CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2022/114

I.Introdução

1. O Tribunal de Justiça da União Europeia (doravante, TJUE), no acórdão do de 21 de junho de 2022, proferido no processo C-817/19 (*Ligue des droits humains* c. *Conseil des ministres*), pronunciou-se no sentido de que 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 passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (doravante, Diretiva PNR), desde que interpretada à luz dos artigos 7.º, 8.º, 21.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (doravante, Carta), é conforme com estes artigos. Mas, entendeu que a conformidade da Diretiva com aqueles artigos da Carta depende da interpretação de alguns dos seus preceitos nos termos que em seguida se transcrevem:

> «[...] 3) O artigo 6.º da Diretiva 2016/681, lido à luz dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma legislação nacional que autoriza o tratamento dos dados dos registos de identificação dos passageiros (dados PNR) recolhidos em conformidade com esta diretiva para fins diferentes dos expressamente indicados no artigo 1.º, n.º 2, da mencionada diretiva.
>
> 4) O artigo 12.º, n.º 3, alínea b), da Diretiva 2016/681 deve ser interpretado no sentido de que se opõe a uma legislação nacional, segundo a qual a autoridade instituída como Unidade de Informação de Passageiros (UIP) tem igualmente a qualidade de autoridade nacional competente habilitada a aprovar a comunicação dos dados PNR, decorrido o prazo de seis meses subsequente à transferência desses dados para a UIP.
>
> 5) O artigo 12.º, n.º 1, da Diretiva 2016/681, lido em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe a uma legislação nacional que prevê um prazo geral de conservação dos dados PNR de cinco anos, aplicável indiferentemente a todos os passageiros aéreos, incluindo àqueles relativamente aos quais nem a avaliação prévia prevista no artigo 6.º, n.º 2, alínea a), desta diretiva, nem as eventuais verificações efetuadas durante o prazo de 6 meses previstos no artigo 12.º, n.º 2, da referida diretiva, nem qualquer outra circunstância, revelaram a existência de elementos objetivos suscetíveis de estabelecer um risco em matéria de infrações terroristas ou de criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros.

6) A Diretiva 2004/82 deve ser interpretada no sentido de que não é aplicável aos voos, regulares ou não, efetuados por uma transportadora aérea, com proveniência do território de um Estado-Membro e que devam aterrar no território de um ou de vários Estados-Membros, sem fazer escala no território de um país terceiro (voos intra-UE).

7) O direito da União, em especial o artigo 2.º da Diretiva 2016/681, lido à luz do artigo 3.º, n.º 2, TUE, do artigo 67.º, n.º 2, TFUE e do artigo 45.º da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de que se opõe:

— a uma legislação nacional que prevê, não havendo uma ameaça terrorista real e atual ou previsível a que o Estado-Membro em causa deva fazer face, um sistema de transferência, pelas transportadoras aéreas e pelo operadores de viagens, e de tratamento, pelas autoridades competentes, dos dados PNR de todos os voos intra-UE e dos transportes efetuados por outros meios dentro da União, com proveniência de ou com destino a esse Estado-Membro ou ainda transitando através dele, a fim de lutar contra as infrações terroristas e a criminalidade organizada. Numa situação dessas, a aplicação do sistema estabelecido pela Diretiva 2016/681 deve limitar-se à transferência e ao tratamento dos dados PNR dos voos e/ou dos transportes relativos, nomeadamente, a certas ligações ou plano de viagem ou ainda a certos aeroportos, estações de caminho-de-ferro ou portos marítimos para os quais existam indicações suscetíveis de justificar essa aplicação. Incumbe ao Estado-Membro em causa selecionar os voos intra-UE e/ou os transportes efetuados por outros meios dentro da União, para os quais existem essas indicações, e reexaminar regularmente a referida aplicação em função da evolução das condições que justificaram a sua seleção, para efeitos de garantir que a aplicação desse sistema a esses voos e/ou a esses transportes continua limitada ao estritamente necessário, e

— a uma legislação nacional que prevê esse sistema de transferência e de tratamento dos referidos dados para efeitos da melhoria dos controlos nas fronteiras e da luta contra a imigração clandestina. [...]»

2. A Diretiva PNR foi transposta para o ordenamento jurídico português através da Lei n.º 21/2019, de 25 de fevereiro, que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados.

3. Os dados pessoais tratados são, nos termos do artigo 4.º da Lei n.º 21/2019, os elencados no Anexo I da mesma lei, que correspondem aos dados do anexo I da Diretiva, destacando-se, «[...] além do nome do ou dos passageiros aéreos, informações necessárias para a reserva, tais como as datas previstas da viagem e o

itinerário de viagem, informações relativas aos bilhetes, os grupos de pessoas registadas sob o mesmo número de reserva, as informações de contacto do ou dos passageiros, informações relativas às modalidades de pagamento ou à faturação, informações relativas às bagagens e observações gerais sobre os passageiros.» (cf. ponto 93 do citado acórdão, de ora em diante referido como acórdão "Diretiva PNR").

4. Do tratamento destes dados decorre um impacto significativo nos direitos, liberdades e garantias dos cidadãos, desde logo, no direito à autodeterminação informativa (também denominado direito à proteção dos dados pessoais), consagrado no artigo 35.º da Constituição da República Portuguesa (CRP) e no artigo 8.º da Carta, por corresponder a um tratamento realizado independentemente da vontade dos titulares dos dados, mas especialmente no direito à reserva da vida privada e familiar, consagrado no artigo 26.º da CRP e no artigo 7.º da Carta, além do artigo 8.º da Convenção Europeia dos Direitos Humanos (cf. pontos 94 a 96 do acórdão "Diretiva PNR").

5. Como se refere no citado acórdão (cf. ponto 100), «[...] ainda que certos dados PNR enumerados no anexo I da Diretiva PNR [...], considerados isoladamente, não pareçam suscetíveis de revelar informações precisas 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 revelar informações sensíveis sobre esses passageiros*» (itálico nosso).

6. Sendo, consabidamente, «[...] jurisprudência constante que a comunicação de dados pessoais a um terceiro, como uma autoridade pública, constitui uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.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 (Acordo PNR UE-Canadá), de 26 de julho de 2017, EU:C:2017:592, n.ºs 124 e 126 e jurisprudência referida]» (cf. ponto 96 do acórdão "Diretiva PNR")».

7. Assim, conclui o TJUE que a Diretiva PNR comporta ingerências de efetiva gravidade nos direitos fundamentais à proteção dos dados pessoais e ao respeito pela vida privada e familiar, na medida em que *visa instaurar um regime de vigilância contínuo, não direcionado e sistemático, que inclui a avaliação automatizada de dados pessoais de todas as pessoas que utilizam serviços de transporte aéreo* (cf. ponto 111 do acórdão "Diretiva PNR").

8. Nessa medida, porque o tratamento de dados pessoais PNR representa uma ingerência grave naqueles direitos fundamentais, é essencial que essa ingerência seja proporcional, reduzida ao mínimo estritamente necessário para a finalidade de segurança visada, razão por que a respetiva regulação legal tem de ser clara e precisa na determinação do alcance e aplicação das medidas por ela previstas, devendo, «[...] em especial, 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» (cf. ponto 117 do acórdão "Diretiva PNR"). Tanto mais quando, como sublinha o TJUE, os dados pessoais são sujeitos a tratamento automatizado e são suscetíveis de revelar informações sensíveis sobre os passageiros.

9. Deste modo, na linha da recomendação aprovada pelo Comité Europeu para a Proteção de Dados, no dia 13 de dezembro de 2022[1], e ao abrigo dos poderes previstos na alínea *c)* do n.º 1 do artigo 57.º e na alínea *b)* do n.º 3 do artigo 58.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e na alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, bem como na alínea *c)* do n.º 1 do artigo 44.º da Lei n.º 59/2019, de 8 de agosto, vem a Comissão Nacional de Proteção de Dados (CNPD) recomendar a revisão da Lei n.º 21/2019, de 25 de fevereiro, que transpõe aquela Diretiva, com os fundamentos e nos termos que a seguir se expõem.

II. Análise da Lei n.º 21/2019

i. A revisão do n.º 1 do artigo 1.º quanto aos voos intra-UE

10. De acordo com a citada jurisprudência, desde logo o n.º 1 do artigo 1.º da Lei n.º 21/2019 tem de ser revisto de modo a garantir a conformidade com a Carta e com a CRP, pois, ao abranger de forma genérica, permanente e sistemática tanto os voos extra-União Europeia (UE) como os voos intra-UE, está a restringir de modo desnecessário e excessivo os direitos fundamentais à proteção dos dados pessoais e à reserva da vida privada e familiar, bem como o direito fundamental à livre circulação e permanência no território dos Estados-Membros (artigos 7.º, 8.º e 45.º da Carta) – cf. ponto 173 do acórdão "Diretiva PNR".

11. Na verdade, embora a Diretiva PNR admita que o regime nela previsto se estenda, se o Estado-Membro assim o entender, aos voos dentro da UE, a verdade é que a conservação, comunicação e análise dos dados PNR de todos os voos intra-UE deve pautar-se pela sua adequação e necessidade face à finalidade deste

[1] *Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States*, acessível em https://edpb.europa.eu/system/files/2022-12/edpb_statement_20221213_on_the_pnr_judgement_en.pdf

regime, ou seja, à finalidade de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave (cf. n.º 2 do artigo 1.º da Lei n.º 21/2019).

12. Ora, de acordo com o entendimento vertido no acórdão do TJUE, o tratamento de dados pessoais relativos aos passageiros dos voos intra-UE só é necessário e não excessivo se estiver justificado por concretas circunstâncias que revelem ou indiciem, fundamentadamente, a existência de reais ou previsíveis ameaças terroristas, por um período de tempo devidamente limitado, e a respetiva decisão deve ser verificada por órgão jurisdicional ou por entidade administrativa independente através de decisão vinculativa (cf. pontos 171 e 172 do acórdão "Diretiva PNR").

13. Assim, e tal como a CNPD já havia assinalado, nos seus Pareceres n.º 61/2017, de 21 de novembro, e n.º 31/2018, de 6 de julho[2], que neste ponto foram incompreensivelmente ignorados, é evidente a desnecessidade e desproporção da permanente e sistemática recolha, comunicação e conservação de dados pessoais com a natureza e extensão dos dados PNR em todos os voos de ou para um Estado-Membro da União.

14. A CNPD recomenda, por isso, que o n.º 1 do artigo 1.º seja revisto, passando a prever-se, aí ou em outra disposição, a aplicação deste regime legal aos voos de e para um Estado-Membro da União apenas quando se verifiquem «[...] circunstâncias suficientemente concretas que permitam considerar estar-se perante uma ameaça terrorista que se afigure real e atual ou previsível» (cf. ponto 171 do acórdão "Diretiva PNR") e que tais circunstâncias estejam densificadas na lei, especificando-se que estejam delimitadas em função da sua conexão a «certas ligações aéreas ou esquemas de viagem, ou a certos aeroportos relativamente aos quais existam indicações suscetíveis de justificar essa aplicação» (cf. ponto 174 do mesmo acórdão).

15. Recorda-se que apenas as atividades que são suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal podem, de acordo com a jurisprudência do TJUE, ser qualificadas como ameaças terroristas, distinguindo-se, pela sua natureza, pela sua particular gravidade e pelo caráter específico das circunstâncias que as constituem, do risco geral e permanente que é o das infrações penais graves (cf. ponto 170 do citado acórdão).

16. Por outras palavras, é entendimento do TJUE que o tratamento de dados pessoais PNR em voos intra-UE apenas é necessário e proporcional se visar, demonstradamente, a prevenção e repressão de *ameaças terroristas*, já não se visar a prevenção e combate à criminalidade grave.

---

[2] Acessíveis, respetivamente, em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/113000 e https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121616.

17. Para assegurar a conformidade da aplicação deste regime aos dados relativos a voos intra-UE importa ainda que a Lei n.º 21/2019 *delimite temporalmente essa aplicação*, sem prejuízo de eventual renovação caso se mantenham as circunstâncias justificadoras da extensão do regime, e exija que a concreta avaliação de que tais circunstâncias se verificam em concreto e justificam o tratamento dos dados PNR seja ainda sujeita a *decisão concreta e vinculativa por órgão judicial* (e não judiciário) ou por entidade administrativa independente (cf. ponto 172 do acórdão "Diretiva PNR"). Deve ainda a Lei prever a reavaliação periódica, dentro de um prazo razoável (eventualmente, três meses), da manutenção dessas circunstâncias, de modo a renovar o interesse com base na necessidade, a deixar de tratar os dados de certos voos intra-UE ou a alterar a recolha para outros voos.

18. Recorda-se a este propósito que, como refere o mesmo Tribunal, no ponto 245 do acórdão "Diretiva PNR", «[a] exigência de independência que deve satisfazer a entidade encarregada de exercer a fiscalização prévia impõe igualmente que esta tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo que a referida entidade possa exercer essa fiscalização de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, *a exigência de independência implica que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja implicada na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal.*» (sublinhado nosso).

ii. A especificação (taxativa) das bases de dados objeto de comparação

19. Da Diretiva PNR resulta que os dados pessoais PNR relativos aos voos extra-UE podem ser tratados para finalidades de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, envolvendo diferentes tipos de operações.

20. Recorda-se que nos termos da alínea *a)* do n.º 2 artigo 5.º da Lei n.º 21/2019, se prevê, num primeiro momento, que os dados PNR recolhidos pelas transportadoras são sistematicamente transferidos para o Gabinete de Informações de Passageiros (GIP), onde são sujeitos a uma avaliação automatizada de acordo com critérios pré-definidos, decorrente da comparação com outros dados pessoais constantes de bases de dados das forças de segurança, o que se processa nos termos descritos nos n.ºs 1 a 3 do artigo 6.º. Os resultados positivos *(hits)* devem, em seguida, ser objeto de uma segunda avaliação, já com intervenção humana (não automatizada), antes da sua comunicação às autoridades competentes previstas no artigo 7.º, nos termos dos n.ºs 4 a 6 do artigo 6.º.

21. Ademais, nos termos da alínea *b)* do n.º 2 artigo 5.º da Lei n.º 21/2019, o GIP está obrigado a comunicar dados pessoais PNR às autoridades competentes a pedido destas. Tal sucede durante o prazo de seis meses,

mas também depois de esgotado esse prazo – período em que os dados conservados estão mascarados, não permitindo a identificação direta dos seus titulares, especificando-se que, nesta última hipótese, os dados comunicados são dados pessoais PNR integrais (*i.e.*, sem mascaramento), embora apenas se cumpridos os pressupostos previstos n.º 3 do artigo 11.º da Lei.

22. Como se referiu, o princípio da proporcionalidade obriga a que a ingerência ou restrição aos dados fundamentais aqui em crise, decorrente do tratamento de dados pessoais PNR, deve cingir-se ao estritamente necessário à prossecução das finalidades de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Assim, a comparação dos dados PNR com outros dados pessoais, realizada de forma automatizada, deve cingir-se às bases de dados da responsabilidade das forças de segurança que foram criadas com a finalidades de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, devendo estar especificadas na lei, como a CNPD recomendou no seu Parecer n.º 61/2017 e reiterou no Parecer n.º 31/2018.

23. Com efeito, as exigências constitucionais de precisão e clareza na delimitação da ingerência ou restrição aos dados fundamentais aqui em crise implicam que aquela norma delimite as bases de dados objeto de comparação com os dados PNR, devendo ser enunciadas, de modo taxativo, as bases de dados pertinentes para este efeito.

24. Assim, a alínea *a)* do n.º 1 do artigo 6.º da Lei n.º 21/2019 deve ser alterada de modo a garantir a proporcionalidade da ingerência nos direitos fundamentais à proteção dos dados pessoais e ao respeito pela vida privada e familiar prevista no artigo 6.º, n.º 3, alínea *a)*, da Diretiva PNR, tal como interpretado pelo TJUE, ou seja circunscrevendo as bases de dados suscetíveis de comparação às indicadas na parte final daquela disposição (cf. ponto 188 do acórdão "Diretiva PNR", onde se pode ler que aquele preceito «[...] *deve, à luz destes direitos fundamentais, ser interpretado no sentido de que estas últimas bases de dados são as únicas bases de dados com as quais a UIP pode comparar os dados PNR*»).

25. Em suma, a CNPD recomenda a alteração da alínea *a)* do n.º 1 do artigo 6.º da Lei n.º 21/2019, de modo a especificar que as bases de dados objeto de comparação são apenas as referidas na sua parte final, a saber: *bases de dados sobre pessoas ou objetos procurados ou alvo de um alerta, de acordo com as regras aplicáveis a essas bases de dados.*

iii. Delimitação dos crimes graves que justificam a análise dos dados PNR

26. Acresce que tem de se assegurar que a análise dos dados PNR depende de uma conexão objetiva, direta ou indireta, entre o transporte aéreo de passageiros e algum ou alguns dos crimes previstos no Anexo II da Lei n.º 21/2019.

27. Com efeito, conclui o TJUE que «[...] o artigo 3.º, pontos 8 e 9, desta diretiva, em conjugação com o anexo II da mesma e à luz dos requisitos resultantes dos artigos os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, exige que os Estados-Membros assegurem, nomeadamente na verificação individual por meios não automatizados prevista no artigo 6.º, n.º 5, da referida diretiva, que a aplicação do sistema estabelecido pela mesma seja limitada às infrações terroristas e apenas à criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros» (cf. ponto 157 do acórdão "Diretiva PNR").

28. Nestes termos, a CNPD recomenda a especificação, eventualmente no n.º 1 do artigo 6.º e no artigo 7.º da Lei n.º 21/2019, de que o tratamento de dados pelas autoridades competentes depende de existir uma *conexão objetiva, direta ou indireta, entre o transporte aéreo de passageiros e um dos crimes graves constantes do Anexo II*.

iv. A limitação de reutilização dos dados pessoais PNR para outras finalidades

29. O n.º 2 do artigo 7.º da Lei n.º 21/2019 limita o tratamento de dados pessoais PNR às finalidades de prevenção, deteção, investigação e repressão das infrações terroristas ou da criminalidade grave, em conformidade com o princípio da limitação de finalidades. Todavia, logo no número seguinte, admite que essa limitação das finalidades não prejudica que, *quando forem detetadas outras infrações ou indícios de outras infrações no decurso de ações desencadeadas na sequência do referido tratamento*, tais dados sejam tratados *pelas autoridades policiais, aduaneiras ou judiciais*.

30. Assim redigida, esta disposição permite que dados PNR sejam utilizados para outras finalidades.

31. Ora, de acordo com a interpretação do TJUE, «[...] a enumeração dos objetivos prosseguidos pelo tratamento dos dados PNR ao abrigo da Diretiva PNR reveste caráter exaustivo, pelo que uma legislação nacional que autoriza o tratamento de dados PNR recolhidos em conformidade com esta diretiva para fins diferentes dos nela previstos, a saber, nomeadamente, para melhorar os controlos nas fronteiras e combater a imigração ilegal, é contrária ao artigo 6.º da referida diretiva, lido à luz da Carta» (cf. ponto 289 do acórdão "Diretiva PNR").

32. E especifica o mesmo Tribunal, no ponto 290, que «[...] os Estados-Membros não podem criar uma base de dados única que contenha tanto os dados PNR recolhidos ao abrigo da Diretiva PNR e relativos aos voos extra-

UE e intra-UE como os dados dos passageiros de outros meios de transporte, bem como os dados referidos no artigo 3.º, n.º 2, da Diretiva API [...]». Precisamente, a Diretiva API (Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras) tem por objeto melhorar os controlos nas fronteiras e combater a imigração ilegal, como resulta dos seus considerandos 1, 7 e 9, bem como do seu artigo 1.º, através da transmissão antecipada, pelas transportadoras, dos dados dos passageiros às autoridades nacionais competentes.

33. É, assim, evidente que as outras finalidades suscetíveis de justificar a reutilização dos dados PNR não podem corresponder aos objetivos de melhorar o controlo de fronteiras e combater a imigração ilegal, sob pena de se contrariar o n.º 2 do artigo 1.º e do artigo 6.º da Diretiva PNR, lidos à luz dos artigos 7.º e 8.º da Carta, tendo de integrar o domínio especificamente delimitado no n.º 2 do artigo 1.º da Diretiva PNR.

34. A este propósito, afigura-se útil recordar a recente jurisprudência do TJUE quanto ao princípio da limitação das finalidades dos tratamentos de dados pessoais, onde este Tribunal explica, embora a propósito da Diretiva 2016/690, que *«prevenção», «deteção», «investigação», «repressão», «execução de sanções penais», «salvaguarda contra as ameaças à segurança pública» e «prevenção de ameaças» visam uma pluralidade de finalidades distintas do tratamento de dados pessoais abrangidos pelo âmbito de aplicação da mesma diretiva* – cf. acórdão de 8 de dezembro de 2022, *VS c. Inspetktor v Inspektorata kam Visshia sadeben savet* (Processo C-180/21), ponto 43.

35. Nessa medida, quando, no âmbito de aplicação de uma Diretiva, se permite o tratamento ulterior de dados para uma finalidade diferente daquela para a qual esses dados foram recolhidos, essa permissão supõe que esta finalidade figura entre as enunciadas para delimitar o domínio ou âmbito de aplicação da mesma diretiva (cf., com as devidas adaptações, o ponto 51 do acórdão de 8 de dezembro de 2022, *VS c. Inspetktor v Inspektorata kam Visshia sadeben savet*).

36. Como explicita ainda o TJUE, no ponto 52 deste último acórdão, «[e]m especial, os dados pessoais recolhidos para efeitos de «prevenção» e de «deteção» das infrações penais ou de «investigação» relativos a tais infrações podem ser ulteriormente tratados, se for caso disso, por autoridades competentes diferentes, com vista à «repressão» ou à «execução de sanções penais», quando uma infração penal tenha sido identificada e exija, por conseguinte, uma ação repressiva».

37. Tendo presente esta jurisprudência, parece-nos dever concluir que também o n.º 5 do artigo 7.º da Diretiva PNR deve ser lido de acordo com o princípio da limitação das finalidades, *i.e.*, interpretado no sentido de que, no âmbito das finalidades da Diretiva PNR (*prevenção, deteção, investigação e repressão das infrações terroristas ou da criminalidade grave*), as autoridades podem reutilizar os dados pessoais PNR para uma dessas finalidades no contexto de uma ação ou processo distinto daquele que originou a primeira utilização dos dados pessoais PNR.

38. Nessa medida, a CNPD recomenda a revisão do n.º 3 do artigo 7.º da Lei n.º 21/2019, para se especificar que a reutilização dos dados aí salvaguardada supõe que a competência a exercer tem diretamente em vista uma finalidade específica de entre as previstas no n.º 2 do artigo 1.º e densificadas pelo catálogo constante do Anexo II da Lei.

v. Prazos de conservação dos dados PNR

39. Também o artigo 11.º da Lei n.º 21/2019 carece de revisão, para assegurar a sua conformidade com o direito da União, em coerência com a interpretação do TJUE da Diretiva PNR. Na verdade, este artigo reproduz, no essencial, o artigo 12.º da Diretiva PNR, fixando, no seu n.º 1, um prazo de cinco anos para a conservação de todos os dados PNR, contado da data da respetiva transferência para o GIP.

40. Demais, o n.º 2 do artigo 11.º da Lei prevê a "anonimização" de todos os dados PNR no prazo de seis meses, contado da data da transferência, mediante o mascaramento de algumas categorias de dados (elencadas nesse preceito), sem prejuízo da possibilidade da reversão desse processo de anonimização, sempre que considerada necessária, *com base em motivos razoáveis, para os fins referidos na alínea b) do n.º 2 do artigo 5.º* da Lei, e mediante *autorização da autoridade judiciária competente*, prevista no n.º 3 do mesmo artigo.

41. Ora, o TJUE entende que «[...] o artigo 12.º , n.º 1, da Diretiva PNR, lido em conjugação com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, deve ser interpretado no sentido de que se opõe a uma legislação nacional que prevê um prazo geral de conservação dos dados PNR de cinco anos, aplicável indiferentemente a todos os passageiros aéreos, incluindo àqueles relativamente aos quais nem a avaliação prévia prevista no artigo 6.º , n.º 2, alínea a), desta diretiva, nem as eventuais verificações efetuadas durante o prazo de seis meses previsto no artigo 12.º, n.º 2, da referida diretiva, nem qualquer outra circunstância, revelaram a existência de elementos objetivos suscetíveis de estabelecer um risco em matéria de infrações terroristas ou de criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com o transporte aéreo de passageiros» (cf. ponto 263 do acórdão "Diretiva PNR").

42. Assim, à luz do princípio da limitação da conservação, a conservação dos dados pessoais PNR de todos os passageiros pelo período de seis meses não merece reservas, assim como não suscita reservas a conservação por período superior de tais dados em relação a passageiros que deram origem a um resultado automático positivo verificado e confirmado como indiciando um risco em termos de infrações terroristas ou de criminalidade grave.

43. Mas quanto aos demais passageiros, em relação aos quais a avaliação automatizada não deu um resultado positivo ou, tendo dado, tal resultado foi infirmado por via de verificação individual não automatizada, a conservação generalizada dos dados pelo período de cinco anos (ainda que com medidas de mitigação dos riscos, *i.e.*, o mascaramento de certos dados) não se revela necessária à prossecução das finalidades do regime PNR, por não existirem elementos objetivos suscetíveis de estabelecer um risco em matéria de infrações terroristas ou de criminalidade grave que apresentem um nexo objetivo, pelo menos indireto, com a viagem aérea efetuada por esses passageiros.

44. Nestes termos, a CNPD recomenda a revisão do artigo 11.º, em especial dos n.ºs 1 e 2, para diferenciar o universo de passageiros cujos dados podem ser conservados por período superior a seis meses. Mais se recomenda que se elimine a referência à anonimização, uma vez que essa expressão deve ficar reservada a situações de irreversibilidade desse processo e o que se regula no n.º 2 desse artigo é um mero mascaramento ou pseudonimização da informação pessoal (cf. artigo 4.º, alínea 5), do RGPD).

45. Ainda quanto ao artigo 11.º da Lei, a CNPD reitera as reservas que assinalou no Parecer n.º 31/2018 a propósito do disposto no n.º 6.

46. Com efeito, a hipótese aí prevista de, nos casos de resultado positivo da avaliação automatizada serem infirmados na sequência de uma verificação individual por meios não automatizados (falso *hit*), poder conservar-se os dados conservados a fim de evitar falsos resultados positivos no futuro, desde que os dados que lhe serviram de base não sejam apagados nos termos do n.º 4 do mesmo artigo, é, se não desnecessária, pelo menos excessiva pelos riscos que implica a sua conservação numa base de dados paralela, que pode, com o decurso do tempo, assumir proporções consideráveis. Sendo que, por esta via, se poderia pretender contornar o princípio da limitação da conservação de dados pessoais.

47. Tal conclusão vem agora reforçada, por força da delimitação do prazo de conservação por seis meses para todos os dados PNR e da permissão de conservação por período superior apenas dos dados relativos a passageiros que deram origem a um resultado automático positivo verificado e confirmado como indiciando um risco em termos de infrações terroristas ou de criminalidade grave. Com efeito, esta delimitação do período de conservação dos dados PNR torna impossível a sua conservação por mais de seis meses no caso de a avaliação humana confirmar que o resultado da avaliação automatizada corresponde a um falso positivo, com o que o disposto n.º 6 do artigo 11.º se torna juridicamente impossível ou inútil, devendo, por isso, ser eliminado.

48. Nestes termos, a CNPD recomenda a revisão do artigo 11.º, em especial dos n.ºs 1 e 2, para diferenciar o universo de passageiros cujos dados podem ser conservados por período superior a seis meses, e a revogação

do n.º 6, em face da impossibilidade jurídica ou inutilidade do nele disposto. Mais se recomenda que se elimine a referência à anonimização.

vi. **A autorização prévia para divulgação de dados PNR integrais**

49. Ainda no contexto do artigo 11.º da Lei n.º 21/2019, cabe destacar o disposto no n.º 3. Aí se prevê, como se referiu já, que durante o período em que os dados pessoais PNR conservados estão mascarados, não permitindo a identificação direta dos seus titulares, os dados possam ser divulgados de forma integral, «[...] caso essa divulgação seja: *a)* Considerada necessária, com base em motivos razoáveis, para os fins referidos na alínea b) do n.º 2 do artigo 5.º; e *b)* Se for caso de isso, autorizada pela autoridade judiciária competente.»

50. Começa-se por assinalar não se perceber o real alcance da formulação condicional do segundo "se for caso disso", uma vez que a Diretiva PNR exige uma autorização prévia, que admite ser emitida 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».

51. Portanto, a formulação condicional desta exigência de um controlo independente prévio não é compatível com a Diretiva PNR, que o impõe aos Estados-Membros.

52. Se, com tal referência se pretende excluir os pedidos de acesso pela Europol, esclarece-se que nada na Diretiva legitima a exclusão de um controlo prévio para o acesso e transmissão dos dados pessoais PNR integrais, decorrido o prazo legal de seis meses, uma vez que o n.º 3 do artigo 12.º da Diretiva não distingue as soluções em função da natureza do requerente, nem exceciona aquela regra para os casos previstos no artigo 10.º da Diretiva.

53. De resto, a eventual hipótese de se pretender que fosse o próprio GIP a emitir a autorização é explicitamente rejeitada pelo TJUE, por não preencher a qualidade de independência exigida pela Diretiva, quando afirma que «[...] não se pode considerar que a UIP tenha a qualidade de terceiro em relação a essas mesmas autoridades e, como tal, disponha de todas as qualidades de independência e de imparcialidade exigidas para exercer a fiscalização prévia mencionada no número anterior do presente acórdão e verificar se estão reunidas as condições de divulgação dos dados PNR integrais, conforme previsto no artigo 12.º, n.º 3, alínea b), da mesma diretiva» (cf. ponto 246 do acórdão "Diretiva PNR").

54. Mas, a mesma exigência de independência, explicitada e desenvolvida pelo TJUE, no ponto 245 do mesmo acórdão, conduz ao resultado de o Ministério Público, enquanto autoridade judiciária competente pela direção da investigação, não poder assumir esta função de controlo prévio da divulgação dos dados.

55. Na verdade, o TJUE, no ponto 245 do acórdão "Diretiva PNR", é claro ao afirmar que «[a] exigência de independência que deve satisfazer a entidade encarregada de exercer a fiscalização prévia impõe igualmente que esta tenha a qualidade de terceiro em relação à autoridade que pede o acesso aos dados, de modo que a referida entidade possa exercer essa fiscalização de maneira objetiva e imparcial, ao abrigo de qualquer influência externa. Em especial, no domínio penal, *a exigência de independência implica que a autoridade encarregada dessa fiscalização prévia, por um lado, não esteja implicada na condução do inquérito penal em causa e, por outro, tenha uma posição de neutralidade relativamente às partes no processo penal.*» (itálico nosso).

56. E o disposto no n.º 4 do artigo 32.º da CRP reforça tal interpretação, ao reconduzir apenas ao juiz a prática de atos instrutórios no processo criminal que se prendam diretamente com os direitos fundamentais.

57. Nestes termos, a CNPD recomenda a revisão da alínea *b)* do n.º 3 do artigo 11.º da Lei n.º 21/2019, no sentido de se eliminar a expressão "se for caso disso" e especificando-se que a autorização prévia aí prevista é da autoridade judicial competente, de modo a respeitar a exigência de uma autorização prévia de autoridade independente imposta pela alínea *b)* do n.º 3 do artigo 12.º da Diretiva PNR.

58. Paralelamente, deve a parte final do n.º 6 do artigo 8.º ser revista, também para prever que a autorização a emitir é da autoridade judicial competente.

vii. Os dados pessoais elencados no Anexo I

59. Finalmente, importa atentar nos anexos à Lei n.º 21/2019, uma vez que, como se explicou supra, precisamente por em causa estar um tratamento de dados pessoais que representa uma ingerência significativa nos direitos ao respeito pela vida privada e à proteção dos dados pessoais, a regulação de tal ingerência tem de ser clara e precisa na determinação do alcance e aplicação das medidas por ela previstas, em conformidade com a jurisprudência do TJUE.

60. Nessa medida, o TJUE entende que os conceitos imprecisos, utilizados no anexo I da Diretiva PNR para caracterizar os dados pessoais a recolher, que não contenham qualquer «limitação quanto à natureza e à extensão das informações que podem ser recolhidas e fornecidas» devem ser interpretados restritivamente, considerando-se apenas o tipo de informação que aí esteja acrescentada a título exemplificativo, como única forma de assegurar a certeza e previsibilidade quanto aos dados pessoais objeto de tratamento (cf. pontos 135 e 138 do acórdão "Diretiva PNR").

61. Assim, no Anexo I da Lei n.º 21/2019, importa considerar os dados indicados no n.º 12, que vêm caracterizados de modo impreciso, por recurso ao conceito «observações gerais», seguido de uma enunciação

exemplificativa do tipo de informações aí compreendidas. Como explica o TJUE, no ponto 136 do citado acórdão, «[...] para dar à rubrica 12 uma interpretação que, em aplicação da jurisprudência recordada no n.º 86 do presente acórdão, a torne conforme com os requisitos de clareza e de precisão e, de forma mais ampla, com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta, há que considerar que só são admitidas a recolha e a comunicação das informações expressamente enumeradas nesta rubrica, a saber, o nome e o sexo do passageiro aéreo menor, a sua idade, a(s) língua(s) falada(s), o nome e os contactos da pessoa que o acompanha no momento da partida e sua relação com o menor, o nome e os contactos da pessoa que o acompanha no momento da chegada e sua relação com o menor, o agente presente na partida e na chegada».

62. Paralelamente, no n.º 18 do Anexo I da Lei, quando se refere «[t]odas as informações prévias sobre os passageiros (dados API) que tenham sido recolhidas, incluindo [...]», tais informações só podem ser os dados API expressamente enumerados nesse número e no artigo 3.º, n.º 2, da Diretiva API (cf. pontos 138 e 139 do acórdão "Diretiva PNR").

63. Nestes termos, a CNPD recomenda a revisão dos n.ºs 12 e 18 do Anexo I da Lei n.º 21/2019, de modo a delimitar com exatidão e clareza os dados pessoais objeto de tratamento.

viii. A integração do GPI no PUC-CPI

64. Da Diretiva PNR e do acórdão do TJUE decorre ainda que a UIP «é uma autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave» (cf. ponto 246 do acórdão). Recorda-se que a Diretiva, no n.º 1 do artigo 4.º, determina que «[c]ada Estado-Membro cria ou designa uma autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave, ou cria ou designa uma secção de tal autoridade, para agir na qualidade da sua «unidade de informações de passageiros».

65. Tendo o Estado português criado o GIP, na qualidade de UIP, este gabinete assume a qualidade de autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave. Nessa qualidade, deve o GIP ser o responsável pela base de dados PNR, o que, de acordo com esta perspetiva, implica dever este organismo estar inserido numa estrutura orgânica com a mesma natureza de autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave.

66. Ora, a integração do GPI no Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI) implica diversos atropelos ao Direito da União Europeia, em especial, como se explicará em seguida, o

tratamento de dados pessoais PNR por um organismo que não tem competência para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave.

67. Ademais, as disposições constantes dos n.º 3 do artigo 8.º e n.º 2 do artigo 13.º da Lei n.º 21/2019, tal como se encontram redigidas, parecem pretender legitimar a duplicação de dados pessoais PNR, o que manifestamente contradiz o previsto na Diretiva PNR e revela ser um tratamento de dados ilícito, à luz do regime de proteção de dados da União, por manifesta desproporcionalidade em relação às atribuições e competências do PUC-CPI, permitindo que outras entidades que integram o PUC-CPI, sem competência de investigação criminal, possam conhecer desta informação sensível, extravasando as respetivas atribuições legais.

68. Recorda-se, a este propósito, que o TJUE no acórdão "Diretiva PNR" insiste que o elenco das finalidades da Diretiva PNR é exaustivo, afirmando mesmo, no ponto 236, que «[...] na medida em que [...] a legislação nacional 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, esta legislação é suscetível de violar o caráter exaustivo da enumeração dos objetivos prosseguidos pelo tratamento dos dados PNR ao abrigo da Diretiva PNR [...]».

69. Como a CNPD referiu no seu Parecer n.º 31/2018,

> «Nos termos do n.º 1 do artigo 23.º-A da Lei de Segurança Interna, o PUC-CPI é o centro operacional responsável pela coordenação da cooperação policial internacional, que assegura o encaminhamento dos pedidos de informação nacionais, a receção, o encaminhamento e a difusão nacional de informação proveniente das autoridades policiais estrangeiras, a transmissão de informação e a satisfação dos pedidos formulados.
>
> Com efeito, o PUC-CPI pretende ser uma porta de entrada e saída comum, a nível nacional, no âmbito da cooperação policial internacional, gerindo de forma mais centralizada as vias para o intercâmbio de informações. O PUC-CPI funciona na dependência e sob a coordenação da Secretária-Geral do Sistema de Segurança Interna (SG/SSI).
>
> Por conseguinte, o PUC-CPI não é uma autoridade nem tem quaisquer atribuições legais que lhe permitam manter e gerir uma base de dados para fins de prevenção e investigação de infrações terroristas ou de criminalidade grave, como a que está aqui em causa com os dados PNR. [...]».

70. Assim, a previsão no n.º 3 do artigo 8.º da Lei n.º 21/2019 de que o GIP dê conhecimento ao centro operacional do PUC-CPI dos dados transmitidos às autoridades nacionais competentes, provenientes de outros Estados-Membros, não tem qualquer suporte na Diretiva, como resulta do seu confronto com o n.º 3 do artigo 9.º da Diretiva PNR.

71. O mesmo se diga quanto à previsão de que, em caso de emergência, havendo pedido direto pelas autoridades nacionais competentes a uma unidade de informação de passageiros de outro Estado-Membro, se remeta cópia do pedido ao PUC-CPI (n.º 7 do artigo 8.º da Lei).

72. Também a previsão, no n.º 2 do artigo 13.º da Lei, de que o PUC-CPI conserve cópia de todos os pedidos apresentados pelas autoridades competentes, pelas unidades de informações de passageiros de outros EM e pela Europol, bem como de todos os pedidos e transferências de dados PNR para um país terceiro, não encontra fundamento em qualquer norma da Diretiva ou qualquer disposição do Direito da União, correspondendo a uma norma manifestamente desnecessária e excessiva na ingerência dos direitos fundamentais à reserva da vida privada e à proteção dos dados pessoais.

73. A existência de uma base de dados PNR está, insiste-se, limitada às finalidades de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, cuja prossecução está a cargo das entidades com competência para o efeito, não estando o PUC-CPI, no exercício de funções auxiliares de ponto único de contacto, legitimado a criar e conservar dados pessoais PNR.

74. Ademais, atendendo à legislação que estabelece a organização e o funcionamento do Ponto Único de Contacto para a Cooperação Policial Internacional, não se encontra fundamento de legitimidade para semelhante previsão.

75. Não há qualquer justificação para prever que o PUC-CPI conserve numa base de dados um vasto conjunto de dados pessoais relativos ao PNR, quando não é uma autoridade competente para efeito da Diretiva PNR, e consequentemente da Lei n.º 21/2019, não estando, por isso, habilitada a conservar estes dados.

76. Nestes termos devem ser revistos o n.º 3 e n.º 7 do artigo 8.º, para expurgar a referência a «com conhecimento ao centro operacional do PUC-CPI» e «remetendo cópia do pedido ao PUC-CPI», respetivamente, e revogado o n.º 2 do artigo 13.º, por não ter qualquer suporte na Diretiva, contrariando o nesta disposto quando limita a criação de uma base de dados PNR sob a responsabilidade exclusiva da UIP, e por consubstanciar uma medida legislativa desnecessária e excessiva face às funções de ponto único de contacto nas transferências de dados.

III. Conclusão

77. Com os fundamentos acima expostos, para garantir a conformidade do regime legal relativo ao registo de identificação dos passageiros aéreos com a Diretiva PNR, interpretada em conformidade com os artigo 7.º, 8.º, 45.º e 52.º da Carta dos Direitos Fundamentais da União Europeia, e para assegurar a restrição proporcional dos direitos à reserva da vida privada e à proteção dos dados pessoais, consagrados nos artigos 26.º e 35.º da Constituição da República Portuguesa, a CNPD recomenda a revisão da Lei n.º 21/2019, de 25 de fevereiro, destacando as seguintes disposições legais:

a. o n.º 1 do artigo 1.º, prevendo-se a aplicação deste regime legal aos voos de e para um Estado-Membro da União Europeia apenas se o tratamento de dados pessoais dos passageiros for efetivo e demonstradamente necessário para a prevenção e repressão de ameaças terroristas e nas circunstâncias explicitadas supra, nos pontos 14 a 18;

b. a alínea *a)* do n.º 1 do artigo 6.º, de modo a especificar que as bases de dados objeto de comparação são apenas as referidas na sua parte final, a saber: *bases de dados sobre pessoas ou objetos procurados ou alvo de um alerta, de acordo com as regras aplicáveis a essas bases de dados* (cf. supra, pontos 23 e 24).;

c. o n.º 3 do artigo 7.º, para se acrescentar que a reutilização dos dados aí salvaguardada supõe a prossecução de uma finalidade específica de entre as previstas no n.º 2 do artigo 1.º e densificadas pelo catálogo constante do Anexo II da Lei, nos termos explicitados supra, nos pontos 30 a 38;

d. o artigo 11.º, em especial dos n.ºs 1 e 2, para diferenciar o universo de passageiros cujos dados podem ser conservados por período superior a seis meses, e a revogação do n.º 6, em face da impossibilidade jurídica ou inutilidade do nele disposto. Mais se recomenda que se elimine a referência à anonimização, nos termos explicitados supra, nos pontos 44, 45 e 48;

e. a alínea *b)* do n.º 3 do artigo 11.º da Lei n.º 21/2019, no sentido de se eliminar a expressão "se for caso disso" e de se especificar, quer nesse inciso, quer no n.º 6 do artigo 8.º da mesma lei, que a autorização prévia é da autoridade judicial competente (cf. supra, pontos 51 a 56);

f. o n.º 3 e n.º 7 do artigo 8.º, para expurgar a referência a «com conhecimento ao centro operacional do PUC-CPI» e «remetendo cópia do pedido ao PUC-CPI», respetivamente, e revogado o n.º 2 do artigo 13.º, por não ter qualquer suporte na Diretiva, contrariando o nesta disposto quando limita a criação de uma base de dados PNR sob a responsabilidade exclusiva da UIP, e por consubstanciar uma medida legislativa desnecessária e excessiva face às funções de ponto único de contacto nas transferências de dados (cf. supra, pontos 66 a 75);;

g. os n.ºs 12 e 18 do Anexo I da Lei n.º 21/2019, de modo a delimitar com exatidão e clareza os dados pessoais objeto de tratamento, nos termos explicitados supra, nos pontos 60 a 62;

h. previsão, eventualmente no n.º 1 do artigo 6.º e no artigo 7.º, de que o tratamento de dados pelas autoridades competentes depende de existir uma *conexão objetiva, direta ou indireta, entre o transporte aéreo de passageiros e um dos crimes graves* constantes do anexo II (cf. supra, ponto 27).

Aprovado na reunião de 21 de dezembro de 2022

Filipa Calvão (Presidente)