez que a proibição de tratamento dos mesmos imposta pela referida diretiva deve operar a partir da primeira etapa de tratamento dos dados PNR. A obrigação de apagar dados sensíveis constitui, portanto, apenas uma garantia adicional que esta diretiva prevê para a hipótese de, excecionalmente, tais dados serem transferidos para as UIP por erro.

182. Saliento, por outro lado, como o advogado-geral P. Mengozzi observou no n.º 222 das suas conclusões no Parecer 1/15¹⁷¹, que, uma vez que as informações abrangidas pelas rubricas «texto livre», como a rubrica «Observações gerais», prevista no ponto 12 do anexo I, suscetíveis de conter dados sensíveis na aceção do artigo 13.º, n.º 4, da Diretiva PNR, só são comunicadas pelos passageiros de forma facultativa, é pouco provável que as pessoas implicadas em infrações de terrorismo ou de criminalidade grave procedam espontaneamente a essa comunicação, pelo que a transferência sistemática de tais dados só é suscetível de afetar, na sua maioria, pessoas que pediram para beneficiar de um serviço adicional que não tem, na realidade, qualquer interesse para os serviços responsáveis pela aplicação da lei¹⁷².

183. No âmbito do exame da terceira questão prejudicial, cheguei à conclusão de que o ponto 12 do anexo I, na parte em que visa a rubrica «Observações gerais», não satisfaz os requisitos de clareza e de precisão exigidos pelo artigo 52.º, n.º 1, primeiro período, da Carta. Pelas razões que acabo de expor, considero que a inclusão dessa rubrica nas categorias de dados que são objeto de transferência sistemática para as UIP, sem que seja incluída qualquer precisão quanto às informações que é suscetível de visar, também não satisfaz o critério de necessidade previsto no artigo 52.º, n.º 1, segundo período, da Carta, conforme interpretado pelo Tribunal de Justiça¹⁷³.

184. Todavia, excluir as rubricas ditas de «texto livre» da lista dos dados PNR a transferir para as autoridades estatais no âmbito de um sistema de tratamento dos dados PNR não basta para eliminar o risco de que dados sensíveis sejam, ainda assim, colocados à disposição dessas autoridades. Tais dados podem, com efeito, não só ser diretamente inferidos de informações abrangidas por essas rubricas, como também ser indiretamente revelados ou presumidos através

¹⁷⁰ A este respeito, não são pertinentes, na minha opinião, as alegações apresentadas por vários Estados-Membros que apresentaram observações sobre a segunda questão prejudicial, relativas à existência de meios técnicos que permitem apagar facilmente os dados sensíveis transmitidos pelas transportadoras aéreas.

¹⁷¹ Conclusões do advogado-geral P. Mengozzi no Parecer 1/15 (Acordo PNR UE-Canadá), EU:C:2016:656.

¹⁷² Saliento que mesmo as Orientações da OACI, embora não excluam que os dados sensíveis que podem ser extraídos das rubricas «texto livre» possam ser úteis na avaliação do risco que um passageiro pode representar, recomendam, todavia, aos Estados contratantes que assegurem que os mesmos só sejam tomados em consideração se existirem indicações concretas que exijam a sua utilização para os fins prosseguidos pelos seus regimes PNR.

¹⁷³ Recordo que tal exclusão já tinha sido sugerida pela AEPD no seu Parecer de 25 de março de 2011, n.º 47.

de informações contidas em rubricas «codificadas». Assim, para dar um exemplo, o nome do passageiro aéreo pode dar indicações ou, pelo menos, permitir avançar hipóteses sobre a origem étnica ou sobre a filiação religiosa do passageiro em causa. O mesmo se aplica à nacionalidade. Estes dados não se prestam, em princípio, a ser excluídos da lista de dados PNR a transferir, nem a ser apagados pelas autoridades habilitadas a recebê-los. Por conseguinte, a fim de evitar o risco de estigmatização, com base em características protegidas, de um grande número de pessoas que não são, todavia, suspeitas de qualquer infração, importa que um sistema de tratamento dos dados PNR preveja garantias suficientes que permitam excluir, em cada fase do tratamento dos dados recolhidos, que esse tratamento possa direta ou indiretamente ter em conta essas características, por exemplo, através da aplicação, na análise automatizada, de seletores baseados nessas características. Voltarei a este ponto na sequência do meu exame.

185. Com base em todas as considerações precedentes, considero, sem prejuízo da conclusão a que cheguei no n.º 183, *supra*, que a Diretiva PNR prevê, na fase da transferência dos dados PNR para as UIP, garantias suficientes destinadas a proteger os dados sensíveis.

iii) Quanto ao conceito de «passageiro» (quarta questão prejudicial)

186. Com a sua quarta questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se o sistema estabelecido pela Diretiva PNR, na medida em que permite a transferência e o tratamento generalizados dos dados PNR de qualquer pessoa que corresponda ao conceito de «passageiro», na aceção do artigo 3.º, ponto 4, desta diretiva, independentemente de qualquer elemento objetivo que permita considerar que a pessoa em causa é suscetível de representar um risco para a segurança pública, é compatível com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta. O órgão jurisdicional de reenvio interroga-se, nomeadamente, sobre a possibilidade de transpor para o sistema de tratamento de dados pessoais instituído pela Diretiva PNR a jurisprudência do Tribunal de Justiça em matéria de conservação e de acesso aos dados no setor das comunicações eletrónicas.

187. Nesta jurisprudência, na parte que tem interesse para o presente processo, o Tribunal de Justiça concluiu que uma regulamentação que prevê a *conservação* preventiva generalizada e indiferenciada de dados de tráfego relativos às comunicações eletrónicas e de dados de localização¹⁷⁴, com vista ao acesso por parte das autoridades responsáveis pela aplicação da lei, sem que seja estabelecida nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido, não pode, em princípio, ser considerada justificada numa sociedade democrática¹⁷⁵. O Tribunal de Justiça decidiu do mesmo modo a respeito de uma regulamentação nacional que, com vista ao combate ao terrorismo, previa a *análise automatizada da totalidade dos referidos dados* através de uma filtragem efetuada pelos prestadores de serviços de comunicações eletrónicas a pedido das autoridades nacionais competentes e em aplicação de parâmetros fixados por estas¹⁷⁶. Segundo o Tribunal de Justiça, tais medidas só podem ser justificadas em situações em que o Estado-Membro em causa se encontra perante uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, e desde que decisão que prevê a sua aplicação seja objeto de fiscalização efetiva quer por um órgão jurisdicional, quer por uma

¹⁷⁴ Trata-se de dados suscetíveis de fornecerem informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais que utiliza.

¹⁷⁵ V., neste sentido, Acórdãos *La Quadrature du Net*, n.ºs 141 a 145 e *Tele2 Sverige*, n.ºs 105 e 106, proferidos no âmbito da interpretação do artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, bem como Acórdão *Digital Rights*, n.ºs 57 e 58, no qual o Tribunal de Justiça declarou a invalidade da Diretiva 2006/24.

¹⁷⁶ V. Acórdão *La Quadrature du Net*, n.º 177.

entidade administrativa independente¹⁷⁷. O recurso a estas medidas em tais situações deve, além disso, segundo o Tribunal de Justiça, ser temporalmente limitado ao estritamente necessário e não pode, em qualquer caso, ter carácter sistemático¹⁷⁸.

188. Observo, por outro lado, que embora nesta jurisprudência o Tribunal de Justiça não tenha chegado ao ponto de declarar expressamente, como no Acórdão Schrems I, a existência de uma violação do conteúdo essencial do direito ao respeito pela vida privada, considerou, no entanto, que as medidas em causa atingiam um tal nível de gravidade da ingerência que, salvo no caso limitado de ameaças específicas à segurança nacional de um Estado-Membro, não podiam pura simplesmente ser consideradas limitadas ao estritamente necessário e, portanto, conformes com a Carta¹⁷⁹, independentemente das eventuais garantidas previstas contra os riscos de abusos e de acesso ilícito aos dados em causa¹⁸⁰.

189. Já tive oportunidade de sublinhar que uma regulamentação como a prevista pela Diretiva PNR partilha, com medidas do tipo das examinadas pelo Tribunal de Justiça na jurisprudência recordada nos números anteriores, um certo número de elementos comuns que lhe conferem um carácter particularmente intrusivo. Assim, esta diretiva institui um sistema generalizado e indiferenciado de recolha e de análise automatizada dos dados pessoais de uma parte significativa da população, que se aplica de forma global a todas as pessoas que correspondam ao conceito de «passageiro» que figura no artigo 3.º, ponto 4, da referida diretiva e, por conseguinte, também àquelas quanto às quais não existe qualquer indício suscetível de levar a crer que os seus comportamentos possam ter uma relação, ainda que indireta ou longínqua, com atividades de terrorismo ou de criminalidade grave. É nestas circunstâncias que o órgão jurisdicional de reenvio coloca a questão de saber se esta jurisprudência é transponível para um sistema de tratamento dos dados PNR como o instituído pela Diretiva PNR.

190. A este respeito, observo que, no Parecer 1/15, ao examinar, nos seus n.ºs 186 a 189, o âmbito de aplicação *ratione personae* do Projeto de Acordo PNR Canadá-UE, o Tribunal de Justiça evitou qualquer paralelismo entre, por um lado, as medidas que visavam a conservação e o acesso generalizado e indiferenciado ao conteúdo das comunicações eletrónicas, aos dados de tráfego e aos dados de localização e, por outro, a transferência dos dados PNR e o seu tratamento automatizado no âmbito da avaliação prévia dos passageiros visada pelo referido acordo. Já existia, contudo, à data da prolação deste parecer, uma jurisprudência bem assente – confirmada, alguns meses apenas antes dessa prolação, pelo Acórdão Tele2 Sverige, para o qual remete o órgão jurisdicional de reenvio – em que as referidas medidas eram, salvo em situações específicas e pontuais¹⁸¹, declaradas incompatíveis com a Carta¹⁸². Os acórdãos mais recentes do Tribunal de Justiça neste domínio, nomeadamente o Acórdão La Quadrature du Net, seguem a esteira desta jurisprudência, precisando-a e, quanto a certos aspetos, matizando-a.

¹⁷⁷ V. Acórdão La Quadrature du Net, n.ºs 134 a 139 e 177. Segundo o Tribunal de Justiça, a responsabilidade que incumbe aos Estados-Membros em matéria de segurança nacional «corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade e inclui a prevenção e a repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas»; v. Acórdãos La Quadrature du Net, n.º 135, e Privacy International, n.º 74.

¹⁷⁸ V. Acórdão La Quadrature du Net, n.ºs 138 e 178.

¹⁷⁹ V., nomeadamente, Acórdão La Quadrature du Net, n.ºs 141 a 145.

¹⁸⁰ V. Acórdão La Quadrature du Net, n.ºs 115 e 116; v., igualmente, Conclusões do advogado-geral M. Campos Sánchez-Bordona nos processos apensos SpaceNet e Telekom Deutschland (C-793/19 e C-794/19, EU:C:2021:939, n.ºs 74 e 75).

¹⁸¹ V. Acórdão Tele2 Sverige, n.º 119.

¹⁸² V., neste sentido, Acórdão Tele2 Sverige, n.ºs 103 a 107 e 119, bem como jurisprudência referida.

191. Nos referidos números do Parecer 1/15, o Tribunal de Justiça considerou explicitamente que não se afigurava que o Acordo PNR Canadá-UE ultrapassasse os limites do estritamente necessário na medida em que permitia a *transferência* e o *tratamento automatizado*, para efeitos da sua avaliação prévia, dos dados PNR de todos os passageiros aéreos com destino ao Canadá, apesar de ter considerado que essa transferência e esse tratamento eram feitos «independentemente de qualquer elemento objetivo que permita considerar que os passageiros são suscetíveis de representar um risco para a segurança pública no Canadá»¹⁸³. No n.º 187 deste parecer, o Tribunal de Justiça foi ao ponto de afirmar que «a exclusão de certas categorias de pessoas ou de certas zonas de origem poderia obstar à realização do objetivo do tratamento automatizado dos dados PNR, em concreto, a identificação, através de uma verificação destes dados, das pessoas suscetíveis de representar um risco para a segurança pública, de entre todos os passageiros aéreos, e permitir que esta verificação pudesse ser contornada»¹⁸⁴.

192. Assim, pelo menos no que respeita à transferência generalizada e indiferenciada dos dados PNR, o Tribunal de Justiça demarcou-se da abordagem, mais rigorosa, adotada em matéria de conservação e de acesso aos metadados.

193. Embora seja inegável que, no seu raciocínio, o Tribunal de Justiça teve em conta, como resulta nomeadamente dos n.ºs 152 e 188 do Parecer 1/15, por um lado, a constatação de que o tratamento automatizado dos dados PNR facilita os controlos de segurança, nomeadamente nas fronteiras, e, por outro, o facto de, em conformidade com a Convenção de Chicago, os passageiros aéreos que pretendam entrar no território de um Estado parte dessa Convenção deverem sujeitar-se aos controlos e respeitar as condições de entrada e de saída prescritas por esse Estado, incluindo a verificação dos seus dados PNR, considero que existem outras razões que militam a favor de tal diferença de abordagem, entre as quais se encontra, em primeiro lugar, a natureza dos dados tratados.

194. O Tribunal de Justiça sublinhou reiteradamente que não só o conteúdo das comunicações eletrónicas, como também os metadados, são suscetíveis de revelar informações sobre «um número significativo de aspetos da vida privada das pessoas em causa, incluindo informações sensíveis, tais como a orientação sexual, as opiniões políticas, as convicções religiosas, filosóficas, sociais ou outras, bem como o estado de saúde», que esses dados, considerados no seu todo, «podem permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam» e que os referidos dados fornecem, em especial, os meios para determinar «o perfil das pessoas em causa, informação tão sensível, à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações»¹⁸⁵. Recordo, por outro lado, que as regulamentações até agora examinadas pelo Tribunal de Justiça, incluindo a contida na Diretiva 2006/24, não previam qualquer exceção e aplicavam-se igualmente às comunicações para ou de serviços de carácter social ou religioso ou de profissionais sujeitos a obrigações de segredo profissional. Assim, embora sem demonstrar uma violação do conteúdo essencial do direito ao respeito pela vida privada, o Tribunal de Justiça afirmou, todavia, que,

¹⁸³ V. Parecer 1/15, n.ºs 186 e 187.

¹⁸⁴ Nos Acórdãos Digital Rights (n.º 59) e Tele2 Sverige (n.º 111), tal como na jurisprudência posterior (v., nomeadamente, Acórdão La Quadrature du Net, n.ºs 143 a 150), é precisamente o facto de a regulamentação em causa não se basear em «elementos objetivos» do tipo dos mencionados pelo Tribunal de Justiça no n.º 187 do Parecer 1/15, que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, que torna esta regulamentação não proporcionada.

¹⁸⁵ V. Acórdão La Quadrature du Net (n.º 117 e jurisprudência referida); v., igualmente, Acórdão Prokuratuur (n.º 36).

«tendo em conta o caráter sensível das informações que os dados de tráfego e os dados de localização podem fornecer, a sua confidencialidade é essencial para o direito ao respeito da vida privada»¹⁸⁶.

195. Em contrapartida, embora seja verdade que, como recordei nos n.ºs 77 e 98 das presentes conclusões, o Tribunal de Justiça reconheceu, no Parecer 1/15, que os dados PNR podem, se for caso disso, revelar informações muito precisas sobre a vida privada de uma pessoa¹⁸⁷, afirmou, no entanto, que a natureza dessas informações está limitada a certos aspetos dessa vida privada¹⁸⁸, o que torna o acesso a tais dados menos intrusivo do que o acesso ao conteúdo das comunicações eletrónicas bem como aos dados de tráfego e aos dados de localização.

196. Em segundo lugar, não só a natureza dos dados PNR difere da dos dados de tráfego e dos dados de localização, como difere também o número e a variedade das informações suscetíveis de serem reveladas por essas diversas categorias de dados, sendo as contidas nos dados PNR mais limitadas tanto quantitativamente como qualitativamente. Tal depende não só da circunstância de os sistemas de tratamento generalizado e indiferenciado dos dados relativos às comunicações eletrónicas serem suscetíveis de dizer respeito à quase totalidade da população em causa, ao passo que os sistemas de tratamento dos dados PNR se aplicam a um círculo mais restrito, embora numericamente significativo, de pessoas, mas também da frequência de utilização dos meios de comunicações eletrónicas e da sua multiplicidade. Por outro lado, a Diretiva PNR prevê a recolha e o tratamento de um número limitado e exaustivamente determinado de dados PNR, com exclusão dos dados abrangidos pelas categorias enumeradas no artigo 13.º, n.º 4, desta diretiva, pelo que, pelo menos a sensibilidade, senão a quantidade, das informações sobre a vida privada das pessoas em causa que daí podem decorrer são suscetíveis de ser, em parte, apreciadas antecipadamente¹⁸⁹. Ora, tal limitação da tipologia dos dados visados, que permite excluir uma grande parte dos que podem conter informações sensíveis, só é possível parcialmente no que respeita aos dados de tráfego e aos dados de localização, tendo em conta o número de utilizadores e de meios de comunicação em causa¹⁹⁰.

197. Em terceiro lugar, qualquer tratamento dos metadados das comunicações eletrónicas não só é suscetível de afetar a esfera íntima da vida da quase totalidade da população, como interfere também no exercício de outras liberdades através das quais se exerce a participação de cada pessoa na vida social e democrática de um país¹⁹¹, com o risco, nomeadamente, de produzir um efeito dissuasivo sobre a liberdade de expressão dos utilizadores dos meios de comunicações eletrónicas¹⁹², que constitui «um dos fundamentos essenciais de uma sociedade democrática e pluralista», fazendo parte dos valores nos quais se baseia a União¹⁹³. Este aspeto é inerente às medidas relativas a essas categorias de dados pessoais, não dizendo respeito, em princípio, aos sistemas de tratamento dos dados PNR.

¹⁸⁶ Acórdão La Quadrature du Net, n.º 142.

¹⁸⁷ V. Parecer 1/15, n.ºs 128 e 150.

¹⁸⁸ V. Parecer 1/15, n.º 150.

¹⁸⁹ Quanto à dificuldade dessa apreciação no que respeita aos metadados, v. Acórdão Prokuratuur, n.º 40.

¹⁹⁰ O legislador alemão fez um esforço nesse sentido na regulamentação que é objeto dos processos apensos C-793/19 e C-794/19, SpaceNet e Telekom Deutschland, em que o advogado-geral M. Campos Sánchez-Bordona apresentou as suas Conclusões (EU:C:2021:939, n.ºs 60 e 61).

¹⁹¹ Remeto, a este respeito, para o n.º 93 das presentes conclusões.

¹⁹² V. Acórdão La Quadrature du Net, n.º 118 e jurisprudência referida.

¹⁹³ V. Acórdão Tele2 Sverige, n.º 93.

198. Em quarto lugar, devido principalmente ao número e à variedade das informações sensíveis que podem ser extraídas do conteúdo das comunicações eletrônicas, bem como dos dados de tráfego e dos dados de localização, existe um risco de arbitrariedade associado ao tratamento desses dados significativamente mais elevado do que no que respeita aos sistemas de tratamento dos dados PNR.

199. Por todas as razões que acabo de expor, sou de opinião que a abordagem mais estrita adotada pelo Tribunal de Justiça no domínio das comunicações eletrônicas não é transponível, enquanto tal, para os sistemas de tratamento dos dados PNR. O Tribunal de Justiça já se pronunciou neste sentido, pelo menos implicitamente, no Parecer 1/15, no contexto de um acordo internacional que instituíra tal sistema para efeitos da proteção da segurança de um país terceiro. A mesma posição justifica-se, na minha opinião, por maioria de razão, no que respeita à Diretiva PNR, cujo objetivo é a proteção da segurança interna da União.

200. Dito isto, há que salientar, como o fez o advogado-geral P. Mengozzi no n.º 216 das suas Conclusões no Parecer 1/15¹⁹⁴, que o próprio interesse dos sistemas de tratamento dos dados PNR, quer sejam adotados de forma unilateral quer sejam objeto de um acordo internacional, é precisamente garantir a transmissão maciça de dados que permitam às autoridades competentes identificar, com o auxílio de instrumentos de tratamento automatizado e de cenários ou critérios de avaliação preestabelecidos, pessoas desconhecidas dos serviços responsáveis pela aplicação da lei, mas que pareçam apresentar um «interesse» ou um risco para a segurança pública e sejam, por isso, suscetíveis de ser posteriormente submetidas a controlos individuais mais rigorosos. A exigência de uma «suspeita razoável» que é afirmada na jurisprudência do TEDH relativa às interceções direcionadas praticadas no âmbito de um inquérito criminal¹⁹⁵ e na do Tribunal de Justiça relativa à conservação dos metadados¹⁹⁶ é, por conseguinte, menos pertinente no contexto de tal transmissão e de tal tratamento¹⁹⁷. O objetivo, nomeadamente, de prevenção prosseguido por tais regimes também não poderia ser realizado limitando a sua aplicação a uma categoria determinada de pessoas, como o Tribunal de Justiça afirmou, de resto, nos números do Parecer 1/15 recordados no n.º 191 das presentes conclusões, pelo que se afigura que o alcance da Diretiva PNR assegura a realização efetiva desse objetivo¹⁹⁸.

201. Há que sublinhar igualmente que a importância estratégica do tratamento dos dados PNR enquanto instrumento essencial da resposta comum da União ao terrorismo e à criminalidade grave e enquanto componente importante da União da segurança foi várias vezes destacada pela Comissão¹⁹⁹. No âmbito de uma «abordagem global» para a luta contra o terrorismo, o papel desempenhado pelos sistemas de tratamento dos dados PNR foi também reconhecido pelo Conselho de Segurança das Nações Unidas que, na Resolução 2396 (2017)²⁰⁰, impôs aos Estados membros das Nações Unidas a obrigação de «desenvolver a capacidade de recolher, tratar e analisar, em conformidade com as [normas e práticas recomendadas] da OACI, os dados [PNR], bem como de assegurar que esses dados sejam utilizados e partilhados com todas as suas autoridades nacionais competentes no pleno respeito dos direitos humanos e das liberdades

¹⁹⁴ Conclusões do advogado-geral P. Mengozzi no Parecer 1/15 [(Acordo PNR UE-Canadá), EU:C:2016:656].

¹⁹⁵ V., nomeadamente, TEDH, 4 de dezembro de 2015, Roman Zakharov c. Rússia (CE:ECHR:2015:1204JUD004714306, § 260).

¹⁹⁶ V. Acórdãos La Quadrature du Net (n.ºs 146 a 151) e Tele2 Sverige (n.º 119).

¹⁹⁷ Neste sentido, no que se refere às medidas de interceção de massa, v. Acórdão Big Brother Watch, § 348.

¹⁹⁸ V., por analogia, Acórdão de 3 de outubro de 2019, A e o. (C-70/18, EU:C:2019:823, n.º 61).

¹⁹⁹ V., recentemente, Comunicação da Comissão sobre a Estratégia da UE para a União da Segurança [COM(2020) 605 final, p. 28], bem como Comunicação da Comissão: Uma Agenda da EU em matéria de Luta contra o Terrorismo: Antecipar, Prevenir, Proteger, Responder [COM(2020) 795 final, pp. 15 e segs.]

²⁰⁰ Resolução de 21 de dezembro de 2017 [a seguir «Resolução 2396 (2017)»], [https://undocs.org/fr/S/RES/2396\(2017\)](https://undocs.org/fr/S/RES/2396(2017)).

fundamentais, para efeitos de prevenção, deteção e investigação de infrações terroristas e viagens conexas»²⁰¹. Esta obrigação é reafirmada na Resolução 2482/2019 em matéria de terrorismo e de criminalidade transnacional grave²⁰².

202. Neste contexto, a adoção de um sistema de tratamento dos dados PNR harmonizado a nível da União, no que respeita tanto aos voos extra-UE como, quanto aos Estados que aplicaram o artigo 2.º da Diretiva PNR, os voos intra-UE, permite assegurar que o tratamento desses dados seja efetuado respeitando o elevado nível de proteção dos direitos consagrados nos artigos 7.º e 8.º da Carta fixado por esta diretiva e proporciona um sistema jurídico de referência para a negociação de acordos internacionais sobre o tratamento e a transferência dos dados PNR²⁰³.

203. Por outro lado, embora seja verdade que o sistema instituído pela Diretiva PNR visa de forma indiferenciada todos os passageiros aéreos, como o Parlamento sublinhou, com razão, nas suas observações escritas e como salientou igualmente o Conselho de Segurança das Nações Unidas na Resolução 2396 (2017), que evoca o risco concreto de utilização da aviação civil para fins terroristas, simultaneamente como meio de transporte e como alvo²⁰⁴, existe uma ligação objetiva entre o transporte aéreo e as ameaças para a segurança pública relacionadas, nomeadamente, com o terrorismo e, pelo menos, com certas formas de criminalidade grave, como, em particular, o tráfico de droga ou o tráfico de seres humanos, que têm, de resto, uma forte componente transfronteiriça.

204. Importa, enfim, sublinhar, como alegaram o Parlamento, o Conselho e vários Estados-Membros que apresentaram observações escritas, que os passageiros aéreos à entrada ou à saída da União são obrigados a submeter-se a controlos de segurança²⁰⁵. A transferência e o tratamento dos dados PNR antes da sua chegada ou antes da sua partida facilita e acelera esses controlos, como o Tribunal de Justiça observou igualmente no Parecer 1/15, permitindo que os serviços responsáveis pela aplicação da lei se concentrem nos passageiros quanto aos quais disponham de elementos factuais que indiquem um risco real para a segurança²⁰⁶.

205. Por último, no que respeita, nomeadamente, à extensão do sistema da Diretiva PNR aos voos intra-UE, embora não possa ser excluído *a priori* qualquer impacto sobre a liberdade de circulação dos cidadãos da União, consagrada, nomeadamente, no artigo 45.º da Carta, a ingerência na vida privada que a Diretiva PNR comporta, ainda que grave, não é, na minha opinião, suscetível de implicar, em si mesma, um efeito dissuasivo no exercício dessa liberdade, uma vez que o

²⁰¹ V. Resolução 2396 (2017), ponto 12; neste mesmo ponto 12, o Conselho de Segurança das Nações Unidas «exorta a OACI a colaborar com os Estados contratantes com vista a estabelecer uma norma para a recolha, utilização, tratamento e proteção dos dados PNR». Na sequência desse convite, em 23 de junho de 2020, a OACI adotou a alteração n.º 28 do anexo 9 da Convenção de Chicago que, como já foi referido, estabelece um novo conjunto de normas internacionais em matéria de facilitação e cujo capítulo 9, secção D, diz especificamente respeito aos PNR. Em 12 de janeiro de 2021, a Comissão adotou uma Proposta de decisão do Conselho relativa à posição a adotar, em nome da União Europeia, na [OACI] relativamente a esta alteração [COM(2021) 16 final].

²⁰² Resolução de 19 de julho de 2019, ponto 15, c), [https://undocs.org/fr/S/RES/2482\(2019\)](https://undocs.org/fr/S/RES/2482(2019)).

²⁰³ Existem atualmente dois acordos internacionais celebrados pela União, respetivamente com a Austrália [Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de [dados PNR] pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano (JO 2012, L 186, p. 4)] e com os Estados Unidos da América [Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos [dados PNR] para o Departamento da Segurança Interna dos Estados Unidos (JO 2012, L 215, p. 5)]. Está em curso uma avaliação conjunta destes dois acordos, com vista à celebração de novos acordos. Em 18 de fevereiro de 2020, o Conselho autorizou, além disso, a Comissão a encetar negociações com o Japão.

²⁰⁴ V. Resolução 2396 (2017), p. 4.

²⁰⁵ Incluindo as pessoas que beneficiam do direito de livre circulação ao abrigo do direito da União; v. Regulamento (UE) 2017/458 do Parlamento Europeu e do Conselho, de 15 de março de 2017, que altera o Regulamento (UE) 2016/399 no que diz respeito ao reforço dos controlos nas fronteiras externas por confronto com as bases de dados pertinentes (JO 2017, L 74, p. 7).

²⁰⁶ Neste sentido, v., igualmente, Parecer 1/15, n.º 187. V., igualmente, Comunicação da Comissão sobre a abordagem global relativa à transferência dos dados [PNR] para países terceiros [COM(2010) 492 final, p. 6, ponto 2.2].

tratamento de dados PNR pode até ser entendido pelo público como uma medida necessária para garantir a segurança das viagens por via aérea²⁰⁷. Todavia, a eventualidade desse efeito dissuasivo deve ser objeto de uma avaliação e de uma monitorização contínuas.

206. Contudo, a fim de respeitar a jurisprudência recordada nos n.ºs 107 e 108 das presentes conclusões, a Diretiva PNR não se pode limitar a exigir que o acesso e o tratamento automatizado dos dados PNR de todos os passageiros aéreos responda à finalidade prosseguida, mas deve igualmente prever, de forma clara e precisa, as condições materiais e processuais que regem esse acesso e esse tratamento, bem como a utilização posterior desses dados²⁰⁸, e prever garantias adequadas em cada fase desse processo. Já evoquei, ao examinar a segunda questão prejudicial, as garantias que rodeiam a transferência dos dados PNR para as UIP. Analisarei, ao examinar a sexta questão prejudicial, as que acompanham mais especificamente o tratamento automatizado desses dados, bem como, no âmbito do exame da oitava questão prejudicial, as relacionadas com a conservação dos mesmos.

207. Antes de prosseguir este exame, gostaria de salientar a importância fundamental que reveste, no âmbito do sistema de garantias instituído pela Diretiva PNR, o controlo exercido pela autoridade independente referida no artigo 15.º desta diretiva. Em conformidade com este artigo, qualquer tratamento de dados previsto pela referida diretiva está sujeito à monitorização de uma autoridade de controlo independente, que tem poderes para verificar a legalidade desse tratamento, proceder a investigações, inspeções e auditorias, e analisar as reclamações apresentadas por qualquer titular de dados. Esse controlo, exercido por uma entidade externa, incumbida da defesa de interesses potencialmente em conflito com os prosseguidos pelos autores dos tratamentos dos dados PNR, e investida do papel de velar pelo respeito de todas as limitações e salvaguardas que rodeiam os referidos tratamentos, constitui uma garantia essencial, explicitamente enunciada no artigo 8.º, n.º 3, da Carta, cuja eficácia, em termos de proteção dos direitos fundamentais em causa, é até superior ao sistema das vias de recurso colocadas à disposição dos particulares. Por conseguinte, é fundamental, na minha opinião, que o Tribunal de Justiça interprete extensivamente o alcance dos poderes de monitorização previstos no artigo 15.º da Diretiva PNR e que os Estados-Membros, ao transporem esta diretiva para o direito interno, reconheçam à sua autoridade nacional de controlo toda a extensão destes poderes, dotando-a dos meios materiais e pessoais necessários para desempenhar a sua função.

208. Com base em todas as considerações precedentes, entendo que a Diretiva PNR não ultrapassa os limites do estritamente necessário, na medida em que permite a transferência e o tratamento automatizado dos dados de qualquer pessoa que corresponda ao conceito de «passageiro», na aceção do artigo 3.º, ponto 4, desta diretiva.

iv) Quanto ao carácter suficientemente claro, preciso e limitado ao estritamente necessário da avaliação prévia dos passageiros (sexta questão prejudicial)

209. Com a sua sexta questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se a avaliação prévia prevista no artigo 6.º da Diretiva PNR é compatível com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta. Embora a redação desta questão se centre no carácter sistemático e generalizado do tratamento automatizado dos dados PNR de todos os passageiros aéreos que esta avaliação prévia comporta, resulta dos fundamentos da decisão de reenvio que a Cour constitutionnelle (Tribunal Constitucional, Bélgica) solicita ao Tribunal de

²⁰⁷ É, de certo modo, o que a Comissão implica na sua Proposta de Diretiva PNR, p. 3.

²⁰⁸ V., neste sentido, Acórdão Prokuratuur, n.º 49 e jurisprudência referida.

Justiça uma apreciação mais global do respeito dos requisitos de legalidade e de proporcionalidade no contexto desse tratamento. Procederei seguidamente a esta apreciação, remetendo para a análise efetuada no exame da quarta questão prejudicial no que respeita ao caráter não direcionado do referido tratamento automatizado.

210. O artigo 6.º, n.º 2, alínea a), da Diretiva PNR prevê que as UIP procedem a uma avaliação prévia dos passageiros aéreos antes da sua chegada prevista ao Estado-Membro ou da sua partida prevista do mesmo. Esta avaliação visa identificar as pessoas que devem ser sujeitas a um controlo mais minucioso pelas autoridades competentes, «pelo facto de poderem estar implicadas numa infração terrorista ou numa forma de criminalidade grave». Em conformidade com o artigo 6.º, n.º 6, da Diretiva PNR, a UIP de um Estado-Membro transmite os dados PNR das pessoas identificadas no âmbito dessa avaliação ou os resultados do tratamento desses dados às autoridades competentes, referidas no artigo 7.º desta diretiva, desse mesmo Estado-Membro, para efeitos de um «controlo mais minucioso».

211. Nos termos do artigo 6.º, n.º 3, da Diretiva PNR, a avaliação prévia efetuada nos termos do n.º 2, alínea a), deste artigo é realizada comparando os dados PNR com os que constam das bases de dados «relevantes» [artigo 6.º, n.º 3, alínea a)] ou tratando-os de acordo com critérios estabelecidos [artigo 6.º, n.º 3, alínea b)].

212. Antes de abordar o exame de cada um destes dois tipos de tratamentos de dados, observo que não resulta claramente da redação do artigo 6.º, n.º 3, acima referido, se os Estados-Membros são obrigados a prever que a avaliação prévia dos passageiros seja feita procedendo sistematicamente e em todos os casos tanto a uma como a outra análise automatizada ou se, como parece ser corroborado pela utilização do verbo «poder» e da conjunção disjuntiva «ou», estão habilitados a adaptar os seus sistemas de modo a reservar, por exemplo, o exame previsto no n.º 3, alínea b), deste artigo 6.º a casos específicos. A este respeito, esclareço que a Proposta de Diretiva PNR previa que este exame fosse realizado apenas no âmbito da luta contra as infrações transfronteiriças graves²⁰⁹.

213. À semelhança da Comissão, considero que resulta, nomeadamente, da economia da Diretiva PNR que os Estados-Membros são obrigados a prever ambos os tipos de tratamentos automatizados, por razões que se prendem igualmente com a exigência de assegurar uma aplicação o mais uniforme possível do sistema de tratamento dos dados PNR da União. No entanto, isto não implica que os Estados-Membros não sejam autorizados — e até mesmo obrigados, para garantir que o tratamento de dados que comporta a avaliação prévia efetuada em conformidade com o artigo 6.º, n.º 2, alínea a), da Diretiva PNR seja limitado ao estritamente necessário — a circunscrever a análise, nos termos do artigo 6.º, n.º 3, alínea b), da Diretiva PNR, em função dos seus resultados em termos de eficácia para cada uma das infrações visadas por esta diretiva e, sendo caso disso, a reservá-la apenas a algumas dessas infrações. Neste sentido milita o considerando 7 da Diretiva PNR, segundo o qual «a fim de assegurar que o tratamento de dados PNR se continua a restringir ao necessário, a fixação e a aplicação de critérios de avaliação deverão limitar-se a infrações terroristas e à criminalidade grave».

²⁰⁹ V. artigo 4.º, n.º 2, alínea a), da Proposta de Diretiva PNR.

– Quanto à comparação com bases de dados na aceção do artigo 6.º, n.º 3, alínea a), da Diretiva PNR

214. A primeira vertente da avaliação prévia a que as UIP procedem, nos termos do artigo 6.º, n.º 2, alínea a), da Diretiva PNR, implica, em conformidade com o n.º 3, alínea a), deste artigo, a comparação dos dados PNR («*data matching*») com bases de dados, a fim de procurar eventuais correspondências positivas («*hits*»). Estes *hits* destinam-se a ser verificados pelas UIP em conformidade com o artigo 6.º, n.º 5, da Diretiva PNR e, se for caso disso, traduzidos num «*match*» antes de serem comunicados às autoridades competentes.

215. Como o Tribunal de Justiça reconheceu no n.º 172 do Parecer 1/15, o alcance da ingerência que estes tipos de análises automatizadas comportam nos direitos consagrados nos artigos 7.º e 8.º da Carta depende essencialmente das bases de dados em que as mesmas assentam. Por conseguinte, é essencial que as disposições que preveem tais tratamentos de dados identifiquem de forma suficientemente clara e precisa quais as bases de dados com as quais é autorizado o cruzamento dos dados a tratar.

216. Nos termos do artigo 6.º, n.º 3, alínea a), da Diretiva PNR, as UIP procedem a uma comparação dos dados PNR com as «bases de dados relevantes»²¹⁰ à luz dos objetivos prosseguidos por esta diretiva. Esta disposição menciona igualmente uma categoria específica de bases de dados, a saber, as relativas às «pessoas ou objetos procurados ou alvo de um alerta», às quais o legislador da União pretendeu, portanto, conferir expressamente a qualificação de «relevantes» na aceção desta disposição.

217. Excetuando esta precisão, o conceito de «bases de dados relevantes» não é objeto de mais explicações. Não se indica, nomeadamente, se, para serem consideradas «relevantes», as bases de dados utilizadas para efeitos do cruzamento dos dados PNR devem ser geridas por autoridades responsáveis pela aplicação da lei ou, mais genericamente, por qualquer autoridade pública, ou simplesmente serem-lhes direta ou indiretamente acessíveis. A natureza dos dados que tais bases são suscetíveis de conter e a sua relação com os objetivos prosseguidos pela Diretiva PNR também não são precisadas²¹¹. Por outro lado, resulta da redação do artigo 6.º, n.º 3, alínea a), da Diretiva PNR que são suscetíveis de ser qualificadas de «bases de dados relevantes» bases de dados tanto nacionais e da União como internacionais, o que aumenta ainda mais a lista das bases de dados potencialmente visadas e aumenta o carácter aberto deste conceito²¹².

218. Nestas condições, em aplicação do princípio geral de interpretação recordado no n.º 151 das presentes conclusões, cabe ao Tribunal de Justiça interpretar, na medida do possível, o artigo 6.º, n.º 3, alínea a), da Diretiva PNR, nomeadamente o conceito de «bases de dados relevantes», em

²¹⁰ Embora na versão em língua francesa o artigo 6.º, n.º 3, alínea a), mencione «bases de données utiles» (bases de dados úteis), na maioria das outras versões linguísticas esta disposição visa antes as «bases de données pertinentes» (bases de dados relevantes): v., nomeadamente, as versões nas línguas espanhola («*pertinentes*»), alemã («*massgeblich*»), inglesa («*relevant*»), italiana («*pertinenti*»), neerlandesa («*relevant*»), e portuguesa («*relevantes*»).

²¹¹ Tal como está redigido, o artigo 6.º, n.º 3, alínea a), da Diretiva PNR parece permitir análises sob a forma de uma pesquisa de dados por cruzamento com dados muito variados, desde que essa pesquisa seja concluída em prossecução dos objetivos visados por esta diretiva. Quanto aos riscos associados ao «*data mining*» em matéria de dados PNR, v. Relatório Korff, p. 77. A AEPD sublinhou veementemente a falta de precisão e de previsibilidade da identificação das bases de dados com as quais os dados PNR podem ser comparados no seu Parecer de 25 de março de 2011, ponto 18.

²¹² O carácter vago e aberto da redação do artigo 6.º, n.º 3, alínea a), da Diretiva PNR traduz-se numa transposição para o direito nacional muito variada, que vai de uma interpretação estrita do conceito de «base de dados relevante», que limita a análise prevista apenas à comparação com as bases de dados explicitamente mencionadas nesta disposição (é o caso da República Federal da Alemanha, como resulta das observações apresentadas pelo seu governo no Tribunal de Justiça) a uma interpretação mais ampla que abrange quaisquer bases de dados disponíveis ou acessíveis às autoridades competentes no âmbito da sua missão (é neste sentido que é redigido, nomeadamente, o artigo 24.º, § 1, ponto 1, da Lei PNR).

conformidade com os requisitos de clareza e de precisão exigidos pela Carta. Além disso, uma vez que esta disposição prevê uma ingerência nos direitos fundamentais enunciados nos artigos 7.º e 8.º da Carta, deve ser interpretada de forma restritiva e tendo em conta a exigência de assegurar um elevado nível de proteção desses direitos fundamentais, conforme afirmada, nomeadamente, no considerando 15 da Diretiva PNR. Além disso, deve ser interpretada à luz do princípio da limitação das finalidades para as quais os dados PNR podem ser tratados, enunciado no artigo 1.º, n.º 2, da Diretiva PNR.

219. Tendo em conta estes critérios, o conceito de «bases de dados relevantes» deve, na minha opinião, ser interpretado no sentido de que visa apenas as bases de dados nacionais geridas pelas autoridades competentes nos termos do artigo 7.º, n.º 1, da Diretiva PNR, bem como as bases de dados da União e internacionais exploradas diretamente por essas autoridades no âmbito das respetivas missões. As referidas bases de dados devem, além disso, ter uma relação direta e estreita com as finalidades de luta contra o terrorismo e a criminalidade grave prosseguidas pela Diretiva PNR, o que implica que tenham sido desenvolvidas para essas finalidades. Interpretado deste modo, este conceito visa essencialmente, senão exclusivamente, as bases de dados relativas às pessoas ou objetos procurados ou alvo de um alerta, expressamente mencionadas no artigo 6.º, n.º 3, alínea a), da Diretiva PNR.

220. Estão, de um modo geral, excluídas do conceito de «bases de dados relevantes» as bases de dados geridas ou exploradas pelos serviços de informações dos Estados-Membros, a menos que satisfaçam estritamente o requisito de terem uma relação estreita com os objetivos prosseguidos pela Diretiva PNR, e que o Estado-Membro em questão reconheça aos seus serviços de informações competências específicas no domínio da aplicação da lei²¹³.

221. A interpretação acima proposta está em consonância com as recomendações formuladas pelo Tribunal de Justiça no n.º 172 do Parecer 1/15.

222. Todavia, mesmo interpretado deste modo, o artigo 6.º, n.º 3, alínea a), da Diretiva PNR não permite uma identificação suficientemente precisa das bases de dados que serão utilizadas pelos Estados-Membros no âmbito do cruzamento com os dados PNR e não se pode considerar que satisfaz os requisitos que decorrem do artigo 52.º, n.º 1, da Carta, conforme interpretado pelo Tribunal de Justiça. Esta disposição deve, por conseguinte, ser interpretada no sentido de que obriga os Estados-Membros, no âmbito da transposição da Diretiva PNR para o direito nacional, a publicarem uma lista das referidas bases de dados e a mantê-la atualizada. Por outro lado, seria desejável que fosse redigida, ao nível da União, uma lista das bases de dados «relevantes», na aceção do artigo 6.º, n.º 3, alínea a), da Diretiva PNR, geridas pela União em colaboração com os Estados-Membros e das bases de dados internacionais, a fim de tornar uniforme, a este respeito, a prática dos Estados-Membros.

– *Quanto ao tratamento dos dados PNR à luz de critérios preestabelecidos*

223. A segunda vertente da avaliação prévia nos termos do artigo 6.º, n.º 2, alínea a), da Diretiva PNR consiste numa análise automatizada à luz de critérios preestabelecidos. No âmbito desta análise, os dados PNR são tratados, essencialmente para fins preditivos, através da aplicação de algoritmos que devem permitir «identificar» os passageiros que possam estar implicados em infrações terroristas ou em formas de criminalidade grave. Neste contexto, a UIP procede, em

²¹³ Na minha opinião, em caso algum deverá um Estado-Membro considerar-se obrigado, com base no artigo 6.º, n.º 3, alínea a), da Diretiva PNR, a autorizar a sua UIP a comparar sistematicamente os dados PNR com «bases de dados relevantes», na aceção desta disposição, geridas pelos seus serviços de informações.

substância, a uma atividade de definição de perfis²¹⁴. Uma vez que é suscetível de ter consequências importantes para as pessoas identificadas pelo algoritmo²¹⁵, tal tratamento exige um enquadramento preciso no que respeita tanto às modalidades da sua realização como às garantias que o devem rodear. Com efeito, como o Tribunal de Justiça observou no n.º 172 do Parecer 1/15, o alcance da ingerência que estes tipos de análises comportam nos direitos consagrados nos artigos 7.º e 8.º da Carta depende essencialmente dos modelos e dos critérios preestabelecidos aplicados.

224. A este respeito, saliento, em primeiro lugar, que o artigo 6.º, n.º 4, segundo período, da Diretiva PNR precisa que os critérios preestabelecidos à luz dos quais é realizada a avaliação prévia prevista no artigo 6.º, n.º 3, alínea b), desta diretiva devem ser «orientados em função dos objetivos, proporcionados e específicos». O primeiro destes requisitos respeita ao objetivo visado pela avaliação prévia prevista no n.º 2, alínea a), deste artigo, a saber, a identificação das pessoas que devem ser sujeitas a um controlo mais minucioso pelas autoridades competentes, e responde, assim, à necessidade, destacada pelo Tribunal de Justiça no Parecer 1/15, de os critérios utilizados conseguirem «orientar-se» para selecionar pessoas sobre as quais possa recair uma «suspeita razoável» de participação em infrações terroristas ou de criminalidade grave²¹⁶. Tal «orientação» implica a aplicação de critérios de avaliação abstratos ou, para utilizar uma expressão que figura na Recomendação de 2021 sobre a definição de perfis, de «perfis»²¹⁷ através dos quais se «filtram» os dados PNR a fim de identificar os passageiros que correspondem aos mesmos e que podem, por conseguinte, ter de ser sujeitos a um controlo mais minucioso. Em contrapartida, a Diretiva PNR não autoriza uma definição de perfil individual de todos os passageiros aéreos cujos dados são analisados, por exemplo, associando a cada um deles uma categoria de risco numa escala predefinida, sob pena de violar tanto o artigo 6.º, n.º 4, desta diretiva como os limites impostos pelo Tribunal de Justiça ao tratamento automatizado dos dados PNR no Parecer 1/15.

225. Em conformidade com o artigo 6.º, n.º 4, segundo período, os critérios preestabelecidos visados no artigo 6.º, n.º 3, alínea b), da Diretiva PNR devem, além disso, ser «específicos»²¹⁸, a saber, adaptados à finalidade prosseguida e pertinentes relativamente à mesma, bem como «proporcionados»²¹⁹, ou seja, não devem exceder os limites desta finalidade. Para satisfazer estes requisitos, nomeadamente «a fim de assegurar que o tratamento de dados PNR se continua a

²¹⁴ O artigo 3.º, ponto 4, da Diretiva Cooperação Policial define a «definição de perfis» como «qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações». A mesma definição figura no artigo 4.º, ponto 4, do RGD e no ponto 1, alínea c), do anexo da Recomendação CM/Rec(2021)8, de 3 de novembro de 2021, do Comité de Ministros do Conselho da Europa sobre a proteção das pessoas relativamente ao tratamento automatizado de dados pessoais no âmbito da definição de perfis, https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46148 (a seguir «Recomendação de 2021 sobre a definição de perfis»).

²¹⁵ O ponto 1, alínea j), i), da Recomendação de 2021 sobre a definição de perfis define como «tratamentos de definição de perfis de risco elevado» a «definição de perfis cujo funcionamento produza efeitos jurídicos ou que tenham um impacto significativo para a pessoa em causa ou para o grupo de pessoas identificado pelo tratamento de definição de perfis».

²¹⁶ V. Parecer 1/15, n.º 272.

²¹⁷ Nos termos do ponto 1.1, alínea d), do anexo da Recomendação de 2021 sobre a definição de perfis, o termo «perfil» designa «um conjunto de dados atribuído a uma pessoa que caracteriza uma categoria de pessoas ou que se destina a ser aplicado a uma pessoa». Como explica o Relatório sobre a evolução da situação após a adoção da Recomendação (2010)13 sobre a definição de perfis (<https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b>, p. 21), que precedeu a adoção da Recomendação de 2021 sobre a definição de perfis, o conceito de «perfil» continua a ter sentido em sistemas que, como a Diretiva PNR, distinguem as operações de criação de perfis [v., nomeadamente, artigo 6.º, n.º 2, alínea b), desta diretiva] das que os aplicam, e permite «uma transparência dos critérios que são aplicados numa segunda fase através da operação de definição de perfis».

²¹⁸ V. artigo 6.º, n.º 4, da Diretiva PNR, bem como Parecer 1/15, n.º 172.

²¹⁹ V. artigo 6.º, n.º 4, da Diretiva PNR.

restringir ao necessário», o considerando 7 da Diretiva PNR, como já salientei, enuncia que «a fixação e a aplicação de critérios de avaliação deverão limitar-se a infrações terroristas e à criminalidade grave para as quais a utilização de tais critérios seja relevante».

226. Resulta, por último, tanto do preâmbulo e das disposições da Diretiva PNR como dos requisitos enunciados pelo Tribunal de Justiça no Parecer 1/15 que os critérios preestabelecidos previstos no artigo 6.º, n.º 3, alínea b), da Diretiva PNR devem igualmente ser «fiáveis»²²⁰, o que significa, por um lado, que devem ser concebidos para minimizar o risco de erros²²¹ e, por outro, devem ser «atuais»²²². A este respeito, o artigo 6.º, n.º 4, terceiro período, da Diretiva PNR obriga os Estados-Membros a assegurar que esses critérios sejam «fixados e revistos regularmente pelas UIP, em cooperação com as autoridades competentes a que se refere o artigo 7.º»²²³. Para garantir a fiabilidade destes critérios e limitar o mais possível resultados falsos positivos, é ainda necessário, como a Comissão reconheceu ao responder a uma pergunta escrita do Tribunal de Justiça, que os mesmos sejam concebidos de forma a tomar em conta tanto elementos incriminatórios como elementos ilibatórios.

227. Em segundo lugar, a Diretiva PNR proíbe expressamente a definição discriminatória de perfis. Assim, o artigo 6.º, n.º 4, primeiro período, desta diretiva prevê que a avaliação prévia à luz de critérios preestabelecidos nos termos do n.º 3, alínea b), deste artigo «é realizada de forma não discriminatória». A este respeito, importa precisar que, embora o terceiro período deste artigo 6.º, n.º 4, enuncie que os referidos critérios «não podem, em caso algum, basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual», a proibição geral da definição discriminatória de perfis deve ser entendida no sentido de que abrange todos os motivos de discriminação mencionados no artigo 21.º da Carta, mesmo os que não são expressamente referidos²²⁴.

228. Em terceiro lugar, resulta tanto da redação do artigo 6.º, n.º 3, alínea b), da Diretiva PNR como do sistema de garantias que rodeia o tratamento automatizado dos dados PNR previsto pela Diretiva PNR que o funcionamento dos algoritmos utilizados no âmbito da análise prevista nesta disposição deve ser transparente e o resultado da sua aplicação deve ser rastreável. Este requisito de transparência não implica, evidentemente, que os «perfis» utilizados devam ser tornados públicos. Em contrapartida, exige que seja assegurada a identificabilidade da tomada de decisão algorítmica. Com efeito, por um lado, o requisito segundo o qual os critérios à luz dos quais esta análise deve ser efetuada devem ser «preestabelecidos» exclui que possam ser alterados sem intervenção humana e opõe-se, portanto, à utilização de tecnologias de inteligência artificial ditas de «*machine learning*»²²⁵, que, embora possam apresentar um grau de precisão mais elevado, são difíceis de interpretar, mesmo para os operadores que tenham procedido ao tratamento

²²⁰ V. Parecer 1/15, n.º 172.

²²¹ V. considerando 7 da Diretiva PNR.

²²² V. Parecer 1/15, n.º 174.

²²³ O mesmo requisito figura no n.º 174 do Parecer 1/15.

²²⁴ Observo que todos os motivos de discriminação que figuram no artigo 21.º da Carta são reproduzidos no considerando 20 da Diretiva PNR. O alinhamento com a lista dos motivos de discriminação proibidos, prevista no artigo 21.º, tinha sido proposto pela FRA no seu Parecer 1/2011, p. 8.

²²⁵ Nos termos do ponto 1.1, alínea g), do anexo da Recomendação de 2021 sobre a definição de perfis, a expressão «*machine learning*» designa «um tratamento que utiliza métodos específicos de inteligência artificial baseado em abordagens estatísticas para dar aos computadores a capacidade de “aprenderem” a partir de dados, ou seja, de melhorarem o seu desempenho na resolução de tarefas sem serem explicitamente programados para cada uma delas».

automatizado²²⁶. Por outro lado, a garantia enunciada no artigo 6.º, n.ºs 5 e 6, da Diretiva PNR, nos termos da qual qualquer resultado positivo obtido através do tratamento automatizado dos dados PNR efetuado nos termos do n.º 2, alínea a), deste artigo deve ser verificado individualmente por meios não automatizados, exige, para ser efetiva — no que respeita à análise prevista no artigo 6.º, n.º 3, alínea b), da Diretiva PNR — que seja possível compreender a razão pela qual o programa chegou a esse resultado, o que não pode ser assegurado, nomeadamente, quando são utilizados sistemas de autoaprendizagem. O mesmo se aplica à fiscalização da legalidade desta análise, incluindo no que respeita ao caráter não discriminatório dos resultados obtidos, que incumbe ao responsável pela proteção de dados e à autoridade nacional de controlo, nos termos, respetivamente, do artigo 6.º, n.º 7, da Diretiva PNR, e do artigo 15.º, n.º 3, alínea b), desta diretiva. A transparência do funcionamento dos algoritmos utilizados é igualmente uma condição necessária para permitir aos interessados exercer os seus direitos de reclamação, bem como o seu direito a um recurso jurisdicional efetivo.

– *Quanto às garantias que rodeiam o tratamento automatizado dos dados PNR*

229. Já tive oportunidade de mencionar algumas das garantias que acompanham o tratamento automatizado dos dados PNR no âmbito da avaliação prévia nos termos do artigo 6.º, n.º 2, alínea a), da Diretiva PNR, e que satisfazem os requisitos enunciados pelo Tribunal de Justiça no Parecer 1/15, a saber, a proibição de tratamento com base em critérios preestabelecidos discriminatórios (artigo 6.º, n.º 4, primeiro e quarto períodos, da Diretiva PNR; Parecer 1/15, n.º 172), a atualização regular dos critérios preestabelecidos à luz dos quais deve ser efetuada a avaliação prévia prevista no artigo 6.º, n.º 3, alínea b), desta diretiva (artigo 6.º, n.º 4, terceiro período, da Diretiva PNR; Parecer 1/15, n.º 174), o reexame por meios não automatizados de qualquer resultado positivo obtido na sequência do tratamento automatizado dos dados PNR (artigo 6.º, n.ºs 5 e 6, da Diretiva PNR; Parecer 1/15, n.º 173) e a fiscalização da legalidade desse tratamento pelo responsável pela proteção de dados e pela autoridade nacional de controlo (artigo 6.º, n.º 7, e artigo 15.º, n.º 3, alínea b), da Diretiva PNR). Neste contexto, é primordial que a fiscalização efetuada por uma autoridade independente, como a autoridade prevista no artigo 15.º da Diretiva PNR, possa, por um lado, incidir sobre qualquer aspeto inerente ao tratamento automatizado dos dados PNR, incluindo a identificação das bases de dados utilizadas para efeitos da comparação nos termos do artigo 6.º, n.º 3, alínea a), desta diretiva e a elaboração dos critérios preestabelecidos aplicados para efeitos da análise nos termos do artigo 6.º, n.º 3, alínea b), da referida diretiva e, por outro, ser exercida tanto *ex ante* como *ex post*.

230. Importa sublinhar que as garantias acima referidas devem ser consideradas aplicáveis de forma transversal a ambos os tipos de análises previstos no artigo 6.º, n.º 3, da Diretiva PNR, apesar dos termos em que são formuladas. Assim, embora o artigo 6.º, n.º 4, primeiro período, desta diretiva recorde a exigência do respeito do princípio da não discriminação apenas em relação à avaliação prévia efetuada à luz de critérios preestabelecidos, esta exigência impõe-se em qualquer fase do processo de tratamento dos dados PNR e, portanto, também quando estes são comparados com as bases de dados relevantes no âmbito da avaliação prévia nos termos do artigo 6.º, n.º 3, alínea a), desta diretiva. O mesmo se aplica à exigência de os critérios preestabelecidos utilizados no âmbito da análise prevista no artigo 6.º, n.º 3, alínea b), da Diretiva PNR serem fiáveis e atualizados, que deve ser entendido no sentido de que visa igualmente os dados contidos nas bases de dados utilizadas para efeitos da comparação prevista no artigo 6.º,

²²⁶ No que respeita aos efeitos da opacidade dos sistemas algorítmicos sobre a possibilidade de um controlo humano destinado a prevenir os efeitos prejudiciais desses sistemas e os seus impactos negativos sobre os direitos humanos, v. Recomendação CM/Rec (2020)1 do Comité de Ministros do Conselho da Europa aos Estados-Membros sobre os impactos dos sistemas algorítmicos sobre os direitos humanos.

n.º 3, alínea a), desta diretiva. A este respeito, observo, mais genericamente, que todas as garantias aplicáveis aos tratamentos automatizados de dados pessoais previstos pela Diretiva Cooperação Policial são igualmente aplicáveis no âmbito da Diretiva PNR, devendo considerar-se que as análises automatizadas realizadas no âmbito desta diretiva estão abrangidas pelo âmbito de aplicação da Diretiva Cooperação Policial.

231. Às garantias enumeradas no n.º 229, *supra*, acresce a prevista no artigo 7.º, n.º 6, da Diretiva PNR que vem completar, por um lado, a proibição de basear qualquer processo decisório exclusivamente nos resultados do tratamento automatizado dos dados PNR e, por outro, a proibição de discriminação no tratamento e na utilização desses dados. Assim, esta disposição prevê que «[a]s autoridades competentes abstêm-se de tomar qualquer decisão que produza efeitos jurídicos adversos para uma pessoa ou que a afete de forma grave apenas com base no tratamento automatizado dos dados PNR» e que estas decisões «não podem basear-se na raça ou origem étnica da pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, filiação sindical nem na sua saúde, vida ou orientação sexual». À semelhança do que indiquei no n.º 227 das presentes conclusões a respeito do artigo 6.º, n.º 4, quarto período, da Diretiva PNR, há que completar esta lista de motivos de discriminação, acrescentando-lhe os que figuram no artigo 21.º da Carta e que não são expressamente mencionados.

232. No que respeita à segurança dos dados PNR, o artigo 6.º, n.º 8, da Diretiva PNR prevê que os dados PNR só podem ser conservados, tratados e analisados pelas UIP em local ou locais seguros no território dos Estados-Membros.

– *Conclusão quanto à sexta questão prejudicial*

233. Tendo em conta todas as considerações precedentes e sem prejuízo das interpretações propostas, nomeadamente, nos n.ºs 213, 219, 220, 222, 227, 228, 230 e 231 das presentes conclusões, considero que o tratamento automatizado dos dados PNR no âmbito da avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), da Diretiva PNR respeita os requisitos de clareza e de precisão e está limitado ao estritamente necessário.

v) *Quanto à conservação dos dados PNR (oitava questão prejudicial)*

234. Com a sua oitava questão prejudicial, o órgão jurisdicional de reenvio pergunta ao Tribunal de Justiça se o artigo 12.º da Diretiva PNR, em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que prevê um prazo geral de conservação dos dados PNR de cinco anos, sem distinguir se os passageiros em causa se revelam, no âmbito da avaliação prévia, suscetíveis ou não de representar um risco para a segurança pública.

235. O artigo 12.º, n.º 1, da Diretiva PNR prevê que os dados PNR são conservados numa base de dados «por um prazo de cinco anos contados a partir da sua transferência para a UIP do Estado-Membro em cujo território o voo aterre ou de cujo território descole». Em conformidade com o n.º 2 deste artigo, decorrido um «prazo inicial de conservação»²²⁷ de seis meses, os dados PNR são anonimizados mediante mascaramento de certos dados suscetíveis de identificar diretamente a pessoa em causa. Nos termos do n.º 3 do referido artigo, decorrido esse prazo de seis meses, só é permitida a divulgação dos dados PNR integrais, incluindo os elementos mascarados, caso essa divulgação seja considerada necessária, com base em «motivos razoáveis», para os fins

²²⁷ Esta definição figura no considerando 25 da Diretiva PNR.

referidos no artigo 6.º, n.º 2, alínea b), da Diretiva PNR, e seja autorizada por uma autoridade judiciária ou outra autoridade nacional competente, nos termos do direito nacional, para verificar se estão reunidas as condições de divulgação. Por último, o n.º 4 do mesmo artigo prevê que, decorrido o prazo de cinco anos referido no n.º 1, os dados PNR são apagados de forma definitiva.

236. Resulta do que precede que a própria Diretiva PNR estabelece o regime de conservação dos dados PNR, incluindo o prazo dessa conservação, fixando-o em cinco anos²²⁸, pelo que os Estados-Membros não dispõem, em princípio, de qualquer margem discricionária a este respeito, o que, de resto, foi confirmado pela Comissão. Nestas circunstâncias, como já tive ocasião de observar, a oitava questão prejudicial, embora seja formulada como uma questão de interpretação, convida, na realidade, o Tribunal de Justiça a pronunciar-se sobre a compatibilidade do referido regime com a Carta.

237. Segundo um princípio geral em matéria de proteção dos dados pessoais, estes dados não devem ser conservados, numa forma que permita a identificação, direta ou indireta, das pessoas em causa, durante um período que exceda o necessário para as finalidades para as quais são tratados²²⁹. Por outro lado, resulta de jurisprudência constante que uma regulamentação que prevê uma conservação de dados pessoais deve sempre pautar-se por critérios objetivos, que estabeleçam uma relação entre os dados pessoais a conservar e o objetivo prosseguido²³⁰.

238. No Parecer 1/15, o Tribunal de Justiça considerou, no que respeita aos dados recolhidos à entrada no Canadá, que a necessária relação entre os dados PNR e o objetivo prosseguido pelo Projeto de Acordo PNR Canadá-UE existia relativamente a todos os passageiros aéreos enquanto estes se encontrassem no território deste país terceiro²³¹. No que respeita, em contrapartida, aos passageiros aéreos que tivessem saído do Canadá e relativamente aos quais não tivesse sido identificado um risco em matéria de terrorismo ou de criminalidade transnacional grave à sua chegada a este país terceiro e até à sua saída do mesmo, o Tribunal de Justiça considerou que não se afigurava existir tal relação, ainda que indireta, que justificasse a conservação dos seus dados PNR²³². O Tribunal de Justiça considerou, contudo, que essa conservação podia ser admissível «na medida em que, em casos particulares, são identificados elementos objetivos que permitem considerar que certos passageiros aéreos poderiam, mesmo depois da sua saída do Canadá, representar um risco em termos de luta contra o terrorismo e a criminalidade transnacional grave»²³³.

239. Transpostos para o contexto da Diretiva PNR, os princípios estabelecidos pelo Tribunal de Justiça no Parecer 1/15 implicariam que os dados PNR dos voos extra-UE recolhidos à entrada na União, bem como os dados PNR dos voos intra-UE recolhidos à entrada no Estado-Membro em causa, só podem ser conservados, após a análise prévia nos termos do artigo 6.º, n.º 2, alínea a), da Diretiva PNR, enquanto os passageiros em causa permanecerem no território da União ou desse Estado-Membro. No que respeita aos dados PNR dos voos extra-UE recolhidos à saída da União

²²⁸ O enunciado do considerando 37 da Diretiva PNR, segundo o qual «os dados PNR [são] conservados nas UIP durante um prazo *não superior a cinco anos*, após o qual tais dados deverão ser apagados» (sublinhado meu), não permite, na minha opinião, pôr em causa a redação clara do artigo 12.º, n.º 1, desta diretiva.

²²⁹ V., no que se refere ao tratamento de dados pessoais para efeitos de deteção, prevenção, repressão e investigação em matéria de infrações penais, Diretiva Cooperação Policial, artigo 4.º, alínea e), e considerando 26. V., mais genericamente, artigo 5.º, n.º 1, alínea e), do RGPD, e artigo 5.º, n.º 4, alínea e), da Convenção 108 modernizada.

²³⁰ V. Acórdãos Schrems I (n.º 93); Tele2 Sverige (n.º 110); Parecer 1/15 (n.º 191), bem como Acórdão La Quadrature du Net (n.º 133.)

²³¹ V. Parecer 1/15, n.º 197.

²³² V. Parecer 1/15, n.º 205.

²³³ V. Parecer 1/15, n.º 207.

e aos dados PNR dos voos intra-UE recolhidos à saída do Estado-Membro em causa, estes só podem, em princípio, ser conservados, após a referida avaliação prévia, no caso dos passageiros quanto aos quais existam elementos objetivos que permitam revelar a existência de um risco em termos de luta contra o terrorismo e a criminalidade grave²³⁴.

240. Os governos e as instituições que apresentaram observações no Tribunal de Justiça opõem-se, em geral, a uma transposição para o âmbito do presente processo dos princípios estabelecidos no Parecer 1/15 em matéria de conservação dos dados PNR. A este respeito, é certo que não se pode excluir que o recurso pelo Tribunal de Justiça a um critério associado à permanência da pessoa em causa no território do Canadá possa ter sido influenciado pela circunstância de o Tribunal de Justiça ter sido confrontado com uma conservação de dados pessoais no território de um país terceiro. É igualmente possível que a aplicação de tal critério no contexto da Diretiva PNR possa traduzir-se, em concreto, numa ingerência nos direitos ao respeito pela vida privada e à proteção dos dados pessoais potencialmente mais importante para certas categorias de pessoas, nomeadamente as que têm residência permanente na União e que se deslocam no interior desta ou que regressam de uma estadia no estrangeiro. Por último, é verdade que o referido critério pode revelar-se difícil de aplicar na prática, pelo menos para os voos intra-EU, como certos Estados-Membros e o Conselho sublinharam.

241. Todavia, mesmo que se pretenda afastar o critério a que o Tribunal de Justiça recorreu no Parecer 1/15, uma conservação da totalidade dos dados PNR de todos os passageiros aéreos, independentemente do resultado da avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), da Diretiva PNR, sem que seja feita qualquer distinção em função do risco em matéria de terrorismo ou de criminalidade grave com base em critérios objetivos e verificáveis, é contrária à jurisprudência constante do Tribunal de Justiça recordada no n.º 237 das presentes conclusões, que o Tribunal de Justiça pretendeu aplicar no referido parecer. Ora, as considerações expostas nos n.ºs 201 a 203 das presentes conclusões no âmbito do exame da quarta questão prejudicial, embora permitam, na minha opinião, justificar a transferência generalizada e indiferenciada dos dados PNR, bem como o seu tratamento automático no âmbito da avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), da Diretiva PNR, não permitem, na minha opinião, justificar por si só uma conservação generalizada e indiferenciada destes dados, mesmo após essa avaliação.

242. Observo, por outro lado, que o mesmo prazo de conservação de cinco anos é aplicado tanto quanto à luta contra o terrorismo como quanto à luta contra a criminalidade grave e, no âmbito desta última finalidade, quanto a todas as infrações previstas no anexo II, sem exceção. Ora, como resulta das considerações desenvolvidas no n.º 121 das presentes conclusões, esta lista é particularmente extensa e abrange infrações de tipologia e gravidade diferentes. A este respeito, importa salientar que a justificação apresentada por praticamente todos os Estados-Membros e pelas instituições que apresentaram observações no presente processo, no que respeita à duração e à complexidade dos inquéritos, só é concretamente evocada quanto às infrações terroristas e a certas infrações de caráter eminentemente transnacional, como o tráfico de seres humanos ou o tráfico de estupefacientes, bem como, mais genericamente, quanto a certas formas de criminalidade organizada. Recordo, por outro lado, que, no Parecer 1/15, uma justificação semelhante só foi aceite pelo Tribunal de Justiça no que respeita à conservação dos dados PNR dos passageiros aéreos relativamente aos quais existe um risco objetivo em termos de luta contra o terrorismo ou a criminalidade transnacional grave, para os quais se considerou que um prazo de conservação dos dados de cinco anos não excedia os limites do estritamente necessário²³⁵. Pelo

²³⁴ Tratar-se-ia, nesse caso, de uma aplicação por analogia dos n.ºs 187 e segs. do Parecer 1/15, uma vez que este último visava apenas a hipótese dos dados PNR recolhidos à entrada no território do Canadá.

²³⁵ V. Parecer 1/15, n.º 209.

contrário, considerou-se que esta justificação não podia permitir «um armazenamento contínuo dos dados PNR de todos os passageiros aéreos [...] para efeitos de um eventual acesso aos referidos dados, independentemente de uma qualquer relação com a luta contra o terrorismo e a criminalidade transnacional grave»²³⁶.

243. É verdade, como sublinham o Conselho, o Parlamento e a Comissão, bem como todos os governos que apresentaram observações sobre a oitava questão prejudicial, que a Diretiva PNR prevê garantias específicas tanto no que respeita à conservação dos dados PNR, que são parcialmente mascarados após um prazo inicial de seis meses, como no que respeita à sua utilização durante o período de conservação, que está sujeita a condições estritas. No entanto, em primeiro lugar, observo, por um lado, que o Projeto de Acordo PNR Canadá-UE previa também um sistema de anonimização dos dados PNR por mascaramento²³⁷ e, por outro, que, embora essa anonimização, como sublinha, nomeadamente, o Comité Consultivo da Convenção 108²³⁸, possa atenuar os riscos gerados por um período prolongado de conservação dos dados, como um acesso abusivo, os dados mascarados permitem ainda, todavia, identificar as pessoas e continuam, desse modo, a ser dados pessoais, cuja conservação deve também ser limitada no tempo a fim de evitar uma vigilância permanente generalizada. A este respeito, saliento que um prazo de conservação de cinco anos tem como consequência que um número significativo de passageiros, nomeadamente os que se deslocam no interior da União, podem encontrar-se registados de forma quase permanente. Em segundo lugar, no que respeita às restrições à utilização dos dados, observo que a conservação de dados pessoais e o acesso a esses dados são ingerências distintas nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, que necessitam de ser justificadas de forma autónoma. Embora a existência de garantias estritas em matéria de acesso aos dados conservados permita apreciar globalmente o impacto de uma medida de vigilância sobre os referidos direitos fundamentais, tais garantias não permitem, contudo, eliminar as ingerências associadas a uma conservação generalizada prolongada.

244. Quanto ao argumento da Comissão, segundo o qual é necessário conservar os dados PNR de todos os passageiros aéreos para permitir às UIP cumprir a missão, prevista no artigo 6.º, n.º 2, alínea c), da Diretiva PNR, de atualizar ou definir novos critérios a utilizar para as avaliações realizadas nos termos do n.º 3, alínea b), deste artigo, observo que, embora admitindo que a precisão desses critérios depende, em parte, da sua comparação com comportamentos «normais», como a Comissão afirma, a sua elaboração deve, contudo, ser feita com base em comportamentos «criminosos». Tal argumento, que é, de resto, apresentado apenas por um número limitado de Estados-Membros, não pode, na minha opinião, revestir a importância decisiva que a Comissão parece atribuir-lhe e justificar, por si só, uma conservação generalizada dos dados PNR de todos os passageiros aéreos, de uma forma não anónima.

245. Tendo em conta as considerações precedentes, a fim de assegurar uma interpretação do artigo 12.º, n.º 1, da Diretiva PNR que seja conforme com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, importa, na minha opinião, interpretar esta disposição no sentido de que a conservação dos dados PNR fornecidos pelas transportadoras aéreas à UIP numa base de dados durante um prazo de cinco anos após a sua transferência para a UIP do Estado-Membro em cujo território o voo aterre ou de cujo território descole só é permitida, depois de efetuada a avaliação prévia nos termos do artigo 6.º, n.º 2, alínea a), desta diretiva, na medida em que se demonstre, com base em

²³⁶ V. Parecer 1/15, n.º 205.

²³⁷ O Projeto de Acordo PNR Canadá-UE previa o mascaramento dos nomes de todos os passageiros trinta dias após a sua receção pelo Canadá e o mascaramento de outras informações expressamente enumeradas dois anos após essa receção: v. artigo 16.º, n.º 3, do Projeto de Acordo PNR Canadá-UE examinado pelo Tribunal de Justiça, e Parecer 1/15, n.º 30.

²³⁸ V. Parecer de 19 de agosto de 2016, p. 9.

critérios objetivos, uma relação entre esses dados e a luta contra o terrorismo ou a criminalidade grave. Uma conservação generalizada e indiferenciada dos dados PNR sob uma forma não anonimizada só pode ser justificada, por analogia com o que o Tribunal de Justiça afirmou nesta mesma jurisprudência, perante uma ameaça grave para a segurança dos Estados-Membros que se revele real e atual ou previsível, associada, por exemplo, a atividades de terrorismo, e na condição de a duração dessa conservação se limitar ao estritamente necessário.

246. A delimitação da medida de conservação prevista no artigo 12.º, n.º 1, da Diretiva PNR pode, por exemplo, basear-se numa avaliação dos riscos ou na experiência adquirida pelas autoridades nacionais competentes, que permita visar certas ligações aéreas, esquemas de viagem definidos, agências através das quais as reservas são feitas ou, ainda, categorias de pessoas ou zonas geográficas determinadas, identificadas com base em elementos objetivos e não discriminatórios, à semelhança do que foi declarado pelo Tribunal de Justiça na sua jurisprudência em matéria de conservação dos metadados das comunicações eletrónicas²³⁹. Por outro lado, por analogia com o Parecer 1/15, a necessária relação entre os dados PNR e o objetivo prosseguido pela Diretiva PNR deve ser considerada demonstrada enquanto os passageiros aéreos se encontrarem na União (ou no Estado-Membro em causa) ou à partida da mesma. O mesmo se aplica aos dados dos passageiros que tenham dado origem a um resultado positivo verificado.

247. Para concluir sobre a oitava questão prejudicial, gostaria de dedicar algumas reflexões às regras que regulam o acesso aos dados PNR e a sua utilização depois de a avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), da Diretiva PNR ter sido realizada e antes da sua anonimização decorrido o prazo inicial de conservação de seis meses previsto no artigo 12.º, n.º 2, da Diretiva PNR.

248. Resulta de uma leitura conjugada do artigo 6.º, n.º 2, alínea b), e do artigo 12.º, n.º 3, da Diretiva PNR que, durante este prazo inicial, os dados PNR não anonimizados ou o resultado do seu tratamento podem ser fornecidos às autoridades competentes em conformidade com a primeira destas disposições, sem que sejam respeitadas os requisitos estabelecidos nas alíneas a) e b) da segunda das referidas disposições²⁴⁰. O artigo 6.º, n.º 2, alínea b), da Diretiva PNR limita-se, com efeito, a prever que os pedidos das autoridades competentes com vista a tal tratamento e a tal fornecimento devem ser «devidamente fundamentados» e «baseados em motivos suficientes».

249. Segundo jurisprudência constante, recordada pelo Tribunal de Justiça no Parecer 1/15, uma regulamentação da União não se pode limitar a exigir que o acesso por uma autoridade a dados pessoais legitimamente conservados responda a uma das finalidades desta regulamentação, devendo igualmente prever as condições materiais e processuais que regulam essa utilização²⁴¹, a fim, nomeadamente, de proteger os referidos dados contra os riscos de abuso²⁴². Neste parecer, o Tribunal de Justiça declarou que a utilização dos dados PNR após a sua verificação à chegada dos passageiros aéreos ao Canadá e durante a sua permanência nesse país devia basear-se em circunstâncias novas que justificassem essa utilização²⁴³, precisando que, «quando haja elementos objetivos que permitam considerar que os dados PNR de um ou mais passageiros aéreos podem

²³⁹ V., nomeadamente, Acórdão La Quadrature du Net, n.ºs 148 e 149.

²⁴⁰ O mesmo se aplica aos pedidos de fornecimento dos dados PNR apresentados pelas UIP de outros Estados-Membros ao abrigo do artigo 9.º, n.º 2, da Diretiva PNR.

²⁴¹ V. Parecer 1/15, n.º 192 e jurisprudência referida. Mais recentemente, v. Acórdãos Privacy Internacional, n.º 77 e, por analogia, Prokuratuur, n.º 49 e jurisprudência referida.

²⁴² V. Parecer 1/15, n.º 200.

²⁴³ V. Parecer 1/15, n.º 200.

trazer uma contribuição efetiva para o objetivo de luta contra as infrações terroristas e a criminalidade transnacional grave, a utilização desses dados não parece ultrapassar os limites do estritamente necessário»²⁴⁴. Remetendo, por analogia, para o n.º 120 do Acórdão Tele2 Sverige, o Tribunal de Justiça declarou que, para garantir, na prática, o pleno cumprimento dessas condições, «é essencial que, durante a permanência dos passageiros aéreos no Canadá, a utilização dos dados PNR conservados seja, em princípio, salvo em casos de urgência devidamente justificados, sujeita a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente e que a decisão desse órgão jurisdicional ou dessa entidade ocorra na sequência de um pedido fundamentado das autoridades competentes, apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal»²⁴⁵. O Tribunal de Justiça submeteu, portanto, a possibilidade de uma utilização dos dados PNR conservados após a sua verificação por ocasião de uma viagem aérea a um duplo requisito, simultaneamente material – a saber, a existência de motivos objetivos que justifiquem tal utilização — e processual — a saber, a fiscalização por parte de um órgão jurisdicional ou de uma entidade administrativa independente. A interpretação adotada pelo Tribunal de Justiça, longe de ser «contextual», constitui a aplicação em matéria de dados PNR da jurisprudência decorrente, nomeadamente, dos Acórdãos Digital Rights e Tele2 Sverige.

250. Ora, o regime instituído pela Diretiva PNR para os primeiros seis meses de conservação dos dados PNR, que autoriza, após a avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), desta diretiva, o fornecimento e o tratamento, potencialmente repetidos, dos dados PNR na falta de garantias processuais adequadas e de regras materiais suficientemente claras e precisas que definam o objeto e as modalidades destas diferentes ingerências, não respeita os requisitos enunciados pelo Tribunal de Justiça no Parecer 1/15. Também não parece preencher o requisito de uma utilização dos dados PNR que se limite ao estritamente necessário.

251. Por conseguinte, proponho ao Tribunal de Justiça que interprete o artigo 6.º, n.º 2, alínea b), da Diretiva PNR de modo a que os tratamentos de dados nos termos desta disposição que ocorram durante o prazo inicial de seis meses previsto no artigo 12.º, n.º 2, desta diretiva respeitem os requisitos fixados pelo Tribunal de Justiça no Parecer 1/15.

252. No que se refere ao primeiro requisito, de ordem material, ao qual o Tribunal de Justiça subordinou a utilização posterior dos dados PNR, sou de opinião que os conceitos de «motivos razoáveis», na aceção do artigo 12.º, n.º 3, alínea a), da Diretiva PNR e de «motivos suficientes», nos termos do artigo 6.º, n.º 2, alínea b), desta diretiva, podem ser interpretados, sem dificuldade, no sentido de que os pedidos das autoridades competentes, referidos nessas disposições, devem indicar «elementos objetivos que permitam considerar que os dados PNR de um ou mais passageiros aéreos podem trazer uma contribuição efetiva para o objetivo de luta contra as infrações terroristas e a criminalidade [...] grave»²⁴⁶.

253. No que respeita ao segundo requisito, de ordem processual, há, na minha opinião, que interpretar o artigo 6.º, n.º 2, alínea b), da Diretiva PNR, em conjugação com o artigo 12.º, n.º 3, da mesma, e à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta, no sentido de que o requisito de aprovação prévia por parte de uma autoridade judiciária ou de uma autoridade administrativa independente prevista no artigo 12.º, n.º 3, alínea b), desta diretiva se aplica a qualquer tratamento dos dados PNR efetuado em aplicação do referido artigo 6.º, n.º 2, alínea b).

²⁴⁴ V. Parecer 1/15, n.º 201.

²⁴⁵ V. Parecer 1/15, n.º 202.

²⁴⁶ V., neste sentido, Parecer 1/15, n.º 201.

2. Conclusões sobre as segunda, terceira, quarta, sexta e oitava questões prejudiciais

254. Com base em todas as considerações precedentes, sugiro ao Tribunal de Justiça que declare inválido o ponto 12 do anexo I, na medida em que inclui as «observações gerais» entre as categorias de dados PNR que as transportadoras aéreas são obrigadas a transmitir às UIP, em conformidade com o artigo 8.º da Diretiva PNR, e que declare que o exame das segunda, terceira, quarta, sexta e oitava questões prejudiciais não revelou outros elementos suscetíveis de afetar a validade desta diretiva, sob reserva das interpretações das disposições da mesma propostas nos n.ºs 153, 160, 161 à 164, 219, 228, 239 e 251 das presentes conclusões.

255. À luz da resposta que sugiro que seja dada às questões prejudiciais relativas à validade da Diretiva PNR, o pedido apresentado, nomeadamente, pelo Conselho, destinado à manutenção dos efeitos da Diretiva PNR no caso de o Tribunal de Justiça decidir declarar inválida, total ou parcialmente, a Diretiva PNR no seu todo, não pode, abstraindo de qualquer outra consideração, ser acolhido.

C. Quanto à quinta questão prejudicial

256. Com a sua quinta questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se o artigo 6.º da Diretiva PNR, em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que admite como finalidade do tratamento dos dados PNR o acompanhamento de certas atividades dos serviços de informações e de segurança. Resulta da decisão de reenvio que estas atividades são as atividades exercidas pela Segurança do Estado e pelo Serviço Geral de Informações e de Segurança no âmbito da sua função relativa à proteção da segurança nacional.

257. Como indiquei nos n.ºs 113 e 114 das presentes conclusões, a limitação das finalidades do tratamento de dados pessoais é uma garantia essencial a respeitar para que as ingerências nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta não ultrapassem o necessário, na aceção da jurisprudência do Tribunal de Justiça. Também já esclareci que, no que respeita às ingerências nesses direitos fundamentais previstas pela Diretiva PNR, incumbia ao legislador da União, a fim de respeitar os princípios da legalidade e da proporcionalidade inscritos, nomeadamente, no artigo 52.º, n.º 1, da Carta, prever regras claras e precisas que regulem o âmbito e a aplicação das medidas que comportem tais ingerências.

258. Ora, o artigo 1.º, n.º 2, da Diretiva PNR precisa que os dados PNR recolhidos nos termos da mesma «só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, conforme previsto no artigo 6.º, n.º 2, alíneas a), b) e c)» desta diretiva. Em conformidade com esta disposição, as UIP só tratam os dados PNR com o objetivo de proceder a uma avaliação prévia dos passageiros aéreos [artigo 6.º, n.º 2, alínea a)], responder aos pedidos pontuais das autoridades competentes [artigo 6.º, n.º 2, alínea b)] e atualizar ou criar novos critérios a utilizar nas avaliações realizadas nos termos do n.º 3, alínea b), do referido artigo 6.º [artigo 6.º, n.º 2, alínea c)]. Nos três casos, são expressamente recordados os objetivos indicados no artigo 1.º, n.º 2, da Diretiva PNR em matéria de luta contra o terrorismo e a criminalidade grave.

259. Por outro lado, o artigo 7.º, n.º 4, desta diretiva precisa que não só o tratamento dos dados PNR previsto no seu artigo 6.º, como também o tratamento posterior desses dados e do resultado desse tratamento pelas autoridades competentes dos Estados-Membros, devem ser limitados «exclusivamente para efeitos específicos de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave».

260. O carácter exaustivo da determinação dos objetivos prosseguidos pela Diretiva PNR resulta claramente da redação do seu artigo 1.º, n.º 2, e é corroborado não só pelos seus artigos 6.º, n.º 2, e 7.º, n.º 4, já referidos, como também por vários artigos e considerandos desta diretiva, que associam sistematicamente cada fase do processo de acesso, de tratamento, de conservação e de partilha dos dados PNR apenas a esses objetivos específicos²⁴⁷.

261. Decorre tanto da redação do artigo 1.º, n.º 2, da Diretiva PNR como da sua interpretação à luz dos princípios da legalidade e da proporcionalidade, que impõem que se limite de forma exaustiva as finalidades das medidas que comportem ingerências nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, que qualquer extensão das finalidades do tratamento dos dados PNR para além dos objetivos de segurança expressamente mencionados nesta disposição é contrária à Diretiva PNR.

262. Esta proibição de alargar os objetivos prosseguidos pela diretiva aplica-se, na minha opinião, muito especialmente no que respeita às atividades dos serviços de segurança e de informações dos Estados-Membros, incluindo em razão da falta de transparência que caracteriza o seu *modus operandi*. Quanto a este aspeto, partilho da opinião da Comissão, a saber, de que estes serviços não devem, regra geral, ter acesso direto aos dados PNR. Neste contexto, considero que já é, em si, criticável a circunstância de as UIP nacionais poderem, como é o caso da UIP belga, contar entre os membros do seu pessoal funcionários destacados dos serviços de segurança²⁴⁸.

263. Com base nas considerações que precedem, há que responder, na minha opinião, à quinta questão prejudicial que a Diretiva PNR, nomeadamente o seu artigo 1.º, n.º 2, e o seu artigo 6.º, deve ser interpretada no sentido de que se opõe a uma legislação nacional que admite como finalidade do tratamento dos dados PNR o acompanhamento de certas atividades dos serviços de informações e de segurança, na medida em que, no âmbito dessa finalidade, a UIP nacional seja levada a tratar os referidos dados e/ou a transmiti-los, ou os resultados do seu tratamento, aos referidos serviços para fins diferentes dos que são exaustivamente indicados no artigo 1.º, n.º 2, desta diretiva, o que cabe ao órgão jurisdicional nacional verificar.

²⁴⁷ V., nomeadamente, artigos 4.º, 7.º, n.ºs 1 e 2, 9.º, n.º 2, 10.º, n.º 2, 12.º, n.º 4, da Diretiva PNR; v., nomeadamente, considerandos 6, 9, 10, 11, 15, 23, 25, 35 e 38 desta diretiva. Recordo, por outro lado, que a Proposta de Diretiva PNR precisava, no seu considerando 28, que «[a] presente diretiva não obsta a que os Estados-Membros possam prever, ao abrigo do direito nacional, um sistema de recolha e tratamento dos dados PNR para objetivos diferentes dos previstos na presente diretiva». Ora, esta precisão não foi retomada no texto final da Diretiva PNR.

²⁴⁸ Esta possibilidade é admitida, contudo, no artigo 4.º, n.º 3, da Diretiva PNR, nos termos do qual «[o]s membros do pessoal das UIP podem ser agentes destacados pelas autoridades competentes», pelo menos na medida em que os serviços de informações e de segurança do Estado-Membro em causa possam ser qualificados de «autoridades competentes», na aceção do artigo 7.º, n.º 2, desta diretiva.

D. Quanto à sétima questão prejudicial

264. Com a sétima questão, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se o artigo 12.º, n.º 3, alínea b), da Diretiva PNR deve ser interpretado no sentido de que a UIP constitui uma «autoridade nacional competente» na aceção desta disposição, que pode autorizar a divulgação dos dados PNR integrais decorrido o prazo inicial de seis meses após a transferência desses dados.

265. Recordo que o artigo 12.º, n.º 2, da Diretiva PNR prevê que, decorrido um prazo de seis meses, os dados PNR são anonimizados mediante mascaramento de certos elementos suscetíveis de identificar diretamente o passageiro ao qual dizem respeito. Após este prazo, a divulgação dos dados integrais só é permitida nas condições previstas no n.º 3 do referido artigo 12.º, nomeadamente, se essa divulgação tiver sido previamente autorizada por uma «autoridade judiciária», [artigo 12.º, n.º 3, alínea b), i)] ou por «outra autoridade nacional competente, nos termos do direito nacional, para verificar se estão reunidas as condições de divulgação, sob reserva de o responsável pela proteção de dados da UIP ser informado e proceder a uma verificação *ex-post*» [artigo 12.º, n.º 3, alínea b), ii)].

266. A maioria dos governos que apresentaram observações escritas no presente processo não se pronunciou sobre a sétima questão prejudicial. O Governo checo considera, à semelhança da Comissão, que o artigo 12.º, n.º 3, da Diretiva PNR não pode ser interpretado no sentido de que a UIP pode constituir uma «autoridade nacional competente». Em contrapartida, os Governos belga²⁴⁹, irlandês, espanhol, francês e cipriota opõem-se a tal interpretação. Consideram, em substância, que nenhuma disposição da Diretiva PNR ou do direito da União obsta à designação da UIP entre as autoridades nacionais competentes na aceção do artigo 12.º, n.º 2, alínea b), ii), da referida diretiva e que a UIP é, por natureza, uma autoridade suficientemente independente para poder proceder à autorização do tratamento dos dados PNR.

267. Pela minha parte, observo, em primeiro lugar, que resulta da redação do artigo 12.º, n.º 3, alínea b), da Diretiva PNR, nomeadamente da utilização da conjunção «ou», que liga as duas hipóteses referidas nas subalíneas i) e ii) desta disposição, que o legislador da União pretendeu colocar no mesmo plano a fiscalização exercida pela autoridade nacional referida na subalínea ii) e a efetuada pela autoridade judiciária referida na subalínea i). Daqui resulta que a referida autoridade nacional deve apresentar um nível de independência e de imparcialidade tal que a fiscalização que exerce possa ser considerada uma alternativa comparável à fiscalização que pode ser efetuada por uma autoridade judiciária²⁵⁰.

268. Em segundo lugar, resulta dos trabalhos preparatórios da Diretiva PNR que o legislador da União, por um lado, não adotou a proposta da Comissão de encarregar o responsável da UIP da tarefa de autorizar a divulgação dos dados PNR integrais²⁵¹, e, por outro, alargou, elevando-o a seis meses, o prazo inicial de conservação desses dados proposto por esta instituição, que era de 30 dias. É neste contexto, caracterizado pela procura de um equilíbrio entre a duração do período de

²⁴⁹ No que respeita às dúvidas manifestadas pelo Governo belga quanto à competência do Tribunal de Justiça para responder à sétima questão prejudicial, importa observar que, segundo os termos desta questão, o órgão jurisdicional de reenvio interroga o Tribunal de Justiça sobre a interpretação do artigo 12.º, n.º 3, da Diretiva PNR e não sobre a compatibilidade da legislação nacional com esta disposição. Em qualquer caso, segundo jurisprudência constante, o Tribunal de Justiça pode dar indicações aos órgãos jurisdicionais nacionais que lhes permitam apreciar essa compatibilidade (v., nomeadamente, Acórdão de 7 de setembro de 2016, ANODE, C-121/15, EU:C:2016:637, n.º 54 e jurisprudência referida).

²⁵⁰ V., a este respeito, Acórdão de 5 de novembro de 2019, Comissão/Polónia (Independência dos tribunais comuns) (C-192/18, EU:C:2019:924, n.ºs 108 a 110).

²⁵¹ O artigo 9.º, n.º 2, quarto período, da Proposta de Diretiva PNR dispunha que «[o] acesso à integralidade dos dados PNR apenas será autorizado pelo responsável da unidade de informações de passageiros».

conservação antes da anonimização dos dados PNR e os requisitos a que está sujeito o seu mascaramento no final desse período, que se situa a decisão do legislador da União de submeter o acesso integral aos dados PNR a requisitos processuais mais estritos do que os inicialmente previstos pela Comissão e de encarregar uma autoridade independente da tarefa de verificar se estão preenchidos os requisitos para a divulgação.

269. Em terceiro lugar, como a Comissão corretamente observou, resulta da economia da Diretiva PNR que a razão de ser do procedimento de autorização previsto no artigo 12.º, n.º 3, da Diretiva PNR reside na atribuição a uma entidade terceira imparcial da tarefa de proceder, em cada caso concreto, a uma ponderação dos direitos das pessoas em causa com a finalidade repressiva prosseguida por esta diretiva.

270. Em quarto lugar, resulta da jurisprudência do Tribunal de Justiça que uma entidade incumbida de proceder à fiscalização prévia exigida para autorizar o acesso das autoridades nacionais competentes a dados pessoais legitimamente conservados deve dispor de todas as atribuições e apresentar todas as garantias necessárias a fim de assegurar uma conciliação dos diferentes interesses e direitos em causa. O Tribunal de Justiça precisou igualmente que essa entidade deve gozar de um estatuto que lhe permita agir, quando desempenha as suas missões, de maneira objetiva e imparcial e, para esse efeito, deve estar ao abrigo de qualquer influência externa²⁵². Em particular, atendendo à exigência de independência requerida, sobretudo no domínio penal, a autoridade encarregada da fiscalização prévia deve ter a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, pelo que não deve estar envolvida na condução de um inquérito penal e deve manter uma posição de neutralidade relativamente às partes no processo penal²⁵³.

271. Ora, há que constatar que a UIP não apresenta todas as garantias de independência e de imparcialidade que a autoridade encarregada de exercer a fiscalização prévia prevista no artigo 12.º, n.º 3, da Diretiva PNR deve satisfazer. Com efeito, as UIP estão diretamente ligadas às autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave. Em conformidade com o artigo 4.º, n.º 1, da Diretiva PNR, a própria UIP é uma dessas autoridades ou uma secção dela. Por outro lado, o n.º 3 deste artigo prevê que os membros do pessoal da UIP podem ser agentes destacados pelas autoridades competentes. É o caso, nomeadamente, da UIP belga que, nos termos do artigo 14.º da Lei PNR, é composta, designadamente, por membros destacados dos serviços policiais, da Segurança do Estado, do Serviço Geral de Informações e de Segurança, e da Administração Geral Aduaneira e dos Impostos Especiais de Consumo.

272. É certo que, de um modo geral, os membros da UIP devem oferecer todas as garantias de integridade, de competência, de transparência e de independência e incumbe aos Estados-Membros assegurar, sendo caso disso, que, tendo em conta os laços que os unem à corporação a que pertencem, essas garantias possam concretamente ser respeitadas, nomeadamente para evitar que as autoridades competentes na estrutura das quais esses membros estão originariamente inseridos tenham acesso direto ao banco de dados PNR, e não apenas aos resultados das recolhas efetuadas pelas UIP. Todavia, os membros das UIP que são destacados das autoridades competentes, na aceção do artigo 7.º, n.º 2, da Diretiva PNR, mantêm inevitavelmente uma ligação com os seus serviços de origem durante o período do seu destacamento, conservando o seu estatuto, mesmo que sejam colocados sob a autoridade funcional e hierárquica do funcionário dirigente da UIP.

²⁵² Acórdão Prokuratuur, n.ºs 52 e 53.

²⁵³ Acórdão Prokuratuur, n.ºs 53 e 54. V., no mesmo sentido, Acórdão Big Brother Watch, §§ 349 a 352.

273. A conclusão segundo a qual a UIP não é uma autoridade nacional na aceção do artigo 12.º, n.º 3, alínea b), ii), da Diretiva PNR é, por outro lado, corroborada pela circunstância de que, em conformidade com esta disposição, o responsável pela proteção de dados da UIP em causa deve ser «informado» do pedido de divulgação e procede a uma «verificação *ex-post*». Com efeito, no caso de a UIP estar habilitada, enquanto «outra autoridade nacional», a autorizar um pedido de divulgação nos termos do artigo 12.º, n.º 3, da Diretiva PNR, o responsável pela proteção de dados, que é incumbido, nomeadamente, em conformidade com o artigo 5.º, n.º 1, desta diretiva, de aplicar as salvaguardas relevantes que rodeiam o tratamento dos dados PNR, seria informado do pedido de acesso no momento da sua apresentação e a sua fiscalização ocorreria necessariamente *ex ante*²⁵⁴.

274. À luz das considerações precedentes, sugiro ao Tribunal de Justiça que responda à sétima questão prejudicial que o artigo 12.º, n.º 3, alínea b), da Diretiva PNR deve ser interpretado no sentido de que a UIP não constitui uma «outra autoridade nacional competente» na aceção desta disposição.

E. Quanto à nona questão prejudicial

275. Com a sua nona questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça, por um lado, se a Diretiva API é compatível com o artigo 3.º, n.º 2, TUE e com o artigo 45.º da Carta, na medida em que se aplica aos voos no interior da União e, por outro, se esta diretiva, em conjugação com o artigo 3.º, n.º 2, TUE e com o artigo 45.º da Carta, deve ser interpretada no sentido de que se opõe a uma legislação nacional que, para efeitos de combate à imigração ilegal e de melhoria dos controlos nas fronteiras, autoriza um sistema de recolha e de tratamento de dados dos passageiros que pode implicar indiretamente o restabelecimento dos controlos nas fronteiras internas.

276. Resulta da decisão de reenvio que esta questão prejudicial se insere no âmbito do exame do segundo fundamento de recurso, invocado pela LDH a título subsidiário. Este fundamento, relativo à violação do artigo 22.º da Constituição belga, em conjugação com o artigo 3.º, n.º 2, TUE e com o artigo 45.º da Carta, é dirigido contra o artigo 3.º, § 1, o artigo 8.º, § 2 e o capítulo 11, nomeadamente os artigos 28.º a 31.º, da Lei PNR. Embora o primeiro destes artigos enuncie, em termos gerais, o objeto desta lei, precisando que «determina as obrigações das transportadoras e dos operadores de viagens relativas à transmissão de dados dos passageiros com destino, proveniência ou trânsito em território nacional», o artigo 8.º, § 2, da referida lei prevê que, «nas condições previstas no capítulo 11 [da mesma], os dados dos passageiros são igualmente tratados a fim de melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal». No âmbito desta finalidade, em conformidade com o artigo 29.º, § 1, da Lei PNR, apenas os «dados dos passageiros» referidos no artigo 9.º, § 1, ponto 18, da mesma (a saber, os dados API mencionados no ponto 18 da Diretiva PNR), relativos a três categorias de passageiros, são transmitidos aos serviços policiais responsáveis pelo controlo nas fronteiras e ao Serviço de Estrangeiros (Bélgica). Trata-se dos «passageiros que tencionam entrar ou entraram no território pelas fronteiras externas da Bélgica», dos «passageiros que tencionam sair ou saíram do território pelas fronteiras externas da Bélgica» e dos «passageiros que tencionam passar, se encontram ou passaram numa zona internacional de trânsito situada na Bélgica»²⁵⁵. Resulta do artigo 29.º, § 3, da Lei PNR que os referidos dados são transmitidos pela UIP aos serviços policiais responsáveis

²⁵⁴ O artigo 9.º, n.º 2, quarto período, da Proposta de Diretiva PNR dispunha que «[o] acesso à integralidade dos dados PNR apenas será autorizado pelo responsável da unidade de informações de passageiros».

²⁵⁵ Lei PNR, artigo 29.º, §§ 1 e 2.

pelo controlo nas fronteiras e ao Serviço de Estrangeiros «imediatamente após o respetivo registo no banco de dados de passageiros» e que são destruídos vinte e quatro horas após a transmissão. Nos termos desta disposição, decorrido este prazo, o Serviço de Estrangeiros pode igualmente enviar à UIP um pedido fundamentado com vista a obter o acesso a esses mesmos dados quando tal se revele necessário no âmbito da sua função legal. Por conseguinte, o quadro jurídico em que se insere a nona questão prejudicial não é o da Diretiva PNR, dada a finalidade prosseguida pelo tratamento de dados previsto nos artigos 28.º e 29.º da Lei PNR, mas o da Diretiva API. Por outro lado, resulta, nomeadamente, dos autos apresentados na Secretaria do Tribunal de Justiça que o segundo fundamento da LDH assenta numa interpretação das disposições do capítulo 11 da Lei PNR segundo a qual estas se aplicam igualmente em caso de passagem das fronteiras internas da Bélgica.

277. A primeira parte da nona questão prejudicial baseia-se numa premissa errada e, na minha opinião, não necessita de resposta por parte do Tribunal de Justiça. Com efeito, resulta de forma inequívoca do artigo 3.º, n.º 1, da Diretiva API, em conjugação com o artigo 2.º, alíneas b) e d), da mesma, que esta diretiva só prevê a obrigação de as transportadoras aéreas transmitirem os dados API às autoridades responsáveis pelos controlos de passageiros nas fronteiras externas no que respeita aos voos que transportem passageiros até um ponto de passagem autorizado para a passagem das fronteiras externas dos Estados-Membros com países terceiros. De igual modo, o artigo 6.º, n.º 1, desta diretiva apenas prevê o tratamento dos dados API relativos a esses voos. Por outro lado, embora seja verdade que a Diretiva PNR prevê a possibilidade de os Estados-Membros alargarem a obrigação de transferir os dados API recolhidos igualmente às transportadoras aéreas que operam voos intra-UE, esse alargamento deve ser entendido sem prejuízo da Diretiva API²⁵⁶. No quadro da Diretiva PNR, os dados API transferidos são tratados apenas no âmbito das finalidades repressivas previstas por esta diretiva. Inversamente, o considerando 34 da Diretiva PNR prevê que esta é aplicável sem prejuízo das atuais regras da União sobre a forma como são efetuados os controlos nas fronteiras, nem das regras da União que regem a entrada e a saída do território da União, e o artigo 6.º, n.º 9, segundo período, desta diretiva dispõe que, quando as avaliações nos termos do n.º 2 deste artigo sejam efetuadas em relação a voos intra-UE operados entre Estados-Membros aos quais seja aplicável o Código das Fronteiras Schengen²⁵⁷, as consequências de tais avaliações devem observar o referido regulamento.

278. A reformulação desta parte da nona questão prejudicial, como sugere, a título subsidiário, a Comissão, no sentido de que visa a compatibilidade com as disposições do Tratado e da Carta não da Diretiva API, mas da Diretiva PNR, nomeadamente do seu artigo 2.º, implicaria não só a alteração do ato quanto ao qual o órgão jurisdicional de reenvio pediu uma apreciação da validade, como significaria igualmente a saída do quadro jurídico em que se situa esta questão prejudicial. Com efeito, como expliquei, as disposições do capítulo 11 da Lei PNR, contra as quais é dirigido o segundo fundamento de recurso, transpõem a Diretiva API e não a Diretiva PNR.

279. Para a hipótese de o Tribunal de Justiça proceder a essa reformulação, limito-me às reflexões que se seguem no que respeita, nomeadamente, à questão de saber se a avaliação prévia que os Estados-Membros estão autorizados a efetuar sobre os dados PNR dos passageiros dos voos intra-UE, em conformidade com a faculdade de que dispõem nos termos do artigo 2.º da Diretiva PNR, pode ser considerada equivalente ao exercício dos «controlos de fronteira» na aceção do

²⁵⁶ V. considerando 10 da Diretiva PNR.

²⁵⁷ Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016, que estabelece o código da União relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen) (JO 2016, L 77, p. 1, a seguir «Código das Fronteiras Schengen»).

artigo 23.º, alínea a), do Código das Fronteiras Schengen²⁵⁸. Em primeiro lugar, embora a avaliação prévia dos dados PNR não seja efetuada «no ponto de passagem de fronteira» ou no «momento da passagem da fronteira», mas antes desse momento, é, todavia, efetuada «devido» à passagem iminente das fronteiras. Em segundo lugar, em conformidade com o artigo 2.º da Diretiva PNR, os Estados-Membros estão autorizados a alargar a avaliação prévia dos dados PNR prevista no artigo 6.º, n.º 2, alínea a), da Diretiva PNR aos passageiros de todos os voos intra-UE, independentemente do comportamento das pessoas em causa e de circunstâncias que demonstrem um risco de perturbação da segurança pública. Esta avaliação prévia tem, além disso, carácter sistemático. Ora, nenhum destes elementos parece satisfazer os indícios visados no artigo 23.º, alínea a), segundo período, ii), iii) e iv), do Código das Fronteiras Schengen²⁵⁹. Em terceiro lugar, no que respeita aos indícios visados na alínea a), segundo período, i) e iii), deste artigo, pergunto-me se a avaliação prévia nos termos do artigo 6.º, n.º 2, alínea a), da Diretiva PNR não coincide, pelo menos em parte, com a finalidade dos controlos nas fronteiras efetuados em aplicação do artigo 8.º, n.º 2, alínea b), e n.º 3, alínea a), vi) e alínea g), iii), do Código das Fronteiras Schengen, conforme alterado pelo Regulamento 2017/458, e, sobretudo, se a mesma se distingue claramente, quanto às suas modalidades, desses controlos sistemáticos²⁶⁰. A este respeito, observo que o artigo 8.º, n.º 2-E e n.º 3, i-A) deste código precisa que os referidos controlos «podem ser realizados previamente, com base em dados dos passageiros recebidos nos termos da Diretiva [API] ou de outra legislação da União ou nacional». Todavia, é verdade que a finalidade da Diretiva PNR não é «garantir que as pessoas possam ser autorizadas a entrar no território do Estado-Membro ou a abandoná-lo», nem «impedir as pessoas de se subtraírem a essas inspeções», que o Tribunal de Justiça reconheceu serem os objetivos do «controlo fronteiriço» nos termos do Código das Fronteiras Schengen²⁶¹, tendo esta diretiva apenas uma finalidade exclusivamente repressiva. Além disso, o artigo 23.º, alínea a), segundo período, ii), do referido código prevê explicitamente que o exercício das competências de polícia não pode considerar-se equivalente ao exercício de controlos de fronteira, nos casos em que tais controlos se destinem particularmente a combater o crime transfronteiras²⁶². Por último, o Tribunal de Justiça deveria igualmente tomar em conta na sua apreciação a circunstância, sublinhada nomeadamente pela Comissão, de que o artigo 2.º da Diretiva PNR só autoriza os Estados-Membros a imporem às transportadoras aéreas a transferência dos dados PNR que tenham recolhido no exercício normal das suas atividades e não prevê, portanto, uma obrigação análoga à prevista pela Diretiva API para a passagem das fronteiras externas.

280. No que respeita à segunda parte da nona questão prejudicial, considero, à semelhança da Comissão, que deve ser entendida no sentido de que se refere à passagem das fronteiras internas e de que visa obter do Tribunal de Justiça esclarecimentos que permitam ao órgão jurisdicional de reenvio apreciar a compatibilidade das disposições do capítulo 11 da Lei PNR com a abolição dos controlos nas fronteiras internas dos Estados-Membros no espaço Schengen.

²⁵⁸ O artigo 23.º, alínea a), do Código das Fronteiras Schengen prevê que o exercício das competências de polícia não pode considerar-se equivalente ao exercício de controlos de fronteira, nomeadamente nos casos em que essas medidas policiais «i) não tiverem como objetivo o controlo fronteiriço; ii) se basearem em informações policiais de carácter geral e na experiência em matéria de possíveis ameaças à ordem pública e se destinarem particularmente a combater o crime transfronteiras; iii) forem concebidas e executadas de forma claramente distinta dos controlos sistemáticos de pessoas nas fronteiras externas; iv) forem aplicadas com base em controlos por amostragem».

²⁵⁹ V., por analogia, Acórdão de 13 de dezembro de 2018, Touring Tours und Travel e Sociedad de transportes (C-412/17 e C-474/17, EU:C:2018:1005, n.º 61 e jurisprudência referida), bem como Despacho de 4 de junho de 2020, FU (C-554/19, não publicado, EU:C:2020:439, n.ºs 51 a 56).

²⁶⁰ A este respeito, observo que, no n.º 188 do Parecer 1/15, o Tribunal de Justiça afirmou que «a identificação, através dos dados PNR, dos passageiros suscetíveis de representar um risco para a segurança pública faz parte dos controlos nas fronteiras».

²⁶¹ V. Acórdão de 13 de dezembro de 2018, Touring Tours und Travel e Sociedad de transportes (C-412/17 e C-474/17, EU:C:2018:1005, n.º 55 e jurisprudência referida).

²⁶² V., neste sentido, nomeadamente, Despacho de 4 de junho de 2020, FU (C-554/19, não publicado, EU:C:2020:439, n.º 46).

281. A este respeito, tendo em conta os poucos elementos de que o Tribunal de Justiça dispõe, limito-me a salientar que as disposições do capítulo 11 da Lei PNR só podem ser compatíveis com o direito da União, nomeadamente com o artigo 67.º, n.º 2, TFUE, se forem interpretadas no sentido de que visam apenas a transferência e o tratamento dos dados API dos passageiros que atravessam as fronteiras externas da Bélgica com países terceiros.

282. Na medida em que o Tribunal de Justiça decida reformular a segunda parte da nona questão prejudicial no sentido de que tem por objeto a interpretação da Diretiva PNR em relação às disposições do capítulo 11 da Lei PNR, limito-me a observar que o tratamento dos dados API previsto nos artigos 28.º e 29.º desta lei assenta no sistema instituído pelo legislador belga para transpor a Diretiva PNR. Assim, em primeiro lugar, os dados API que são objeto de tratamento são os enumerados no ponto 12 do anexo I desta diretiva e não apenas os contidos na lista que figura no artigo 3.º, n.º 2, da Diretiva API. Em segundo lugar, em conformidade com o artigo 29.º, § 1, da Lei PNR, esses dados são transmitidos aos serviços policiais responsáveis pelo controlo nas fronteiras e ao Serviço de Estrangeiros pela UIP — que é responsável pela recolha e pelo tratamento dos dados PNR apenas no âmbito das finalidades prosseguidas pela Diretiva PNR — e não, como previsto na Diretiva API, diretamente pelas transportadoras aéreas. Por outro lado, esta transmissão abrange igualmente os dados dos passageiros que tencionem sair ou tenham saído do território belga e não tem como únicos destinatários as autoridades responsáveis pelos controlos nas fronteiras, mas também o Serviço de Estrangeiros, que é responsável pela gestão da população imigrante e pelo combate à imigração clandestina. Em terceiro lugar, nos termos do artigo 29.º, § 4, segundo parágrafo, da Lei PNR, o Serviço de Estrangeiros parece estar habilitado a enviar à UIP pedidos de acesso aos dados API mesmo após o tratamento desses dados por ocasião da passagem das fronteiras pelos passageiros em causa. Neste sentido, este serviço é, de facto, equiparado a uma autoridade competente nos termos do artigo 7.º da Diretiva PNR, embora não tenha essa natureza e não figure na lista dessas autoridades que foi comunicada à Comissão pela Bélgica. Ora, esta amálgama entre os sistemas previstos pela Diretiva API e pela Diretiva PNR não pode, na minha opinião, ser admitida, na medida em que viola o princípio da limitação das finalidades consagrado no artigo 1.º, n.º 2, da Diretiva PNR²⁶³.

283. Com base em todas as considerações precedentes, proponho ao Tribunal de Justiça que responda à nona questão prejudicial que o artigo 3.º, n.º 1, da Diretiva API, nos termos do qual os Estados-Membros devem tomar as disposições necessárias para obrigar as transportadoras aéreas a transmitirem, até ao final do registo de embarque e a pedido das autoridades responsáveis pelos controlos de passageiros nas fronteiras externas, as informações relativas aos passageiros previstas no n.º 2 deste artigo, em conjugação com o artigo 2.º, alíneas b) e d), desta diretiva, diz apenas respeito aos passageiros transportados até um ponto de passagem autorizado para a passagem das fronteiras externas dos Estados-Membros com países terceiros. Uma legislação nacional que, com o único objetivo de melhorar os controlos nas fronteiras e de combater a imigração ilegal, alargasse essa obrigação aos dados das pessoas que atravessam as fronteiras internas do Estado-Membro em causa por avião ou por outros meios de transporte seria contrária ao artigo 67.º, n.º 2, TFUE e ao artigo 22.º do Código das Fronteiras Schengen.

²⁶³ No seu Documento de trabalho de 2020 sobre a Diretiva API (p. 20), a Comissão sublinha igualmente o carácter problemático de uma sobreposição dos sistemas de tratamento dos dados PNR e API a nível nacional.

F. Quanto à décima questão prejudicial

284. Com a sua décima questão prejudicial, o órgão jurisdicional de reenvio pergunta, em substância, ao Tribunal de Justiça se, no caso de concluir que a Lei PNR viola os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, pode manter provisoriamente os efeitos dessa lei a fim de evitar uma insegurança jurídica e permitir que os dados recolhidos e conservados anteriormente possam ainda ser utilizados para os fins previstos pela Lei PNR.

285. O Tribunal de Justiça respondeu a uma questão com o mesmo teor no Acórdão La Quadrature du Net, relativo ao armazenamento dos metadados das comunicações eletrónicas, proferido após a apresentação do presente pedido prejudicial. Nesse acórdão, o Tribunal de Justiça começou por recordar a sua jurisprudência segundo a qual, se os órgãos jurisdicionais nacionais pudessem, ainda que a título provisório, dar primado sobre o direito da União a disposições nacionais a ele contrárias, ficariam comprometidos o primado e a aplicação uniforme do direito da União. Em seguida, recordou que, no Acórdão de 29 de julho de 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen²⁶⁴, em que estava em causa a legalidade de medidas adotadas em violação da obrigação, imposta pelo direito da União, de ser efetuada uma avaliação prévia do impacto de um projeto no ambiente e num local protegido, admitiu que um órgão jurisdicional nacional pode, se o direito interno o permitir, excecionalmente manter os efeitos de medidas quando esta manutenção seja justificada por considerações imperiosas ligadas à necessidade de afastar uma ameaça real e grave de rutura do abastecimento em eletricidade do Estado-Membro em causa, pelo período de tempo estritamente necessário para sanar essa ilegalidade. Concluiu, todavia, que, contrariamente à omissão de uma obrigação processual como a avaliação prévia do impacto de um projeto no domínio específico da proteção do ambiente, uma violação dos direitos fundamentais garantidos nos artigos 7.º e 8.º da Carta não pode ser objeto de regularização por meio de um procedimento comparável ao previsto no acórdão acima mencionado²⁶⁵. A mesma resposta deve, na minha opinião, ser dada à décima questão prejudicial no presente processo.

286. Na medida em que tanto o órgão jurisdicional de reenvio como o Governo belga, bem como a Comissão e o Conselho, se interrogam sobre a questão de saber se o direito da União se opõe a uma exploração, no âmbito de um processo penal, de informações ou elementos de prova obtidos utilizando os dados PNR recolhidos, tratados e/ou conservados de forma incompatível com o direito da União, recordo que, no n.º 222 do Acórdão La Quadrature du Net, o Tribunal de Justiça precisou que, na fase atual do direito da União, em princípio, cabe exclusivamente ao direito nacional determinar as regras relativas à admissibilidade e à apreciação, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de criminalidade grave, de informações e de elementos de prova obtidos através de uma conservação de dados contrária ao direito da União, sob reserva do respeito dos princípios da equivalência e da efetividade. No que respeita a este último, o Tribunal de Justiça declarou que este princípio impõe que o tribunal penal nacional rejeite as informações e elementos de prova obtidos através de uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização incompatível com o direito da União, no âmbito de um processo penal instaurado contra pessoas suspeitas da prática de crimes, se essas pessoas não estiverem em condições de se pronunciarem eficazmente sobre essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de forma preponderante a apreciação dos factos. Estes princípios são igualmente transponíveis, *mutatis mutandis*, para as circunstâncias do processo principal.

²⁶⁴ C-411/17, EU:C:2019:622, n.ºs 175, 176, 179 e 181.

²⁶⁵ V. Acórdão La Quadrature du Net, n.ºs 217 a 219.

III. Conclusão

287. Com base em todas as considerações precedentes, sugiro ao Tribunal de Justiça que responda do seguinte modo às questões prejudiciais submetidas pela Cour constitutionnelle (Tribunal Constitucional, Bélgica):

- 1) O artigo 23.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), em conjugação com o artigo 2.º, n.º 2, alínea d), deste regulamento, deve ser interpretado no sentido de que:
 - é aplicável a uma legislação nacional que transpõe a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, na medida em que essa legislação regule os tratamentos dos dados PNR efetuados pelas transportadoras aéreas e por outros operadores económicos, incluindo a transferência de dados PNR para as unidades de informações de passageiros (UIP) a que se refere o artigo 4.º desta diretiva, prevista no artigo 8.º da mesma;
 - não é aplicável a uma legislação nacional que transpõe a Diretiva 2016/681, na medida em que regule os tratamentos de dados efetuados, para as finalidades previstas no artigo 1.º, n.º 2, desta diretiva, pelas autoridades competentes, incluindo as UIP e, se for caso disso, os serviços de segurança e de informações do Estado-Membro em causa;
 - é aplicável a uma legislação nacional que transpõe a Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras, e a Diretiva 2010/65/UE do Parlamento Europeu e do Conselho, de 20 de outubro de 2010, relativa às formalidades de declaração exigidas aos navios à chegada e/ou à partida dos portos dos Estados-Membros e que revoga a Diretiva 2002/6/CE com vista a melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal.
- 2) O ponto 12 do anexo I da Diretiva 2016/681 é inválido na medida em que inclui as «observações gerais» entre as categorias de dados PNR que as transportadoras aéreas são obrigadas a transmitir às UIP, em conformidade com o artigo 8.º desta diretiva.
- 3) O exame das segunda, terceira, quarta, sexta e oitava questões não revelou outros elementos suscetíveis de afetar a validade da Diretiva 2016/681.
- 4) O ponto 12 do anexo I da Diretiva 2016/681, na parte que não é declarada inválida, deve ser interpretado no sentido de que abrange apenas as informações relativas aos menores que nele são expressamente mencionadas e que têm uma relação direta com o voo.
- 5) O ponto 18 do anexo I da Diretiva 2016/681 deve ser interpretado no sentido de que abrange apenas as informações prévias sobre os passageiros expressamente enumeradas neste ponto bem como no artigo 3.º, n.º 2, da Diretiva 2004/82 e que tenham sido recolhidas pelas transportadoras aéreas no exercício normal das suas atividades.

- 6) O conceito de «bases de dados relevantes» previsto no artigo 6.º, n.º 3, da Diretiva 2016/681 deve ser interpretado no sentido de que visa apenas as bases de dados nacionais geridas pelas autoridades competentes nos termos do artigo 7.º, n.º 1, desta diretiva, bem como as bases de dados da União e internacionais exploradas diretamente por essas autoridades no âmbito das respetivas missões. As referidas bases de dados devem ter uma relação direta e estreita com as finalidades de luta contra o terrorismo e a criminalidade grave prosseguidas pela referida diretiva, o que implica que tenham sido desenvolvidas para essas finalidades. No âmbito da transposição da Diretiva 2016/681 para o seu direito nacional, os Estados-Membros são obrigados a publicar uma lista das referidas bases de dados e a mantê-la atualizada.
- 7) O artigo 6.º, n.º 3, alínea b), da Diretiva 2016/681 deve ser interpretado no sentido de que se opõe à utilização, no âmbito do tratamento automatizado previsto nesta disposição, de sistemas algorítmicos que possam resultar numa alteração, sem intervenção humana, dos critérios preestabelecidos com base nos quais esse tratamento foi efetuado e que não permitam identificar de forma clara e transparente os motivos que conduziram a um resultado positivo na sequência do referido tratamento.
- 8) O artigo 12.º, n.º 1, da Diretiva 2016/681, lido em conformidade com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que a conservação dos dados PNR fornecidos pelas transportadoras aéreas à UIP numa base de dados por um prazo de cinco anos após a sua transferência para a UIP do Estado-Membro em cujo território o voo aterre ou de cujo território descole só é permitida, depois de efetuada a avaliação prévia nos termos do artigo 6.º, n.º 2, alínea a), desta diretiva, na medida em que se demonstre, com base em critérios objetivos, uma relação entre esses dados e a luta contra o terrorismo ou a criminalidade grave. Uma conservação generalizada e indiferenciada dos dados PNR sob uma forma não anonimizada só pode ser justificada perante uma ameaça grave para a segurança dos Estados-Membros que se revele real e atual ou previsível, associada, por exemplo, a atividades de terrorismo, e na condição de a duração dessa conservação se limitar ao estritamente necessário.
- 9) O artigo 6.º, n.º 2, alínea b), da Diretiva 2016/681 deve ser interpretado no sentido de que a disponibilização dos dados PNR ou do resultado do tratamento desses dados nos termos desta disposição, que ocorra durante o prazo inicial de seis meses previsto no artigo 12.º, n.º 2, desta diretiva, deve respeitar os requisitos enunciados no artigo 12.º, n.º 3, alínea b), da referida diretiva.
- 10) A Diretiva 2016/681, nomeadamente o seu artigo 1.º, n.º 2, e o seu artigo 6.º, deve ser interpretada no sentido de que se opõe a uma legislação nacional que admite como finalidade do tratamento dos dados PNR o acompanhamento de certas atividades dos serviços de informações e de segurança, na medida em que, no âmbito dessa finalidade, a UIP nacional seja levada a tratar os referidos dados e/ou a transmiti-los, ou os resultados do seu tratamento, aos referidos serviços para fins diferentes dos que são exaustivamente indicados no artigo 1.º, n.º 2, desta diretiva, o que cabe ao órgão jurisdicional nacional verificar.
- 11) O artigo 12.º, n.º 3, alínea b), da Diretiva PNR deve ser interpretado no sentido de que a UIP não constitui uma «outra autoridade nacional competente» na aceção desta disposição.

- 12) O artigo 3.º, n.º 1, da Diretiva 2004/82, nos termos do qual os Estados-Membros devem tomar as disposições necessárias para obrigar as transportadoras aéreas a transmitirem, até ao final do registo de embarque e a pedido das autoridades responsáveis pelos controlos de passageiros nas fronteiras externas, as informações relativas aos passageiros previstas no n.º 2 deste artigo, em conjugação com o artigo 2.º, alíneas b) e d), desta diretiva, diz apenas respeito aos passageiros transportados até um ponto de passagem autorizado para a passagem das fronteiras externas dos Estados-Membros com países terceiros. Uma legislação nacional que, com o único objetivo de melhoria dos controlos nas fronteiras e de combate à imigração ilegal, alargasse essa obrigação aos dados das pessoas que atravessam as fronteiras internas do Estado-Membro em causa por avião ou por outros meios de transporte seria contrária ao artigo 67.º, n.º 2, TFUE e ao artigo 22.º do Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016, que estabelece o código da União relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen).
- 13) Um órgão jurisdicional nacional não pode aplicar uma disposição de direito nacional que o habilite a limitar no tempo os efeitos de uma declaração de ilegalidade que lhe incumbe, por força desse direito, relativamente a uma legislação nacional que impõe às transportadoras aéreas, terrestres e marítimas, bem como aos operadores de viagens, com vista a lutar contra o terrorismo e a criminalidade grave, uma transferência dos dados PNR dos passageiros e prevê um tratamento e uma conservação generalizados e indiferenciados desses dados incompatíveis com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais. Em aplicação do princípio da efetividade, o tribunal penal nacional deve rejeitar as informações e elementos de prova obtidos em aplicação de tal legislação incompatível com o direito da União, no âmbito de um processo penal instaurado contra pessoas suspeitas de atos de terrorismo ou de criminalidade grave, se essas pessoas não estiverem em condições de se pronunciar eficazmente sobre essas informações e elementos de prova, provenientes de um domínio que escapa ao conhecimento dos juízes e que são suscetíveis de influenciar de forma preponderante a apreciação dos factos.

ⁱ — Os n.ºs 37, 107, 119, 121, 144, 168, 189, 203, 228, 268 e as notas de pé de página 184 e 211 do presente texto foram objeto de uma alteração de ordem linguística, posteriormente à sua disponibilização em linha.