O *Passanger Name Record* e a Proteção de Dados Pessoais: Uma análise sobre a transferência da informação dos passageiros aos Estados

Emellin de Oliveira*

Resumo: Em 27 de abril de 2016, foi aprovada a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, sobre a utilização dos dados dos registos de identificação dos passageiros (PNR ou *Passenger Name Record*) como instrumento de combate ao terrorismo e à criminalidade grave. A Diretiva estabelece a obrigação de as transportadoras aéreas transferirem para os Estados-Membros as informações do PNR relativas aos voos provenientes/destinados a/de países terceiros. Neste contexto, analisaremos de forma crítica o conteúdo da Diretiva UE-PNR face às normas do Regulamento de Proteção de Dados Pessoais de 2016, com vista a averiguar as convergências e incongruências entre os dois atos legislativos.

Palavras-Chave: *Proteção de Dados; Transferência de dados; Terrorismo; Criminalidade Grave.*

Abstract: On the 27th April 2016, the Directive 2016/681 (EU) of the European Parliament and of the Council was approved, regulating the use of Passenger Name Record (PNR) data as an instrument to combat terrorism and serious crimes. The Directive lays down an obligation for air carriers to transfer PNR information of flights to/from third countries to Member States. In this context, the research's aim is to critically analyse the content of the EU-PNR Directive in relation to the 2016 rules of the Personal Data Protection Regulation, in order to ascertain the convergences and inconsistencies between the two legislative acts.

Keywords: *Data Protection; Data Transfer; Terrorism and Serious Crimes.*

---

* Emellin de Oliveira é Doutoranda em Direito na Universidade Nova de Lisboa (FDUNL), Investigadora no Centro de I&D em Direito e Sociedade (CEDIS) e Bolseira de Doutoramento da Fundação para a Ciência e a Tecnologia (FCT). É Mestre em Migrações Internacionais pelo Instituto Universitário de Lisboa (ISCTE-IUL), Especialista em Estudos da Paz e da Segurança pela Universidade de Coimbra (FEUC) e Licenciada em Direito pela Universidade Federal do Ceará (UFC-CE, Brasil).

Introdução

De acordo com o art. 13.º da Convenção de Aviação Civil Internacional (Convenção de Chicago de 1944), as leis e os regulamentos de um Estado contratante devem ser cumpridos pelos passageiros, tripulação e seu representante aquando da entrada ou saída do seu território. Diante desta determinação da ICAO (*International Civil Aviation Organization*) e com o intuito de adotar medidas contra o terrorismo e a criminalidade grave, no dia 14 de abril, o Parlamento Europeu aprovou uma Resolução Legislativa[1], a respeito do tratamento de dados contidos no PNR. Aquela resolução estabelece para as companhias aéreas, especificamente as transportadoras, a obrigação de fornecer as informações relativas ao registo dos seus passageiros nos voos com proveniência e/ou destino países terceiros, extra-UE.

Posteriormente, no dia 27 de abril de 2016, foi aprovada a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, cuja publicação ocorreu no dia 24 de maio, determinando que a transposição das regras inerentes ao documento citado seja realizada até 25 de maio de 2018. Ainda, a Diretiva prevê uma data para o reexame dos termos aprovados e a formulação de um relatório pela Comissão a ser apresentado ao Parlamento e ao Conselho em 2020.

Apesar de a Diretiva ir ao encontro das medidas de caráter securitário desenvolvidas na União Europeia com a finalidade de combater a imigração ilegal, a criminalidade grave e detetar infrações terroristas, algumas preocupações surgiram com o texto legislativo apresentado. Diana Dimitrova[2], aquando da Comunicação[3] da Comissão Europeia a propor a Diretiva UE-PNR ao Parlamento e ao Conselho, destacava a problemática

---

[1] Resolução legislativa do Parlamento Europeu (P8_TA-PROV (2016) 0127), de 14 de abril de 2016, COM (2011) 0032 – C7-0039/2011 – 2011/0023 (COD), sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

[2] Dimitrova, D. "Passenger Name Records and data protection issues: busting some myths", *Media Policy Project Blog*, de 19 de maio de 2015. Disponível em: <http://blogs.lse.ac.uk/mediapolicyproject/2015/05/19/passenger-name-records-and-data-protection-issues-busting-some-myths/> (acedido a 12/12/2017).

[3] Proposta de Diretiva do Parlamento Europeu e do Conselho, COM (2011) 32 final da Comissão, de 2 de fevereiro de 2011, relativa à utilização dos dados dos registos de identificação

que se gerava em volta da vigilância proposta a todos os indivíduos. A autora menciona como questões a refletir: a precisão e o tratamento dos dados transferidos pelas companhias aéreas; a inexatidão da eficácia, proporcionalidade e necessidade da transmissão de informações; além da possível violação de princípios consagrados em documentos comunitários e internacionais, entre os quais se encontra a proteção de dados pessoais[4].

Tendo em conta a aprovação do Regulamento[5] sobre a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades, é necessário abordar o tema do PNR no contexto da proteção de dados pessoais na União Europeia.

Posto isto, o presente artigo visa, na sua primeira secção, analisar o conteúdo da Diretiva UE-PNR. Na segunda secção, um quadro comparativo será desenhado de modo a destacar as convergências e incongruências entre a Diretiva UE-PNR e o Regulamento de Proteção de Dados. Na terceira secção, apreciamos a prática das companhias aéreas no que diz respeito à obtenção das informações dos passageiros e ao tratamento dado àquelas, para que se possa perceber o impacto das obrigações contidas na Diretiva do PNR. Por fim, pretende-se criticamente averiguar a aplicabilidade e a eficácia no combate ao terrorismo e à criminalidade grave desses atos legislativos face ao imposto às transportadoras.

Para fins de limitação do objeto de estudo, o presente artigo assumirá a definição dos dados do PNR como descrita pelo Parlamento Europeu, que seria a informação fornecida pelos passageiros e coletada pelas transportadoras aéreas durante os procedimentos de reserva e *check-in*[6].

---

dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave (2011/0023 (COD) C7-0039/11).

[4] Dimitrova, D. "Passenger Name Records and data protection issues: busting some myths", cit.

[5] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[6] Parlamento Europeu, *EU Passenger Name Record (PNR) directive: an overview*, de 1 de junho de 2016. Disponível em: <http://www.europarl.europa.eu/news/pt/news-room/20150123BKG12902/eu-passenger-name-record-(pnr)-directive-an-overview> (acedido a 5/12/2016).

1. A Diretiva UE-PNR e a transferência de informações dos passageiros

A compreensão da motivação e do objetivo da Diretiva UE-PNR, pressupõe o conhecimento das razões de sua origem, daí o breve historial que se passa resumidamente a traçar.

I. Em novembro de 2001, entre uma das medidas securitárias desenvolvidas pelos Estados Unidos em resposta aos atentados terroristas de setembro do mesmo ano, o governo norte-americano passou a exigir das companhias aéreas o acesso eletrónico aos dados contidos nos registos de passageiros.

Em resposta ao requerimento, a Comissão Europeia, em junho de 2002, comunicou aos EUA que aquela exigência poderia gerar conflitos com as legislações, da União Europeia e dos seus Estados-Membros, em matéria de proteção de dados, nomeadamente no que toca à extensão desta obrigação às transportadoras com base operacional na UE. No entanto, em fevereiro de 2003, os EUA e a UE emitiram conjuntamente uma declaração em que assumiam o compromisso de continuar a negociar a respeito da comunicabilidade dos dados do PNR à alfândega norte-americana.

A administração dos EUA, impaciente com os diversos adiamentos por parte da UE à efetivação da transmissão das informações, impôs às transportadoras aéreas penalidades caso o acesso ao PNR dos passageiros não fosse disponibilizado a partir de 5 de março de 2003[7].

---

[7] Sobre este tema, o Parlamento Europeu emitiu a Resolução P5_TA (2003) 0429, cujo seguinte excerto se destaca: "3. Convida, por conseguinte, a Comissão a: A) Determinar de imediato, com base nos limites delineados pelo grupo de trabalho criado pela Directiva 95/46/CE, quais os dados que podem legitimamente ser transmitidos pelas companhias aéreas e/ou pelos sistemas informatizados de informações a terceiros, e em que condições, desde que: não exista discriminação contra passageiros não nacionais dos EUA e os dados não sejam retidos para além do período de estada do passageiro em território dos EUA; os passageiros sejam informados plenamente e com precisão antes da aquisição do seu bilhete e dêem o seu consentimento informado no que se refere à transmissão dos dados em causa para os EUA; os passageiros tenham acesso a um procedimento de recurso rápido e eficaz, na eventualidade de qualquer problema. B) Proibir às companhias aéreas e aos sistemas de reserva informatizados qualquer acesso e/ou transmissão que não respeite os princípios estabelecidos na alínea a) ou caso as mesmas companhias e sistemas estejam em aparente violação das obrigações decorrentes da Directiva 95/46/CE e do Regulamento (CEE) n.º 2299/89".

II. Ainda, em dezembro do ano de 2003, a Comissão publicou um Comunicado[8] ao Conselho e ao Parlamento Europeu, com as ideias de base consideradas como "uma abordagem global da UE" relativamente à transferência de dados do PNR. Ao defender uma abordagem equilibrada e abrangente, as componentes do plano europeu sobre a transmissão de informações dos passageiros aos EUA seriam: um quadro jurídico para as transferências existentes de dados dos PNR para os EUA; o fornecimento de informações completas, exatas e oportunas aos passageiros, a fim de que estes consentissem na transferência dos seus dados; a substituição do método de extração direta dos dados pelo governo norte-americano, "método *pull*", pelo método de exportação, "método *push*", no qual se poderia usar filtros que impedissem a transmissão de informações por outros canais[9]; o desenvolvimento de uma posição da UE sobre a utilização dos dados dos passageiros para a segurança da aviação e das fronteiras; a criação de um quadro multilateral para a transferência de dados dos PNR's no âmbito da Organização Internacional da Aviação Civil[10].

Da análise dos documentos referidos, é notória a preocupação da UE sobre a transferência de dados do PNR. Visa-se estabelecer um modelo jurídico da União que permita autorizar as companhias aéreas a transferir as informações dos passageiros para os EUA, como uma obrigação legal e, ao mesmo tempo, garantir que cidadãos europeus sob investigação do governo norte-americano sejam sujeitos a um processo legal justo, com respeito pelos seus direitos fundamentais.

Esta preocupação também se encontra na Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras. Apesar desta Diretiva

---

[8] Comunicação da Comissão ao Conselho e ao Parlamento Europeu sobre a transferência de dados contidos nos registos de identificação dos passageiros aéreos, COM (2003) 826 final, de 16 de dezembro de 2003, (PNR – *Passenger Name Record*): uma abordagem global da UE, Bruxelas.

[9] Sobre esses métodos, destaca-se o que veio delineado na Proposta de Decisão-Quadro do Conselho, COM (2007) 654 final, de 6 de novembro de 2007, p. 5: "(...) A principal diferença entre os dois métodos reside no facto de, no método de transferência por exportação, os dados serem enviados pela transportadora à autoridade nacional, enquanto nos métodos de transferência por extracção a autoridade nacional obter acesso ao sistema de reservas da transportadora aérea e extrair os dados".

[10] COM (2003) 826 final, cit., pp. 10 e 11.

estabelecer como legítimo o processamento dos dados do PNR para controlo fronteiriço e a utilização dessas informações como meio de prova em ações judiciais, estipula que "qualquer tratamento de algum modo incompatível com esta finalidade é contrário ao princípio enunciado na alínea b) do n.º 1 do art. 6.º da Directiva 95/46/CE[11-12].

Neste sentido, as companhias aéreas passaram a ter como obrigação legal a transmissão, até ao final do registo do embarque, das "Informações Prévias sobre Passageiros" (*Advance Passanger Information* – API). Entre as informações a comunicar encontram-se, nomeadamente: o número e tipo de documento de viagem utilizado; a nacionalidade; o nome completo; a data de nascimento; o ponto de passagem da fronteira à entrada no território dos Estados-Membros; o código do transporte; a hora de partida e de chegada do transporte; o número total de passageiros incluídos nesse transporte; o ponto inicial do embarque. No entanto, por ser uma transcrição das informações contidas no passaporte e/ou Bilhete de Identidade, o API apenas permite a identificação de suspeitos de terrorismo e crime organizado já conhecidos pelas autoridades.

III. No sentido de colmatar esta lacuna, em novembro de 2007, o Conselho comunicou uma Proposta de Decisão-Quadro[13] sobre a utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* – PNR) pelos Estados-Membros da União Europeia. Na proposta, destacava-se que seriam necessários "uma cooperação e um maior intercâmbio de informações entre os Estados-Membros e os seus serviços, bem como com a Europol" a fim de que se pudesse enfrentar o caráter transnacional adquirido pelo terrorismo e pela criminalidade organizada. Para o Conselho, a recolha e a análise dessas informações dos passageiros permitiriam às autoridades estatais competentes identificar pessoas consideradas

---

[11] Directiva 95/46/CE, alínea b) do n.º 1 do art. 6.º: "Recolhidos para finalidades determinadas, explícitas e legitimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades. O tratamento posterior para fins históricos, estatísticos ou científicos não é considerado incompatível desde que os Estados-Membros estabeleçam garantias adequadas".

[12] Directiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação dos dados dos passageiros pelas transportadoras.

[13] Proposta de Decisão-Quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (UE – PNR) para efeitos de aplicação da lei, COM (2007) 654 final, de 6 de novembro de 2007.

de alto risco e tomar medidas adequadas antecipadamente, usando como exemplos positivos as iniciativas já materializadas nos EUA, Canadá e Reino Unido.

Assim, a base jurídica da proposta ancorava-se no art. 29.º, na alínea b) do n.º 1 do art. 30.º e na alínea b) do n.º 2 do art. 34.º, do Tratado da União Europeia, bem como nos princípios da subsidiariedade, no que toca à harmonização das obrigações jurídicas que recaem sobre todas as companhias aéreas operadoras de voos da/para União Europeia, e da proporcionalidade, relativamente ao objeto de harmonização, pois o uso e o tratamento dos dados deverão restringir-se ao estritamente necessário.

Ao verificar que a proposta do Conselho não havia avançado e que ainda se mantinham as discussões entre a UE e os EUA a respeito da transmissão das informações relativas ao registo de passageiros, o Conselho Europeu relembrou a questão do PNR no "Programa de Estocolmo – Uma Europa aberta e segura que sirva e proteja os cidadãos", projeto apresentado pela Presidência em outubro de 2009. No Programa, o Conselho solicitava à Comissão a proposta de adoção de uma medida por parte da UE no âmbito do PNR que garanta um elevado nível de proteção de dados[14].

Assim, findo o período de negociação com os EUA sobre a transferência de dados do PNR e assinado um acordo para tal efeito, que foi repetido com o Canadá e a Austrália, a UE, por via do Comunicado[15] da Comissão em setembro de 2010, retomou o discurso em prol de uma abordagem global relativa à transferência dos dados do PNR para países terceiros. Nesta comunicação, ressalta-se o PNR como uma importante ferramenta em matéria de informações criminais, servindo mais do que um sistema de verificação de identidade – como ocorre com o API – e podendo ser utilizado de modo: "reativo", em investigações iniciadas após a prática do

---

[14] Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos, Jornal Oficial da União Europeia, 2010/C 115/01, p. 9: "Com base nos debates realizados no Conselho e no Parlamento Europeu tendo em vista a criação na União de um sistema de registo de identificação dos passageiros (PNR), o Conselho Europeu exorta a Comissão a: — propor a adopção de uma medida da União, que garanta um elevado nível de protecção de dados, no domínio do PNR no intuito de prevenir, detectar, investigar e reprimir infracções terroristas e formas graves de criminalidade com base numa avaliação de impacto".

[15] Comunicação da Comissão Europeia sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros, COM (2010) 492 final, de 21 de novembro de 2010.

crime; "real", quando um crime está a ser cometido ou na iminência de ocorrer, em que se se pode evitar a conclusão do ato ilícito; e "pró-ativo", possibilitando a criação de padrões de viagem e de comportamento, o que facilitaria a identificação de perfis criminosos.

IV. Não obstante a clara e explícita intenção em criar-se uma legislação específica sobre PNR para a UE, a Comissão deparou-se com um óbice prático: a possibilidade de requisição de reciprocidade na transmissão de dados de PNR por Estados terceiros que aceitarem fornecer estas informações à União Europeia. Tal preocupação subjaz no arcabouço legislativo da União, especificamente no relativo à proteção de dados. Isto porque a transferência de dados de passageiros a países terceiros só pode ocorrer caso estes assegurem garantias adequadas para a proteção das informações disponibilizadas.

Neste sentido, ainda no Comunicado da Comissão, estabeleceu-se quais seriam os princípios básicos em matéria de proteção de dados que deveriam ser aplicados pelo país terceiro que requeira reciprocidade na transmissão dos dados do PNR, designadamente: finalidade clara e objetiva da utilização dos dados do PNR; intercâmbio de dados em caráter mínimo e proporcional à finalidade; dados sensíveis não devem ser utilizados, salvo face à uma ameaça iminente e sob garantias de adequação à finalidade original; proteção contra a utilização incorreta e o acesso ilegal; sistema de fiscalização sobre as autoridades que tratam os dados do PNR; transparência e comunicação do uso e do tratamento dos dados; possibilidade de acesso, retificações e supressão dos dados de PNR; via de recurso efetiva para os indivíduos que entenderem ter seus direitos violados; decisões individuais de caráter não-automatizado; conservação dos dados apenas no tempo estritamente necessário para a finalidade; restrições às transferência dos dados a outras autoridades que não tenham competência em matéria de luta contra o terrorismo e a criminalidade grave; e restrições a transferências ulteriores para países terceiros.

Dando continuidade à abordagem global relativa à transferência dos dados do PNR, em 11 novembro de 2010, o Parlamento Europeu lança a "Estratégia externa da UE relativamente aos dados dos registos de identificação dos passageiros (PNR)". Nesta estratégia, o Parlamento relembra a importância em combater o terrorismo e a criminalidade transnacional, mas sem mitigar a proteção das liberdades cívicas e dos direitos fundamentais.

Neste contexto, é chamada a atenção para que fossem respeitados os arts. 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia e o art. 8.º da Convenção Europeia dos Direitos Humanos, apontando ainda a base jurídica da legislação europeia a ser criada nesta matéria, designadamente o art. 16.º do Tratado de Funcionamento da União Europeia, cujo texto remete para o art. 39.º do Tratado da União Europeia. Ainda, ressalta que a necessidade e a proporcionalidade são princípios que devam estar consagrados nos acordos, bem como medidas políticas em matéria de proteção de dados, mostrando-se contrário a ações que utilizem as informações transmitidas no sentido de "prospeção de dados" ou "determinação de perfis".

V. Apesar de todos os avanços legislativos e estratégicos desenvolvidos no ano de 2010, apenas a 14 de abril de 2016 é que foi aprovada, com emendas, a Resolução Legislativa do Parlamento Europeu sobre a "Utilização dos Dados dos Registos de Identificação dos Passageiros (PNR)[16]". A Diretiva UE-PNR 2016/681, do Parlamento Europeu e do Conselho, foi publicada em 27 de abril de 2016, sobre a utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

No Considerando (7) da Diretiva mencionada, defende-se que o resultado da avaliação dos dados do PNR permite a identificação de suspeitos de infrações terroristas ou criminalidade grave antes que pratiquem o ato. Daí a importância do uso deste método para fins policiais. No entanto, o uso dos dados do PNR para identificar indivíduos para fins deteção e repressão ao terrorismo e à criminalidade grave não poderá ultrapassar os objetivos da Diretiva.

Assim, no art. 1.º prevê-se que as transportadoras aéreas deverão transmitir os dados do PNR de voos extra-UE e que estes dados serão recolhidos, tratados, utilizados e conservados pelos Estados-Membros, que deverão trocar entre si informações dos resultados obtidos. Importa ainda verificar que, no art. 2.º, a Diretiva não afasta a obrigação de transferência de dados

---

[16] Resolução legislativa do Parlamento Europeu, sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, P8_TA-PROV (2016) 0127, de 14 de junho de 2016.

do PNR também de voos intra-UE, sob notificação prévia por escrito dos Estados-Membros à Comissão.

Nos termos do art. 4.º, estabelece-se que cada Estado-Membro deverá criar ou designar uma autoridade capaz de cumprir com os objetivos da Diretiva, a qual será nomeada de "Unidade de Informações de Passageiros" (UIP). A constituição da UIP, que poderá representar um ou mais EM, deverá ser notificada à Comissão no prazo de um mês após a sua constituição. Um responsável de proteção de dados será designado pela UIP, tendo como competência o controlo do tratamento dos dados do PNR e a aplicação das salvaguardas relevantes durante a atuação da Unidade. No caso de considerar que os dados do PNR não estão a ser tratados em conformidade com a lei, o citado responsável pela proteção de dados poderá informar a autoridade nacional de controlo.

O art. 9.º da Diretiva, por sua vez, estabelece em que termos ocorrerá a troca de informações entre os Estados-Membros. Tendo por base o disposto no n.º 6 do art. 6.º, os Estados-Membros ficam obrigados a transmitir às UIP's dos outros Estados os dados de PNR, ou o resultado do tratamento destes, sobre as pessoas já identificadas como prováveis terroristas ou criminosos de elevada gravidade, a fim de que as autoridades competentes nacionais possam ser informadas pelas Unidades sobre estes indivíduos. Contudo, tal ação apenas pode ser realizada após análise individualizada e não automatizada dos dados, de forma a assegurar o respeito pelas pessoas que se encontrem identificadas devido à suspeita das atividades criminosas objeto da Diretiva.

Outrossim, a UIP de um Estado-Membro poderá solicitar acesso aos dados do PNR ainda não encriptados a outras UIP's, mediante pedido fundamentado em um caso específico, com o fim de que encontrar maiores indícios no âmbito de uma investigação que vise prevenir, detetar ou repreender infrações terroristas ou de criminalidade grave. As autoridades competentes nacionais não estão completamente impedidas de realizar a requisição de dados de PNR diretamente às UIP's de outros Estados-Membros, mas apenas poderão fazê-lo em caso de emergência, sendo a UIP nacional informada do pedido direto por meio de uma cópia do requerimento. Apesar de deixar claro que o procedimento normal será requerer o acesso das informações de passageiros à UIP nacional, que fará o papel de mediadora com as suas congéneres nos outros Estados-Membros, a

Diretiva não esclarece o que seriam os chamados "casos de emergência", deixando esta tarefa ao legislador nacional.

A Agência da União Europeia responsável por garantir o cumprimento da lei, conhecida pela abreviação "Europol", está também habilitada a requerer diretamente às UIP's dados de PNR, nos termos do art. 10.º da Diretiva. Este requerimento deverá ser fundamentado e claro, de modo a evidenciar o "contributo substancial" das informações do PNR à prevenção, deteção ou investigação de uma infração a ser inspecionada pela Agência, nos limites de sua competência. A Europol, no entanto, está obrigada a comunicar ao responsável pela proteção de dados do Estado-Membro da UIP que contactar a fim de obter dados de um PNR.

Vale destacar que as transferências de dados de PNR efetuadas pelas companhias aéreas, conforme estabelece o art. 16.º, devem ocorrer por via eletrónica e oferecer garantias suficientes de segurança. Inclusive, em caso de avarias, a modalidade de envio poderá alterar-se, mas as garantias de seguranças devem permanecer. Contudo, está prevista a adoção de protolocos a respeito dos formatos de dados que serão reconhecidos para a transferência de todos os dados de PNR após um ano da data que a Comissão vier a adotar. Novamente, caberá ao Estado-Membro viabilizar os meios para que os protocolos sejam implementados e utilizados.

VI. Antes de passarmos a uma análise da transferência destes dados face à proteção de dados pessoais, importa trazer à baila a disposições finais constantes na Diretiva UE-PNR, de 27 de abril de 2016. O prazo para os Estados-Membros transporem a Diretiva para o seu direito interno é até 25 de maio de 2018. É previsto um reexame de todos os elementos da Diretiva é 25 de maio de 2020 pela Comissão, que apresentará um relatório ao Parlamento Europeu e ao Conselho com base nas informações prestadas pelos Estados-Membros anualmente, os quais comunicam as estatísticas sobre os dados de PNR comunicados às UIP's.

Especificamente sobre o Relatório da Comissão, é relevante mencionar que o reexame, nos termos do n.º 2 do art. 19.º, deve ter atenção especial ao cumprimento das normas aplicáveis de proteção de dados pessoais; à necessidade e proporcionalidade da recolha e do tratamento dos dados de PNR; à duração do prazo de conservação dos dados; à eficácia do intercâmbio de informações com os Estados-Membros; e, à qualidade das avaliações, nomeadamente as estatísticas fornecidas.

No que toca à relação da Diretiva UE-PNR com outros instrumentos, o art. 21.º estabelece que os Estados-Membros podem continuar a aplicar acordo e/ou convénios que façam parte em matéria de intercâmbio de informações entre si e/ou com Estados-terceiros. Não obstante, ressalva que a aplicação de tais instrumentos não pode prejudicar o que está previsto em matéria de proteção de dados pessoais. Este tema será abordado com mais detalhes no tópico que se segue.

2. A Diretiva UE-PNR e o Regulamento de Proteção de Dados Pessoais: convergências e incongruências

Desde que os dados do PNR passaram a ser usados como fonte de informação para prevenir, detetar e investigar eventuais suspeitos de terrorismo ou criminalidade grave, já se evidenciava a violação do direito de proteção de dados pessoais dos passageiros cujas informações seriam transferidas aos Estados. De facto, esta foi uma das razões – talvez a principal – que motivou o adiamento de um ato legislativo europeu sobre o PNR, mas que acabou por efetivar-se em prol de um almejado ambiente de segurança no ELSJ.

Segundo Niovi Vavoula[17], a Diretiva relativa a dados de identificação dos registos de identificação dos passageiros, mesmo antes da sua aplicação, já esbarra em dois direitos: respeito pela vida privada e familiar e a proteção dos dados pessoais. O primeiro direito encontra-se no art. 7.º da Carta dos Direitos Fundamentais da União Europeia e no art. 8.º da Convenção Europeia dos Direitos Humanos, encontrando-se nesta última a exceção na qual se vislumbra a interferência de autoridade pública quando estabelecido por lei e na defesa da segurança nacional, segurança pública e no bem-estar económico do Estado[18].

---

[17] Vavoula, Niovi. "I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive", *EU Immigration and Asylum Law and Policy*, 2016. Disponível em: <http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/> (acedido a 5/12/2017).

[18] CEDH, Convenção Europeia dos Direitos Humanos, n.º 2 do art. 8.º. "Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem – estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros".

No entanto, a mencionada autora chama a atenção para o facto de que as informações a disponibilizar pelas companhias aéreas permitirão às autoridades traçar um perfil de cada viajante e de sua família apenas sob suspeita de eventual ligação com atividades ligadas ao terrorismo e à criminalidade grave. Por isso, não parece que a segunda parte do artigo citado venha a justificar de uma forma clara e objetiva esta atuação europeia.

Trazendo ao debate o considerando (1) do Regulamento de Proteção de Dados, deste dispositivo consta que a "proteção de dados de pessoas singulares relativamente ao tratamento de dados pessoas é um direito fundamental". Ainda, o mesmo Regulamento estabelece no considerando (2) que esse direito subsiste e aplica-se "independentemente da nacionalidade ou do local de residência dessas pessoas".

Neste sentido, a Diretiva UE-PNR enuncia, nos termos do n.º 1 do art. 13.º, que os Estados-Membros devam assegurar a todos os passageiros "o mesmo direito à proteção dos seus dados pessoais, os direitos de acesso, retificação, apagamento e limitação". Os Estados-Membros também estão obrigados a garantir o respeito pela confidencialidade e pela segurança dos dados e do tratamento dos mesmos, devendo evitar que indivíduos sejam discriminados devido à sua origem étnica, opiniões políticas, religião, convicção filosófica, filiação sindical, saúde, vida ou orientação sexual.

Ainda, devem os Estados executar medidas que garantam a manutenção e a sistematização do trabalho desenvolvido pelas suas respetivas UIP's, de modo a reter a documentação sobre, nos termos das alíneas do n.º 5 do art. 13.º: o nome e os contactos da organização e do pessoal da UIP a quem confiar o tratamento de dados dos PNR, bem como os diferentes níveis de acesso; os pedidos apresentados pelas autoridades competentes e pelas UIP's de outros Estados-Membros; e, todos os pedidos e transferências de dados PNR para um país terceiro.

É de salientar que a UIP poderá disponibilizar, se requerido, a documentação à autoridade de controlo nacional. Ainda, cabe aos Estados-Membros assegurar que, face a uma violação de dados pessoais de elevado risco para a proteção de dados pessoais ou dano para a privacidade do titular dos dados, as UIP's deverão comunicar àquele e à autoridade de controlo o ocorrido.

Nos termos do art. 11.º, os Estados-Membros apenas poderão enviar os dados de PNR, ou o resultado do seu tratamento, a países terceiros desde que, segundo a alínea a) do n.º 1 do art. indicado, preencham as seguintes condições estabelecidas no art. 13.º da Decisão-Quadro 2008/977/JAI, de

28 de novembro: tal seja necessário para a prevenção, investigação, deteção ou repressão de infrações penais ou para a execução de sanções penais; a autoridade recetora no Estado terceiro ou o organismo internacional de receção seja responsável pela prevenção investigação, deteção ou repressão de infrações penais ou pela execução de sanções penais; o Estado-Membro que forneceu os dados tenha consentido na transferência, de acordo com a sua legislação nacional; e que o Estado terceiro ou o organismo internacional em causa assegurem um nível de proteção adequado para o tratamento previsto dos dados.

Somam-se a estas condições, a necessidade de que a transferência de dados de PNR se coadune com o objetivo da Diretiva UE-PNR e o compromisso de que o país terceiro recetor das informações apenas transmitirá os dados recebidos para um outro Estado, caso seja estritamente necessário e mediante notificação do Estado-Membro europeu que lhe tenha transmitido os dados de PNR. É possível, todavia, que seja realizada a transferência de informações para um Estado terceiro diferente daquele que recebeu os dados de PNR sem autorização prévia do Estado-Membro que facultou as tais informações, desde que esta transferência seja essencial para responder a uma ameaça específica e concreta no que toca a infrações terroristas ou a criminalidade grave ou porque não foi possível obter em tempo útil tal autorização.

Em todo o caso, deverá sempre o responsável pela proteção de dados da UIP do Estado-Membro ser informado sobre as transferências de dados de PNR, sejam as que ocorrem entre Estados-Membros, sejam as destinadas a países terceiros, bem como as que são transferidas de países terceiros a outros interessados.

No caso específico dos Estados-Membros da UE, as transferências devem observar o Capítulo V do Regulamento de Dados Pessoais, que trata das transferências de dados pessoais para países terceiros ou organizações internacionais. De acordo com este capítulo, as transferências devem ter por base uma decisão de adequação, que constate o nível de proteção dos dados enviados, ou poderá ser sujeita a outras garantias consideradas adequadas, nomeadamente um instrumento juridicamente vinculativo e com força executiva, entre outras garantias citadas no n.º 2 do art. 46.º.

O Regulamento de Proteção de Dados também chama atenção para o consentimento necessário ao tratamento de dados de crianças. Contudo, a questão securitária parece ainda prevalecer e o consentimento expresso

parece sucumbir à obrigação de que todos os dados de PNR nas rotas indicadas na Diretiva devem ser enviados às UIP's.

Importa ainda indicar que no Plano de Implementação da Diretiva[19], sobre a transposição da Diretiva UE-PNR, prevê-se que um dos desafios na implementação das normas relativas à transferência de dados de PNR é a experiência seja dos Estados-Membros, seja de Estados-terceiros, no que toca aos recursos, tempo e complexidade técnica para adaptação dos sistemas de PNR. Por isso, além da própria transferência, há dificuldades relativas à introdução e ao uso dos sistemas pelas autoridades responsáveis.

Outro artigo da Diretiva UE-PNR que merece destaque é o 12.º, designadamente o prazo de conservação e anonimização dos dados do PNR. As UIP's dos Estados-Membros devem conservar nas suas bases de dados as informações recebidas das companhias aéreas por um prazo máximo de cinco anos, a contar da data em que a transferência foi recebida pela UIP. No entanto, seis meses após o recebimento dos dados de PNR, esses deverão ser anonimizados, através do mascarar de algumas das informações constantes nos dados recebidos, tais como: nome, morada, contactos, forma e dados de pagamentos, número de passageiro frequente, eventuais dados de API e observações que permitam identificar o passageiro.

Tenha-se em mente que não é totalmente vedado o acesso às informações integrais do PNR após o decurso dos seis meses, mas para tanto será necessária uma motivação razoável, bem como uma autorização, que poderá ser emitida por autoridade judiciária ou por outra autoridade nacional competente. Neste último caso, também será obrigatório informar o responsável de proteção de dados sobre o referido acesso, a fim de que este possa realizar uma verificação *ex post* da situação.

Decorridos os cinco anos, as informações do PNR deverão ser apagadas definitivamente do banco de dados das UIP's.

Sublinhe-se novamente o art. 13.º, que liga expressamente a Diretiva UE-PNR ao Regulamento de Proteção de Dados Pessoais, referindo a obrigação dos Estados-Membros em assegurar a igualdade no tratamento de dados de todos os passageiros, assim como os direitos advindos do uso de tais dados, tal como a proteção dos dados pessoais, o acesso, a retificação, apagamento e limitação. Este artigo estabelece que fica a cargo também

[19] Commission Staff Working Document SWD (2016) 426 final, de 28 de novembro de 2016.

dos Estados-Membros estabelecer uma autoridade nacional de controlo que terá como responsabilidade aconselhar e monitorar a aplicação das normas nacionais provenientes da Diretiva UE-PNR. Caberá a esta autoridade, nos termos do n.º 3 do art. 15.º, as seguintes funções, entre outras: analisar as reclamações apresentadas por qualquer titular de dados, verificar a legalidade no tratamento dos dados e proceder a auditorias, nos termos nas legislações nacionais.

O que não parece claro é quais serão os meios a utilizar para garantir os tais níveis de segurança adequados aquando das transferências de dados de PNR, em especial para países terceiros. VanWasshnova[20] aborda esta questão quando compara os conflitos que emergem em matéria de proteção de entre os Estados Unidos e a União Europeia. Destaca o autor que enquanto a UE tenta limitar a quantidade de informações a serem transmitidas a fim de garantir a proteção dos dados pessoais, os EUA requerem uma transferência irrestrita. No entanto, a limitação da informação recebida pela UE e pelos seus Estados-Membros não garante a proteção completa destes dados, muito menos a criação de perfis, visto que apenas o nome de um passageiro e o trajeto de sua viagem poderão implicar, por si sós, em um perfil, indo de encontro ao estabelecido no art. 22.º do Regulamento de Proteção de Dados.

Nesta mesma perspetiva, Gavin Robinson[21] critica o uso de dados do PNR para os fins supra identificados, pois permitem criar perfis e aplicar processos de *data mining*, que não identificam criminosos ou terroristas, mas apenas antecipam possíveis ações criminosas, que podem não ter relação com o terrorismo ou a criminalidade grave. No que se refere ao equilíbrio entre privacidade e segurança, Georgio Nouskalis[22] chama a atenção para

---

[20] Vanwasshnova, Mattheew R. "Data Protection Conflicts between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange", *Case Western Reserve Journal of International Law (JIL),* vol. 39, 2008, p. 827.

[21] Robinson, Gavin. "Data protection reform, passenger name record and telecommunications data retention: – Mass Surveillance Measures in the E. U. and the Need for a Comprehensive Legal Framework", *Critical Quarterly for Legislation and Law/Revue critique trimestrielle de jurisprudence et de législation,* vol. 95, n.º 4, 2012, pp. 394-416.

[22] Nouskalis, Georgio. "Biometrics, e-identity, and the balance between security and privacy: case study of the passenger name record (PNR) system", *ScientificWorldJournal*, n.º 11, 2011 march 1, pp. 474-477.

a mitigação do princípio da presunção de inocência, analisando o facto de que a partir da Diretiva UE-PNR a maioria das pessoas poderia ser considerada suspeita de crimes, o que permitirá um contínuo Estado de Exceção, cujo fundamento seria a luta contra o terrorismo.

Soma-se à questão do uso de dados de PNR como método de prevenção do terrorismo e da criminalidade grave outro problema: e quando uma pessoa tem os seus dados pessoais utilizados para a compra de bilhetes sem a sua autorização prévia, como nos casos de fraudes a cartões de crédito ou *hacking*? Domingues & Al.[23], apresentaram um estudo sobre o Sistema de Distribuição Global (GDS – *Global Distribution System*), uma plataforma bastante avançada para criação e gestão de reservas de viagem, ambiente em que se criam os PNR's. Os autores afirmam que, mesmo diante dos avanços referentes aos sistemas de segurança e informação, ainda hoje a plataforma GDS não está imune a ações fraudulentas, que buscam obter informações indevida ou mesmo alterar informações constantes no sistema.

Por fim, deve-se ter em conta não apenas os aspetos relativos ao Estado e aos titulares dos dados, mas também o impacto que a Diretiva em análise terá na prática laboral das companhias aéreas, sendo este tópico analisado de seguida.

3. As companhias aéreas e a transferência de dados dos passageiros: o que mudará na prática?

Nos termos do art. 3.º da Diretiva UE-PNR, transportadora aérea é "uma empresa de transporte aéreo titular de uma licença de exploração válida ou equivalente que lhe permite transportar passageiros por via aérea".

No mercado da aviação civil, todavia, nem sempre a transportadora aérea é a companhia responsável pela venda do bilhete. A transportadora é aquela responsável pelo cumprimento do objeto do contrato de transporte, ou seja, a viagem. No entanto, por uma questão comercial, as companhias

---

[23] Domingues, Rémi *et al*. An application of unsupervised fraud detection to Passenger Name Records", *46th Annual Conference IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, 2016. Disponível em: <http://www.eurecom.fr/fr/publication/5058/download/data-publi-5058.pdf> (acedido a 28/11/2017).

unem-se e fazem contratos entre si, que podem ser bilaterais ou em aliança com diversas transportadoras. Assim, uma companhia aérea poderá vender um bilhete cujo voo não operará por si mesma ou com a sua tripulação, sendo o agente comercial de venda do transporte aéreo, por isso é nomeada de *Market Carrier.*

Esta explanação serve para indicar que a companhia aérea que vender o bilhete deverá ser a responsável por obter todos os dados pessoais do passageiro, visto que, mesmo não operando o voo, será aquela que criará o PNR no sistema, sendo a detentora das informações até ao embarque. No entanto, nos termos do art. 8.º da Diretiva, caberá à companhia que opera o voo informar os dados que constam do Anexo II. Tal informação poderá ser feita até o momento do *check-in*, mas não se pode deixar de assinalar que a possibilidade de atuar preventivamente para detetar eventuais criminosos poderá ser comprometida, tendo em consideração que o registo para embarque poderá ser feito alguns minutos antes do voo, diretamente no aeroporto.

Assim, será na transposição das regras europeias para as legislações nacionais que se poderá verificar o momento exato em que a obrigação de informar os dados de PNR deverão ser realizadas pelas companhias operadoras, devendo o legislador nacional ter conta os óbices técnicos e temporais para que as informações sejam enviadas em tempo útil. Isto especialmente na expectativa de que os dados do PNR serão efetivamente utilizados para prevenir o terrorismo e a criminalidade grave, evitando ferir e/ou denegrir a reputação de indivíduos por uma avaliação rápida e destoante da realidade das verdadeiras intenções de uma viagem.

Neste contexto, a Diretiva traçou prazos mais exatos para evitar diferenças temporais consideráveis referentes à obrigação de transmissão dos dados dos passageiros. Nos termos do n.º 3 do art. 8.º, as transportadoras transferem os dados do PNR, sob "um nível adequado de segurança": a) 24 a 48 horas antes da hora programada da partida do voo; e b) imediatamente após o encerramento do voo. Entretanto, nos termos do direito nacional, as companhias aéreas poderão enviar informações de dados de PNR noutro momento e não apenas as especificadas anteriormente, "caso a caso e mediante pedido apresentado por uma UIP".

Importa verificar ainda, neste momento anterior à data limite para a transposição, que nos termos do art. 7.º, os Estados-Membros devem adotar

uma lista na qual designarão quais as autoridades habilitadas a solicitar das UIP's e receber destas informações sobre os dados de PNR ou os resultados advindos do tratamento dos mesmos. Assim, as companhias aéreas deixam de ter a obrigação de fornecer diretamente às autoridades competentes as informações necessárias a fundamentar um procedimento policial ou investigatório. A obrigação subjaz, portanto, em transmitir os dados de PNR à UIP, que será a responsável por analisar e conservar os dados, atuando como base das informações relativas aos passageiros.

Deve-se salientar, no entanto, que tal obrigação não prejudica a competência das autoridades policiais e judiciárias, designadamente de atuação face a indícios de outras infrações, que não o terrorismo e a criminalidade grave.

Outra questão que se deve ter em atenção é a existência de, até ao momento, seis tipos diferentes de programas de reservas, sendo alguns incompatíveis entre si. Nos aeroportos, os computadores costumam funcionar com um programa universal que tenta convergir as informações dos passageiros. Contudo, a criação de vários departamentos com diversas pessoas a utilizar este mecanismo é um investimento vultuoso para as companhias aéreas. Tendo em consideração este alto investimento e procurando evitar o incumprimento das companhias sob esta fundamentação, a Diretiva, de acordo com enunciado no n.º 1 do art. 8.º, prevê que os Estados-Membros devem adotar as medidas consideradas necessárias para que as companhias sejam capazes de transferir pelo método de exportação os dados do PNR às UIP's e, em combinação com o previsto no Considerando n.º 14, os Estados-Membros deverão suportar os custos da utilização, conservação e do intercâmbio de dados de PNR.

Relativamente à transferência de dados para as UIP's, merece também destaque que os voos que incluam escalas na sua rota obrigam as companhias aéreas a transferir os dados de todos os passageiros a todas as UIP's dos Estados-Membros por onde o passageiro passará. O mesmo será aplicável aos voos intra-UE, no caso dos Estados-Membros que exigirão também receber informações referentes a este tipo de viagem.

Diga-se também que as sanções relativas a não ou má-aplicação das regras nacionais, após transposta a Diretiva UE-PNR, serão estabelecidas pelos Estados-Membros, que também se obrigam a assegurar a aplicação das normas. Conforme estabelecido no texto do art. 14.º, "as sanções previstas devem ser efetivas, proporcionadas e dissuasivas".

Relativamente a este ponto, a Associação das Companhias Aéreas Regionais Europeias[24] esclareceu, por meio de um comunicado, que os dados de API e de PNR estão localizados em diferentes sistemas. Por esta razão, a exportação desses dados pode demorar de 3 a 6 meses para um pedido das informações de um API, e de 6 a 12 meses transferência de um PNR. Portanto, além dos custos associados, a rapidez não é apenas uma questão de vontade ou não em aplicar as normas, mas também do desenvolvimento tecnológico que vá ao encontro das expectativas criadas relativas aos sistemas de reserva de viagens.

Avizinham-se outras questões técnicas e económicas ligadas às transferências de dados de PNR após as transposições. A título de ilustração, podem-se citar eventuais falhas nas transferências dos dados, ocasionando a chegada de informações incompletos à UIP, bem como a fechamento ou falência de companhias aéreas de pequeno porte que não consigam arcar com o investimento tecnológico e humano para transferir dados de PNR para a UIP. Uma nova análise sobre o impacto à prática laboral das companhias aéreas será certamente um tópico que importará uma nova análise no futuro.

Considerações Finais

A escolha dos dados PNR's transferidos, em detrimento dos API, já demonstra a quantidade de informação que se pode aferir a partir desses dados. Contudo, é verdade também que a transferência das informações de PNR obtidas pelas companhias aéreas não garante que tais dados sejam corretos e idóneos.

Destacam-se, portanto, duas questões que foram debatidas no presente texto: a capacidade de identificar e prevenir terroristas, sem que tal constitua uma discriminação de grupos ou indivíduos; e a garantia do tratamento adequado dos dados, seja pela companhia, seja pelos Estados-Membros, seja ainda pelos países terceiros.

---

[24] ERA, European Regions Airlines Association, API-PNR, de 14 de dezembro de 2016. Disponível em: <http://www.eraa.org/policy/security/advance-passenger-information-api--and-passenger-notifications-records-pnr> (acedido a 3/12/2017).

A possibilidade de que inocentes sejam identificados erroneamente como eventuais criminosos ou terroristas é um facto já reconhecido pela Diretiva UE-PNR, bem como a abertura a que outros Estados requeiram reciprocidade no tratamento de dados. No entanto, o que ainda não é evidente é se a transposição e a aplicação das normas contidas na Diretiva em análise serão realizadas em conformidade e respeito pelo Regulamento de Proteção de Dados, que se coaduna com as normas de direitos fundamentais referidas ulteriormente.

A certeza, por agora, é que as companhias aéreas poderão incorrer diversas vezes em sanções, de carácter primordialmente pecuniário, para que cumpram normas que, até ao momento, não se sabe se serão transpostas a tempo e com a mesma ordem que foi estabelecida pelo ato legislativo europeu, a Diretiva UE-PNR.

Ademais, a validade da Diretiva poderá ser objeto de apreciação pelo Tribunal de Justiça da União Europeia, o qual já se pronunciou anteriormente, aquando da análise da Diretiva de Retenção de Dados[25], que a prevenção ao terrorismo não seria suficiente para mitigar a proteção e a inviolabilidade dos dados pessoais. Destaca-se ainda que, em 26 de julho 2017, o TJ proferiu parecer[26] no sentido de considerar a incompatibilidade do acordo entre o Canadá e a UE, sobre a transferência e o tratamento dos dados dos registos de identificação dos passageiros, com os arts 7.º, 8.º, 21.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia "na medida em que não exclui a transferência de dados sensíveis da União Europeia para o Canadá nem a utilização e a conservação desses dados".

Por fim, apesar de a data limite para a transposição da Diretiva UE-PNR aos direitos nacionais ser 25 de maio de 2018, pouco debate sobre o tema tem ocorrido nos meios sociais e comerciais. Contudo, é percetível a relevante preocupação nestes meios no que toca ao Regulamento de Proteção de Dados, que será aplicável a partir da mesma data limite para a transposição da Diretiva UE-PNR.

---

[25] Acórdão do TJ, C-293/12, *Digital Rights Ireland*, de 8 de abril de 2014 e processos apensos C-293/12 e C-594/12.

[26] Acórdão do TJ, 2017/C 309/03, "Projeto de acordo entre o Canadá e a União Europeia", Parecer 1/15 (Grande Secção), de 26 de julho 2017.