

PARECER N.º 61/2017

I. Pedido

O Gabinete de Sua Excelência a Ministra da Justiça remeteu à Comissão Nacional de Protecção de Dados (CNPD), para parecer, o anteprojeto de Lei que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (PNR) dos voos extra-UE e intra-UE, programados para partir, aterrar ou fazer escala em território nacional, e o respetivo intercâmbio entre os Estados-Membros da União Europeia, transpondo para a ordem jurídica interna 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.

O pedido formulado decorre das atribuições conferidas à CNPD pelo n.º 2 do artigo 22.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015 de 24 de agosto – Lei de Protecção de Dados Pessoais (LPDP) –, e o parecer é emitido no uso da competência fixada na alínea a) do n.º 1 do artigo 23.º do mesmo diploma legal.

A apreciação da CNPD no presente parecer restringe-se aos aspetos relativos à protecção de dados pessoais.

II. Apreciação

- Objeto

Importa principiar a análise do texto deste anteprojeto pelo objeto do mesmo¹, uma vez que nele se identifica uma das questões verdadeiramente críticas em matéria de protecção de dados pessoais. Como é sabido, os princípios de protecção de dados pessoais estabelecidos no art. 5.º, da LPDP, transpostos, de resto, do art.º 6.º da Diretiva 95/46/CE do Parlamento

¹ Que, como decorre do pedido, respeita à regulação das «transferência[s], pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (PNR) dos voos extra-UE e intra-UE, programados para partir, aterrar ou fazer escala em território nacional, e o respetivo intercâmbio entre os Estados-Membros da União Europeia, transpondo para a ordem jurídica interna 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».

Europeu e do Conselho, e mantidos praticamente inalterados pelo Regulamento 2016/679² que a vem revogar e pela Diretiva 680/2016³, estabelecem, entre outros, a minimização de dados como vetor essencial para garantir a legalidade dos tratamentos de dados pessoais. Significa isto que o responsável pelo tratamento se deve abster de efetuar aquelas operações sobre dados que não sejam indispensáveis para o cumprimento da finalidade visada.

Ao perscrutar o objeto deste anteprojeto, encontramos assente que o Governo português entende como boa a opção pelo acionamento de uma possibilidade (que não obrigatoriedade) prevista na Diretiva, e que se haverá de transpor no futuro diploma legal final, de englobar nos dados dos registos de identificação dos passageiros regulados pela lei nacional aqueles pertencentes aos voos intracomunitários.

Lembre-se que a Diretiva 2016/681 admitia, no seu art.º 2.º, que os Estados-Membros, se assim o entendessem, a aplicassem aos voos intra-UE. Constituía, pois, esta prerrogativa, uma mera e eventual hipótese aberta aos Estados-Membros, no que se demonstrava a dúbia utilidade desta faculdade aos olhos do legislador europeu. Desta forma, por se assumir expressamente como informação de inconclusivo relevo, parece-nos que, por princípio, e salvo uma aturada e clara justificação por parte dos Estados-membros, estes voos internos na UE e os dados que deles resultam não deveriam fazer parte de uma transposição orientada pelo respeito dos direitos fundamentais dos cidadãos e pelo quadro supralegal nacional e europeu de proteção de dados pessoais⁴.

² Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE).

³ 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.

⁴ Quer o art.º 35.º da Constituição da República Portuguesa (CRP), quer os art.º 7.º e 8.º da Carta dos Direitos Fundamentais da UE (Carta), quer também o art.º 16.º do Tratado sobre o Funcionamento da UE, quer ainda o art.º 8.º da Convenção Europeia dos Direitos do Homem têm sistematicamente sido interpretados como sustentando e apenas autorizando uma ingerência tão restrita quanto possível no direito fundamental à proteção de dados pessoais quanto tal seja necessário ao cumprimento ou respeito de outros direitos fundamentais.



Tanto mais que, a apoiar esta interpretação está não só o n.º 1 do referido art.º 2.º, como também o seu n.º 3. Se dúvidas existissem quanto à dispensabilidade da informação ligada aos voos intracomunitários, bem como quanto à necessidade de fundamentar um desvio à opção padrão de não incluir aquela informação no âmbito da Diretiva (por via da transposição nacional), o sobredito n.º 3 dissipa claramente esta questão. Ao permitir uma granularidade ainda maior na aplicação da «diretiva apenas a voos intra-UE selecionados», voos esses que «considerem necessário[s] a fim de prosseguir os objetivos» nela delineados, o legislador europeu apontou indiscutivelmente para uma lógica de pertinência e não excessividade, em suma, de proporcionalidade na avaliação individualizada dos casos em que os Estados-membros viessem a ponderar estender o âmbito da diretiva aos titulares dos dados que se deslocassem unicamente no espaço da UE. Seja pela existência, já hoje, de suficientes meios e procedimentos de interação entre as autoridades nacionais dos Estados-membros da UE para sinalizar e atuar perante casos de hipotéticos suspeitos de crimes terroristas e demais criminalidade grave, seja pela discutível utilidade dessa informação, atrás suscitada, o certo é que, ao remeter esta opção para os Estados, nos termos em que o faz, o legislador europeu assinala a excecionalidade que deve estar ligada ao tratamento destes dados.

O Estado português, mantendo a opção e os moldes em que a consagra, viola claramente o princípio da minimização dos dados, porquanto obriga e procede ao tratamento de dados pessoais, manifestamente dispensáveis ou, na versão negativa correspondente, sem utilidade reconhecida e reconhecível. Assim, preferencialmente, dever-se-ia optar por não incluir estes dados no âmbito da diretiva ou, em alternativa, por estouta se constituir como ingerência menor e, portanto, de maior conformidade com os princípios jurídicos já aludidos, limitar esse alargamento a alguns voos selecionados, de forma devidamente fundamentada, nos termos do n.º 3 da diretiva.

Ainda neste ponto, se o Estado português decidiu considerar, no objeto deste anteprojeto, os voos intra-UE, então não deve esquecer o que o n.º 9 do art.º 6.º, da Diretiva 2016/681, dispõe quanto às consequências das avaliações levadas a cabo sobre a informação recolhida, em matéria de aplicação do Regulamento 2016/399 (Código das Fronteiras Schengen)⁵.

⁵ Este regulamento revogou o Regulamento (CE) n.º 562/2006, a que alude a diretiva.

- Da transposição

Sem prejuízo de uma análise mais cuidada a aspetos particulares de proteção de dados pessoais que serão englobados na menção ao Parecer n.º 1/2015, do Tribunal de Justiça da União Europeia, de 26 de julho de 2017, sistematizamos desde já os aspetos mais relevantes ligados à transposição da Diretiva 2016/681 por parte do presente anteprojeto de lei.

É assinalável que a exposição de motivos saliente que «O tratamento dos dados PNR transferidos pelas transportadoras aéreas permitirá às autoridades policiais e judiciárias utilizar essa informação no âmbito da sua atividade e dos processos a que digam respeito e identificar pessoas suspeitas de atividades criminosas ou terroristas...» [sublinhado nosso]. Esta noção básica e essencial de identificação de pessoas suspeitas deste tipo de atividades ilícitas serve como horizonte de legitimidade para os tratamentos de dados pessoais aqui levados a cabo e previstos na diretiva a transpor. É nesse objetivo fundamental que reside a *ratio* deste instrumento jurídico e é nos estritos limites da sua interpretação conforme ao respeito pelos direitos fundamentais dos cidadãos que deveremos balizar a sua aplicabilidade.

- Imperfeições conceptuais
 - Anonimização

É sintomático do problema que se tem vindo a assistir em algumas traduções oficiais para português que o anteprojeto de lei mantenha alguns conceitos errados, ao mesmo tempo que parece renegar (e bem) outros.

Atente-se no caso dos “dados anonimizados” a que se refere a exposição de motivos, conceito repetido no art.º 8.º (n.ºs 4 e 6), a propósito do intercâmbio de informações entre Estados-Membros e plenamente assumido na epígrafe do art.º 11.º «Prazo de Conservação e anonimização dos dados». Ao contrário do que indicia a utilização desta expressão, em nenhum momento se prevê a anonimização da informação recolhida no âmbito deste anteprojeto, como nunca, de resto, se previu, qualquer anonimização de dados na Diretiva 2016/681. Tal facilmente se alcança da leitura da versão inglesa do art.º 3.º, n.º 10⁶, que

⁶ Que dispõe o seguinte: «‘to depersonalise through masking out of data elements’ means to render those data elements which could serve to identify directly the data subject invisible to a user.». Numa tradução livre diríamos que o conceito aqui em causa se reportaria à despersonalização através do mascaramento de elementos de dados, por forma a evitar a identificação direta do titular dos dados pelo utilizador.

demonstra que o que sempre se pretendeu foi permitir (ou obrigar à) “despersonalização” através da aposição de máscaras sobre alguns dos dados recolhidos.

O que se conclui é, portanto, que a tradução do artigo que vimos de citar⁷ não corresponde nem à letra nem ao espírito da norma aprovada pelo legislador europeu, indo ao arrepio também do que já foi clarificado pelo Grupo de Trabalho do art.º 29.^º, no seu Parecer 5/2014, de 10 de abril⁸, quanto à distinção entre a verdadeira anonimização de dados e, em contraponto, conceitos como o da pseudonimização. Enquanto o primeiro corresponde à efetiva e irreversível anonimização dos dados, sendo impossível re-identificar o titular dos dados após tal operação, o segundo, nos termos inscritos na Directiva 2016/680, significa «o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável». E aqui, nem sequer estamos perante uma real pseudonimização de dados, antes meramente se tratando de um mascaramento dos mesmos.

Talvez por isso, neste anteprojeto, deliberadamente se exclui das definições aquela respeitante à «Anonimiza[ção] mediante mascaramento de elementos de dados». Julgamos apenas que, tal opção deve ser consequente nos demais artigos da transposição, enquadrando corretamente o conceito em todos os momentos em que ele é referido.

▪ Responsável pela proteção de dados

Um outro conceito que aparece erradamente enquadrado é o de responsável pela proteção de dados. Na exposição de motivos este é referido (e bem) como a figura a quem se aloca a tarefa de «controlar as operações de tratamento de dados e de assegurar a observância das normas legais aplicáveis a estas operações». No entanto, no art.º 15.º («Responsável pela

⁷ A versão portuguesa da Directiva 2016/681 refere-se a «Anonimizar mediante mascaramento de elementos de dados».

⁸ Órgão consultivo da Comissão Europeia, composto por representantes de todas as autoridades de controlo dos Estados-Membros e previsto no art.º 29.º da Directiva 95/46/CE.

⁹ Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

proteção de dados»), dispõe-se que «O Diretor Nacional da Polícia Judiciária é o responsável pelo tratamento de dados PNR a que se refere a presente lei.».

Ora, novamente em face de uma tradução dúbia para o português, inscrita no art.º 5.º da Diretiva 2016/681, o previsto “responsável pela proteção de dados”¹⁰ mais não é do que a figura do «encarregado de proteção de dados», a quem compete, com efeito, fiscalizar a ação do responsável pelo tratamento, auxiliando e garantindo que o(s) tratamento(s) de dados pessoais decorra(m) em conformidade com a lei, para além do papel de charneira que desempenha na ligação à autoridade de controlo nacional e aos titulares dos dados.

Julgamos, por isso, que este artigo deve passar a referir-se somente ao “responsável pelo tratamento de dados pessoais”, esse sim, o Diretor Nacional da Polícia Judiciária, em face da criação da Unidade de Informação de Passageiros (UIP) nesta polícia.

- Remissões para a Diretiva 2016/680

Compreende-se que o atual anteprojeto faça já menção expressa às disposições da futura lei que transpõe a Diretiva 2016/680¹¹ (que revogará a Decisão-Quadro 2008/977/JAI, a partir de 6 de maio) e da futura lei que completa o Regulamento 2016/679, ainda que de forma necessariamente precária. Tais remissões não podem ser avaliadas pela CNPD por força da inexistência sequer de um projeto de transposição dessa diretiva ou de lei que complete o regulamento. Desta forma, apenas se presume, quanto à transposição da Diretiva 2016/680, que a futura lei venha a incorporar *ipsis verbis* as disposições a que se reporta, só assim se admitindo um juízo provisório da correção das soluções. O mesmo não se passa quanto à lei que completa o regulamento, uma vez que ainda não existe qualquer projeto que autorize uma semelhante conclusão, até porque, nesse caso, existirão seguramente soluções para lá da letra do texto já conhecido e em vigor.

¹⁰ A versão inglesa refere-se ao «Data Protection Officer» que é usualmente traduzido por “Encarregado de Proteção de Dados”, quer no Regulamento 2016/679 (art.º 37.º e seguintes), quer na Diretiva 2016/680 (art.º 32.º e seguintes).

¹¹ Cfr. art.ºs 10.º («Transferência de dados para países terceiros»), 12.º («Proteção de dados pessoais»), 14.º («Autoridade de controlo») e 16.º («Encarregado de proteção de dados»).



o Omissões na transposição

Sem prejuízo da avaliação dos dados utilizados e dos tratamentos levados a cabo que se há-de efetuar adiante, não vemos que prejuízo haveria em repetir, no art.º 7.º do anteprojeto, o que dispõe o n.º 6 do art.º 7.º da diretiva, em matéria de proibição, quanto às autoridades competentes, de tomadas de decisões baseadas «...na raça ou origem étnica da pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, filiação sindical nem na sua saúde, vida ou orientação sexual».

Seria igualmente relevante conhecer a lista das autoridades competentes habilitadas a solicitar à UIP ou a dela receber dados PNR, para avaliar da adequação da sua previsão neste rol e assim melhor analisar o quadro genérico dos acessos aos dados PNR em Portugal. Tanto assim que o art.º 7.º, n.º 3, da diretiva, obriga a que os Estados-Membros comuniquem à Comissão Europeia essa lista até 25 de maio de 2017, pelo que a mesma já deverá existir, não se descortinando qualquer óbice a que seja conhecida pela CNPD. Aliás, o art.º 13.º, n.º 5, do anteprojeto, permite à autoridade de controlo aceder a um conjunto de informação justamente sobre quem tem ou não privilégios de acesso à informação, pelo que o conhecimento da lista citada seria um elemento clarificador e admissível para a análise ao texto proposto, no quadro da proteção dos direitos fundamentais dos cidadãos.

Bem sabemos que a proposta de legislação complementar ao anteprojeto, sujeita a parecer autónomo, faz incluir na UIP elementos designados pelo Serviço de estrangeiros e Fronteiras e pela Autoridade Tributária e Aduaneira, contudo, tal poderia (e deveria) ser, já nesta sede, claramente assumido. De todo o modo, e tendo conhecimento dessa proposta, o que se pode desde já dizer é que tal inclusão não pode deixar de ser circunstanciada por garantias de acesso estratificadas em função das competências destes dois órgãos de polícia criminal. Dada a longa, mas taxativa, lista de infrações sujeitas a controlo por parte da UIP e sendo certa a limitação jurídica da atuação quer do SEF, quer da AT, torna-se inaceitável que, por via da sua integração na UIP, lhes seja possível aceder a informação (dados pessoais) aos quais ordinária e legalmente estejam impedidos de aceder.

Uma nota breve também para a omissão, no n.º 9, do art.º 4.º do anteprojeto, do que vem prescrito na Diretiva 2016/681, quanto à possibilidade (que mais parece um poder-dever) de os Estados-Membros autorizarem as transportadoras aéreas a limitar as transferências imediatamente após o encerramento do voo às atualizações que se revelem necessárias face

à informação originalmente enviada até 24 horas antes da partida do voo. Ou seja, autorizar a duplicação da informação, obrigando à transferência de novos dados que não tivessem já sido transmitidos previamente, no pleno respeito pelo princípio da minimização dos dados.

- Avaliação da conformidade do anteprojeto à luz do Parecer n.º 1/2015, do Tribunal de Justiça da União Europeia

Como é sabido, o Tribunal de Justiça da União Europeia (TJUE) foi chamado a pronunciar-se pelo Parlamento Europeu a propósito da celebração do Acordo de transferência de dados PNR entre a UE e o Canadá. Em concreto, o objeto do parecer era o seguinte: «Parecer proferido nos termos do artigo 218.º, n.º 11, TFUE — Projeto de acordo entre o Canadá e a União Europeia — Transferência dos dados dos registos de identificação dos passageiros aéreos da União para o Canadá — Bases jurídicas adequadas — Artigo 16.º, n.º 2, artigo 82.º, n.º 1, segundo parágrafo, alínea d), e artigo 87.º, n.º 2, alínea a), TFUE — Compatibilidade com os artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia»¹².

As questões abordadas pelo TJUE no parecer proferido incluíram a resposta à adequação dos elementos formais do acordo, com as bases jurídicas do mesmo em destaque, mas também a avaliação de aspetos concretos e substantivos como o da quantidade e qualidade de dados pessoais recolhidos, o universo de titulares afetados, a hipótese de o Canadá poder transferir esses dados para países terceiros, a proporcionalidade do prazo de conservação dos mesmos, bem como o respeito pelos direitos dos titulares dos dados, por forma a assegurar a existência de um quadro jurídico de proteção dos dados pessoais dos cidadãos da UE que garanta substancial equivalência àquele existente na União.

Sendo certo e líquido que a questão da cedência ou troca dos dados incluídos nesse acordo não ofereceu dúvidas, na interpretação do TJUE, sobre a importância de convocar as bases jurídicas previstas «conjuntamente no artigo 16.º, n.º 2, e no artigo 87.º, n.º 2, alínea a), TFUE» (parágrafo 232), não importará aqui determo-nos sobre ela.

12

Disponível

em

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1071747>.

Igualmente assumido pelo TJUE foi a adequação da maioria dos dados tratados ao abrigo do acordo PNR com o Canadá, tendo, no entanto, emitido um juízo crítico sobre a possibilidade de troca de dados sensíveis (parágrafo 167). Como, no presente caso, estão excluídos tratamentos de dados sensíveis e os dados recolhidos correspondem a uma lista prevista na diretiva, estranha, de resto, ao tipo de dados imprecisos a que o TJUE aludiu no seu parecer, entende-se, *a contrario* do que vem descrito no parágrafo 156 do dito, que os dados recolhidos são, em abstrato, adequados e não representam uma ingerência desproporcionada e contrária ao regime de proteção de dados pessoais em vigor na UE, embora se salvasse a avaliação que efetuaremos no ponto seguinte “aspectos críticos”, a propósito da sua recolha e conservação para efeitos de «prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave».

Sem prejuízo desta avaliação genérica do TJUE, o princípio que tem sustentado a orientação da CNPD quanto à própria sensibilidade do conjunto da informação aqui em causa mantém-se inalterado. O próprio Advogado-Geral, nas suas conclusões¹³, reafirma o nosso entendimento, no parágrafo 170, ao especificar que «Estes dados, considerados no seu conjunto, roçam a esfera da vida privada, ou mesmo íntima, das pessoas e dizem, incontestavelmente, respeito a uma ou a várias «pessoa(s) singular(es) identificada(s) ou identificáveis(is)» [...]. Por conseguinte, não há qualquer dúvida, à luz da jurisprudência do Tribunal de Justiça, de que a transmissão sistemática dos dados PNR para as autoridades públicas canadianas, o acesso a esses dados e a utilização e a conservação desses dados por essas autoridades públicas por um prazo de cinco anos, bem como, se for o caso, a sua transferência posterior para outras autoridades públicas, incluindo de outros países terceiros, por força das disposições do acordo projetado, são operações que entram no âmbito de aplicação do direito fundamental ao respeito pela vida privada e familiar garantido pelo artigo 7.º da Carta, bem como do direito, «indissociavelmente relacionado» [...], mas todavia distinto, relativo à proteção dos dados pessoais garantido pelo artigo 8.º, n.º 1, da Carta, e constituem uma ingerência nesses direitos fundamentais». E não nos parece que este juízo se possa circunscrever unicamente aos dados PNR do acordo UE-Canadá, dado que as diferenças entre esses dados e os que agora se analisam no anexo I, do anteprojeto, não se apartam

¹³ Disponíveis em

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=769416#Footnote16>.

suficientemente para que se aceite, sem mais, estarmos perante categorias de dados não sensíveis.

Além do mais, existem categorias de dados que, utilizadas como indicadores por si só, podem levar a resultados discriminatórios nas avaliações que vierem a ser produzidas (veja-se, como exemplo, o caso da nacionalidade). No ordenamento jurídico nacional, a Lei n.º 93/2017, de 23 de agosto¹⁴, demonstra bem a preocupação legítima do Estado português com esta matéria e que deve, obviamente, merecer concretização prática na mais diversa legislação produzida e aprovada por quem de direito.

Questão polémica, mas que também mereceu aprovação do crivo dos juízes do TJUE, foi a da conservação dos dados recolhidos pelo prazo de cinco anos. No parágrafo 209, o TJUE aludiu e aderiu ao argumentário da Comissão Europeia e do Canadá sobre a necessidade de conservar os dados previstos pelo prazo de cinco anos, tendo em vista a especial natureza dos crimes em causa.

Também ao contrário do que acontecia no acordo da UE com o Canadá, aqui as transferências para países terceiros surgem enquadradas por garantias de verificação prévia da sua admissibilidade à luz do critério de substancial equivalência com o nível de proteção oferecido pela UE, critério repetidamente enunciado pelo Tribunal de Justiça¹⁵ como determinante (cfr. art.º 10.º do anteprojeto). Existem, ainda, circunstâncias excecionais, previstas no n.º 3 do art.º 10.º que, apesar de divergirem do critério apresentado e validado pela jurisprudência comunitária, limitam-se a possibilitar a transmissão dos dados obtidos ao abrigo da transferência entre Estados-Membros para um país terceiro em caso de efetiva urgência (por aquela transferência se constituir como «essencial para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com criminalidade grave num Estado-Membro ou um país terceiro») e apenas quando «a autorização prévia não puder ser obtida em tempo útil», o que aparece como proporcionado.

Os direitos dos titulares dos dados vêm previstos tanto neste anteprojeto (art.º 12.º), como na Diretiva 2016/681 (art.º 13.º, embora aqui por remissão para a Decisão-Quadro 2008/977/JAI,

¹⁴ Que estabelece o regime jurídico da prevenção, da proibição e do combate à discriminação, em razão da origem racial e étnica, cor, nacionalidade, ascendência e território de origem,

¹⁵ Sendo disso o melhor exemplo o Acórdão do TJUE C-362/14 (disponível em <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=PT>).



que será revogada pela Diretiva 2016/680 a partir de 6 de maio de 2018), o que ultrapassa igualmente uma das críticas ao acordo entre a UE e o Canadá que não concretizava suficientemente esses direitos.

Outro dos aspetos que aqui, ao contrário do que acontecia no acordo bilateral, não se coloca é aquele ligado à existência de decisões automatizadas sem o competente escrutínio ou intervenção humana, já que o anteprojeto explicita claramente que «Qualquer resultado positivo obtido através do tratamento automatizado dos dados PNR [...] é verificado individualmente por meios não automatizados, para aferir se é ou não necessário que a autoridade competente referida no art.º 7.º intervenha nos termos da lei» (art.º 6.º, n.º 4, do anteprojeto). Para além de que, não só essas avaliações têm de ser realizadas com base em critérios não discriminatórios, como também deverá existir uma revisão regular destes últimos.

- Aspetos críticos

Onde, com efeito, se denota grande identidade entre as críticas apontadas pelo TJUE ao acordo transatlântico e as disposições do presente anteprojeto (e concomitantemente às da Diretiva 2016/681) é na matéria do universo de titulares de dados afetados e, reflexamente, na matéria dos prazos de conservação ligados aos dados de algumas dessas pessoas.

Tal como refere o TJUE na avaliação ao acordo PNR, no parágrafo 186, «O acordo projetado abrange os dados PNR de todos os passageiros aéreos que voam entre a União e o Canadá. A transferência destes dados para o Canadá é feita independentemente de qualquer elemento objetivo que permita considerar que os passageiros são suscetíveis de representar um risco para a segurança pública no Canadá.», o que o tribunal admite, à luz da impossibilidade, em abstrato, de controlar previamente todos os passageiros que queiram viajar para o Canadá sem ser concedido acesso ao seus dados pelo país de destino.

Sucede, porém que, como o TJUE ressalva nos parágrafos 199 e 200 «[...] importa salientar que, durante a permanência dos passageiros aéreos no Canadá e independentemente do resultado da análise automatizada dos dados PNR efetuada antes da sua chegada a este país terceiro, podem ocorrer situações em que a autoridade canadiana competente disponha de indicações, recolhidas durante essa permanência, de que a utilização dos seus dados se pode revelar necessária para lutar contra o terrorismo e a criminalidade transnacional grave.

[200] Contudo, no tocante à utilização dos dados PNR nas situações previstas no número anterior, há que salientar que, uma vez que os passageiros aéreos foram autorizados a entrar no território deste país terceiro, após verificação dos seus dados PNR, a utilização destes dados durante a sua permanência no Canadá se deve basear em circunstâncias novas que justifiquem essa utilização. A referida utilização carece, portanto, em conformidade com a jurisprudência mencionada nos n.ºs 141 e 192 do presente parecer, de regras que prevejam as condições materiais e processuais que regulam esta mesma utilização [sublinhado nosso], a fim de, nomeadamente, proteger os referidos dados contra os riscos de abuso. Tais regras devem basear-se em critérios objetivos para definir as circunstâncias e as condições em que as autoridades canadianas previstas no acordo projetado estão autorizadas a utilizá-los.

[201] Neste contexto, quando haja elementos objetivos que permitam considerar que os dados PNR de um ou mais passageiros aéreos podem trazer uma contribuição efetiva para o objetivo de luta contra as infrações terroristas e a criminalidade transnacional grave, a utilização desses dados não parece ultrapassar os limites do estritamente necessário».

Daqui parece decorrer que a conservação indiscriminada de todos os dados indicados no anteprojeto e na diretiva sobre todos os passageiros com destino na UE (sejam provenientes de voos de países terceiros ou, como no caso da transposição portuguesa da Diretiva 2016/681, de voos de outros Estados-Membros), após a sua chegada e sem que nenhum elemento objetivo concorra para a sua manutenção para os efeitos previstos neste anteprojeto, não pode deixar de ser considerado excessivo, logo, como uma ingerência desproporcionada, por violadora do princípio da minimização dos dados (art.º 5.º, n.º 1, al. c), da LPDP).

Ainda que se admita que as regras previstas na Diretiva 2016/681 correspondam às tais «regras que prevejam as condições materiais e processuais que regulam [a] utilização [dos dados PNR]», a manutenção desta informação pelo período previsto (cinco anos) parece ultrapassar qualquer limite de razoabilidade, sobretudo perante os prazos de conservação dos dados de passageiros que entretanto já abandonaram o destino UE. Atente-se no que releva para o TJUE, a propósito de idênticas formulações no acordo UE-Canadá, nos parágrafos 204, 205 e 206 do referido parecer: «Os passageiros aéreos que deixaram o Canadá foram, regra geral, objeto de controlos à entrada e à saída daquele país. Do mesmo modo, os seus dados PNR foram verificados antes da sua chegada ao Canadá e, sendo caso disso, durante



COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

a sua permanência e quando da sua saída deste país terceiro. Nestas condições, há que considerar que estes passageiros não representam, em princípio, um risco em matéria de terrorismo ou de criminalidade transnacional grave, na medida em que nem estes controlos, nem estas verificações, nem nenhuma outra circunstância revelaram a existência de elementos objetivos nesse sentido [sublinhado nosso]. Em qualquer caso, não se afigura que todos os passageiros aéreos que viajaram para o Canadá representem, após a sua saída deste país, um risco mais elevado do que outras pessoas que não viajaram para o referido país durante os últimos cinco anos e relativamente às quais o Canadá não dispõe, por conseguinte, de dados PNR.

[205 -] Assim, quanto aos passageiros aéreos relativamente aos quais esse risco não tenha sido identificado à sua chegada ao Canadá e até à sua saída deste país terceiro, não se afigura existir, uma vez saídos desse país, qualquer relação, ainda que indireta, entre os seus dados PNR e o objetivo prosseguido pelo acordo projetado, que justifique a conservação destes dados [sublinhado nosso]. As considerações tecidas, nomeadamente, pelo Conselho e pela Comissão perante o Tribunal de Justiça, sobre a duração média de vida das redes internacionais de criminalidade grave e a duração e complexidade das investigações sobre estas redes não são suscetíveis de justificar um armazenamento contínuo dos dados PNR de todos os passageiros aéreos, depois da sua saída do Canadá, para efeitos de um eventual acesso aos referidos dados, independentemente de uma qualquer relação com a luta contra o terrorismo e a criminalidade transnacional grave.

[206 -] Por conseguinte, não se afigura que o armazenamento contínuo dos dados PNR de todos os passageiros aéreos, após a sua saída do Canadá, se limite ao estritamente necessário.».

Aplicando o juízo crítico do TJUE ao anteprojeto (e à diretiva que este visa transpor) teremos que a conservação dos dados PNR de todos os passageiros que entrem, permaneçam e saiam da UE ou ainda, nos casos, como o português, em que se estendam as obrigações previstas na diretiva aos voos intra-UE, se desloquem apenas entre os países da UE, sempre que a tais passageiros se não liguem, antes e durante esse período de permanência no país de destino, quaisquer suspeitas de atividades ilícitas, na aceção do art.º 1.º, n.º 2, do anteprojeto, se constitui igualmente como uma ingerência desproporcionada, novamente por violadora do princípio da minimização dos dados (art.º 5.º, n.º 1, al. c), da LPDP).

Perante tal conclusão, não pode aceitar-se a conservação dessa informação pelo período de cinco anos propugnado pelo anteprojeto e pela diretiva, já que nenhum motivo válido se pode convocar para justificar a sua manutenção, sobretudo numa base de dados deste tipo, ligada única e exclusivamente à «prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave».

Uma permissão de tratamentos de dados pessoais em termos tão latos atinge o núcleo de proteção essencial da proteção de dados de forma desmesurada e desproporcionada face à finalidade visada, sendo inadmissível por inconstitucional, violando o art.º 18.º e o art.º 35.º (direito à autodeterminação informacional), para além de se demonstrar, como o aponta o TJUE, violadora dos art.ºs 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da UE.

- Outros aspetos

Causa, ainda, estranheza que o legislador nacional não possa ou não queira definir as bases de dados a utilizar para a comparação dos dados PNR (art.º 6.º, n.º 1, al. a), do anteprojeto), por forma a permitir ajuizar da proporcionalidade de tal uso e possibilitar, desde já, uma avaliação crítica dos méritos, conveniências, inconveniências e fundamentalmente da legalidade das mesmas.

Com efeito, a lista de infrações a que alude o Anexo II permite, desde logo, estabelecer quantas, quais e até que limites podem ser utilizadas as bases de dados já hoje existentes e que servirão para proceder aos tratamentos de dados previstos no anteprojeto. Tal limitação é ainda mais facilitada pela existência de um catálogo de dados a recolher, os quais serão processados a coberto de critérios pré-estabelecidos (para levar a cabo as avaliações de aqui tratamos) e serve, de forma muito concreta, para evitar riscos de abusos ou discricionariedades excessivas.

Finalmente, o art.º 4.º, n.º 5, do anteprojeto refere-se, salvo melhor opinião, erradamente à Lei n.º 23/2008, de 4 de julho (autoriza o Governo a aprovar um regime especial aplicável à expropriação e alienação de terrenos incluídos na área das plataformas logísticas que integram a Rede Nacional de Plataformas Logísticas), quando deveria citar a Lei n.º 23/2007, de 4 de julho, sucessivamente alterada, em último pela Lei n.º 59/2017, de 31 de julho (lei da entrada, permanência, saída e afastamento de estrangeiros do território nacional).



III. Conclusão

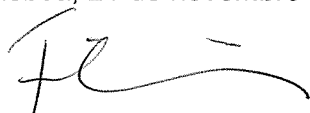
Com os fundamentos acima expostos, a CNPD recomenda:

- a. A reponderação da inclusão dos voos intra-UE no âmbito do anteprojeto, visto que o alargamento do universo de dados pessoais assim conseguido não se demonstra justificado e, portanto, respeitador do princípio da minimização dos dados;
- b. Subsidiariamente a inclusão de apenas alguns voos intra-UE, tal como previsto no n.º 3, do art.º 2.º, da Diretiva 2016/681, de acordo com critérios objetivos e verificáveis, relembrando-se que a diretiva prevê expressamente a possibilidade de os Estados-Membros alterarem, a todo o tempo e sem limite, a seleção de voos que vierem a fazer;
- c. A inserção das entidades competentes no articulado do anteprojeto, tal como previstas no art.º 7.º, com a previsão expressa das restrições de ação dos elementos por elas indicados para a UIP, de acordo com os limites funcionais das competências originárias dessas mesmas entidades;
- d. A correção dos aspetos formais e omissões ligados à transposição da diretiva, acima assinalados;
- e. Apesar de a transposição da Diretiva 2016/681 não dever contrariar o sentido e alcance fundamentais daquela, é de ponderar:
 - i. a conformidade constitucional da recolha, utilização, transmissão e conservação dos dados PNR, nos moldes latos em que estão previstos, sobretudo quando nenhum critério objetivo é avançado para continuar a proceder aos tratamentos desses dados, para efeitos de «prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave», após a entrada dos passageiros no país de destino;
 - ii. A conformidade da conservação e utilização dos dados PNR de titulares dos dados que hajam já abandonado o país de destino, sem que qualquer elemento objetivo ou indício de atividade ligada a infrações terroristas e da criminalidade grave tenha sido registado antes ou ao longo da estadia daqueles nesse país;

- f. A definição das bases de dados das autoridades competentes a utilizar para comparação dos dados PNR, por forma a garantir suficiente previsibilidade e a possibilitar a verificação da adequação das mesmas à finalidade visada.

É este o parecer da CNPD.

Lisboa, 21 de novembro de 2017



Filipa Calvão (Presidente)