

PARECER N.º 31/2018

A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Protecção de Dados (CNPd) que se pronunciasse sobre a Proposta de Lei n.º 137/XIII/3ª (GOV), que regula a transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros, bem como o tratamento desses dados, transpondo a Diretiva (UE) 2016/681.

O pedido formulado visa cumprir as 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), sendo o parecer emitido no uso da competência fixada na alínea a) do n.º 1 do artigo 23.º da citada lei.

A CNPD já se pronunciou sobre esta matéria, a pedido da Ministra da Justiça, sobre um texto de anteprojeto de Lei, transpondo a Diretiva acima indicada, e sobre legislação complementar¹, relativa ao funcionamento da Unidade de Informação de Passageiros e quanto aos procedimentos e soluções tecnológicas para o tratamento dos dados, tendo emitido respetivamente o Parecer n.º 61/2017 e o Parecer n.º 62/2017.

Assim, dão-se aqui por reproduzidas as conclusões do Parecer n.º 61/2017, por se manterem válidas, em especial quanto à opção do legislador nacional de incluir no âmbito da proposta os voos intra-UE sem justificar a necessidade de tal alargamento², bem como quanto à conservação dos dados pessoais de todos os passageiros aéreos, mesmo após verificação de não existirem quaisquer indícios de suspeita de atividade criminosa e muito tempo depois de estes terem deixado o território nacional, em evidente desapeço pelo entendimento do Tribunal de Justiça da União Europeia (TJUE)³.

¹ Alteração ao Decreto-Lei n.º 42/2009, de 12 de fevereiro e projeto de Portaria.

² A referência a uma Declaração do Conselho é claramente insuficiente, além de esta declaração salvaguardar a existência de eventuais reservas dos Estados-Membros, pelo que permanece por fundamentar a posição de Portugal nesta matéria.

³ Parecer 1/2015 do TJUE sobre o projeto de Acordo entre o Canadá e a União Europeia para a transferência dos dados dos registos de identificação dos passageiros da União para o Canadá,



Todavia, a atual Proposta de Lei contém alterações significativas em relação ao texto anteriormente sujeito a parecer, as quais merecem sem dúvida uma análise específica por parte da CNPD, até pelo impacto negativo que podem ter nos direitos e liberdades individuais.

I. Apreciação

A presente Proposta de Lei visa transpor a Diretiva (UE) 2016/681, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR)⁴ para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave⁵ (doravante «Diretiva»).

Esta Diretiva assenta a sua base legal no artigo 82.º, n.º 1, alínea d), e no artigo 87.º, n.º 2, alínea a) do Tratado de Funcionamento da União Europeia (TFUE), isto é, propõe-se *facilitar a cooperação entre as autoridades judiciárias, no âmbito do exercício da ação penal*, e, para efeitos de cooperação policial entre autoridades competentes, *estabelece medidas para a recolha, armazenamento, tratamento, análise e intercâmbio de informações pertinentes*.

No considerando 6, afirma-se que *a utilização eficaz de dados PNR (...), a fim de obter provas e, se for caso disso, detetar cúmplices de criminosos e dismantelar redes criminosas, é necessária para prevenir, detetar, investigar e reprimir infrações terroristas e a criminalidade grave (...)*.

Adianta-se no considerando 7 que a avaliação dos dados PNR permite identificar pessoas insuspeitas de envolvimento naquele tipo de infrações antes de tal avaliação e que deverão ser sujeitas a um controlo mais minucioso pelas autoridades competentes. *Contudo, a fim de assegurar que o tratamento de dados PNR se continua a restringir ao necessário, a fixação e*

proferido nos termos do artigo 218.º, n.º 11, do TFUE, a pedido do Parlamento Europeu, com vista a aferir da sua compatibilidade com a Carta dos Direitos Fundamentais da UE.

⁴ PNR – *Passenger Name Record*

⁵ JO L 119 de 4.5.2016, pp132-149



a aplicação de critérios de avaliação deverão limitar-se a infrações terroristas e à criminalidade grave para as quais a utilização de tais critérios seja relevante. (...).

No considerando 11, declara-se que *o tratamento de dados pessoais deverá ser proporcionado em relação aos objetivos específicos de segurança* visados pela Diretiva.

O enquadramento legal da aplicação da Diretiva está, pois, bem delimitado, remetendo-se inclusivamente para definição precisa do que constitui infração terrorista e para um catálogo estrito de crimes considerados graves, que vêm enumerados em anexo à Diretiva.

A marcar o regime de exceção na utilização dos dados PNR, a Diretiva determina que *só podem ser tratados para fins de prevenção, deteção, investigação e repressão de infrações terroristas e da criminalidade grave* (cf. n.º 2 do artigo 1.º), não se confundindo de todo com o tratamento de dados e o intercâmbio de informação policial que possa ocorrer no âmbito dos restantes mecanismos de cooperação (considerando 23), nem tão-pouco com objetivos de controlo da passagem de passageiros na fronteira nacional, no âmbito do qual são remetidos à autoridade competente para o controlo de fronteiras os chamados dados API⁶ (considerando 10).

Atenta a sensibilidade dos dados e o facto de ocorrer uma recolha e subsequente processamento massivo de informação pessoal por um alargado período de tempo de cinco anos, o legislador europeu optou por restringir o tratamento destes dados a finalidades muito específicas, limitando conseqüentemente o acesso a esta informação apenas às autoridades competentes para os fins visados.

A Diretiva aqui em transposição não deixou, por isso, grande margem de manobra aos Estados-Membros neste domínio; apenas aquela que resulta do regime constitucional de cada

⁶ Os dados API (*Advance Passenger Information* – Informação Antecipada de Passageiros) são dados rigorosos de identificação de passageiros que efetivamente viajam (tais como nome, número do documento de identificação, nacionalidade) que são remetidos pelas transportadoras aéreas ao Serviço de Estrangeiros e Fronteiras, no caso português. Esta obrigação resulta de uma diretiva europeia, só aplicável a voos extra-UE, e tem uma finalidade de controlo de fronteira. Os dados PNR, embora também possam incluir os dados API, são constituídos por muito mais informação, incluindo toda a informação relativa a uma fase prévia à viagem, a qual pode até não se realizar. Ao contrário dos dados API, os dados PNR são constituídos por muita informação que pode não ser rigorosa porque não verificada.



país e da legislação nacional em matéria de competências atribuídas às entidades que prosseguem os fins em causa.

Ora, analisando a Proposta de Lei, resulta haver violação drástica dos condicionalismos impostos pela Diretiva, bem como da ordem jurídica interna. Senão vejamos.

1. Autoridades competentes para efeitos desta Diretiva

Uma das formas de conter a utilização de dados PNR aos fins para que são tratados no âmbito desta Diretiva é através da exigência legal de que as autoridades com acesso a estes dados sejam as *competentes para fins de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave* (cf. n.º 2 do artigo 7.º da Diretiva).

A lista destas autoridades competentes deve ser comunicada à Comissão Europeia e será publicada no Jornal Oficial da União Europeia (cf. n.º 3 do mesmo artigo). Trata-se de um processo público, transparente e clarificador.

Não se entende, pois, os motivos por que a Proposta de Lei não identifica objetivamente as autoridades competentes, limitando-se a prescrever que são autoridades competentes *as entidades policiais e aduaneiras e as autoridades judiciais com competência, nos termos da lei, para a prevenção, deteção, investigação e repressão das infrações terroristas ou da criminalidade grave* (cf. n.º 1 do artigo 7.º da Proposta de Lei).

Mesmo que a lista de autoridades fosse extensa, ela teria sempre de ser feita e deveria estar prevista no articulado ou, quando muito, num anexo à Lei, de modo a poder ser avaliada a adequação da sua inclusão nesse rol, permitindo analisar o quadro genérico de acessos aos dados PNR em Portugal.⁷⁷

Todavia, parece não haver em Portugal muitas autoridades competentes para os fins da Diretiva e, nessa medida, habilitadas a tratar os dados PNR.

⁷⁷ Tal como já defendido pela CNPD no Parecer n.º 61/2017, pág. 7.



De acordo com a Lei de Organização da Investigação Criminal (LOIC)⁸, a Polícia Judiciária tem competência em matéria de investigação criminal para todos os crimes graves elencados na Diretiva, sendo que para a grande maioria deles tem inclusivamente competência reservada (cf. n.ºs 2, 3 e 4 do artigo 7.º da LOIC).

Ainda em conformidade com o n.º 1 do artigo 2.º da LOIC, *a direção da investigação cabe à autoridade judiciária competente em cada fase do processo.*

Não se vislumbra, pois, a dificuldade em listar na Proposta de Lei quais são as autoridades competentes para o tratamento dos dados PNR. A formulação genérica do articulado é inibidora de um escrutínio rigoroso quanto à transposição correta da Diretiva, indiciando simultaneamente o alargamento do acesso aos dados PNR a outras entidades que possam não reunir os requisitos da competência exigida.

Esta questão é tanto mais premente quanto a Proposta de Lei autoriza genericamente que as autoridades competentes possam tratar posteriormente os dados PNR que lhes forem transmitidos (cf. n.º 2 do artigo 7.º).

Nessa medida, reitera-se a imprescindibilidade de a lei nacional identificar claramente quem são as autoridades competentes para fins de prevenção, deteção, investigação e repressão de infrações terroristas e da criminalidade grave, na aceção da Diretiva.

2. Criação da unidade de informação de passageiros no PUC-CPI

A Proposta de Lei cria o Gabinete de Informações de Passageiros (GIP), como unidade nacional de informações de passageiros, no Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), ficando sob a sua gestão.

É à unidade nacional de passageiros que incumbe, segundo a Diretiva, o tratamento de dados PNR, que é realizado através de diferentes operações: receção dos dados provenientes das transportadoras aéreas, a avaliação subsequente dos passageiros antes da sua chegada, com recurso ao cruzamento de informação com outras bases de dados relevantes para os

⁸ Lei n.º 49/2008, de 27 de agosto, alterada por último pela Lei n.º 57/2015, de 23 de junho



fins em vista, a análise massiva dos dados segundo critérios pré-estabelecidos, a resposta aos pedidos de acesso a dados, o intercâmbio de dados com as unidades de outros Estados-Membros e com a Europol, a transferência de dados para países terceiros, as ações de mascaramento e desmascaramento, a conservação e o apagamento dos dados.

Trata-se sem dúvida do tratamento de um gigantesco volume de dados, para o qual confluem os dados PNR de todos os passageiros aéreos⁹ que transitam, entram ou saem do território nacional, incluindo nos voos entre países da UE, num período de cinco anos. Um efetivo repositório de *big data* assumidamente usado para fins de análise criminal, o que não tem aliás precedente no nosso país.

Daí que a Diretiva imponha limitações à criação e composição da unidade nacional de passageiros, com o propósito de garantir um maior controlo da utilização dos dados PNR.

Desde logo, a Diretiva prescreve que o 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».*

Na Proposta de Lei, o Governo optou por não designar uma autoridade já existente com competência para os fins visados, mas antes proceder à criação de um gabinete. No entanto, o GIP não preenche as exigências da Diretiva, naquilo que é obviamente uma violação da Diretiva e do regime jurídico interno.

O GIP não é, em si, uma autoridade nem é competente na aceção da Diretiva. A criação do GIP na gestão do PUC-CPI não resolve a questão, pois este também não é uma autoridade nem é competente na aceção da Diretiva.

Nos termos do n.º 1 do artigo 23.º-A da Lei de Segurança Interna¹⁰, 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*

⁹ Com exclusão dos passageiros de voos privados que não estão sujeitos à obrigatoriedade de comunicação destes dados para estes fins.

¹⁰ Lei n.º 53/2008, de 29 de agosto, alterada por último pela Lei n.º 49/2017, de 24 de maio



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.

Além disso, é visível pela composição proposta do GIP – constituído por elementos da Guarda Nacional Republicana, da Polícia de Segurança Pública, da Polícia Judiciária e do Serviço de Estrangeiros e Fronteiras, com possibilidade de integrar ainda um elemento de ligação da Autoridade Tributária e Aduaneira e da Polícia Marítima – que se pretende replicar o modelo de outros gabinetes que se encontram atualmente sob a alçada funcional do PUC-CPI, como suas unidades orgânicas¹¹.

Mas se eventualmente esse tipo de composição está conforme os respetivos quadros legais aplicáveis a esses gabinetes, o que não está aqui sob apreciação, no presente caso da Diretiva relativa aos dados PNR, a unidade de informação de passageiros tem de ser ela própria uma autoridade competente para fins de prevenção e investigação criminal de infrações terroristas e de criminalidade grave, e admite-se que integre no seu pessoal membros *destacados* por outras autoridades competentes (n.º 3 do artigo 4.º da Diretiva).

Não se afigura, pois, que todas as entidades que, na Proposta se pretende que estejam representadas no GIP, sejam autoridades competentes para os fins enunciados pela Diretiva, pelo que também neste aspeto se verifica haver violação dos preceitos da Diretiva.

¹¹ São eles atualmente o Gabinete SIRENE, o Gabinete Europol e Interpol, o Gabinete para os Centros de Cooperação Policial e Aduaneira e o Gabinete para os Oficiais de Ligação e para os Pontos de Contacto das Decisões Prüm (cf. n.º 4 do artigo 2.º do Decreto Regulamentar n.º 7/2017, de 7 de agosto).



Nos termos do n.º 8 do artigo 3.º da Proposta de Lei, a *designação dos trabalhadores autorizados a proceder ao tratamento de dados PNR* é efetuada por despacho da SG/SSI *ou, se necessário, mediante despacho* desta e dos membros do Governo das áreas donde provenham os funcionários a designar.

Independentemente de formalidades de designação, esta norma demonstra a subversão da *ratio* da Diretiva nesta Proposta de Lei, ao criar um gabinete a quem se dá competência para tratar os dados PNR sem preencher os requisitos legais da norma europeia de ter de ser uma autoridade competente para fins de prevenção e investigação criminal de infrações terroristas e outros crimes graves, não obedecendo também a escolha do pessoal a quaisquer critérios pré-definidos de acordo com o conhecimento e a experiência das autoridades competentes.

Em suma, a forma como a Proposta de Lei transpõe a Diretiva, no que diz respeito à unidade nacional de informações de passageiros, viola manifestamente o ato legislativo da União, pois o GIP e o PUC-CPI não são autoridades nem têm competência para a prevenção ou investigação criminal de infrações terroristas e de crimes graves, não podendo, nessa medida, proceder ao tratamento dos dados PNR. Sublinhe-se que estes constituem repositórios de dados pessoais de milhões de passageiros aéreos, que têm uma natureza de especial sensibilidade pelo potencial de monitorização das deslocações dos cidadãos ao longo de meia década. A solução encontrada terá necessariamente de ser revista.

3. Envolvimento do PUC-CPI no tratamento dos dados PNR

No seguimento do atrás exposto quanto à falta de qualificação do PUC-CPI como autoridade competente, é preocupante verificar que se prevê que a unidade nacional de informações de passageiros (GIP) dê conhecimento ao PUC-CPI, em cópia, dos dados transmitidos às autoridades competentes nacionais, provenientes de outros Estados-Membros (cf. n.º 3 do artigo 8.º da Proposta).

Do mesmo modo se prevê que, em caso de emergência, havendo pedido direto pelas autoridades nacionais competentes a uma unidade de informação de passageiros de outro EM, se remeta cópia do pedido ao PUC-CPI (n.º 7 do mesmo artigo).



No n.º 2 do artigo 13.º da Proposta, prevê-se ainda 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 há qualquer justificação para a proposição destas normas, que colocam na posse do PUC-CPI um vasto conjunto de dados pessoais relativos ao PNR, quando este não é uma autoridade competente, logo não habilitada a tratar estes dados. 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 esta exigência nem se vislumbra como se materializa o tratamento destes dados pessoais, e sob a responsabilidade de quem, e em que suportes físicos ou eletrónicos, e quem a eles tem acesso.

Por outro lado, prevê-se que o intercâmbio de dados com as unidades de informação de passageiros de outros EM se faça através do PUC-CPI, uma vez que o GIP passaria a ser uma unidade orgânica do PUC-CPI, com a responsabilidade de garantir a ligação aos outros EM.

Como resulta do acima explanado, o GIP não pode atuar como unidade nacional de informação de passageiros por não ser uma autoridade competente na aceção da Diretiva.

Por conseguinte, mesmo admitindo que o PUC-CPI pudesse de alguma forma relacionar-se com a unidade de informação de passageiros, tal só poderia ocorrer na sua qualidade de ponto único de contacto, como canal virtual de entrada e saída de comunicações, à semelhança do que irá acontecer com o acesso da Europol aos dados PNR, através da rede Siena¹² e por intermédio da Unidade Nacional Europol.

¹² A referência legislativa feita no n.º 5 do artigo 9.º da Proposta de Lei já está desatualizada. A chamada Decisão Europol (Decisão 2009/371/JAI do Conselho) foi revogada pelo Regulamento (UE) 2016/794, de 11 de maio – Regulamento Europol (JO L 135, de 24.5.2016).



O PUC-CPI não poderá, deste modo, ter qualquer tipo de interferência no tratamento dos dados PNR, uma vez que tal só é possível às autoridades competentes na aceção da Diretiva, pelo que também não reúne as condições exigíveis no ato legislativo agora em transposição.

Não há, pois, motivo algum para que o PUC-CPI conserve cópia com dados pessoais PNR de todos os pedidos realizados para fins de prevenção, deteção, investigação e repressão de infrações terroristas e outros crimes graves.

Nesse sentido, as três disposições citadas devem ser eliminadas do texto da Proposta, por consubstanciarem um tratamento de dados ilícito, mercê da ausência de fundamento de legitimidade.

4. Cruzamento de informação com outras bases de dados

De acordo com o entendimento da CNPD, já plasmado no Parecer n.º 61/2017, a Proposta de Lei deveria identificar as bases de dados consultadas no contexto da avaliação dos passageiros, uma vez que a Diretiva exige que tais bases de dados sejam as relevantes para efeitos de prevenção e investigação das infrações terroristas ou da criminalidade grave.

Por outro lado, a redação da alínea a) do n.º 1 do artigo 6.º é ambígua, pois remete genericamente para as bases de dados das forças e serviços de segurança, não se percebendo se o fim descrito diz respeito em geral às finalidades da Diretiva para o tratamento de dados PNR, ou se, como decorre do texto da Diretiva, as bases de dados a consultar deveriam ser apenas as relevantes para alcançar esse fim, o que significa que nem todas as bases de dados disponíveis e da responsabilidade das forças e serviços de segurança seriam idóneas para atingir os objetivos pretendidos.

Com efeito, uma pesquisa mais alargada, além de constituir uma maior intrusão nos direitos dos cidadãos, poderia retornar informação não pertinente do ponto de vista da *criminal intelligence*.

Acresce ainda que a Diretiva abre a possibilidade de comparar os dados PNR com bases de dados reguladas pelo direito da União e bases de dados internacionais¹³, designadamente

¹³ Alusão evidente ao Sistema de Informação Schengen e a bases de dados da Interpol



quanto a sistemas de informação europeus centralizados, e o legislador nacional fecha essa possibilidade ao reduzir tal expediente às bases de dados das forças e serviços de segurança – admite-se que de modo fortuito.

Reitera-se assim a necessidade de prever em lei quais as bases de dados que podem ser consultadas para efeitos da avaliação dos passageiros no âmbito do tratamento de dados PNR, até para permitir um controlo efetivo de acessos.

De qualquer modo, deve ser revista a redação da norma citada da Proposta de Lei.

5. Falsos *hits*

O n.º 6 do artigo 11.º da Proposta de Lei prevê que seja conservada a informação relativa a um acerto (*hit*), isto é, quando uma pesquisa automática com dados PNR a outra base de dados para cruzamento de informação retorna um resultado positivo, mesmo quando da verificação posterior obrigatória por meios não automatizados decorre um resultado negativo.

O objetivo será *evitar falsos positivos no futuro*. A manutenção desta informação não evitaria, por si só, de novo, um *hit* positivo. Poderia eventualmente permitir o cruzamento automatizado com a lista de falsos positivos já verificados para ultrapassara necessidade de outra verificação manual.

Embora se possa tentar compreender o objetivo, suscitam-se dúvidas sobre a adequação de tal prática e sobre as consequências de acumular uma base de dados paralela que pode rapidamente ganhar grandes proporções - considerando o enorme volume de dados tratados e a proposta de conservar esses falsos *hits* por um prazo de cinco anos -, na esfera jurídica dos cidadãos identificados num primeiro momento como tendo eventuais ligações a atividade criminosa.

A obrigação de realizar uma verificação individual sempre que ocorra um acerto assenta na pretensão de proteger as pessoas de decisões totalmente automatizadas que impactem nos seus direitos, designadamente para garantir que o acerto não é, afinal, negativo. Se nas situações em que essa verificação individual conclui pela existência de um falso *hit* e, apesar disso, a informação dos titulares dos dados é mantida, então a compressão do direito à proteção de dados é evidente, ocorrendo a mesma numa medida desrazoável e, portanto, não permitida à luz do princípio da proporcionalidade.



A abordagem da questão dos futuros falsos hits teria necessariamente de ser acompanhada de salvaguardas especiais, concebidas à medida desta situação, e que não resultem num impacto negativo para os cidadãos. Aliás, seria também essencial perceber por que motivos não se consegue identificar as pessoas de forma inequívoca e, eventualmente, procurar uma solução nesse contexto.

Assim, a norma deveria ser, no mínimo, revista, no sentido de introduzir as garantias suficientes e adequadas que permitam obviar à existência de futuros falsos *hits*, sob pena de ser uma disposição excessiva e, por isso, violadora do n.º 2 do artigo 18.º da Constituição.

6. Regime sancionatório

A Proposta de Lei prevê sanções para penalizar o incumprimento de algumas disposições legais. Deste modo, no que diz respeito às matérias atinentes à proteção de dados pessoais, a Proposta remete para o regime sancionatório que vier a ser fixado na lei nacional de transposição da Diretiva (UE) 2016/680, o que não nos merece reparo.

Quanto à violação das obrigações impostas às transportadoras aéreas, previstas no artigo 19.º da Proposta de Lei, por falta de envio dos dados PNR ou transmissão de forma incompleta, determina-se que seja a CNPD a entidade competente para a aplicação das coimas.

Ora esta proposta não é de todo adequada, na medida em que se trata de matéria fora das atribuições da CNPD. Sendo a CNPD uma autoridade de garantia dos direitos fundamentais, com atribuições no controlo do tratamento de dados para a salvaguarda do direito dos cidadãos à proteção dos seus dados pessoais e à sua privacidade, e apenas neste contexto, afigura-se absurda a imputação de uma competência sancionatória por desrespeito de uma obrigação que consiste em transmitir a terceiros dados pessoais de todos os passageiros, recolhidos inicialmente com uma finalidade bem distinta.

O que é ainda reforçado por se inserir num quadro legislativo de evidente violação do princípio da proporcionalidade e de intrusão excessiva na privacidade das pessoas. Neste sentido, pela natureza da missão prosseguida pela CNPD, não lhe deve ser fixada uma competência, sancionatória, fora das, ou no mínimo estranha, às suas atribuições.



II. Conclusões

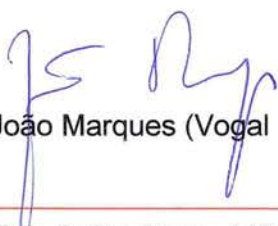
1. Introduzir na Proposta, no texto do artigo 7.º ou em anexo à lei, a lista identificativa das autoridades competentes para fins de prevenção, deteção, investigação e repressão de infrações terroristas e da criminalidade grave, na aceção da Diretiva, a fim de poder ser avaliada a conformidade da sua inserção nesse rol com as competências que lhe estão legalmente atribuídas.
2. A solução encontrada para a unidade nacional de informação de passageiros, através da criação de um Gabinete de Informação de Passageiros (GIP), na dependência funcional do Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI), terá de ser forçosamente revista, pois é violadora de modo evidente da Diretiva em transposição, por não se tratar, em ambos os casos, de autoridades competentes para fins de prevenção, deteção, investigação e repressão de infrações terroristas e de criminalidade grave, tal como é exigível pela Diretiva.
3. Apenas as autoridades competentes na aceção da Diretiva podem proceder ao tratamento de dados PNR, pois só assim é possível garantir que os dados só são utilizados para os fins em causa, por quem tem a competência para a investigação daquela lista de crimes, e não para outras finalidades, e restringir o acesso a um gigantesco repositório de informação sobre a vida privada dos passageiros para análise criminal, incluindo o rastreamento das deslocações aéreas pelo período de cinco anos de todos os voos que chegam ou partem do território nacional.
4. As disposições previstas no artigo 8.º, n.º 3 e 7, e no artigo 13.º, n.º 2, da Proposta têm de ser eliminadas, pois preveem a conservação pelo PUC-CPI de 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, o que consubstancia um tratamento de dados ilícito, pelo facto de o PUC-CPI não ser uma autoridade



competente, na aceção desta Diretiva e não ter, por isso, legitimidade para tratar dados PNR.

5. Devem estar especificadas na lei as bases de dados que podem ser consultadas para efeitos de cruzamento de informação com os dados PNR, atendendo a que devem ser as relevantes para os fins da Diretiva e não quaisquer outras desde que detidas por forças e serviços de segurança. Nesse sentido deve ser revista a redação da alínea a) do n.º 1 do artigo 6.º da Proposta, até no sentido de a conformar com a norma similar da Diretiva, não alargando nem reduzindo o âmbito aí previsto.
6. A previsão do n.º 6 do artigo 11.º da Proposta, sobre a conservação de *hits* que uma verificação individual não automatizada concluiu serem negativos apenas para evitar nova verificação quando voltarem a ocorrer no futuro esses falsos *hits*, deveria ser eliminada pelo impacto muito negativo que tem na esfera jurídica dos titulares dos dados ao implicar um tratamento de dados adicional relacionado com uma falsa ligação a atividade criminosa. Trata-se de uma disposição excessiva e, por isso, violadora do n.º 2 do artigo 18.º da Constituição.
7. Por manifesta contradição com a missão de defesa dos direitos fundamentais da CNPD, e em particular do direito à proteção de dados pessoais, não lhe deve ser imputada a competência sancionatória no que diz respeito à aplicação de coimas às transportadoras aéreas por violação da obrigação de envio de dados à unidade nacional de passageiros ou pelo seu cumprimento defeituoso.

Lisboa, 6 de julho de 2018


João Marques (Vogal Relator)