Processo C-817/19

Resumo do pedido de decisão prejudicial em aplicação do artigo 98.°, n.° 1, do Regulamento de Processo do Tribunal de Justiça

Data de entrada:

31 de outubro de 2019

Órgão jurisdicional de reenvio:

Cour constitutionnelle (Tribunal Constitucional, Bélgica)

Data da decisão de reenvio:

17 de outubro de 2019

Recorrente:

ASBL «Ligue des droits humains»

I. Objeto do recurso e posição das partes

1 O legislador belga adotou a 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) (*Moniteur belge* de 25 de janeiro de 2017, a seguir «Lei PNR»), para transpor essencialmente:

– 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 para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (a seguir também «Diretiva PNR»).

– 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 também «Diretiva API»).

2 A Lei PNR obriga diferentes setores de transporte internacional de pessoas (aéreo, ferroviário, rodoviário internacional e marítimo) e operadores de viagens a transmitir os dados dos seus passageiros a um banco de dados gerido pelo SPF Interior.

3 Para o efeito, a lei cria dentro do SPF Interior uma «unidade de informações de passageiros» (artigos 12.° a 14.°), composta, designadamente, por membros destacados de serviços de polícia, de segurança do Estado, de informações e de segurança e aduaneiros, e encarregada, nomeadamente, da recolha, da conservação e do tratamento de dados dos passageiros transmitidos pelas transportadoras e pelos operadores de viagens.

4 O «banco de dados dos passageiros» inclui, por um lado, os dados da reserva e, por outro, os dados de registo e de embarque [designados de «API» *Advance Passenger Information* e de «PNR» (*Passenger Name Record)*] (artigo 9.°).

5 Estes dados são tratados, nomeadamente, para efeitos de investigação, repressão e execução de penas, relativas a infrações penais previstas na lei, bem como para efeitos de prevenção de perturbações graves da segurança pública no contexto da radicalização violenta, do acompanhamento das atividades dos serviços de informações e de segurança e com vista a melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal (artigo 8.°).

6 O tratamento de dados pode intervir no âmbito da avaliação prévia dos passageiros (antes da sua partida ou chegada) (artigos 24.° a 26.°) ou no âmbito de investigações pontuais (artigo 27.°).

7 A lei prevê que os dados dos passageiros são conservados no banco de dados dos passageiros por um período máximo de cinco anos a contar do respetivo registo (artigos 18.° a 23.°).

8 A ASBL «Ligue des droits humains» critica a lei nas sete vertentes seguintes:

– as modalidades de execução da Lei de 25 de dezembro de 2016 (artigo 3.°, n.° 2, e artigo 7.°, n.° 3);

– os conceitos de «documentos de identidade» e de «documentos de viagem» (artigo 7.°, n.os 1 e 2);

– os dados abrangidos (artigos 4.°, 9.°, e 9.°);

– o conceito de «passageiro» (artigo 4.°, 10.°);

– as finalidades do tratamento de dados «PNR» (artigo 8.°);

– a gestão do banco de dados dos passageiros e o tratamento de dados no âmbito da avaliação prévia dos passageiros e de investigações pontuais (artigos 12.° a 16.° e 24.° a 27.° e artigos 50.° e 51.°);

– o prazo de conservação dos dados PNR (artigo 18.°).

9 A ASBL «Ligue des droits humains» denuncia irregularidades na referida lei e interpôs na Cour constitutionnelle (Tribunal Constitucional, Bélgica) um recurso de anulação baseado em dois fundamentos.

10 O primeiro fundamento é relativo, essencialmente, ao artigo 23.° do Regulamento (UE) 2016/679 [1], aos artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta») e ao artigo 8.° da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a seguir «CEDH»).

11 Sustenta, em substância, que a ingerência no direito ao respeito da vida privada e no direito à proteção dos dados pessoais é ilícita na medida em que não satisfaz os critérios de legalidade, de necessidade e de proporcionalidade.

12 Em primeiro lugar, a Lei PNR confere uma importante margem de apreciação ao poder executivo, encarregando-o de definir, por decreto real, determinados elementos essenciais, em violação do princípio da legalidade, que exige que a ingerência seja prevista por lei ou, em caso de delegação no Rei, que os elementos essenciais sejam previstos por lei de forma suficientemente precisa e pormenorizada.

Por outro lado, a lei impugnada não prossegue um objetivo legítimo. Com efeito, a lei prevê uma avaliação prévia dita «*pre-screening*», que consiste em avaliar o risco que representam os passageiros, antes da chegada, do trânsito ou da partida em território nacional.

13 A recorrente contesta, em seguida, a necessidade das medidas impugnadas para realizar o fim visado.

Sustenta que uma correspondência dos dados, nitidamente menos intrusiva na vida privada do que a criação de um banco de dados, permite igualmente atingir o objetivo prosseguido.

14 Por último, a recorrente sustenta que a lei impugnada não respeita o princípio da proporcionalidade, na medida em que os dados são recolhidos de forma indiferenciada e generalizada pelos operadores, e transmitidos às autoridades competentes para serem conservados durante cinco anos, sem distinção, diferenciação, limitação ou exceção em função do objetivo prosseguido.

15 Mais especificamente, a lei viola o princípio da proporcionalidade, atendendo a) ao seu âmbito de aplicação e às categorias de dados abrangidos, b) aos tratamentos de dados que institui, c) às suas finalidades e d) ao prazo de conservação dos dados.

16 Antes de mais, a lei impugnada define de forma muito lata os dados recolhidos, que excedem manifestamente o que é estritamente necessário.

[1] 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), JO 2016, L 119, p. 1 (a seguir também «RGPD»).

17 A recorrente refere que parece – mas a lei não é clara – que o *pre-screening* deve ser efetuado no banco de dados centralizado na UIP, com a ajuda de critérios preestabelecidos que servem de indicadores da ameaça. Ora, a Lei PNR não define nem a natureza precisa dos bancos de dados utilizados para a correlação, nem as modalidades desta última. A Lei PNR também não prevê que esta correlação esteja limitada às bases de dados exploradas para o combate ao terrorismo e à criminalidade grave.

18 A recorrente critica igualmente as investigações pontuais que a lei prevê sem precisar os dados efetivamente acessíveis.

19 A recorrente também denuncia as finalidades do tratamento de dados, que são nitidamente mais amplas do que as previstas pela Diretiva PNR, como a luta contra a imigração ilegal, atividades suscetíveis de constituir uma ameaça para os interesses fundamentais do Estado ou ainda a luta contra a «radicalização violenta», definida somente numa circular.

20 Por último, a recorrente critica o prazo de conservação dos dados de cinco anos. O legislador não justificou a escolha do prazo máximo autorizado pela Diretiva PNR, o que revela o caráter desproporcionado da medida.

21 O Conselho de Ministros (que defende a lei) suscita, a título principal, a inadmissibilidade do primeiro fundamento, na medida em que se baseia na violação do artigo 23.° do RGPD, quando resulta claramente tanto do considerando 19 do RGPD como do artigo 1.° da Diretiva PNR que o tratamento de dados «PNR» não é abrangido pelo RGPD, mas pela cooperação judiciária e policial entre os Estados-Membros e pela Diretiva (UE) 2016/680 [2].

22 Por outro lado, o Conselho de Ministros sustenta que o princípio da legalidade não é violado, uma vez que a lei contém os elementos essenciais das medidas que prevê e que a habilitação concedida ao Rei é suficientemente precisa. De resto, a exigência de legalidade deve ser entendida num sentido material segundo o Tribunal Europeu dos Direitos do Homem, de modo que os atos regulamentares satisfazem o conceito de «lei» na aceção da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

A Lei PNR visa garantir a segurança pública, permitindo não só a repressão das infrações terroristas ou de certas formas de criminalidade grave, mas também, através de uma análise prévia dos dados recolhidos, a prevenção destas infrações. O Tribunal de Justiça reconheceu que esses objetivos são legítimos na aceção do artigo 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, tanto no

[2] 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 (JO 2016, L 119, p. 89) (a seguir «Diretiva 2016/680»).

seu Acórdão de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), como no seu Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592.

23 O Conselho de Ministros considera que as medidas impugnadas são proporcionadas.

24 No que respeita à criação de um banco de dados «passageiros», o Conselho de Ministros salienta que a recorrente se limita a afirmar, sem o demonstrar, que uma correspondência dos dados permitia realizar o objetivo prosseguido e era menos intrusiva no direito ao respeito da vida privada. Acrescenta que uma simples correspondência não é suficiente para realizar as avaliações prévias com vista a identificar os riscos para a segurança. A criação de uma base de dados permite, aliás, respeitar o considerando 25 da Diretiva PNR, que convida a conservar os dados durante o período necessário tendo em conta os objetivos prosseguidos.

25 No que respeita à correlação entre as diferentes bases de dados, o Conselho de Ministros recorda que os artigos 24.° e 25.° da Lei PNR transpõem o artigo 6.° da Diretiva PNR. Por outro lado, resulta dos trabalhos preparatórios que o legislador não pretende operar uma correlação entre o banco de dados «passageiros» e todos os bancos de dados a que têm acesso as autoridades competentes, mas apenas entre o banco de dados «passageiros» e os que correspondem às finalidades prosseguidas pela lei impugnada. Estas medidas estão em conformidade com os ensinamentos do Parecer 1/15 do Tribunal de Justiça, uma vez que o artigo 6.°, n.° 3, da Diretiva PNR também não precisa quais os bancos de dados que podem ser correlacionados. O poder de apreciação também não é incompatível com o princípio da legalidade, tal como interpretado pelo Tribunal Europeu dos Direitos do Homem.

Por outro lado, o objetivo da lei não pode ser alcançado se os viajantes conhecessem antecipadamente os critérios que irão resultar numa correspondência positiva, pois poderiam adaptar o seu comportamento em conformidade. Além disso, o artigo 16.° da lei impugnada indica claramente que o *pre-screening* deve ser efetuado na base de dados «passageiros», o que é, portanto, conforme com o princípio da legalidade.

26 No que respeita ao prazo de conservação dos dados, o Conselho de Ministros considera que não é irrazoável prever um prazo de conservação de cinco anos, o que corresponde, aliás, ao prazo mínimo de prescrição do procedimento criminal.

O prazo de conservação destes dados, que é conforme com o prazo previsto pela Diretiva PNR, não é, portanto, desproporcionado.

27 O segundo fundamento, invocado a título subsidiário, é relativo, em substância, à violação das disposições conjugadas do artigo 3.°, n.° 2, TFUE e do artigo 45.° da Carta.

28 A recorrente sustenta que o artigo 3.°, n.° 1, o artigo 8.°, n.° 2, e o capítulo 11, que contém os artigos 28.° a 31.°, da Lei PNR são contrários à livre circulação de pessoas, na medida em que abrangem não só os transportes extra-UE, mas também os transportes intra-UE (incluindo as escalas). Por outras palavras, a recorrente considera que, ao alargar o sistema «PNR» aos voos intra-UE, as disposições impugnadas restabelecem indiretamente controlos nas fronteiras que são contrários à liberdade de circulação das pessoas.

29 O Conselho de Ministros considera que a lei impugnada não restabelece nenhum controlo nas fronteiras e não viola a liberdade de circulação das pessoas. A Diretiva PNR não se aplica à imigração ilegal e a lei impugnada transpõe não só a Diretiva PNR, mas também a Diretiva API.

O fundamento, tal como formulado, visa apenas o artigo 3.°, n.° 1, o artigo 8.°, n.° 2, e o capítulo 11 da lei impugnada. Ora, resulta da definição do conceito de «fronteiras externas» que a Lei PNR visa apenas os controlos extra-UE. Além disso, a Lei PNR transpõe a Diretiva 2004/82/CE, pelo que não pode ser interpretada no sentido de restaurar um controlo nas fronteiras do espaço Schengen.

A título infinitamente subsidiário, o considerando 10 da Diretiva PNR prevê expressamente a possibilidade de alargar a utilização dos dados «PNR» aos voos intra-UE, o que demonstra que esta medida não é, em si mesma, contrária à liberdade de circulação nem ao Regulamento (CE) n.° 562/2006.

II. Quadro jurídico

Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais

30 O artigo 8.° dispõe:

«1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.»

Direito da União

Carta dos Direitos Fundamentais da União Europeia

31 O artigo 7.° da Carta («Respeito pela vida privada e familiar») dispõe:

«Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.»

32 O artigo 8.° da Carta («Proteção de dados pessoais») dispõe:

«1. Todas as pessoas têm direito à proteção dos dados de caráter 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.»

33 O artigo 52.°, n.° 1, da Carta dispõe:

«Qualquer 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.»

Regulamento Geral sobre a Proteção de Dados (RGPD)

34 O artigo 2.°, n.° 2, alínea d), dispõe:

«2. O presente regulamento não se aplica ao tratamento de dados pessoais:

[…]

d) 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.»

35 O artigo 23.° dispõe:

«1. 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.° a 22.° e no artigo 34.°, bem como no artigo 5.°, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.° a 22.°, 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:

a) A segurança do Estado;

b) A defesa;

c) A segurança pública;

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;

e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;

f) A defesa da independência judiciária e dos processos judiciais;

g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;

h) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a e) e g);

i) A defesa do titular dos dados ou dos direitos e liberdades de outrem;

j) A execução de ações cíveis.

2. Em especial, as medidas legislativas referidas no n.° 1 incluem, quando for relevante, disposições explícitas relativas, pelo menos:

a) Às finalidades do tratamento ou às diferentes categorias de tratamento;

b) Às categorias de dados pessoais;

c) Ao alcance das limitações impostas;

d) Às garantias para evitar o abuso ou o acesso ou transferência ilícitos;

e) À especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

f) Aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento;

g) Aos riscos específicos para os direitos e liberdades dos titulares dos dados; e

h) Ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.»

Diretiva PNR

36 O artigo 3.° tem a seguinte redação:

Para efeitos da presente diretiva, entende-se por:

«[…]

4) "Passageiro", uma pessoa, incluindo pessoas em trânsito ou em correspondência e excluindo membros da tripulação, transportada ou a transportar numa aeronave com o consentimento da transportadora aérea, decorrendo esse consentimento do registo dessa pessoa na lista de passageiros.»

37 O artigo 4.° dispõe:

«Unidade de informações de passageiros

1. Cada 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).

2. A UIP é responsável:

a) Pela recolha dos dados PNR junto das transportadoras aéreas, pela conservação e pelo tratamento desses dados e pela transferência desses dados ou dos resultados do seu tratamento às autoridades competentes referidas no artigo 7.°;

b) Pelo intercâmbio de dados PNR e dos resultados do seu tratamento com as UIP de outros Estados-Membros e com a Europol, nos termos dos artigos 9.° e 10.°

[…].»

38 O artigo 6.° dispõe:

«1. Os dados PNR transferidos pelas transportadoras aéreas são recolhidos pela UIP do Estado-Membro em causa, conforme previsto no artigo 8.° Caso 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.

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.° e, se for caso disso, pela Europol, nos termos do artigo 10.°;

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.° 3, alínea b), a fim de identificar pessoas que possam estar implicadas em infrações terroristas ou em formas de criminalidade grave.

[…]»

39 O artigo 12.° dispõe:

«1. Os Estados-Membros asseguram que os dados PNR fornecidos pelas transportadoras aéreas à UIP sejam conservados numa base de dados dessa UIP 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.

2. Decorrido um prazo de seis meses após a transferência dos dados PNR referida no n.° 1, todos os dados PNR são anonimizados mediante mascaramento dos seguintes elementos de dados suscetíveis de identificar diretamente o passageiro ao qual dizem respeito os dados PNR:

a) Nome(s), incluindo os nomes de outros passageiros mencionados nos PNR, bem como o número de passageiros nos PNR que viajam em conjunto;

b) Endereço e informações de contacto;

c) Todas as informações sobre os meios de pagamento, incluindo o endereço de faturação, na medida em que contenham informações suscetíveis de identificar diretamente o passageiro ao qual os PNR dizem respeito ou quaisquer outras pessoas;

d) Informação de passageiro frequente;

e) Observações gerais, na medida em que contenham informações suscetíveis de permitir identificar diretamente o passageiro ao qual os PNR dizem respeito; e

f) Quaisquer dados API que tenham sido recolhidos.

3. Decorrido o prazo de seis meses referido no n.° 2, só é permitida a divulgação dos dados PNR integrais caso essa divulgação seja:

a) Considerada necessária, com base em motivos razoáveis, para os fins referidos no artigo 6.°, n.° 2, alínea b); e

b) Autorizada por:

i) uma autoridade judiciária, ou

ii) 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*.

4. Os Estados-Membros asseguram que os dados PNR sejam apagados de forma definitiva no termo do prazo referido no n.° 1. Esta obrigação aplica-se sem prejuízo dos casos em que dados PNR específicos tenham sido transferidos para uma autoridade competente e sejam utilizados no âmbito de um caso específico para efeitos de prevenção, deteção, investigação ou repressão de infrações terroristas ou criminalidade grave; nesse caso a conservação dos dados pela autoridade competente rege-se pelo direito nacional.

5. O resultado do tratamento a que se refere o artigo 6.°, n.° 2, alínea a), só é conservado pela UIP durante o período necessário para informar as autoridades competentes e, nos termos do artigo 9.°, n.° 1, as UIP de outros Estados-Membros, de um resultado positivo. Caso se constate, na sequência de uma verificação individual por meios não automatizados referida no artigo 6.°, n.° 5, alínea a), que o resultado do tratamento automatizado é negativo, este pode, ainda assim, ser conservado a fim de evitar "falsos" resultados positivos no futuro, desde que os dados de base não sejam apagados, nos termos do n.° 4 do presente artigo.»

40 O anexo I da Diretiva PNR, intitulado «Dados dos registos de identificação dos passageiros recolhidos pelas transportadoras aéreas», menciona nomeadamente:

«[…]

12. 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)

[…]

18. 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)

[…]»

Diretiva API

41 O artigo 1.° dispõe:

«A presente diretiva tem por objeto melhorar os controlos de fronteira e combater a imigração ilegal através da transmissão antecipada, pelas transportadoras, dos dados dos passageiros às autoridades nacionais competentes.»

Direito belga

42 As disposições pertinentes da **Lei PNR** (conforme alterada pelas Leis de 15 e 30 de julho de 2018 e pela Lei de 2 de maio de 2019) são as seguintes:

«CAPÍTULO 2. Âmbito de aplicação

Artigo 3.° § 1 A presente lei 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.

§ 2. O Rei determina por decreto aprovado em Conselho de Ministros, por setor de transportes e para os operadores de viagens, os dados dos passageiros a transmitir e as respetivas modalidades de transmissão, após parecer da autoridade competente de fiscalização dos tratamentos de dados pessoais. […]

CAPÍTULO 3. Definições

Artigo 4.° Para efeitos da aplicação da presente lei e dos seus decretos de execução, entende-se por:

[...]

9.° "PNR": o registo das formalidades de viagem impostas a cada passageiro, que contém as informações referidas no artigo 9.°, necessárias para permitir o tratamento e o controlo das reservas feitas pelas transportadoras e operadores de

viagens 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 utilizados para efetuar o controlo dos passageiros embarcados nos voos, ou de sistemas equivalentes que ofereçam as mesmas funcionalidades;

10.° "Passageiro", uma pessoa, incluindo pessoas em trânsito ou em correspondência e excluindo membros da tripulação, transportada ou a transportar pela transportadora com o consentimento desta última, decorrendo esse consentimento do registo dessa pessoa na lista de passageiros;

[…]

CAPÍTULO 5. Finalidades do tratamento de dados

Artigo 8.° § 1 Os dados dos passageiros são tratados para efeitos de:

1.° Investigação e repressão, incluindo a execução de penas ou medidas restritivas da liberdade, relativas às infrações previstas [no] Code d'Instruction criminelle (Código de Processo Penal);

2.° Investigação e repressão, incluindo a execução de penas ou medidas restritivas da liberdade, relativas às infrações previstas [no] Code pénal (Código Penal);

3.° 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, § 1, 2.° e 3.°, e § 2, da loi du 5 août 1992 sur la fonction de police (Lei, de 5 de agosto de 1992, relativa à função de polícia);

4.° Acompanhamento das atividades referidas no artigo 7.°, 1.° e 3.°/l, e no artigo 11.°, § 1, 1.° a 3.° e 5.°, 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);

5.° Investigação e repressão das infrações previstas [em diferentes leis].

§ 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.

CAPÍTULO 6. Dados dos passageiros

Artigo 9.° § 1 No que respeita aos dados da reserva, os dados dos passageiros devem, no máximo, incluir:

1.° o código de identificação do registo PNR;

2.° a data da reserva e de emissão do bilhete;

3.° as datas da viagem prevista;

4.° os apelidos e nomes próprios e a data de nascimento;

5.° o endereço e as informações de contacto (número de telefone, endereço de correio eletrónico);

6.° as informações sobre as modalidades de pagamento, incluindo o endereço de faturação;

7.° o itinerário completo para o passageiro em causa;

8.° as informações relativas ao "passageiro registado", ou seja, ao passageiro frequente;

9.° a agência de viagens ou agente de viagens;

10.° a situação do passageiro, incluindo confirmações, situação do registo, não comparência ou passageiro de última hora sem reserva;

11.° a informação do PNR separada ou dividida;

12.° as observações gerais, incluindo 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;

13.° as informações sobre a emissão dos bilhetes, incluindo número do bilhete, data de emissão, bilhetes só de ida, dados ATFQ (*Automatic Ticket Fare Quote*);

14.° o número do lugar e outras informações relativas ao lugar;

15.° as informações sobre a partilha de código;

16.° todas as informações relativas às bagagens;

17.° o número e os nomes dos outros passageiros que figuram no PNR;

18.° todos os dados prévios sobre os passageiros (dados API) que tenham sido recolhidos e são enumerados no § 2;

19.° o historial completo das modificações dos dados enumerados de 1.° a 18.°;

§ 2. No que respeita aos dados do registo e do embarque, os dados prévios referidos no § 1, 18°, são:

1.° o tipo de documento de viagem;

2.° o número do documento;

3.° a nacionalidade;

4.° o país de emissão do documento;

5.° a data de validade do documento;

6.° os apelidos, o nome próprio, o sexo, a data de nascimento;

7.° a transportadora/o operador de viagens;

8.° o número do transporte;

9.° a data de partida, a data de chegada;

10.° o local de partida, o local de chegada;

11.° a hora de partida, a hora de chegada;

12.° o número total de passageiros incluídos nesse transporte;

13.° o número do lugar;

14.° o código de identificação do registo PNR;

15.° o número, o peso e a identificação da bagagem;

16.° o ponto de passagem da fronteira à entrada no território nacional.

[…]

CAPÍTULO 7. Unidade de informações de passageiros

Artigo 12.° É criada, no Serviço Público Federal Interior, uma Unidade de Informações de Passageiros.

Artigo 13.° § 1 A UIP é responsável:

1.° Pela recolha, a conservação e o tratamento dos dados dos passageiros transmitidos pelas transportadoras e pelos operadores de viagens, bem como pela gestão do banco de dados dos passageiros;

2.° Pelo intercâmbio de dados dos passageiros e dos resultados do seu tratamento com as UIP de outros Estados-Membros da União Europeia, com a Europol e com países terceiros, em conformidade com o capítulo 12.

§ 2. Sem prejuízo de outras disposições legais, a UIP não pode utilizar os dados conservados nos termos do capítulo 9 para fins diferentes dos referidos no artigo 8.°

Artigo 14.° § 1 A IUP é composta:

1.° por um funcionário […] responsável:

a) pela organização e funcionamento da UIP;

b) pela fiscalização do cumprimento pelas transportadoras e pelos operadores de viagens das obrigações previstas no capítulo 4;

c) pela gestão e exploração do banco de dados dos passageiros;

d) pelo tratamento dos dados dos passageiros;

e) pelo respeito da legalidade e da regularidade dos tratamentos referidos no capítulo 10;

[…].

2.° por membros destacados provenientes dos seguintes serviços […]:

a) dos Serviços de Polícia […];

b) da Segurança do Estado […];

c) do Serviço Geral de Informações e de Segurança […];

d) da Administração […] Aduaneira e dos Impostos Especiais de Consumo […]

[…].

CAPÍTULO 8. Banco de dados dos passageiros

Artigo 15.° § 1 É criado um banco de dados dos passageiros, gerido pelo Serviço Público Federal Interior, no qual são registados os dados dos passageiros.

[…]

§ 4. Os tratamentos de dados dos passageiros efetuados ao abrigo da presente lei estão sujeitos à loi relative à la protection des données (Lei relativa à proteção de dados). A autoridade competente para a fiscalização dos tratamentos de dados pessoais exerce as competências previstas na loi relative à la protection de la vie privée (Lei relativa à proteção da vida privada). […]

[...]

CAPÍTULO 9. Prazos de conservação

Artigo 18.° 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.

[...]

CAPÍTULO 10. Tratamento de dados

Secção I. Tratamento de dados dos passageiros no âmbito da avaliação prévia dos passageiros

Artigo 24.° § 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.

[métodos de avaliação prévia]

Artigo 25.° […]

§ 2. A avaliação dos passageiros antes da sua chegada, do seu trânsito ou da sua partida, de acordo com os critérios preestabelecidos, é realizada de forma não discriminatória. Estes critérios não podem visar a identificação de um indivíduo e devem ser orientados em função dos objetivos, proporcionados e específicos.

§ 3. Esses critérios não podem basear-se em dados que revelam a origem racial ou étnica de uma pessoa, as suas convicções religiosas ou filosóficas, as suas opiniões políticas, a sua filiação numa organização sindical, o seu estado de saúde, a sua vida sexual ou a sua orientação sexual.

[…]

Secção 2. - O tratamento de dados no âmbito de investigações pontuais

Artigo 27.° Os dados dos passageiros são explorados a fim de proceder a investigações pontuais para os fins referidos no artigo 8.°, § 1, 1.°, 2.°, 4.° e 5.°, e nas condições previstas no artigo 46.°-F do Código de Processo Penal ou no artigo 16.°/3 da Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998, ou no artigo 281.°, § 4, da loi générale sur les douanes et accises (Lei geral em matéria aduaneira e de impostos especiais de consumo), coordenada em 18 de julho de 1977.

CAPÍTULO 11. O tratamento de dados dos passageiros a fim de melhorar o controlo nas fronteiras e combater a imigração ilegal

Artigo 28.° § 1 O presente capítulo aplica-se ao tratamento de dados dos passageiros pelos serviços de polícia encarregados do controlo nas fronteiras e pelo Office des étrangers (Serviço de Estrangeiros) a fim de melhorar os controlos de pessoas nas fronteiras externas e combater a imigração ilegal.

[…]

Artigo 29.° § 1 […]

§ 2. Apenas são transmitidos os dados [API] relativos às seguintes categorias de passageiros:

1.° Os passageiros que tencionam entrar ou entraram no território pelas fronteiras externas da Bélgica;

2.° Os passageiros que tencionam sair ou saíram do território pelas fronteiras externas da Bélgica;

3.° Os passageiros que tencionam passar, se encontram ou passaram numa zona internacional de trânsito situada na Bélgica.

§ 3. Os dados dos passageiros referidos no § 2 são transmitidos aos serviços de polícia referidos no artigo 14.°, § 1, 2.°, a), imediatamente após o respetivo registo no banco de dados de passageiros. Esses serviços conservam os referidos dados num ficheiro temporário e destroem-nos nas vinte e quatro horas seguintes à transmissão.

§ 4. […] os dados dos passageiros referidos no § 2 são transmitidos ao Serviço de Estrangeiros imediatamente após o respetivo registo no banco de dados dos passageiros. Esse serviço conserva os referidos dados num ficheiro temporário e destrói-os nas vinte e quatro horas seguintes à transmissão.

[…].

Artigo 31.° Nas vinte e quatro horas após o fim do transporte a que se refere o artigo 4.°, 3.° a 6.°, as transportadoras e os operadores de viagens destroem todos os dados dos passageiros referidos no artigo 9.°, § 1, 18°, […].

[...]

CAPÍTULO 15. Disposições modificativas

Secção I. Modificação do Código de Processo Penal

Artigo 50.° É aditado ao Código de Processo Penal o artigo 46.°-F, com seguinte redação:

“Artigo 46.°-F. Ao investigar os crimes previstos no artigo 8.°, § 1, 1.°, 2.° e 5.°, da Lei, de 25 de dezembro de 2016, relativa ao tratamento de dados dos passageiros, o Procurador do Rei pode, por decisão escrita e fundamentada, encarregar o agente de polícia judiciária de solicitar à UIP a comunicação dos dados dos passageiros, em conformidade com o artigo 27.° da Lei, de 25 de dezembro de 2016, relativa ao tratamento de dados dos passageiros”.

[…]

Secção 2. Modificação da Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998

Artigo 51.° É aditado ao capítulo III, secção I, subsecção 2, da Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998, o artigo 16.°/3, com seguinte redação:

"Artigo 16.°/3 § 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 27.° da Lei, de 25 de dezembro de 2016, relativa ao tratamento de dados dos passageiros [...]".»

III. Apreciação da Cour constitutionnelle (Tribunal Constitucional)

43 A Cour constitutionnelle (Tribunal Constitucional) esclarece, desde logo, apreciar o recurso tendo em conta as alterações à Lei de 25 de dezembro de 2016 introduzidas pelas Leis de 15 e 30 de julho de 2018 e pela Lei de 2 de maio de 2019.

44 A Cour constitutionnelle (Tribunal Constitucional) reduz, por outro lado, o âmbito do recurso de anulação ao determinar que o primeiro fundamento é apenas dirigido contra o artigo 3.°, n.° 2, o artigo 4.°, 9.° e 10.°, os artigos 7.° a 9.°, os artigos 12.° a 16.°, o artigo 18.°, os artigos 24.° a 27.°, os artigos 50.° e 51.° da lei e que o segundo fundamento é dirigido contra o artigo 3.°, n.° 1, o artigo 8.°, n.° 2, e contra os artigos 28.° a 31.° da lei.

1. Quanto à admissibilidade do primeiro fundamento: é o artigo 23.° do RGPD aplicável à Lei PNR?

45 O órgão jurisdicional de reenvio recorda que a proteção conferida pela RGPD é baseada no artigo 16.°, n.° 2, TFUE e que, em princípio, o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais não está abrangido pelo RGPD, mas pela Diretiva 2016/680. Esta diretiva estabelece regras específicas relativas 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 de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, no respeito da natureza específica dessas atividades.

46 A Lei PNR regula a recolha e a transferência dos dados PNR, a criação de um banco de dados dos passageiros, gerido pela UIP, as finalidades do tratamento deste banco de dados e o acesso a este último. A Lei PNR transpõe essencialmente a Diretiva PNR, mas o seu conteúdo vai além da transposição desta diretiva.

47 Referindo-se ao Parecer 1/15 (Acordo PNR UE-Canadá) de 26 de julho de 2017 (UE:C:2017:592), o órgão jurisdicional de reenvio constata que as disposições que regulam a recolha, a transferência e o tratamento de dados «PNR» podem ser abrangidas tanto pela proteção de dados (artigo 16.° TFUE) como pela cooperação policial (artigo 87.° TFUE).

O órgão jurisdicional de reenvio salienta igualmente que o considerando 5 da Diretiva PNR indica que esta diretiva tem *«nomeadamente por objetivos garantir a segurança e proteger a vida e a segurança das pessoas e criar um regime jurídico aplicável à proteção dos dados PNR no que respeita ao seu tratamento pelas autoridades competentes»*. O considerando 38 da mesma diretiva indica, todavia, que os objetivos da diretiva são *«a transferência de dados PNR pelas transportadoras aéreas e o tratamento desses dados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave»*, o que pode conferir a esses objetivos um caráter preponderante sobre o da proteção dos dados.

O órgão jurisdicional de reenvio constata, por outro lado, que o direito nacional não exclui a Lei PNR na sua totalidade do âmbito de aplicação do artigo 23.° do RGPD.

48 A Cour constitutionnelle conclui assim que, para determinar se as exigências do artigo 23.° do RGPD se aplicam à lei PNR, que transpõe, entre outros e principalmente, a Diretiva PNR, há que submeter ao Tribunal de Justiça uma primeira questão prejudicial.

2. Quanto ao mérito do primeiro fundamento

A Cour constitutionnelle (Tribunal Constitucional) examina, em seguida, o mérito do fundamento nas sete vertentes mencionadas no ponto 8 do presente resumo. A Cour constitutionnelle (Tribunal Constitucional) considerou que as duas primeiras alegações formuladas contra as «modalidades de execução» e contra os conceitos de «documentos de identidade» e de «documento de viagem» são desprovidas de fundamento. Prossegue a sua análise das cinco outras alegações e duvida da interpretação a dar a certas disposições da Diretiva PNR e da validade das mesmas à luz da Carta.

Quanto aos dados abrangidos (artigos 4.°, 9.°, e 9.° da Lei PNR)

49 A recorrente entende que o âmbito de aplicação, muito amplo, relativo aos dados dos passageiros referidos nos artigos 4.°, 9.°, e 9.° da Lei PNR é manifestamente desproporcionado à luz do objetivo prosseguido. Em sua opinião, os dados visados podem revelar dados sensíveis, tais como a filiação numa organização sindical, as afinidades pessoais e as relações pessoais ou profissionais.

50 O órgão jurisdicional de reenvio recorda que a ingerência dos poderes públicos no exercício do direito ao respeito da vida privada deve não só basear-se numa

disposição legislativa suficientemente precisa, mas também responder a uma necessidade social imperiosa numa sociedade democrática e ser proporcionada ao objetivo legítimo prosseguido. O legislador dispõe nesta matéria de uma margem de apreciação que não é, porém, ilimitada: para que uma norma seja compatível com o direito ao respeito da vida privada, é necessário que o legislador tenha estabelecido um justo equilíbrio entre todos os direitos e interesses em causa.

No seu Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017 (EU:C:2017:592), o Tribunal de Justiça recordou que uma ingerência no direito à proteção dos dados pessoais deve ser limitada ao «estritamente necessário» (v. n.os 140 e 141).

51 A Cour constitutionnelle (Tribunal Constitucional) salienta que a Lei PNR tem por objetivo garantir a segurança pública, instituindo a transferência dos dados dos passageiros e a utilização dos mesmos, no âmbito da luta contra as infrações terroristas e a criminalidade transnacional grave. Estes objetivos constituem objetivos de interesse geral suscetíveis de justificar ingerências no direito ao respeito da vida privada e no direito à proteção dos dados pessoais (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.° 42). O Tribunal de Justiça confirmou, aliás, que estes objetivos de interesse geral podiam justificar a transferência e a utilização dos dados dos registos de identificação dos passageiros [Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.os 148 e 149].

52 O órgão jurisdicional de reenvio examina, em seguida, se essas ingerências são suficientemente precisas, proporcionadas e limitadas ao «estritamente necessário», tendo em conta a amplitude dos dados abrangidos pela Lei PNR.

A recolha dos dados dos passageiros abrangidos pela Lei PNR está rodeada de garantias quanto ao conteúdo dos mesmos. Com efeito, estes dados são determinados de forma exaustiva pelo artigo 9.° da Lei PNR. Trata-se de informações diretamente relacionadas com a viagem que dá origem ao transporte abrangido pelo âmbito de aplicação da Lei PNR, de que, em princípio, as transportadoras e os operadores de viagens já dispõem. Além disso, estes dados correspondem ao anexo I das Orientações da Organização da Aviação Civil Internacional (ICAO). Os referidos dados são, portanto, pertinentes atendendo aos objetivos prosseguidos pela Lei PNR.

Além disso, os artigos 10.° e 11.°, não impugnados, da Lei PNR preveem que os dados dos passageiros não podem dizer respeito à origem racial ou étnica de uma pessoa, às suas convicções religiosas ou filosóficas, às suas opiniões políticas, à sua filiação numa organização sindical ou aos dados relativos ao seu estado de saúde, à sua vida sexual ou à sua orientação sexual. Quando os dados dos passageiros transferidos pelas transportadoras e pelos operadores de viagens incluem outros dados que não os enumerados no artigo 9.° ou dados enumerados no artigo 10.°, a UIP apaga esses dados adicionais logo na sua receção e de forma

definitiva. Estas disposições garantem que os dados sensíveis não podem, em princípio, ser recolhidos ou conservados como «dados de passageiros».

53 No seu Parecer 1/15, *supra* referido, de 26 de julho de 2017, o Tribunal de Justiça considerou igualmente, no que respeita aos dados sensíveis, que «*os artigos 7.°, 8.°, 21.° e 52.°, n.° 1, da Carta se opõem quer à transferência dos dados sensíveis para o Canadá quer ao enquadramento, negociado pela União com este Estado terceiro, das condições relativas à utilização e à conservação de tais dados pelas autoridades deste Estado terceiro*» (n.° 167).

Esta observação é transponível para o caso vertente. Embora existam garantias que rodeiam os dados dos passageiros abrangidos pela Lei PNR, importa, no entanto, questionar se essas garantias são suficientes, tendo em conta a amplitude dos dados abrangidos. Os dados referidos no artigo 9.°, n.° 1, da Lei PNR, que reproduz os dados referidos no anexo I da Diretiva PNR, incluem, efetivamente, dados muito amplos, para além dos dados de registo e de embarque, designadamente: o itinerário completo para o passageiro, a agência de viagens, o número do lugar, todas as informações relativas à bagagem, as informações relativas aos meios de pagamento, incluindo o endereço de faturação, as observações gerais, «incluindo todas as informações disponíveis sobre menores não acompanhados com idade inferior a 18 anos».

No seu Parecer 1/15 de 26 de julho de 2017, *supra* referido, o Tribunal de Justiça observou, aliás, que, «*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, conforme definidas no artigo 2.°, alínea e), do acordo projetado*» (n.° 128).

No seu Parecer de 19 de agosto de 2016 sobre as implicações do tratamento dos registos de identificação dos passageiros em matéria de proteção de dados (a seguir «Parecer de 19 de agosto de 2016»), o Comité Consultivo da Convenção n.° 108 do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (a seguir «Comité Consultivo da Convenção n.° 108») observou igualmente que «*[o]s PNR contêm informações que visam facilitar a viagem do passageiro e podem incluir um determinado número de dados sensíveis (dados que podem servir para indicar a origem racial, as opiniões políticas, as convicções religiosas e outras, o estado de saúde ou a orientação sexual de uma pessoa), não só em determinados dados "codificados", mas também em campo aberto contendo observações gerais (tais como pedidos dietéticos e médicos, ou o facto de uma associação política ou religiosa ter beneficiado de bilhetes a preços reduzidos para a viagem dos seus*

membros), o que pode conduzir a uma discriminação direta» (Conselho da Europa, Parecer de 19 de agosto de 2016, T-PD(2016)18rev, p. 7).

A Agência dos Direitos Fundamentais da União Europeia observou igualmente que os dados PNR «*podem incluir dados sensíveis ou específicos sob o título "observações gerais"*» (Parecer 1/2011 da Agência dos Direitos Fundamentais da União Europeia sobre a Proposta de Diretiva 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 ([COM(2011) 32 final], 14 de junho de 2011, p. 8; v. também *ibidem*, p. 13).

54 Tendo em conta o seu âmbito de aplicação, muito vasto, os dados referidos no artigo 9.° da Lei PNR, ainda que não possam conter diretamente dados sensíveis, podem, no entanto, revelar, indiretamente, elementos sensíveis abrangidos pela proteção dos dados pessoais e pelo respeito da vida privada. Tendo em conta o Parecer 1/15 do Tribunal de Justiça, a Cour constitutionnelle (Tribunal Constitucional) questiona se estes dados, que incluem os dados referidos no anexo I da Diretiva PNR, não vão além do «estritamente necessário» para atingir os objetivos prosseguidos por essa mesma diretiva. A Cour constitutionnelle (Tribunal Constitucional) decide, portanto, submeter ao Tribunal de Justiça uma segunda questão prejudicial.

55 No seu parecer 1/15, *supra* referido, de 26 de julho de 2017, o Tribunal de Justiça formulou, além disso, as observações seguintes, no que respeita à exigência de uma definição clara e precisa dos dados abrangidos pelo projeto de acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros:

«*156. A este respeito, embora as 19 rubricas dos dados PNR que constam do anexo do acordo projetado correspondam, segundo as observações da Comissão, ao anexo I das orientações da Organização Internacional da Aviação Civil (ICAO) em matéria de dados PNR, importa, contudo, sublinhar, como salientou o advogado-geral no n.° 217 das suas conclusões, que a rubrica 5, que respeita às "[i]nformações disponíveis sobre passageiros frequentes e outras vantagens (como sejam bilhetes gratuitos, subidas de categoria, etc.)", e a rubrica 7, que abrange "[t]odas as coordenadas de contacto disponíveis (incluindo informações sobre a fonte)", não definem de maneira suficientemente clara e precisa os dados PNR a transferir.*

157. Com efeito, no que respeita à rubrica 5, a utilização do termo "etc." não determina suficientemente a extensão dos dados a transferir. Além disso, os termos desta rubrica não permitem saber se a mesma visa apenas informações relativas ao estatuto dos passageiros aéreos quanto a essas vantagens ou se, pelo contrário, visa todas as informações relativas aos voos e às transações efetuadas no âmbito dessas vantagens.

158. Do mesmo modo, ao utilizar os termos "todas as coordenadas de contacto disponíveis", a rubrica 7 não determina suficientemente a extensão dos dados a transferir. Nomeadamente, não precisa qual o tipo de coordenadas de contacto que visa nem se essas coordenadas de contacto abrangem igualmente, como se pode deduzir da resposta escrita da Comissão às questões colocadas pelo Tribunal de Justiça, as coordenadas de contacto dos terceiros que efetuaram a reserva do voo para o passageiro aéreo, dos terceiros por intermédio dos quais um passageiro aéreo pode ser contactado ou ainda dos terceiros que devem ser informados em caso de emergência.

159. No que diz respeito à rubrica 8, a mesma é relativa a "[t]odas as informações disponíveis sobre pagamentos/faturas (excetuando detalhes sobre outras transações efetuadas por meio de cartões de crédito ou contas bancárias não relacionadas com a transação relativa à viagem)". É verdade que esta rubrica pode parecer particularmente vasta ao utilizar a expressão "todas as informações disponíveis". No entanto, conforme resulta da resposta da Comissão às questões colocadas pelo Tribunal de Justiça, deve considerar-se que a referida rubrica é apenas relativa às informações sobre as modalidades de pagamento e a faturação do bilhete de avião, excluindo qualquer outra informação sem relação direta com o voo. Interpretada neste sentido, pode considerar-se, portanto, que esta rubrica respeita os requisitos de clareza e de precisão.

*160. Quanto à rubrica 17, a mesma visa as "[o]bservações gerais, incluindo outras informações de serviço (OSI), informações de serviço especiais (SSI) e informações sobre pedidos de serviços especiais (SSR)". Segundo as explicações fornecidas, nomeadamente, pela Comissão, esta rubrica constitui uma rubrica dita de "texto livre" (*free text*), que se destina a abranger "todas as informações adicionais", além das enumeradas no anexo do acordo projetado. Assim, 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 as informações previstas na referida rubrica são fornecidas apenas a título de exemplo, como demonstra a utilização do termo "incluindo", esta rubrica não fixa nenhuma limitação quanto à natureza e à extensão das informações que a mesma poderá conter. Nestas condições, não se pode considerar que a rubrica 17 esteja delimitada com clareza e precisão suficientes.*

161. Por último, a rubrica 18 é relativa a "[t]odas as informações antecipadas sobre os passageiros (API) recolhidas para efeitos de reserva". Segundo os esclarecimentos prestados pelo Conselho e pela Comissão, estas informações correspondem às informações previstas no artigo 3.°, n.° 2, da Diretiva 2004/82, ou seja, 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 e o ponto inicial de embarque. Desde que interpretada no sentido de

que abrange apenas as informações expressamente previstas nesta última disposição, pode considerar-se que esta rubrica satisfaz os requisitos de clareza e de precisão.

162. As disposições do artigo 4.°, n.° 3, do acordo projetado, que preveem a obrigação de o Canadá suprimir quaisquer dados PNR que lhe tenham sido transferidos, se não figurarem na lista do anexo deste acordo, não permitem colmatar a imprecisão das rubricas 5, 7 e 17 deste anexo. Com efeito, na medida em que esta lista não delimita, enquanto tal, com clareza e precisão suficientes, os dados PNR a transferir, tais disposições não são suscetíveis de corrigir as incertezas quanto aos dados PNR que devem ser objeto de transferência.

163. Nestas condições, no que toca aos dados PNR a transferir para o Canadá, as rubricas 5, 7 e 17 do anexo do acordo projetado não enquadram de maneira suficientemente clara e precisa o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta».

56 Como algumas dessas observações podem ser transponíveis para o caso vertente, no que respeita ao caráter exemplificativo e não exaustivo de certos dados constantes do anexo I da Diretiva PNR, que o artigo 9.° da Lei PNR transpõe, o órgão jurisdicional de reenvio decide submeter uma terceira questão prejudicial.

Quanto ao conceito de «passageiro» (artigo 4.°, 10.°, da Lei PNR)

57 A recorrente critica o caráter amplo do conceito de «passageiro», que dá origem a um tratamento automatizado sistemático, não direcionado, dos dados de todos os passageiros.

58 A definição do conceito de «passageiro» (artigo 4.°, 10.°, da Lei PNR) tem como consequência que a recolha, a transferência e o tratamento dos dados PNR dos «passageiros» constituem obrigações gerais e indiferenciadas, que se aplicam a qualquer pessoa transportada ou que deva ser transportada e inscrita na lista de passageiros. As obrigações que a Lei PNR impõe aplicam-se, assim, independentemente da existência de motivos sérios para crer que as pessoas em causa cometeram uma infração ou estão prestes a cometer uma infração ou foram consideradas culpadas de uma infração.

59 No seu Parecer de 19 de agosto de 2016, o Comité Consultivo da Convenção n.° 108 observou a este respeito que «[o] tratamento dos dados PNR - que tem a vantagem única de permitir a identificação de pessoas de interesse - é uma filtragem geral e não seletiva de todos os passageiros, incluindo os que não são suspeitos de ter cometido qualquer infração penal, por diferentes autoridades competentes, e diz respeito a dados inicialmente recolhidos para fins comerciais por entidades privadas. Tendo em conta a amplitude da violação dos direitos à vida privada e da proteção dos dados que decorre do tratamento dos dados PNR, deve ser claramente demonstrado que o referido tratamento é uma medida necessária numa sociedade democrática com um objetivo legítimo; além disso, é

necessário que sejam estabelecidas garantias apropriadas. É indispensável demonstrar expressamente a necessidade da recolha e da exploração ulterior dos dados PNR» (Parecer de 19 de agosto de 2016, T-PD(2016)18rev, p. 5).

60 No domínio das comunicações eletrónicas, o Tribunal de Justiça pronunciou-se sobre uma regulamentação nacional que previa uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica, bem como a obrigação de os prestadores de serviços de comunicações eletrónicas conservarem esses dados de forma sistemática, contínua e sem nenhuma exceção (Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970).

O Tribunal de Justiça considerou que, «*embora a eficácia da luta contra a criminalidade grave, nomeadamente contra a criminalidade organizada e o terrorismo, possa depender em larga medida da utilização de técnicas modernas de investigação, um objetivo de interesse geral desse tipo, por muito fundamental que seja, não pode por si só justificar que uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização seja considerada necessária para efeitos da referida luta*» (n.° 103).

O Tribunal de Justiça declarou, por um lado, que uma regulamentação deste tipo tem por efeito que a conservação dos dados de tráfego e dos dados de localização constitui a regra, ao passo que o sistema implementado pela Diretiva 2002/58 exige que essa conservação de dados seja a exceção, e, por outro, que «*uma regulamentação nacional [...] que abrange de forma generalizada todos os assinantes e utilizadores registados e que visa todos os meios de comunicação eletrónica, bem como todos os dados de tráfego, não prevê nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido. Essa regulamentação afeta globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que essas pessoas se encontrem, mesmo indiretamente, numa situação suscetível de justificar um procedimento penal. Por conseguinte, aplica-se inclusivamente a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações penais graves. Além disso, não prevê nenhuma exceção, pelo que também é aplicável a pessoas cujas comunicações estão sujeitas ao segredo profissional, segundo as regras do direito nacional (v., por analogia, no que se refere à Diretiva 2006/24, Acórdão Digital Rights, n.os 57 e 58).*

106. Uma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus

dados, podiam contribuir para a luta contra a criminalidade (v., por analogia, no que se refere à Diretiva 2006/24, Acórdão Digital Rights, n.° 59).

107. Por conseguinte, uma regulamentação nacional como a que está em causa no processo principal excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta.

108. Em contrapartida, o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, não se opõe a que um Estado-Membro adote uma regulamentação que permita, a título preventivo, a conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos de luta contra a criminalidade grave, desde que a conservação dos dados seja limitada ao estritamente necessário, no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada.

109. Para cumprir os requisitos enunciados no número anterior do presente acórdão, esta regulamentação nacional deve, em primeiro lugar, prever normas claras e precisas que regulem o âmbito e a aplicação dessa medida de conservação dos dados e que imponham exigências mínimas, de modo a que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida de conservação dos dados, a título preventivo, garantindo assim que essa medida se limita ao estritamente necessário (v., por analogia, a propósito da Diretiva 2006/24, Acórdão Digital Rights, n.° 54 e jurisprudência referida).

110. Em segundo lugar, relativamente às condições materiais que uma regulamentação nacional deve satisfazer que permitam, no âmbito da luta contra a criminalidade, a conservação, a título preventivo, dos dados de tráfego e dos dados de localização, para garantir que se limita ao estritamente necessário, há que salientar que, embora essas condições possam variar em função das medidas adotadas para efeitos da prevenção, da investigação, da deteção e da repressão da criminalidade grave, a conservação dos dados deve sempre responder, em todo o caso, a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido. Em especial, tais condições devem revelar-se, na prática, suscetíveis de limitar efetivamente o alcance da medida e, consequentemente, o público afetado.

111. No que se refere à delimitação de uma medida deste tipo quanto ao público e às situações potencialmente abrangidas, a regulamentação nacional deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir de uma maneira ou outra para a luta contra a

criminalidade grave ou de prevenir um risco grave para a segurança pública. Tal delimitação pode ser assegurada através de um critério geográfico quando as autoridades nacionais competentes considerem, com base em elementos objetivos, que existe um risco elevado de preparação ou de execução desses atos, numa ou em mais zonas geográficas.

112. Atendendo a todas as considerações que precedem, importa responder à primeira questão no processo C-203/15 que o artigo 15.°, n.° 1, da Diretiva 2002/58, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica».

À segunda questão prejudicial no processo C-203/15 e à primeira questão prejudicial no processo C-698/15, o Tribunal de Justiça responde que o artigo 15.°, n.° 1, da Diretiva 2002/58/CE, lido à luz dos artigos 7.°, 8.° e 11.°, bem como do artigo 52.°, n.° 1, da Carta, deve ser interpretado «*no sentido de que se opõe a uma regulamentação nacional que regula a proteção e a segurança dos dados de tráfego e dos dados de localização, em especial, o acesso das autoridades nacionais competentes aos dados conservados, sem limitar, no âmbito da luta contra a criminalidade, esse acesso apenas para efeitos de luta contra a criminalidade grave, sem submeter o referido acesso a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, e sem exigir que os dados em causa sejam conservados em território da União*» (n.° 125).

61 Por sua vez, o TEDH declarou, entretanto, que a legislação sueca relativa à interceção em massa de comunicações eletrónicas é conforme ao artigo 8.° da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, no seu acórdão Centrum för Rättvisa c. Suécia, de 19 de junho de 2018. Indicou, em especial, o seguinte:

«*O Tribunal reconheceu expressamente que as autoridades nacionais dispõem de uma ampla margem de apreciação para escolher os meios que garantam a segurança nacional […]. Nos processos Weber e Saravia e Liberty e o., o Tribunal admitiu que os regimes de interceção em massa não excedem, por si só, esta margem de apreciação. Atendendo à fundamentação do Tribunal nestas decisões e tendo em conta as ameaças com que são confrontados inúmeros Estados contratantes (designadamente, o flagelo do terrorismo internacional e outras formas de criminalidade grave, tais como o tráfico de estupefacientes, o tráfico de seres humanos, a exploração sexual de crianças e a cibercriminalidade), os avanços tecnológicos que permitem aos terroristas e aos criminosos escaparem mais facilmente à deteção na internet e a impossibilidade de prever as vias pelas quais as comunicações eletrónicas serão transmitidas, o Tribunal considera que a decisão de recorrer a um regime de interceção em*

massa a fim de identificar ameaças à segurança nacional até então desconhecidas está abrangida pela margem de apreciação dos Estados» (TEDH, 19 de junho de 2018, Centrum för Rättvisa c. Suécia, § 112).

O mesmo órgão jurisdicional declarou, em contrapartida, que a lei inglesa relativa à interceção de comunicações violava o artigo 8.° da CEDH ao não respeitar os critérios enunciados na sua jurisprudência. O TEDH considerou igualmente que «*o funcionamento dos regimes de interceção em massa está abrangido, em princípio, pela margem de apreciação do Estado. A interceção em massa é, por definição, não direcionada, e subordiná-la à presença de uma "suspeita razoável" torna a sua execução impossível*» (TEDH, 13 de setembro de 2018, Big Brother Watch e o. c. Reino Unido, § 317).

62 Coloca-se a questão de saber em que medida a jurisprudência *supra* referida, que diz respeito à conservação generalizada e indiferenciada de dados em matéria de comunicações eletrónicas, é transponível para a recolha, a transferência e o tratamento generalizados e indiferenciados de dados dos passageiros, conforme regulados pela Lei de 25 de dezembro de 2016.

63 No seu Parecer 1/15, *supra* referido, de 26 de julho de 2017, o Tribunal de Justiça pronunciou-se sobre um sistema PNR análogo, mas com um âmbito de aplicação mais limitado, uma vez que o projeto de acordo entre o Canadá e a União Europeia sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros previa «*a transferência sistemática e contínua dos dados PNR de todos os passageiros aéreos que voam entre a União e o Canadá*» (n.° 127). O Tribunal de Justiça considerou 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, prosseguido pelo acordo projetado*» (n.° 153).

No que respeita aos passageiros em causa, o Tribunal de Justiça considerou:

«*186. O acordo projetado abrange os dados PNR de todos os passageiros aéreos que voam entre a União e o Canadá. A transferência destes dados para o Canadá é feita independentemente de qualquer elemento objetivo que permita considerar que os passageiros são suscetíveis de representar um risco para a segurança pública no Canadá.*

187. A este respeito, há que salientar que, como foi recordado nos n.os 152 e 169 do presente parecer, os dados PNR se destinam, nomeadamente, a ser submetidos a tratamento automatizado. Ora, como observaram vários intervenientes, este tratamento visa identificar o risco que, eventualmente, poderiam representar para a segurança pública pessoas que, nesta fase, não são conhecidas dos serviços competentes e que, devido a esse risco, poderiam ser submetidas a um exame aprofundado. Neste contexto, o tratamento automatizado destes dados, previamente à chegada dos passageiros ao Canadá, facilita e acelera os controlos de segurança, nomeadamente nas fronteiras. Acresce 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.

188. De resto, em conformidade com o artigo 13.° da Convenção de Chicago, ao qual se referiram, em particular, o Conselho e a Comissão nas suas respostas às questões colocadas pelo Tribunal de Justiça, todos os passageiros aéreos devem, tanto à chegada como à partida ou enquanto permanecerem no território de um Estado contratante, cumprir as leis e os regulamentos em vigor no território desse Estado, relativos à entrada ou à saída de passageiros por via aérea. Todos os passageiros aéreos que pretendam entrar no Canadá ou sair deste país estão, pois, sujeitos, com fundamento neste artigo, aos controlos de fronteiras e devem respeitar as condições de entrada e de saída prescritas pela legislação canadiana em vigor. Além disso, conforme resulta dos n.os 152 e 187 do presente parecer, a identificação, através dos dados PNR, dos passageiros suscetíveis de representar um risco para a segurança pública faz parte dos controlos nas fronteiras. Consequentemente, uma vez que são objeto destes controlos, os passageiros aéreos que pretendam entrar e permanecer no Canadá são, devido à própria natureza desta medida, submetidos à verificação dos seus dados PNR.

189. Nestas condições, não se afigura que o acordo projetado ultrapasse os limites do estritamente necessário ao permitir a transferência dos dados PNR de todos os passageiros aéreos para o Canadá».

64 A Cour constitutionnelle (Tribunal Constitucional) questiona se estas considerações podem ser aplicadas à Diretiva PNR e a uma legislação nacional, como a Lei PNR, que, ao transpor a Diretiva PNR, institui a recolha, a transferência e a utilização generalizadas e indiferenciadas dos dados «PNR» para todos os passageiros que viajam em transporte aéreo, ferroviário ou de autocarro, independentemente de uma passagem nas fronteiras externas da União. Este sistema aplica-se, efetivamente, a pessoas em relação às quais não existem indícios de que a sua conduta possa ter qualquer ligação, mesmo indireta ou longínqua, com infrações graves e é mais amplo do que o sistema previsto no Acordo PNR com o Canadá. Atendendo à amplitude dos dados abrangidos, coloca-se a questão de saber se esta medida respeita os limites do «estritamente necessário». Antes de se pronunciar sobre o mérito, a Cour constitutionnelle (Tribunal Constitucional) decide, portanto, submeter ao Tribunal de Justiça uma quarta questão prejudicial.

Quanto às finalidades do tratamento dos dados «PNR» (artigo 8.° da Lei PNR)

65 A recorrente critica a definição das finalidades do tratamento dos dados «PNR», constante do artigo 8.° da Lei PNR, que é muito mais lata do que as «finalidades específicas», que se restringem apenas às infrações terroristas e à criminalidade

grave previstas na Diretiva PNR. A recorrente entende que aquelas finalidades excedem os limites do «estritamente necessário».

As finalidades do tratamento dos dados «PNR», conformes previstas nos artigos 1.°, n.° 2, e 6.°, n.° 2, da Diretiva PNR, constituem apenas objetivos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (v., igualmente, considerando 7 da Diretiva PNR).

Algumas das finalidades do tratamento referidas no artigo 8.° da Lei PNR correspondem às infrações previstas no anexo II da Diretiva PNR, em conformidade com os objetivos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, visados pela referida diretiva. Em contrapartida, outras finalidades do tratamento dos dados «PNR» acrescem às finalidades previstas nesta diretiva. É o caso, entre outros, do «acompanhamento das atividades referidas nos artigos 7.°, 1.° e 3.°/l, e 11.°, § 1, 1.° a 3.° e 5.°, da Lei Orgânica dos Serviços de Informações e de Segurança, de 30 de novembro de 1998» (artigo 8.°, n.° 1, 4.°).

O órgão jurisdicional de reenvio examina se essas outras finalidades são expressas em regras claras, precisas e limitadas ao estritamente necessário e tem dúvidas quanto à finalidade prevista no artigo 8.°, n.° 1, 4.° da Lei PNR.

A exposição de motivos da Lei PNR indica que esta «finalidade diz respeito às competências dos serviços de informações, a saber, a Segurança do Estado e o Serviço Geral de Informações e de Segurança (SGRS). Para desempenharem as suas funções de pesquisa, análise e tratamento de informações relativas às atividades suscetíveis de ameaçar os interesses fundamentais do Estado, esses serviços devem poder analisar os dados dos passageiros a fim de detetar o mais cedo possível ameaças concretas, acompanhar as deslocações de pessoas específicas ou efetuar análises de fenómenos ou tendências mais amplos. As funções de pesquisa, análise e tratamento de informações relacionadas com as atividades dos serviços de informações estrangeiros em território belga integram esta finalidade.» (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 19-20).

Embora as funções dos serviços de informações e de segurança contribuam, de forma geral, para a segurança nacional e internacional, o tratamento de dados «PNR» à luz da finalidade referida no artigo 8.°, n.° 1, 4.°, da Lei PNR parece muito vago e geral.

Esta finalidade é ainda objeto, no que respeita à avaliação prévia dos passageiros, do mesmo tratamento que as finalidades previstas nos artigos 8.°, n.° 1, 1.°, 2.° e 5.°, da Lei PNR (artigos 24.°, n.° 2, e 26.°, n.° 2).

Neste contexto, a Cour constitutionnelle (Tribunal Constitucional) decide submeter ao Tribunal de Justiça uma quinta questão prejudicial a fim de poder decidir se essa finalidade é suficientemente clara, precisa e limitada ao estritamente necessário.

Quanto à gestão do banco de dados dos passageiros e ao tratamento dos dados no âmbito da avaliação prévia dos passageiros e das investigações pontuais (artigos 16.°, 24.° a 27.°, 50.° e 51.° da Lei PNR)

66 A recorrente considera que os diferentes tratamentos e fluxos de dados pessoais são manifestamente desproporcionados.

67 O artigo 16.° da Lei PNR prevê que, no âmbito das finalidades referidas no artigo 8.°, n.° 1, os dados dos passageiros são objeto dos tratamentos previstos nos artigos 24.° a 27.°

– *Avaliação prévia dos passageiros (artigos 24.° a 26.°)*

68 Os dados dos passageiros são tratados para efeitos de realização de uma avaliação prévia (*pre-screening*) dos passageiros antes da sua chegada, da sua partida ou ou do seu trânsito previsto em território nacional, a fim de determinar as pessoas que devem ser submetidas a um exame mais aprofundado. «Trata-se de avaliar a ameaça potencial e determinar os passageiros que são de interesse para o exercício das funções ou, por exemplo, exigem a aplicação de uma medida (execução de um mandado de detenção, revistas, etc)». (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 28).

A avaliação prévia assenta em dois eixos: por um lado, a correlação dos dados dos passageiros com os bancos de dados, e, por outro, a correlação dos dados com critérios preestabelecidos.

69 No que respeita à correlação com os bancos de dados, os trabalhos preparatórios da Lei PNR referem que «[o] primeiro eixo consiste na procura de correspondências positivas através de correlações de dados dos passageiros com os dados tratados nos bancos de dados geridos pelos serviços competentes. Isso permite, por exemplo, avaliar se uma pessoa apresenta um elevado grau de perigosidade, porque é conhecida num banco de dados da polícia no âmbito de um registo de identificação de terroristas e relativamente à qual resulta da análise dos seus dados de passageiro que se desloca regularmente para países que abrigam campos de treino para terroristas ou para países de trânsito para esses lugares. Pode, por exemplo, tratar-se também de uma pessoa relativamente à qual as informações disponíveis junto dos serviços de informações indicam que estaria a preparar uma tomada de reféns e que, com base nos dados de transporte, se desloca para um país cujos serviços de informações sabem, com base nas informações recebidas, que essa pessoa poderia proceder a recrutamentos neste país para a execução dos seus planos. Além disso, quanto maior for o número de correspondências positivas descobertas por vários serviços relativamente a uma única e mesma pessoa, maior será a probabilidade de a ameaça ser real.

A correspondência positiva pode igualmente exigir a adoção de uma medida por ordem das autoridades judiciárias, como a execução de um mandado de detenção de uma pessoa que estás prestes a deixar a Bélgica.

A correspondência positiva pode também resultar de uma correlação com os bancos de dados internacionais, como o SIS II e a Interpol (SLTD).

O objetivo não é, naturalmente, ligar todos os bancos de dados dos serviços com o banco de dados dos passageiros, mas sim limitar tecnicamente as correlações com os bancos de dados em relação direta com as finalidades determinadas pela lei.

[...]

Esta correlação poderá igualmente ser feita através de listas de pessoas elaboradas especificamente para o efeito pelos serviços competentes. Em conformidade com a Lei relativa à proteção da vida privada, mais especificamente o seu artigo 4.°, n.° 1, 4.°, essas listas deverão ser atualizadas regularmente» (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 28-29).

70 No que respeita à correlação com critérios preestabelecidos, os trabalhos preparatórios da Lei PNR expõem:

«O segundo eixo consiste na procura de correspondências positivas através de critérios preestabelecidos pela UIP (um ou vários) aplicados aos dados dos passageiros. Estes critérios são compostos por um ou mais indicadores objetivos com base nos quais se pode deduzir que as pessoas que deles são objeto apresentam um comportamento de risco específico suscetível de constituir uma ameaça à luz das finalidades do artigo 8.°, n.° 1, pontos 1, 4 e 5, da lei.

Estes critérios podem incluir, por exemplo, certos comportamentos específicos em matéria de reservas ou de viagens.

A sua utilização apresenta a vantagem de poder fazer emergir perfis de passageiros de risco que não são necessariamente conhecidos ou mencionados nos bancos de dados dos serviços.

Estes critérios podem dizer respeito, por exemplo, a um país de destino ou de partida, conjugado com determinadas informações sobre a viagem, como o meio de pagamento e a data de reserva» (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, p. 29-30).

«A avaliação prévia realizada no âmbito da finalidade relativa ao acompanhamento dos fenómenos de polícia administrativa e dos grupos ligados à radicalização violenta está sujeita a condições muito mais restritivas do que as outras finalidades [...].

Para a avaliação prévia realizada no âmbito das outras finalidades, é autorizado o acesso a todos os dados de passageiros enumerados no artigo 9.°» (*ibidem*, p. 31).

«A correspondência positiva deve em todos os casos ser validada pela UIP. Com efeito, para assegurar o respeito total do direito à proteção dos dados pessoais [...] nenhuma decisão com consequências jurídicas para uma pessoa ou suscetível de a

prejudicar gravemente pode ser tomada apenas com base no tratamento automatizado dos dados do ficheiro que contem informações sobre a sua viagem. É por este motivo que a avaliação humana precederá sempre qualquer decisão vinculativa para a pessoa em causa.

Para dar acesso ao banco de dados dos passageiros, esta validação deve ocorrer nas 24 horas.

Após a validação da correspondência positiva, os serviços que estão na origem desta correspondência asseguram o acompanhamento útil num prazo adequado. Um acompanhamento útil pode significar uma intervenção ativa (revista, detenção...), mas pode também implicar a não realização provisória de uma intervenção ativa. Esta apreciação operacional pertence plenamente aos serviços competentes» (*ibidem*, pp. 30-31).

71 Quanto aos critérios de avaliação preestabelecidos pela UIP, estes não se podem basear em dados que revelem a origem racial ou étnica de uma pessoa, as suas convicções religiosas ou filosóficas, as suas opiniões políticas, a sua filiação numa organização sindical, o seu estado de saúde, a sua vida sexual ou a sua orientação sexual. A avaliação dos passageiros antes da sua chegada, trânsito ou partida, de acordo com os critérios preestabelecidos, é realizada de forma não discriminatória. Estes critérios não podem visar a identificação de um indivíduo e devem ser orientados em função dos objetivos, proporcionados e específicos.

72 No seu Parecer de 19 de agosto de 2016, o Comité Consultivo da Convenção n.° 108 observou o seguinte:

«*O tratamento de dados pessoais pode dizer respeito a todos os passageiros e não apenas a indivíduos específicos suspeitos de terem cometido uma infração penal ou de constituírem uma ameaça imediata à segurança nacional ou à ordem pública.*

[…]

A avaliação dos passageiros através da correspondência de dados pode suscitar a questão da previsibilidade, em especial quando efetuada com base em algoritmos preditivos que utilizam critérios dinâmicos suscetíveis de evoluir em permanência segundo as capacidades de autoaprendizagem.

O desenvolvimento de algoritmos de exploração de dados deveria basear-se nos resultados de avaliações regulares do impacto provável do tratamento de dados nos direitos e liberdades fundamentais das pessoas em causa.

A estrutura de base das análises deveria basear-se em indicadores de risco predefinidos que tenham sido previamente estabelecidos de forma clara.

A pertinência dos resultados individuais dessas avaliações automáticas deveria ser examinada com cuidado, caso a caso, por uma pessoa e de forma não automatizada» (Parecer de 19 de agosto de 2016, T-PD (2016)18rev, p. 8).

73 No caso vertente, os bancos de dados referidos no artigo 24.° encontram-se definidos com precisão e estão diretamente relacionados com as finalidades previstas no artigo 8.° da Lei PNR. Com efeito, trata-se de bancos de dados dos «serviços competentes», isto é, dos serviços de polícia, da Segurança do Estado, do Serviço Geral de Informações e de Segurança e da Autoridade Aduaneira.

Além disso, o artigo 24.°, n.os 4 e 5, da Lei PNR garante que, em caso de concordância positiva, o tratamento sistemático automatizado é objeto de verificação individual por meios não automatizados, a fim de apreciar se a autoridade competente deve intervir de acordo com o direito nacional, conforme exige o artigo 6.°, n.° 5, da Diretiva PNR.

74 No seu Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017 (EU:C:2017:592), o Tribunal de Justiça insistiu igualmente na necessidade de um reexame individual, através de meios não automatizados, antes da adoção de uma medida individual (n.° 173).

A exigência de uma intervenção humana após uma correspondência positiva constitui uma garantia que é suscetível de assegurar que a avaliação prévia não assente apenas em meios automatizados, contribuindo assim para a eficácia do sistema.

Uma avaliação prévia sistemática dos passageiros constitui, portanto, em princípio, uma medida pertinente à luz do objetivo que consiste em identificar e prevenir ameaças para a segurança pública.

Conforme referiu, todavia, o Tribunal de Justiça no seu Parecer 1/15, de 26 de julho de 2017, supra referido, os tratamentos decorrentes da avaliação prévia «*são suscetíveis de fornecer informações adicionais sobre a vida privada dos passageiros aéreos*» (n.° 131); além disso, «*as referidas análises são efetuadas sem que existam razões fundadas em circunstâncias individuais que permitam considerar que as pessoas em causa podem representar um risco para a segurança pública*» (*ibidem*, n.° 132).

Por constatar que o tratamento automatizado dos dados «PNR», baseado em modelos e critérios preestabelecidos, apresenta uma taxa de erro não negligenciável (*ibidem*, n.os 169-170), o Tribunal de Justiça considerou, todavia, que «*os modelos e os critérios preestabelecidos devem ser, por um lado, específicos e fiáveis, permitindo [...] alcançar resultados orientados para a seleção das pessoas sobre as quais possa recair uma suspeita razoável de participação em infrações terroristas ou de criminalidade transnacional grave e, por outro, não discriminatórios*» e que «*as bases de dados com as quais são cruzados os dados PNR devem ser fiáveis, atuais e limitadas a bases de dados exploradas pelo Canadá em relação com a luta contra o terrorismo e a*

criminalidade transnacional grave» (*ibidem*, n.° 172). Por último, para garantir que essa avaliação não apresente um caráter discriminatório e seja limitada ao estritamente necessário, o Tribunal de Justiça considerou que «*a fiabilidade e a atualidade desses modelos e desses critérios preestabelecidos assim como das bases de dados utilizadas deveriam, tendo em conta os dados estatísticos e os resultados da investigação internacional, ser objeto do reexame conjunto da execução do acordo projetado*», um ano após a sua entrada em vigor e depois em intervalos regulares (*ibidem*, n.° 174).

75 De resto, é tecnicamente impossível definir mais os critérios preestabelecidos que servirão para determinar perfis de risco. Conforme referido *supra*, esses critérios devem ser específicos, fiáveis e não discriminatórios.

76 Embora a Diretiva e a Lei PNR não deem indicações sobre a forma como são preestabelecidos, pela UIP, os critérios em que se baseia a avaliação prévia, as garantias que envolvem o estabelecimento desses critérios parecem suficientes para que a medida impugnada não seja declarada desproporcionada. No entanto, a fim de decidir se esta avaliação prévia sistemática é suficientemente clara, precisa e limitada ao estritamente necessário, há que submeter ao Tribunal de Justiça uma sexta questão prejudicial.

– *Investigações pontuais (artigos 27.°, 50.° e 51.°)*

77 O artigo 27.° da Lei PNR autoriza o tratamento de dados dos passageiros a fim de proceder a investigações pontuais para os fins referidos no artigo 8.°, n.° 1, 1.°, 2.°, 4.° e 5.°, e nas condições previstas no artigo 46.°-F do Código de Processo Penal ou no artigo 16.°/3 da Lei de 30 de novembro de 1998, aditados respetivamente pelos artigos 50.° e 51.° da Lei PNR. Em conformidade com o artigo 20.° da Lei PNR, os requisitos de aplicação do artigo 27.° aplicam-se igualmente aos pedidos de acesso decorrido o prazo de seis meses previsto no artigo 19.°

78 O artigo 46.°-F do Código de Processo Penal diz respeito às investigações pontuais no âmbito da finalidade prevista no artigo 8.°, n.° 1, 1.°, 2.° e 5.°, da Lei PNR. Esta medida está rodeada de várias garantias, designadamente a autorização prévia do Procurador do Rei.

79 O artigo 16.°/3 da Lei de 30 de novembro de 1998 diz respeito, por sua vez, às investigações pontuais no âmbito da finalidade prevista no artigo 8.°, n.° 1, 4.°, da Lei PNR. Esta medida está rodeada de várias garantias, designadamente a informação e a fiscalização do Comité Permanente R.

80 A recorrente considera que os membros destacados dos serviços de polícia que pertencem à UIP não são suficientemente independentes para responder aos pedidos de acesso no âmbito dessas investigações pontuais.

81 O artigo 14.°, n.° 1, da Lei PNR determina a composição da UIP. Os trabalhos preparatórios expõem a este respeito que: «O modelo belga assenta num conceito de unidade multidisciplinar composta por um funcionário dirigente que assegura uma função de direção, por membros administrativos e por membros destacados provenientes dos serviços competentes.

A UIP será composta:

– *por um funcionário dirigente, assistido por um serviço de apoio, que, dentro do SPF Interior, será responsável, nomeadamente, pela gestão do banco de dados, pelo cumprimento das obrigações das transportadoras e dos operadores de viagens, pelos relatórios, pela celebração de protocolos com os serviços competentes e pelo respeito das condições de tratamento. O serviço de apoio será composto, designadamente, por analistas, juristas, peritos em ICT e pelo responsável pela proteção de dados, que disporão das habilitações de segurança necessárias.*

– *por membros destacados provenientes dos serviços competentes taxativamente enumerados no ponto 2 do n.° 1, a saber: os serviços de polícia, os serviços de informações e a Autoridade Aduaneira. As finalidades precisas constituem, enquanto tais, a primeira limitação. Por exemplo, a nível dos serviços da polícia integrada, é evidente que um agente de bairro numa polícia local nunca poderá aceder aos dados dos passageiros, uma vez que as finalidades não fazem parte das suas funções.*

O destacamento dos serviços competentes tem por objetivo garantir um certo grau de perícia, mas não exclui acordos entre estes serviços a fim de mutualizar os destacamentos» (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, p. 22).

O Ministro da Segurança e da Administração Interna acrescentou que «[s]*erá igualmente designado um "data protection officer" encarregado de apresentar relatórios à Commission de la protection de la vie privée (Comissão para a proteção da vida privada)*» (Doc. parl, Chambre, 2015-2016, DOC 54-2069/003, p. 24).

O arrêté royal du 21 décembre 2017 relatif à l'exécution de la loi PNR (Decreto Real, de 21 de dezembro de 2017, relativo à execução da Lei PNR) determina as modalidades de composição e organização da UIP. O relatório ao Rei que antecede este decreto real precisa que «[o] *banco de dados só pode [...] ser consultado na UIP, e apenas pelos membros da UIP, no âmbito das suas funções, bem como pelo responsável pela proteção de dados*» [3].

O procedimento de destacamento é regulado pelos artigos 12.° a 21.° deste mesmo decreto real. O facto de os membros destacados de serviços competentes participarem no funcionamento da UIP visa garantir que esta seja composta por

[3] *Moniteur belge* de 29 de dezembro de 2017, segunda edição, p. 116833.

pessoas que gozem de uma determinada perícia, a fim de reforçar assim a eficácia da UIP. Esta possibilidade de destacamento está, aliás, expressamente prevista no artigo 4.°, n.° 3, da Diretiva PNR.

Nada permite considerar que essas pessoas, embora mantenham o seu estatuto no seu serviço de origem, não exercem as suas funções com independência na UIP. Os membros da UIP são, além disso, passíveis de sanções penais se não respeitarem o segredo profissional ou retiverem, consciente e deliberadamente, dados e informações que obstam às finalidades previstas no artigo 8.° (artigos 48.° e 49.°).

82 No que respeita ao acesso aos dados «PNR» no âmbito de investigações pontuais decorrido o prazo de seis meses, o Tribunal de Justiça considerou, no seu Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017 (EU:C:2017:592), que a utilização dos dados PNR assim armazenados deveria «*basear-se em critérios objetivos, para definir as circunstâncias e as condições em que as autoridades canadianas previstas no acordo projetado podem ter acesso a esses dados tendo em vista a sua utilização*» *e que «esta utilização deveria, salvo em casos de urgência devidamente justificados, ser sujeita a uma fiscalização prévia efetuada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão de autorizar a utilização ocorra na sequência de um pedido fundamentado dessas autoridades, apresentado, nomeadamente, no âmbito de processos de prevenção, de deteção ou de ação penal*» (n.° 208).

83 A fim de verificar se a UIP pode ser considerada esta «outra autoridade nacional competente» na aceção do artigo 12.°, n.° 3, da Diretiva PNR, há que submeter uma sétima questão prejudicial ao Tribunal de Justiça antes de proferir uma decisão.

Quanto ao prazo de conservação dos dados «PNR» (artigo 18.° da Lei PNR)

84 A recorrente considera que o prazo de cinco anos durante o qual são conservados os dados «PNR» é desproporcionado.

85 O considerando 25 da Diretiva PNR dispõe:

«O prazo durante [o] qual deverão ser conservados os dados PNR deverá ser tão longo quanto necessário e proporcionado à consecução dos objetivos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Atendendo à natureza dos dados e à sua utilização, é necessário que os dados PNR sejam conservados durante um prazo suficientemente longo para permitir a realização de análises e a sua utilização no âmbito de investigações. A fim de evitar uma utilização desproporcionada, após o prazo inicial de conservação, os dados PNR deverão ser anonimizados mediante a ocultação de elementos dos dados. A fim de assegurar o nível mais elevado de proteção de dados, o acesso aos dados PNR integrais, que permitem a

identificação direta do seu titular, só deverá ser concedido em condições muito estritas e limitadas após aquele prazo inicial».

86 Segundo a jurisprudência do Tribunal de Justiça, o período de conservação dos dados deve «responder sempre a critérios objetivos, que estabeleçam uma relação entre os dados pessoais a conservar e o objetivo prosseguido» (Acórdão de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.° 93; Despacho de 16 de março de 2017, Tele2 Sverige e Watson e o., C-203/15 REC e C-698/15 REC, EU:C:2017:222, n.° 110; e Parecer 1/15 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.° 191).

87 No que se refere mais especificamente aos dados «PNR», o Tribunal de Justiça considerou, no seu Parecer 1/15, *supra* referido, de 26 de julho de 2017, que o prazo de cinco anos «*não parece exceder os limites do estritamente necessário para efeitos de luta contra o terrorismo e a criminalidade transnacional grave*» (n.° 209), com a ressalva de que, «*quanto aos passageiros aéreos relativamente aos quais esse risco não tenha sido identificado à sua chegada ao Canadá e até à sua saída deste país terceiro, não se afigura existir, uma vez saídos desse país, qualquer relação, ainda que indireta, entre os seus dados PNR e o objetivo prosseguido pelo acordo projetado, que justifique [...] um armazenamento contínuo dos dados PNR de todos os passageiros aéreos, depois da sua saída do Canadá, 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 (v., por analogia, Acórdão de 21 de dezembro de 2016, Tele2 Sverige e Watson e o., C-203/15 e C-698/15, EU:C:2016:970, n.° 119)*» (n.° 205).

88 O artigo 18.° da Lei PNR prevê que os dados dos passageiros são conservados no banco de dados dos passageiros por um período máximo de cinco anos a contar do respetivo registo, e que, decorrido esse prazo, são destruídos. Em conformidade com o artigo 21.°, n.° 1, da mesma lei, a UIP assegura que os dados dos passageiros sejam apagados do seu banco de dados, de forma definitiva, no termo do prazo previsto no artigo 18.°

O prazo de cinco anos deve, todavia, ser lido em conjugação com os artigos 19.° e seguintes da mesma lei, que regulam igualmente as modalidades de conservação dos dados. O artigo 19.° desta lei deve, ele próprio, ser lido em conjugação com o artigo 4.°,14.°, que define a «anonimização mediante mascaramento de elementos de dados» como «o facto de tornar invisíveis para os utilizadores os elementos dos dados suscetíveis de identificar diretamente o seu titular, a que se refere o artigo 19.°».

O artigo 20.° da Lei PNR prevê que, decorrido o período de seis meses referido no artigo 19.°, é permitida a divulgação de todos os dados dos passageiros apenas para o tratamento de dados previsto no artigo 27.° e nas condições previstas por esta disposição.

Por outro lado, o resultado do tratamento a que se refere o artigo 24.° só é conservado pela UIP durante o período necessário para informar as autoridades competentes e as UIP dos outros Estados-Membros da existência de uma correspondência positiva (artigo 21.°, n.° 3, primeiro parágrafo).

O artigo 22.° da Lei PNR garante que o funcionário dirigente e o responsável pela proteção de dados apenas tenham acesso a todos os dados relevantes no âmbito do exercício das suas funções.

Por último, o tratamento dos dados é objeto de registo e está em correlação direta com as finalidades previstas no artigo 8.° (artigo 23.°, n.° 1). A UIP assegura o registo, conservando durante cinco anos a documentação de todos os sistemas e procedimentos de tratamento sob a sua responsabilidade (artigo 23.°, n.° 2, primeiro parágrafo).

89 O prazo de conservação dos dados dos passageiros deve ser determinado tendo em conta às finalidades do tratamento desses dados, em relação direta com os objetivos de prevenção, investigação e repressão das infrações terroristas e da criminalidade grave.

90 A Comissão para a proteção da vida privada tinha, contudo, referido que, quando o prazo de conservação dos dados é longo e os dados são armazenados em massa, «o risco de traçar o perfil das pessoas em causa aumenta, tal como o risco de desvio de finalidade (*fonction creep*), isto é, o desvio potencial da utilização de dados para outras infrações relativamente às quais não houve inicialmente um acordo (político) de troca de dados» (Comissão para a proteção da vida privada, Parecer de iniciativa n.° 01/2010, de 13 de janeiro de 2010, relativo ao projeto de lei que aprova o Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento de dados em causa pelo mesmo departamento (Acordo PNR 2007), feito em Bruxelas, a 23 de julho de 2007, e em Washington, a 26 de julho de 2007, ponto 3.3, pp. 17-18).

No seu Parecer n.° 55/2015, de 16 de dezembro de 2015, sobre o anteprojeto de lei que deu origem à Lei PNR, a Comissão para a proteção da vida privada também entendeu que a necessidade de um prazo de conservação dos dados de cinco anos devia ser justificada de forma mais precisa e fundamentada.

No seu Parecer de 19 de agosto de 2016, o Comité Consultivo da Convenção n.° 108 tinha igualmente observado que «os dados ocultados ainda permitem identificar as pessoas e, como tal, continuam a ser dados pessoais, e a sua conservação deveria também ser limitada no tempo para prevenir uma vigilância permanente generalizada» (Parecer de 19 de agosto de 2016, T-PD (2016)18rev, p. 9).

91 A Cour constitutionnelle (Tribunal Constitucional) considera que, a fim de verificar se este prazo de conservação de cinco anos, autorizado pela Diretiva

PNR, é, atendendo ao que foi acima exposto e às diferentes garantias enumeradas no n.° 88, *supra*, compatível com as observações do Tribunal de Justiça mencionadas no n.° 87, *supra*, uma vez que não estabelece uma distinção consoante os passageiros em causa se mostrem, no âmbito da avaliação prévia, suscetíveis ou não de apresentar um risco para a segurança pública, é necessário submeter ao Tribunal de Justiça uma oitava questão prejudicial.

3. Quanto ao segundo fundamento

92 A recorrente considera que, ao alargar o sistema «PNR» aos voos intra-UE, as disposições impugnadas restabelecem indiretamente controlos nas fronteiras que são contrários à liberdade de circulação das pessoas.

93 No que respeita ao âmbito de aplicação da Lei PNR, os trabalhos preparatórios expõem:

«A inclusão intra-UE na recolha de dados permitirá obter um quadro mais completo das deslocações dos passageiros que constituam uma potencial ameaça para a segurança intracomunitária e nacional. A prática já demonstrou que certos "*returnees*" (também chamados *foreign fighters* que regressam à Europa) embarcam em voos diferentes antes de chegarem ao seu destino final.

A Diretiva UE PNR prevê expressamente a possibilidade de os Estados-Membros tratarem os dados dos passageiros da UE no que respeita ao tráfego internacional na União Europeia. Além disso, todos os Estados-Membros aprovaram, em 21 de abril de 2016, no Conselho dos Ministros do Interior e da Justiça, uma declaração destinada a transpor a Diretiva UE PNR para as legislações nacionais também no que respeita ao tráfego intra-União Europeia» (Doc. Parl., Chambre, 2015-2016, DOC 54-2069/001, p. 7).

94 A Cour constitutionnelle (Tribunal Constitucional) salienta que os passageiros a que se refere o capítulo 11 da Lei PNR, bem como os dados abrangidos e o prazo de conservação, são limitados.

Com efeito, os trabalhos preparatórios expõem que «[...] só são abrangidos os passageiros que pretendam atravessar ou que tenham atravessado as fronteiras externas da Bélgica para entrar ou sair, e isso independentemente do tipo de transporte utilizado (marítimo, ferroviário, terrestre, aéreo). Apenas os dados desses passageiros serão, portanto, tratados pelos serviços de polícia encarregados do controlo nas fronteiras e pelo Serviço de Estrangeiros.

Os passageiros que pretendam transitar pela zona internacional de trânsito, por exemplo, de um aeroporto situado na Bélgica, estão igualmente abrangidos, na medida em que lhes são igualmente aplicáveis as regras relativas à entrada no território, à permanência, ao estabelecimento e ao afastamento dos estrangeiros. Assim, essas pessoas devem dispor dos documentos de viagem exigidos. Determinadas pessoas estão sujeitas à obrigação de visto de escala aeroportuária;

os controlos nestas zonas são autorizados e podem, em alguns casos, conduzir a uma medida de repulsão.

[…] apenas os dados de passageiros ditos "API" serão transmitidos aos serviços de polícia e ao Serviço de Estrangeiros ao abrigo do presente capítulo. Estes dados são enumerados no artigo 9.°, n.° 2, do anteprojeto de lei.

Os referidos dados correspondem, em substância, aos dados que as transportadoras aéreas já estão obrigados a transmitir por força do Decreto Real de 11 de dezembro de 2006.

[...]

A utilização dos dados é igualmente limitada a vinte e quatro horas. Decorrido esse prazo, se o acesso aos dados dos passageiros for necessário no âmbito do exercício das suas funções legais, o Serviço de Estrangeiros apresenta um pedido fundamentado à UIP» (*ibidem*, pp. 34-35).

95 Conforme *foi acima dito*, o considerando 10 da Diretiva PNR autoriza o alargamento do sistema «PNR» aos voos intra-UE. O artigo 2.° da Diretiva PNR regula o procedimento destinado a alargar o âmbito de aplicação.

A finalidade de lutar contra a imigração ilegal e de melhorar o controlo nas fronteiras apenas diz respeito às categorias de passageiros enumeradas no artigo 29.°, n.° 2, da Lei PNR, e limita-se aos dados «API» referidos no artigo 9.°, n.° 1, 18.°, desta mesma lei. Os tratamentos efetuados no âmbito desta finalidade também são limitados. As disposições impugnadas inserem-se no âmbito da transposição da Diretiva «API», que prossegue igualmente como objetivos a luta contra a imigração ilegal e a melhoria do controlo nas fronteiras.

96 No seu Parecer n.° 55/2015, de 16 de dezembro de 2015, sobre o anteprojeto de lei que deu origem à Lei de 25 de dezembro de 2016, a Comissão para a proteção da vida privada interroga-se, no entanto, sobre a compatibilidade com o princípio da livre circulação de pessoas do sistema «PNR» implementado, que visa «tanto os transportes com chegada e partida no espaço Schengen (extra-Schengen) como os transportes que entram e saem do espaço Schengen (intra-Schengen)», o que pode conduzir «indiretamente a um restabelecimento dos controlos nas fronteiras internas» (n.os 21-25).

97 Por duvidar da interpretação e da validade da Diretiva 2004/82 «API» à luz da Carta e do TUE, a Cour constitutionnelle (Tribunal Constitucional) decide submeter uma nona questão prejudicial ao Tribunal de Justiça.

98 A Cour constitutionnelle (Tribunal Constitucional) submete uma última questão, relativa à eventual calendarização dos efeitos do seu acórdão.

IV. Questões prejudiciais

A Cour constitutionnelle (Tribunal Constitucional) submete, portanto, as seguintes questões prejudiciais:

1. Deve o artigo 23.° 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 – RGPD), lido em conjugação com o artigo 2.°, n.° 2, alínea d), deste regulamento, ser interpretado no sentido de que se aplica a uma legislação nacional como a Lei de 25 de dezembro de 2016, relativa ao tratamento dos dados dos passageiros, 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, bem como 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?

2. O anexo I da Diretiva (UE) 2016/681 é compatível com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, no sentido de que os dados que enumera são muito vastos – nomeadamente os dados referidos no ponto 18 do anexo I da Diretiva (UE) 2016/681, que excedem os dados referidos no artigo 3.°, n.° 2, da Diretiva 2004/82/CE – 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 da Diretiva (UE) 2016/681 são compatíveis com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, 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.°, ponto 4, da Diretiva (UE) 2016/681 e o anexo I da mesma diretiva são compatíveis com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, 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.° da Diretiva (UE) 2016/681, lido em conjugação com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, 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.° da Diretiva (UE) 2016/681 é compatível com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, 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.°, n.° 3, da Diretiva (UE) 2016/681 ser interpretado no sentido de que abrange a UIP criada pela Lei de 25 de dezembro de 2016, 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.° da Diretiva (UE) 2016/681, lido em conjugação com os artigos 7.°, 8.° e 52.°, n.° 1, da Carta dos Direitos Fundamentais da União Europeia, 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 2004/82/CE é compatível com o artigo 3.°, n.° 2, do Tratado da União Europeia e com o artigo 45.° da Carta dos Direitos Fundamentais da União Europeia, na medida em que as obrigações que institui se aplicam aos voos no interior da União Europeia?

b) Deve a Diretiva 2004/82/CE, lida em conjugação com o artigo 3.°, n.° 2, do Tratado da União Europeia e com o artigo 45.° da Carta dos Direitos Fundamentais da União Europeia, 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 (UE) 2016/681, viola uma ou mais das obrigações decorrentes das disposições

mencionadas nestas questões, poderia a Cour constitutionnelle (Tribunal Constitucional) manter provisoriamente os efeitos da Lei de 25 de dezembro de 2016, relativa ao tratamento de dados dos passageiros, 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 referida lei?