

Processo C-215/20**Resumo do pedido de decisão prejudicial em aplicação do artigo 98.º, n.º 1, do Regulamento de Processo do Tribunal de Justiça****Data de entrada:**

19 de maio de 2020

Órgão jurisdicional de reenvio:

Verwaltungsgericht Wiesbaden (Tribunal administrativo de Wiesbaden, Alemanha)

Data da decisão de reenvio:

13 de maio de 2020

Autor:

JV

Recorrido:

Bundesrepublik Deutschland (República Federal da Alemanha)

Objeto do processo principal

Admissibilidade da transferência de dados pessoais de passageiros aéreos

Objeto e fundamento jurídico do pedido prejudicial

Interpretação do direito da União, artigo 267.º TFUE

Questões prejudiciais

1. 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 (JO EU L 119, de 4 de maio de 2016, p. 132; a seguir Diretiva PNR), nos termos da qual as transportadoras aéreas transmitem dados muito amplos relativos a todos os passageiros, sem exceção, às unidades de informação de passageiros (UIP)

criadas pelos Estados-Membros, sendo os dados nelas utilizados, sem uma razão especial, para comparação automatizada com bases de dados e padrões, e a seguir conservados durante cinco anos, considerando os objetivos prosseguidos pela Diretiva PNR e a exigência de determinabilidade e de proporcionalidade, é compatível com a Carta dos Direitos Fundamentais, especialmente com os seus artigos 7.º, 8.º e 52.º?

2. Em especial:

- a) O artigo 3.º, n.º 9, da Diretiva PNR, em conjugação com o seu anexo II, ao estabelecer que o conceito de «criminalidade grave», na aceção da Diretiva PNR, designa as infrações enumeradas no anexo II da Diretiva PNR puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos nos termos do direito nacional de um Estado-Membro, é compatível com os artigos 7.º e 8.º da Carta dos Direitos Fundamentais, na perspetiva da exigência de determinabilidade e de proporcionalidade?
- b) Os dados dos registos de identificação dos passageiros (a seguir, dados PNR) que devem ser transferidos, ao abrangerem os nomes (artigo 8.º, n.º 1, primeira frase, em conjugação com o n.º 4 do anexo I da Diretiva PNR), a informação de passageiro frequente (artigo 8.º, n.º 1, primeira frase, em conjugação com o n.º 8 do anexo I da Diretiva PNR) e a informação constante do campo de um «texto livre» com informações gerais (artigo 8.º, n.º 1, primeira frase, em conjugação com o n.º 12 do anexo I da Diretiva PNR), estão suficientemente determinados para poderem justificar uma restrição aos artigos 7.º e 8.º da Carta dos Direitos Fundamentais?
- c) É compatível com os artigos 7.º e 8.º da Carta dos Direitos Fundamentais e com os objetivos da Diretiva PNR que, além dos dados dos passageiros, sejam igualmente incluídos os dados de terceiros, tal como da agência/agente de viagens (n.º 9 do anexo I da Diretiva PNR), das pessoas que acompanham os menores (n.º 12 do anexo I da Diretiva PNR) e de outros passageiros (n.º 17, do anexo I da Diretiva PNR)?
- d) É a Diretiva PNR compatível com os artigos 7.º, 8.º e 24.º da Carta dos Direitos Fundamentais, ao prever que os dados PNR relativos a passageiros menores devem ser transmitidos, tratados e conservados?
- e) O artigo 8.º, n.º 2, da Diretiva PNR, em conjugação com o n.º 18 do anexo I da Diretiva PNR, e à luz do princípio da limitação dos dados ao mínimo necessário, é compatível com os artigos 8.º e 52.º da Carta dos Direitos Fundamentais, ao prever que os dados API, mesmo que sejam iguais aos dados PNR, são transmitidos à UIP dos Estados-Membros?
- f) É o artigo 6.º, n.º 4, da Diretiva IVA, enquanto base legal para a fixação dos critérios utilizados para a comparação dos dados dos registos (os chamados padrões), um fundamento previsto por lei suficientemente legítimo, no

- sentido dos artigos 8.º, n.º 2, e 52.º da Carta dos Direitos Fundamentais e do artigo 16.º, n.º 2, do TFUE?
- g) O artigo 12.º da Diretiva PNR limita a restrição dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais ao estritamente necessário, quando os dados transmitidos às UIPs dos Estados-Membros são conservados durante cinco anos?
- h) A anonimização prevista no artigo 12.º, n.º 2, da Diretiva PNR reduz os dados pessoais ao mínimo necessário, nos termos dos artigos 8.º e 52.º da Carta dos Direitos Fundamentais, quando essa anonimização não é mais do que uma pseudonimização, reversível a todo o tempo?
- i) Devem os artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais ser interpretados no sentido de que exigem que os passageiros de transporte aéreo, cujos dados sejam desanonimizados no quadro do tratamento de dados de passageiros aéreos (artigo 12.º, n.º 3, da Diretiva PNR), sejam disso informados, dando-lhes assim a possibilidade de recurso judicial?
3. O artigo 11.º da Diretiva PNR, ao permitir a transferência de dados PNR para Estados terceiros que não dispõem de um nível adequado de proteção de dados, é compatível com os artigos 7.º e 8.º da Carta dos Direitos Fundamentais?
4. O artigo 6.º, n.º 4, quarto período, da Diretiva PNR confere proteção suficiente perante o tratamento de categorias especiais de dados pessoais, no sentido do artigo 9.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (JO UE L 119, de 4 de maio de 2016, p. 1; a seguir Regulamento 2016/679) e do artigo 10.º da 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 UE L 119, de 4 de maio de 2016, p. 89; a seguir Diretiva 2016/680), quando, no campo de texto livre «informações gerais» (n.º 12 do anexo I da Diretiva PNR), podem ser transmitidas, por exemplo, encomendas de comida que permitem extrair conclusões sobre essas categorias especiais de dados pessoais?
5. É compatível com o artigo 13.º do Regulamento 2016/679 que a transportadora aérea, através do seu sítio Internet, se limite a remeter os passageiros para a lei de transposição nacional (in casu: Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU

2016/681 (Fluggastdatengesetz) [Lei Sobre o Tratamento de Dados de Passageiros de Transporte Aéreo e que transpõe a Diretiva (UE) 2016/681, de 6 de junho de 2017, BGBl. I, p. 1484; a seguir FlugDaG]?

Disposições de direito da União invocadas

Carta dos Direitos Fundamentais da União Europeia (a seguir, «Carta») artigos 7.º, 8.º, 24.º, 47.º e 52.º

Artigo 16.º TFUE

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 (JO L 119 4 de maio de 2016, p. 132).

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 L 119 de 4 de maio de 2016, p. 89.

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 (a seguir, Regulamento 2016/679) (JO L 119 de 4 de maio de 2016).

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23 de novembro de 1995, p. 31).

Disposições de direito nacional invocadas

Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Lei Sobre o Tratamento de Dados de Passageiros de Transporte Aéreo e que transpõe a Diretiva (UE) 2016/681; a seguir, FlugDaG).

Apresentação sucinta dos factos e do processo principal

- 1 Em 10 de junho de 2017 entrou em vigor a Lei Sobre o Tratamento de Dados, que transpõe para o direito alemão a Diretiva 2016/681. Esta diretiva regula a transferência de dados de voos de Estados-Membros da União Europeia para

Estados terceiros e de Estados terceiros para Estados-Membros da União Europeia, bem como o tratamento desses dados.

- 2 O objetivo da Diretiva 2016/681, de acordo com o seu artigo 1.º, n.º 2, é a prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. O artigo 4.º da diretiva obriga os Estados-Membros a criarem uma autoridade central para agir na qualidade da sua «unidade de informações de passageiros» (UIP), competente para efeitos da recolha de dados PNR junto das transportadoras aéreas, pela sua conservação e tratamento e pela transferência desses dados PNR ou dos resultados do seu tratamento às autoridades competentes. Nos termos do artigo 8.º, em conjugação com o anexo I da Diretiva 2016/681, os Estados-Membros devem assegurar que as transportadoras aéreas transferem uma quantidade definida de dados PNR para a base de dados da UIP do Estado-Membro em cujo território o voo aterrará ou do qual descolará. Nos termos do artigo 9.º da Diretiva 2016/681, os Estados-Membros podem solicitar e transmitir entre si dados PNR. Os Estados-Membros podem também transferir esses dados para Estados terceiros, nas condições previstas no artigo 11.º da diretiva. Nos termos do artigo 12.º, n.º 2, da Diretiva 2016/681 os dados dos passageiros, que devem ser conservados pelo prazo de cinco anos, devem ser anonimizados após seis meses, o que significa que os elementos desses dados que permitem identificar diretamente o passageiro, deixam de poder ser conhecidos. Todavia, nas condições previstas no n.º 3 do artigo 12.º da Diretiva 2016/681, é possível a desanonimização. O artigo 6.º da diretiva regula o tratamento de dados, que é feito através da sua comparação automatizada com dados que constam de bases de dados e de acordo com critérios previamente estabelecidos (que a FlugDaG designa por «padrões»).
- 3 O autor voou com a companhia aérea Lufthansa, em 28 de abril de 2019, de Frankfurt am Main (Alemanha) para Bogotá (Colômbia) e, em 7 de maio de 2019, do Rio de Janeiro (Brasil) de volta para Frankfurt am Main. O autor pretende que a demandada apague os seus dados relativos a estes voos.

Apresentação sucinta da fundamentação do pedido de decisão prejudicial

- 4 Para a decisão do litígio do processo principal é relevante saber se a Diretiva 2016/681, total ou parcialmente, viola a Carta. Nesse caso, a FlugDaG, enquanto lei de transposição, não seria aplicável, e o tratamento de dados litigioso seria ilegal e a pretensão do autor de apagamento dos dados seria procedente.

Quanto à questão 1: A Diretiva 2016/681 é, na sua totalidade, compatível com a Carta?

- 5 Os diversos tratamentos de dados PNR previstos na Diretiva 2016/681 e na FlugDaG entram no campo de proteção do direito fundamental de respeito pela vida privada garantido no artigo 7.º da Carta. Este direito aplica-se a todas as informações relativas a uma pessoa singular identificada ou identificável

(Acórdão de 9 de novembro de 2010, Volker und Markus Schecke und Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.º 52), pelo que é também aplicável às informações indicadas no anexo I da Diretiva 2016/618 sobre o tratamento de dados PNR das pessoas em causa. O tratamento de dados PNR previsto na Diretiva 2016/681 está igualmente no âmbito de aplicação do artigo 8.º da Carta, por se tratar de dados de carácter pessoal no sentido desse artigo, e deve, assim, necessariamente, respeitar os requisitos da proteção de dados previstos neste artigo (Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 123).

- 6 Segundo jurisprudência do Tribunal de Justiça, a comunicação de dados de carácter pessoal a um terceiro, como uma autoridade pública, constitui uma ingerência no direito fundamental consagrado no artigo 7.º da Carta, seja qual for a utilização posterior das informações comunicadas. O mesmo se diga da conservação dos dados pessoais e do acesso aos referidos dados com vista à sua utilização pelas autoridades públicas. A este respeito, pouco importa que as informações relativas à vida privada em questão sejam ou não sensíveis, ou que os interessados tenham ou não sofrido inconvenientes em razão dessa ingerência (Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.º 124). O mesmo é válido para o artigo 8.º da Carta, na medida em que constituem tratamento de dados pessoais (Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.º 126).
- 7 Com efeito, os direitos consagrados nos artigos 7.º e 8.º da Carta não podem ser considerados prerrogativas absolutas, mas devem ser considerados de acordo com a sua função na sociedade (Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.º 136). A restrição destes direitos deve ser amplamente possível na prossecução de fins de interesse geral, entre os quais se inclui a luta contra o terrorismo e a criminalidade grave (v. Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 149). No entanto, as restrições aos direitos fundamentais devem ser adequadas e necessárias para atingir esses objetivos e não serem desproporcionais em sentido estrito. Além disso, segundo o artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades por esta reconhecidos 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 (Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 138).
- 8 O princípio da proporcionalidade exige, segundo jurisprudência constante do Tribunal de Justiça, que os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos (v. Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 46). Relativamente ao direito fundamental do respeito da vida privada, a proteção deste direito fundamental exige, segundo a jurisprudência constante do Tribunal de Justiça, em quaisquer circunstâncias, que as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer

na estrita medida do necessário (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 und C-594/12, EU:C:2014:238, n.º 52).

- 9 Para satisfazer estes requisitos a lei que estabelece essa restrição tem de prever regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e imponham exigências mínimas. As pessoas cujos dados são transferidos têm de dispor de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Essa legislação deve concretamente indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados, garantindo, assim, que a ingerência se limita ao estritamente necessário. A necessidade de dispor de tais garantias é ainda mais importante quando os dados pessoais são sujeitos a tratamento automatizado. Isto aplica-se especialmente quando se trata da proteção de dados pessoais sensíveis (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.ºs 54 e segs.).
- 10 Subsistem sérias dúvidas de que a Diretiva 2016/681 satisfaça estas exigências em todos os seus aspetos.
- 11 Segundo as disposições da Diretiva 2016/681, as companhias aéreas são obrigadas a transmitir, relativamente a cada voo, os dados PNR, sem exceção, de todos os passageiros à «unidade de informações de passageiros» (UIP) dos Estados-Membros, em que esses dados serão tratados de forma automatizada e são conservados duradouramente. Para esse efeito, não é necessário que exista uma razão concreta, por exemplo, um indício de uma ligação ao terrorismo internacional ou à criminalidade organizada. Isto conduz a que, num curto espaço de tempo, sejam tratados e conservados centenas de biliões de dados. O «stock de dados» de passageiros aéreos afeta assim patentemente os direitos fundamentais de uma grande parte da população europeia.
- 12 Os dados a transferir, indicados no artigo 8.º, n.º 1, primeiro período da Diretiva 2016/681, em conjugação com o seu anexo I, são muitos amplos e incluem, para além do nome e morada dos passageiros, também todo o percurso realizado, a sua bagagem, as pessoas que os acompanhavam, todo o tipo de informações sobre pagamentos e também «informações gerais», de que não é dada uma definição precisa. De todos estes dados é possível fazer deduções muito precisas sobre a vida privada e económica das pessoas em causa. A partir delas é possível saber, designadamente, quem, quando, com quem e para onde foi feita a viagem, qual o meio de pagamento utilizado e quais os dados para contacto indicados e se a pessoa viajou com bagagem ligeira ou mais pesada. A partir da indicação genérica «informações gerais» podem ainda ser indicados outros dados, cujo âmbito é totalmente obscuro (sobre este ponto v. as observações infra).
- 13 O órgão jurisdicional de reenvio considera comparáveis o tratamento e conservação de dados PNR com a stockagem de dados no domínio das telecomunicações. Sobre esta o Tribunal de Justiça declarou que tal conservação de dados constitui uma ingerência de grande amplitude nos direitos fundamentais

consagrados nos artigos 7.º e 8.º da Cartade e deve ser considerada particularmente grave. Pois a conservação massiva e sem fundamento de dados pessoais muito amplos e que permitem tirar ilações sobre a vida privada e económica das pessoas e causa é suscetível de gerar no espírito dessas pessoas a sensação de que estão a ser constantemente vigiadas (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 37).

- 14 No seu primeiro acórdão sobre conservação de dados, o Tribunal de Justiça considerou que tal situação viola os direitos fundamentais por serem conservados os dados de pessoas relativamente às quais não existem indícios de que o seu comportamento possa ter umnexo, ainda que indireto ou longínquo, com infrações graves (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:C:2014:238, n.º 58). Isto aplica-se igualmente ao tratamento e conservação de dados PNR, o que significa que as disposições da Diretiva 2016/681 excedem o limite do que é necessário para atingir os objetivos desta diretiva, sendo por isso desproporcionais no sentido da jurisprudência do Tribunal de Justiça. A isto acresce que os dados PNR, ao contrário dos dados de tráfego de telecomunicações no quadro da conservação de dados, não apenas são conservados sem razão, mas são também tratados, i.e., comparados de forma automatizada com bases de dados e com os chamados «padrões».

Quanto à questão 2 a): conceito de «criminalidade grave»

- 15 Igualmente questionável é a determinabilidade e a proporcionalidade da recolha e tratamento de dados PNR em função dos crimes que através deste procedimento se pretendem combater. O fim declarado da Diretiva 2016/681 é a prevenção, a deteção, a investigação e a repressão das infrações terroristas e da criminalidade grave. O n.º 9 do artigo 3.º define «criminalidade grave» como as infrações enumeradas no anexo II puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos nos termos do direito nacional de um Estado-Membro. O anexo II da Diretiva 2016/681 tem uma lista de 26 crimes no sentido do n.º 9 do artigo 3.º Entre eles contam-se, por exemplo, a corrupção (n.º 6), a fraude (n.º 7), a criminalidade informática/cibercrime (n.º 9) e os crimes contra o ambiente (n.º 10).
- 16 Em primeiro lugar, coloca-se a questão da determinabilidade desta norma. Assim, por exemplo, o direito penal alemão não conhece um crime de «corrupção», que corresponde antes a um conceito genérico que abrange vários tipos de crimes. O mesmo se aplica a «fraude», a «criminalidade informática/cibercrime» e a «crimes contra o ambiente».
- 17 Esta circunstância e a remissão do n.º 9 do artigo 3.º da Diretiva 2016/681 para a medida da pena nos Estados-Membros levam a que os dados PNR sejam utilizados de modo não uniforme nos diferentes Estados-Membros da União. Por exemplo, é deixada aos Estados-Membros, através da moldura penal dos códigos penais nacionais respetivos, a faculdade de qualificarem determinados crimes

como «criminalidade grave» no sentido da diretiva, ou de não os qualificarem como tal.

- 18 Duvidosa é também, do ponto de vista da adequação deste regime, a fixação do limite mínimo da pena previsto no n.º 9 do artigo 3.º da Diretiva 2016/681, numa pena privativa da liberdade com a duração máxima não inferior a três anos. No direito penal alemão fica assim abrangida uma enorme variedade de crimes cuja qualificação de «criminalidade grave» parece muito discutível. Por exemplo, nos termos do § 263 do Código Penal alemão (StGB), a moldura penal do crime de burla simples tem o máximo de cinco anos de prisão. O mesmo se aplica, por exemplo, à recetação (§ 259 do StGB), à fraude informática (§ 263a do StGB) ou à infidelidade (§ 266 do StGB). Todos estes crimes se subsumem nos crimes previstos no anexo II da Diretiva 2016/681 (especialmente nos crimes de fraude indicados no n.º 6). No entanto estes delitos correspondem a diversas formas de «criminalidade comum» e podem corresponder a delitos leves. Assim, a sua inclusão na Diretiva 2016/681 nada tem que ver com a prevenção e a repressão da criminalidade grave.

Quanto à questão 2 b): determinabilidade dos dados PNR

- 19 Considerando o facto de o Tribunal de Justiça exigir normas claras e precisas que regulem o âmbito e a aplicação das medidas em causa (v. Parecer 1/15 de 26 de julho de 2017 EU:C:2017:592, n.º 141), alguns dos dados PNR que as companhias aéreas devem transmitir à UIP dos Estados-Membros não estão suficientemente determinados no anexo I da Diretiva 2016/681.
- 20 Não se vê claramente o que se entende com a informação a transmitir «nome(s)» (anexo I, n.º 4 da Diretiva 2016/681). Isto traduz-se na transposição alemã feita pelo § 2, n.ºs 1 e 9, da FlugDaG, segundo o qual devem ser transmitidos o apelido, o nome de solteiro, o nome próprio, eventuais graus académicos e outras informações sobre o nome. No uso geral da linguagem a identificação pelo nome não inclui o nome de solteiro. Assim, não é claro se este se deve incluir no nome(s) indicado no n.º 4 do anexo I da Diretiva 2016/681. Duvidoso é também se um título académico deve ser considerado como parte do nome, no sentido da diretiva.
- 21 Relativamente à comunicação e tratamento de dados sobre passageiros frequentes (n.º 8 do anexo I da Diretiva 2016/681) existe uma indeterminação do regime aplicável. Não é claro, designadamente, se apenas está em causa a participação nos programas de bónus para passageiros frequentes ou se também estão incluídas informações concretas sobre voos e reservas da pessoa que participa nesse programa.
- 22 A formulação do n.º 12 do anexo I da Diretiva 2016/681 «Observações gerais (designadamente...)» é muito vaga e incompreensível. Como resulta do advérbio «designadamente», trata-se de uma enumeração exemplificativa e não taxativa. Além disso, no preenchimento deste «texto livre» podem até incluir-se

informações que não têm qualquer relação com a finalidade da transferência de dados de passageiros aéreos (neste sentido, v. Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 160). Esta formulação pode até permitir transmitir informações que a Diretiva 2016/681 pretende proibir, nomeadamente dados sensíveis que, como decorre do considerando 15 da mesma diretiva, não podem ser recolhidos (v. a questão 4).

Quanto à questão 2 c): terceiros afetados

- 23 Nos termos do seu artigo 1.º, n.º 1, a Diretiva 2016/681 regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (PNR) de voos extra-UE e o seu tratamento pelos Estados-Membros. Nos termos do n.º 4 do artigo 3.º da mesma diretiva entende-se por passageiro, a 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. No entanto, no anexo I da Diretiva 2016/681 são mencionados vários dados que devem ser transferidos que não se referem a passageiros, tal como definidos. Assim, as disposições da diretiva são neste aspeto contraditórias.
- 24 Assim, o n.º 9 do anexo I da Diretiva 2016/681, ao incluir, no âmbito do tratamento de dados de passageiros aéreos, a informação sobre agências de viagens e sobre os agentes de viagens, contradiz o artigo 3.º, n.º 4, da Diretiva 2016/681. Segundo o n.º 12 do anexo I, da diretiva, no campo do texto livre «informações gerais» são essencialmente informações sobre as pessoas que acompanham menores à partida e à chegada dos voos e também sobre os funcionários do aeroporto que os acompanham que devem ser indicadas.
- 25 Manifestamente, nenhum destes dados se enquadra na categoria «passageiros» definida no n.º 4 do artigo 3.º da Diretiva 2016/681. Mesmo assim devem ser comunicados pelas companhias aéreas à UIP dos Estados-Membros e ser por elas conservados. Assim, o órgão jurisdicional parte do princípio que esta regulamentação não se limita ao estritamente necessário, no sentido da jurisprudência do Tribunal de Justiça (v. parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 141). No caso de todos os terceiros afetados, coloca-se ainda a questão de saber como devem eles ser informados sobre o tratamento dos seus dados pessoais, nos termos do artigo 14.º do Regulamento 2016/679.
- 26 Nos termos do n.º 17 do anexo I da Diretiva 2016/681, os dados PNR das pessoas que viajam com o passageiro também devem ser comunicados e tratados. Relativamente às pessoas que viajam com os passageiros, isto conduz a um duplo registo, uma vez que estas pessoas já se encontravam abrangidas pelo tratamento de dados enquanto passageiros. Neste aspeto, é violado gravemente o princípio da limitação ao mínimo necessário (v. artigo 5.º, n.º 1, alínea c) do Regulamento 2016/679).

Quanto à questão 2 d): menores

- 27 Segundo a Diretiva 2016/681 as transportadoras aéreas são obrigadas a transferir todos os dados PNR de todos os passageiros, sem exceção, à UIP do Estado-Membro respetivo, pelo que são também abrangidos os passageiros menores de idade.
- 28 O tratamento de dados relativos a menores pode servir, por um lado, para prevenir e/ou reprimir os atos contra menores que (presumivelmente) estão envolvidos no terrorismo ou na criminalidade grave e, por outro, para a proteção dos menores, por exemplo para a descoberta ou perseguição de tráfico de menores. Estes dois objetivos distintos obrigam a dois regimes diferenciados. É o que o artigo 6.º da Diretiva 2016/680 esclarece, ao preceituar que se deve fazer, na medida do possível, uma distinção clara entre os dados pessoais de diferentes categorias de titulares de dados. Nestas diferentes categorias contam-se especialmente as pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal (artigo 6.º, alínea a), da Diretiva 2016/680), e as pessoas que foram vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal (artigo 6.º, alínea c), da Diretiva 2016/680).
- 29 Na parte em que os dados são recolhidos e tratados para efeitos de prevenção ou repressão de atos contra menores deve observar-se que a perseguição criminal com base em conhecimento obtido a partir do tratamento de dados de passageiros aéreos apenas pode ser considerada relativamente a jovens criminalmente responsáveis. Nesta base, a Diretiva 2016/681 vai para além do estritamente necessário, ao não prever uma limitação aos dados referentes a menores criminalmente responsáveis.
- 30 Relativamente à recolha e tratamento de dados PNR com o objetivo de proteção dos menores deve observar-se que as crianças e jovens já são objeto de um direito de proteção. É o que estabelece o artigo 24.º da Carta, que cria para sua especial proteção um direito fundamental ao nível do direito da União. Esta necessidade especial de proteção aplica-se igualmente ao tratamento dos seus dados pessoais. No que se refere à recolha e tratamento de dados PNR de passageiros menores com vista à prevenção e repressão da criminalidade contra crianças, as disposições da Diretiva 2016/681 não parecem ser adequadas para esse fim. O tratamento de dados PNR é dirigido para a descoberta e identificação de pessoas suspeitas. Para esse efeito, os dados PNR são comparados de forma automatizada com bases de dados e padrões, para descobrir pessoas suspeitas (v. artigo 6.º, n.º 2, da Diretiva 2016/681). Os dados referentes a menores no contexto da proteção de menores contra o tráfico de menores não são dados de suspeitos, mas, pelo contrário, de pessoas que carecem de proteção. Por isso têm também de ser tratados de forma diferente. A necessidade de proceder a comparação com padrões, neste caso, precisamente não existe. Assim a Diretiva 2016/681 carece manifestamente de regulamentações suficientemente diferenciadoras no que se refere ao tratamento de dados PNR dos passageiros menores.

Quanto à questão 2 e): dados API

- 31 O artigo 8.º, n.º 2, da Diretiva 2016/681 dispõe que os Estados-Membros tomam as medidas necessárias para garantir que também os dados alargados sobre passageiros aéreos no sentido do n.º 18 do anexo I desta Diretiva (dados API), incluindo tipo e número de documento, país de emissão e termo de validade dos documentos, nacionalidade, nome e apelido, 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, são transmitidos à UIP. Assim, verificam-se inúmeras redundâncias dos dados API com os dados PNR que têm também de ser transmitidos, como a data da viagem prevista (n.º 3 do anexo I da Diretiva 2016/681), o nome (n.º 4 do anexo I da Diretiva 2016/681) ou o itinerário completo (n.º 7 do anexo I da Diretiva 2016/681).
- 32 Este duplo tratamento de dados de passageiros está em contradição com o princípio consagrado, entre outras, na Diretiva 2016/680 de minimização da recolha de dados. Este princípio decorre, em primeiro lugar, do artigo 4.º, n.º 1, alínea c), da Diretiva 2016/680, que dispõe que os dados pessoais devem ser limitados ao mínimo necessário relativamente às finalidades para as quais são tratados. O artigo 20.º, n.º 1, da Diretiva 2016/680 concretiza este princípio partindo do pressuposto de que os Estados-Membros devem prever que quem for responsável pelo tratamento de dados deve prever as medidas para que os princípios de proteção dos dados, como a minimização dos dados, sejam corretamente aplicados. Além disso, o n.º 2 do artigo 20.º desta Diretiva dispõe que só devem ser tratados os dados pessoais que sejam necessários para cada finalidade específica.

Quanto à questão 2 f): Fundamento jurídico dos padrões

- 33 Nos termos do artigo 6.º, n.º 3, alínea b), da Diretiva 2016/681, os dados transferidos pelas transportadoras aéreas à UIP dos Estados-Membros podem ser comparados de acordo com critérios preestabelecidos (designados «padrões»). O artigo 6.º, n.º 4, segundo e quarto períodos, da Diretiva 2016/681 determina que os critérios preestabelecidos devem ser utilizados em função dos objetivos, e devem ser proporcionados e específicos, não podendo basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual. A fixação desses critérios, nos termos do artigo 6.º, n.º 4, terceiro período da Diretiva 2016/681, compete às UIPs dos Estados-Membros.
- 34 A fixação dos padrões de comparação é portanto integralmente deixada ao poder executivo dos Estados-Membros. Isto conduz a que os Estados-Membros da União Europeia apliquem padrões diferentes e que aos passageiros sejam sujeitos a diferentes padrões, dependendo do objetivo da viagem, que podem conduzir a resultados totalmente diferentes.

- 35 É duvidoso que isto seja compatível com os artigos 8.º, n.º 2, e 52.º da Carta e com o artigo 16.º, n.º 2, do TFUE. Segundo o artigo 8.º, n.º 2, da Carta, os dados pessoais 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. Nos termos do artigo 52.º, n.º 1, da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esse diploma deve estar prevista na lei. Nos termos do artigo 16.º, n.º 2, do TFUE, o Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União.
- 36 Para justificar as restrições aos direitos fundamentais da União Europeia não é necessária apenas a existência de uma qualquer norma, mas é ainda necessário que essa norma seja suficientemente precisa (v. Acórdão de 21 de dezembro de 2016, AGET Iraklis, C-201/15, EU:C:2016:972, n.º 99). Os destinatários da lei devem poder prever os efeitos da lei, devendo considerar-se que a norma é indeterminada se não for possível determinar um regime exato para a situação regulada (Acórdão de 20 de maio de 2003, Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.º 77).
- 37 O artigo 6.º, n.º 4, da Diretiva 2016/681 não preenche este critério. O artigo 6.º, n.º 4, segundo período, desta diretiva é um jogo de palavras imprecisas, que pretendem ser a concretização de critérios que, na realidade, não existem. O artigo 6.º, n.º 4, terceiro período, da diretiva deixa integralmente aos Estados-Membros a decisão essencial sobre quais os dados que podem ser utilizados na fixação de critérios ou padrões de comparação automatizada. Mas tal não é necessário em função do objeto normativo. O legislador europeu tinha a possibilidade de indicar dados e critérios determinados que podiam ou não ser utilizados na fixação dos critérios. Dessa forma não diferiria de Estado-Membro para Estado-Membro nem a qualificação da criminalidade, por exemplo o terrorismo, existente em cada Estado-Membro, nem os critérios segundo os quais os suspeitos podiam ser objeto de averiguação.
- 38 O único mecanismo de controlo da proporcionalidade dos padrões desenvolvidos pelos Estados-Membros é o previsto no artigo 6.º, n.º 7, em conjugação com o artigo 5.º, da Diretiva 2016/681, ao assegurar que o responsável pela proteção de dados tenha acesso a todos os dados tratados pela UIP. No entanto, o responsável pela proteção de dados, nos termos do artigo 5.º, n.º 1, da diretiva é nomeado pela própria UIP e é normalmente seu funcionário, pelo que a sua independência não fica à partida garantida (sobre a questão da independência das autoridades de controlo, v. Acórdãos de 9 de março de 2020, Comissão/Alemanha, C-518/07, EU:C:2010:125, e de 16 de outubro de 2012, Comissão/Áustria, C-614/10, EU:C:2012:631).

Quanto à questão 2 g): duração da conservação dos dados

- 39 Nos termos do n.º 1 do artigo 12.º da Diretiva 2016/681, os dados PNR são conservados pelo prazo de cinco anos. De acordo com a segunda frase do considerando 25 desta diretiva, a natureza dos dados PNR e os objetivos do seu tratamento implicam que os mesmos sejam conservados durante o tempo necessário. A razão por que seria necessário um prazo de conservação de cinco anos não é no entanto esclarecida.
- 40 Para o órgão jurisdicional de reenvio não é visível a razão por que é necessário um prazo tão longo de conservação. Após o passageiro, nos termos previstos no artigo 6.º, n.º 4, primeira frase, da Diretiva 2016/681, ter sido avaliado antes da sua chegada prevista ao Estado-Membro ou da sua partida prevista do Estado-Membro, sem se ter detetado qualquer anomalia, não existe nenhum indício objetivo de que ele pudesse estar relacionado mesmo indiretamente com atos terroristas ou com criminalidade grave. Falta por isso uma ligação suficiente entre a conservação dos dados e os objetivos prosseguidos pela Diretiva 2016/681. Só se houver indícios concretos de ameaça relativamente a determinados passageiros é que parece adequada a conservação prolongada dos dados (v. Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.ºs 204 e segs.). A mera possibilidade teórica de que os dados num qualquer momento possam tornar-se relevantes em termos de segurança não chega para justificar uma grave restrição a um direito fundamental que consiste na conservação de dados pessoais durante vários anos.
- 41 O Tribunal de Justiça já declarou, no contexto de outra forma de conservação massiva de dados pessoais sem motivos justificativos, que uma diretiva que prevê a conservação de dados por um prazo de 24 meses não limita a restrição ao estritamente necessário (Acórdão de 8 de abril de 2014, Digital Rights Ireland e o., C-293/12 e C-594/12, EU:2014:238, n.º 63). Se 24 meses são demasiado para a conservação de dados, então cinco anos, como no caso em apreço, também o são seguramente.

Quanto à questão 2 h): anonimização

- 42 A chamada anonimização deve garantir, segundo o considerando 25 da Diretiva 2016/681, um elevado nível de proteção dos dados pessoais. Mas isso é altamente duvidoso. A chamada «anonimização» dos dados, mencionada no artigo 12.º, n.º 2, desta diretiva, que deve ocorrer passados seis meses, nada altera à desproporcionalidade do prazo de conservação dos dados.
- 43 Em primeiro lugar deve constatar-se que a designação «anonimização» é alheia ao sistema e enganadora. Trata-se simplesmente de uma pseudonimização dos dados, no sentido do n.º 5 do artigo 3.º da Diretiva 2016/680. A pseudonimização distingue-se da anonimização pelo facto de, ao contrário desta, a atribuição dos dados a uma determinada pessoa não ser duradoura e definitivamente tornada impossível, mas subsistir a possibilidade de desanonimização (v. artigo 12.º, n.º 3,

da Diretiva 2016/681), ou seja a atribuição direta a uma pessoa pode ser restabelecida sem qualquer problema. Não é clara a razão por que não é utilizado o conceito de pseudonimização como na Diretiva 2016/680. A pseudonimização, devido ao seu caráter reversível, diminui a intensidade da restrição do direito fundamental substancialmente menos do que uma verdadeira anonimização.

- 44 Além disso, deve ser cumprido o artigo 4.º, n.º 1, alínea d), da Diretiva 2016/680. Nos termos desta disposição, os dados pessoais só podem ser conservados de forma a permitir a identificação dos titulares dos dados durante o período necessário para as finalidades para as quais são tratados. No caso da anonimização prevista no n.º 2 do artigo 12.º da Diretiva 2016/681, a identificação da pessoa continua a ser possível durante a totalidade do período de cinco anos de conservação dos dados, como demonstra o artigo 12.º, n.º 3, da Diretiva 2016/681, que regula a divulgação dos dados decorridos seis meses. Não se vê que isso seja estritamente necessário para a prossecução dos fins da Diretiva 2016/681, nem tal solução foi fundamentada pelo legislador da diretiva.

Quanto à questão 2 i): informação após a desanonimização

- 45 Não existe na Diretiva 2016/681 nenhuma norma que preveja a informação dos interessados quando os seus dados conservados pela UIP dos Estados-Membros são desanonimizados nos termos do artigo 12.º, n.º 3, desta diretiva. Apenas está previsto que a desanonimização seja autorizada por uma «autoridade judiciária» ou outra autoridade nacional (artigo 12.º, n.º 3, alínea b) da Diretiva 2016/681).
- 46 O Tribunal de Justiça já declarou no seu parecer sobre o Acordo UE-Canadá que, segundo esse projetado Tratado, os passageiros são informados através de um website sobre o tratamento genérico dos seus dados pessoais no contexto das medidas de segurança e do controlo das fronteiras, mas esta informação genérica não lhes dá a possibilidade de saber se os seus dados foram utilizados para além destes controlos pelas autoridades competentes (Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 223). Diz ainda o Parecer do Tribunal de Justiça, textualmente: «[Nos] casos [...] que contêm elementos objetivos que justificam essa utilização e que carecem de uma autorização prévia de uma autoridade judiciária ou de uma entidade administrativa independente, afigura-se necessária uma informação individual dos passageiros. O mesmo se diga dos casos em que os dados PNR dos passageiros aéreos são comunicados a outras autoridades públicas ou a particulares (Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 223).
- 47 O órgão jurisdicional de reenvio considera que esta avaliação do Tribunal de Justiça é aplicável à Diretiva 2016/681 e é por isso de opinião de que as pessoas afetadas devem ser individualmente informadas sobre a desanonimização dos seus dados. Se o Tribunal de Justiça entender que a informação imediata do interessado sobre a desanonimização pode gravemente impedir a prossecução dos fins prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, então, na opinião do órgão jurisdicional de reenvio, a

informação do interessado deveria ocorrer o mais tardar no momento em que o risco para a prossecução dos fins da desanonimização, por exemplo, com o encerramento da investigação, deixe de existir.

- 48 O interessado, nos termos do artigo 47.º da Carta, tem igualmente o direito a que a sua causa seja julgada de forma equitativa, publicamente e num prazo razoável, por um tribunal independente e imparcial, previamente estabelecido por lei, e não apenas por um uma «autoridade judiciária». Neste caso, este direito é excluído.

Quanto à questão 3: Transmissão de informações a Estados terceiros

- 49 Nos termos do artigo 11.º, n.º 1 da Diretiva 2016/681, os dados PNR e os resultados do seu tratamento podem ser transferidos, caso a caso, para um Estado terceiro se estiverem preenchidas as condições previstas no artigo 13.º da Decisão-Quadro 2008/977/JAI, se a transferência for necessária para os fins prosseguidos pela presente diretiva e o Estado terceiro declarar só aceitar transferir os dados para outro país terceiro caso tal seja estritamente necessário para os fins desta diretiva e unicamente mediante autorização expressa do Estado-Membro que os transfere e ainda se as condições previstas no artigo 9.º, n.º 2, da diretiva estiverem preenchidas.
- 50 O artigo 11.º, n.º 2, prevê uma exceção a esta condição, ao estabelecer que, sem prejuízo do artigo 13.º, n.º 2, da Decisão-Quadro 2008/977/JAI (atualmente artigo 38.º da Diretiva 2016/680) a transferência de dados PNR sem autorização prévia do Estado-Membro a partir do qual foram obtidos os dados é permitida em circunstâncias excecionais e apenas quando essa transferência for essencial para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com criminalidade grave num Estado-Membro ou num país terceiro e a autorização prévia não puder ser obtida em tempo útil.
- 51 Uma vez que através da transferência para Estados terceiros as respetivas autoridades passam a ter acesso aos dados PNR, todos os princípios aplicáveis à utilização dos dados – que visam garantir a proporcionalidade das inerentes restrições aos direitos fundamentais e um adequado nível de proteção dos dados pessoais – devem igualmente ser aplicáveis aos Estados terceiros. A este respeito, o Tribunal de Justiça esclareceu no seu Parecer sobre o Acordo UE-Canadá que a transferência de dados pessoais da União para um país terceiro só poder ocorrer se esse país assegurar um nível de proteção das liberdades e dos direitos fundamentais substancialmente equivalente ao garantido na União. Este requisito visa impedir que o nível de proteção previsto neste acordo possa ser contornado por transferências de dados pessoais para outros países terceiros e também garantir a continuidade do nível de proteção oferecido pelo direito da União (Parecer 1/15 de 26 de julho de 2017, EU:C:2017:592, n.º 214). Daí concluiu o Tribunal de Justiça que a transferência de dados pessoais para um País terceiro só é admissível se entre esse País terceiro e a União existir um acordo equivalente ao acordo UE-Canadá ou for tomada uma decisão da Comissão nos termos do artigo 25.º, n.º 6 da Diretiva 95/46 (atualmente artigo 45.º, n.º 3, do Regulamento

2016/679) que declare que o referido país terceiro assegura um nível de proteção adequado na aceção do direito da União e que abranja as autoridades para as quais se pretendem transferir os dados PNR (Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.º 214).

- 52 Estas condições são postas em causa no artigo 11.º, n.º 1, alínea a), da Diretiva 2016/681. O artigo 11.º, n.º 1, alínea a) desta diretiva remete para o artigo 13.º da Decisão-Quadro 2008/977/JI. Mas esta Decisão-Quadro foi revogada pela Diretiva 2016/680, pelo que as remissões para a Decisão-Quadro entendem-se agora feitas para a Diretiva 2016/680, mais concretamente para o artigo 59.º desta diretiva. Os artigos 35.º a 38.º da Diretiva 2016/680 correspondem essencialmente ao artigo 13.º da revogada Decisão-Quadro 2008/977/JAI.
- 53 Nos termos do artigo 35.º, n.º 1, alínea d) da Diretiva 2016/680, a transferência de dados pessoais para um Estado terceiro pressupõe que a Comissão tenha tomado uma decisão de adequação nos termos do artigo 36.º ou, na falta dessa decisão de adequação, tenham sido apresentadas ou existam garantias adequadas nos termos do artigo 37.º, ou, na falta de decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, se forem aplicáveis derrogações a situações específicas nos termos do artigo 38.º Assim, a remissão do artigo 11.º, n.º 1, alínea a) da Diretiva 2016/681 para o artigo 13.º da Decisão-Quadro 2008/977/JAI e, por essa via, para o artigo 35.º da Diretiva 2016/680 não garante uma adequado nível de proteção dos dados pessoais no Estado terceiro, uma vez que, através da remissão para o artigo 38.º da Diretiva 2016/680, permite que os dados PNR sejam transferidos para Estados terceiros mesmo sem uma decisão de adequação ou a apresentação de garantias adequadas. E isto porque as situações excecionais previstas no artigo 38.º da Diretiva 2016/680 estão formuladas em termos muito amplos. Esta norma permite, nomeadamente, transferir para Estados terceiros dados PNR sem um adequado nível de proteção de dados pessoais, se tal for necessário no caso concreto para a consecução dos fins do artigo 1.º, n.º 1, da Diretiva 2016/680 (prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública), ou se, em ligação com estes objetivos, tal for necessário para declarar, exercer ou defender um direito num processo judicial (artigo 38.º, n.º 1, alíneas d) e e) da Diretiva 2016/680).

Quanto à questão 4: preferências alimentares no texto livre

- 54 Nos termos do artigo 6.º, n.º 4, quarta frase, da Diretiva 2016/681, os critérios que podem ser utilizados pelas UIP dos Estados-Membros para realizar a comparação automatizada dos dados PNR não podem em caso algum basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual.
- 55 No entanto, esta norma mais não é do que uma declaração de intenções, logo contrariada pelo n.º 12 do anexo I da Diretiva 2016/681. Pois no campo do «texto livre» «informações gerais», que tem obrigatoriamente de ser transmitido sem

exceções, em cada caso concreto à UIP, um número considerável de informações podem ser transmitidas à UIP e serem por ela utilizados, especialmente dados sensíveis. Por exemplo, através deste campo de «texto livre» pode ser transmitida a informação de que um passageiro pediu comida Kosher ou Halal. A partir desta informação pode ser tirada uma conclusão sobre as convicções religiosas da pessoa em causa, de forma que se trata de um dado sensível no sentido anteriormente mencionado.

Quanto à questão 5: informações obtidas a partir das transportadoras aéreas.

- 56 Segundo o artigo 13.º, n.º 3, da Diretiva 2016/681, esta diretiva não prejudica a aplicabilidade da Diretiva 95/46 ao tratamento dos dados pessoais pelas transportadoras aéreas, em especial as suas obrigações de tomarem as medidas técnicas e organizativas adequadas para proteger a segurança e confidencialidade dos dados pessoais. Também o artigo 21.º, n.º 2, da Diretiva 2016/681 deixa claro que esta diretiva não prejudica a aplicabilidade da Diretiva 95/46/CE ao tratamento de dados pessoais pelas transportadoras aéreas.
- 57 A Diretiva 95/46 foi substituída pelo Regulamento 2016/679 (v. artigo 94.º, n.º 2, do Regulamento 2016/679, segundo o qual as remissões para a Diretiva 95/46 devem entender-se como remissões para o Regulamento 2016/679).
- 58 Segundo o artigo 13.º do Regulamento 2016/679, quando são recolhidos dados pessoais, o responsável pelo tratamento deve facultar ao titular dos dados as informações aí indicadas. O conceito de «dados pessoais» é definido no n.º 1 o artigo 4.º do Regulamento 2016/679. A recolha de dados PNR dos passageiros aéreos e de terceiros pela transportadora aérea constitui uma recolha de dados pessoais neste sentido, pelo que o artigo 13.º do Regulamento 2016/679 é presentemente aplicável às transportadoras aéreas.
- 59 Devido à já demonstrada gravidade da restrição dos direitos fundamentais resultante do tratamento dos dados PNR, na opinião do órgão jurisdicional de reenvio, devem ser aplicados critérios muito estritos ao dever de informação.
- 60 Na opinião do órgão jurisdicional de reenvio, é dever das transportadoras aéreas informar os interessados nos termos dos artigos 13.º e 14.º do Regulamento 2016/679, pois, de contrário, existiria uma lacuna incompatível com os artigos 7.º e 8.º da Carta. Assim, pode ser necessário que as companhias aéreas informem expressamente os passageiros sobre a totalidade dos dados PNR que recolheram, sobre a intenção de os transmitirem à UIP dos Estados-Membros e sobre o tratamento dos dados que por aquelas será feito, inclusive sobre o prazo de conservação de cimo anos, e que informem os passageiros sobre os seus direitos concretos enquanto titulares. Porquanto, sem estas informações, os passageiros em causa dificilmente poderão exercer os seus direitos de titulares da informação. A Diretiva 2016/681 nada prevê sobre isto.

- 61 O Tribunal de Justiça já declarou no seu Parecer sobre o Acordo UE-Canadá que para garantir esses direitos é necessário que os passageiros aéreos sejam informados da transferência dos seus dados PNR para o Canadá e sobre a utilização desses dados, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo pelas autoridades públicas previstas no acordo projetado. Com efeito, essa informação é, de facto, necessária para permitir aos passageiros aéreos exercer os seus direitos de pedir o acesso aos dados PNR que lhes dizem respeito e, sendo caso disso, a retificação dos mesmos e de intentar, nos termos do artigo 47.º, primeiro parágrafo, da Carta, uma ação perante um tribunal (Parecer 1/15, de 26 de julho de 2017, EU:C:2017:592, n.º 220).
- 62 Como exemplo da insuficiente informação prestada pelas companhias aéreas aos passageiros, vejam-se as informações obtidas pela companhia aérea usada pelo autor. As informações prestadas pela Lufthansa AG na sua página Internet (<https://www.lufthansa.com/xx/de/informationen-zum-datenschutz>, alterada por último em 11 de maio de 2020) são as seguintes:

«Quem é o responsável?

A Deutsche Lufthansa [...] informa-o a seguir sobre o tratamento dos seus dados pessoais [...]

[...]

A quem me posso dirigir?

Se tiver... questões sobre a proteção de dados pessoais... contacte o nosso responsável pela proteção de dados:

[...]

Qual a base legal (...) do tratamento dos seus dados pessoais?

Tratamos os seus dados relativos ao voo com base na obrigação legal decorrente do artigo 6.º, n.º 1, primeiro período, alínea c) do Regulamento 2016/679:

Por estarmos legalmente obrigados, tratamos os seus dados pessoais para satisfazer exigências de segurança (...)

Informações prestadas a autoridades do país de chegada:

- Com base no Acordo sobre dados de passageiros aéreos celebrado entre a UE e os USA e o Canadá
- Com base na Lei Sobre Dados dos Passageiros Aéreos Alemã

- *API* (Advance Passenger Information) transmissão de dados por estarmos obrigados a colaborar nas atividades de controlo relativas ao tráfego internacional de viagens*

**Dados da zona de leitura automática do passaporte ou do documento de identificação*

Pode obter mais informações junto das autoridades competentes.

[...]

Quem recebe os seus dados?

[...] Os seus dados podem ser transmitidos às seguintes categorias de entidades recetoras:

Entidades e autoridades estatais, por exemplo, com base em disposições sobre entrada no território nacional, ou devido a atividades ou investigação policial.

Os seus dados podem ser transmitidos a Países terceiros ou a organizações internacionais. Para sua proteção e dos seus dados pessoais no caso dessa transmissão estão previstas garantias adequadas de acordo com os respetivos requisito legais.

Na parte em que esta transmissão não tenha um fundamento legal ou ocorram num País para o qual não exista uma decisão de adequação da Comissão Europeia, aplicam-se as cláusulas gerais da UE.

Quais são os seus direitos relativamente à proteção de dados?

Para a Lufthansa é muito importante realizar os nossos processos de tratamento de dados de forma justa e transparente. Por isso, é importante para nós que as pessoas afetadas, para além do direito de recurso, no caso de se verificarem as respetivos pressupostos legais, possam exercer os seguintes direitos:

Direito de acesso à informação, artigo 15.º do Regulamento 2016/679

Direito de retificação, artigo 16.º do Regulamento 2016/679

Direito de apagamento (“direito de ser esquecido”), artigo 17.º do Regulamento 2016/679

Direito à limitação do tratamento, artigo 18.º do Regulamento 2016/679

Direito de portabilidade dos dados, artigo 20.º do Regulamento 2016/679

Direito de oposição, artigo 21.º do Regulamento 2016/679

[...]»

- 63 Estas informações podem ser insuficientes e enganadoras. Assim, a indicação de que, no caso dos dados API, só a parte automaticamente legível do passaporte ou do documento de identificação é afetada, é manifestamente insuficiente. Porquanto, segundo o n.º 18 do anexo I da Diretiva 2016/681, os dados API que tenham sido recolhidos, entre outros, sobre a companhia aérea, número de voo, data de partida, data de chegada, aeroporto de partida, aeroporto de chegada, hora de partida e hora de chegada, devem ser transmitidos, e portanto não apenas os que constam da parte automaticamente legível dos documentos de identificação. Além disso, não é nunca referida a Diretiva 2016/681, mas apenas a FlugDaG. Acresce que falta também qualquer indicação sobre o conteúdo da Diretiva 2016/681 ou da FlugDaG. Para um passageiro não é portanto transparente, antes de efetuar uma reserva, qual a entidade que é a UIP do Estado-Membro em causa e como a ele se pode dirigir, como são tratados os dados PNR pela UIP ou durante quanto tempo podem os seus dados ser conservados por ela. Assim, não parece que a informação prestada pela Lufthansa AG aos passageiros cumpra os requisitos previstos no artigo 13.º do Regulamento 2016/679, isto para já não falar das outras pessoas que igualmente vão ser objeto da informação.

DOCUMENTO DE TRABALHO