

## I

(Resoluções, recomendações e pareceres)

## PARECERES

## AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

**Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de decisão do Conselho relativa à conclusão do Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Protecção das Fronteiras australiano**

(2011/C 322/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os artigos 7.º e 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados <sup>(1)</sup>,

Tendo em conta o artigo 41.º, n.º 2, do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados <sup>(2)</sup>,

ADOPTOU O SEGUINTE PARECER

### 1. INTRODUÇÃO

#### 1.1. Consulta da AEPD

1. Em 19 de Maio de 2011, a Comissão adoptou a proposta relativa à conclusão do Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas trans-

portadoras aéreas para o Serviço Aduaneiro e de Protecção das Fronteiras australiano <sup>(3)</sup>. A proposta foi enviada à AEPD no dia 23 de Maio.

2. A AEPD foi consultada informalmente, em Maio de 2011, no contexto de um procedimento acelerado, sobre a proposta relativa ao Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados PNR.
3. Considerando que as suas observações se mantêm válidas no que diz respeito à substância da proposta adoptada pela Comissão e apresentada ao Conselho e ao Parlamento, a AEPD decidiu divulgar mais amplamente as suas observações sob a forma de um parecer público. Deste modo, as observações poderão ser integradas nos futuros debates sobre a proposta.
4. A AEPD aproveita esta oportunidade para levantar mais algumas questões e incentiva o Conselho e o Parlamento a terem estes pontos de vista em conta quando deliberarem sobre a proposta nos termos do artigo 218.º do TFUE.

#### 1.2. Contexto da proposta

5. O Acordo entre a UE e a Austrália sobre os dados PNR constitui um passo em frente na agenda da UE, que inclui o estabelecimento de directrizes PNR globais, a criação de um sistema PNR da UE e a negociação de acordos com países terceiros <sup>(4)</sup>.

<sup>(1)</sup> JO L 281 de 23.11.1995, p. 31.

<sup>(2)</sup> JO L 8 de 12.1.2001, p. 1.

<sup>(3)</sup> COM(2011) 281 final.

<sup>(4)</sup> Ver, em particular, a Comunicação da Comissão, de 21 de Setembro de 2010, sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros, COM(2010) 492 final.

6. A AEPD tem acompanhado atentamente a evolução relativa ao PNR e adoptou recentemente dois pareceres sobre o «pacote PNR» da Comissão e sobre a proposta de directiva relativa ao PNR da UE <sup>(1)</sup>. As opiniões expressas pela AEPD sobre os sistemas PNR complementam e correspondem, em grande medida, às do Grupo de Trabalho do artigo 29.º <sup>(2)</sup>, mas também às de outros documentos recentes, incluindo o Parecer do Comité Económico e Social Europeu <sup>(3)</sup> e o Parecer da Agência dos Direitos Fundamentais da União Europeia <sup>(4)</sup>.
7. Como é a seguir explicado, a AEPD sempre adoptou a abordagem coerente de confrontar a finalidade dos sistemas PNR com os requisitos fundamentais de necessidade e proporcionalidade, e analisar, numa segunda fase, os elementos respeitantes às disposições a fim de sugerir melhorias, se fosse caso disso.

### 1.3. Observação preliminar

8. A AEPD congratula-se com a abordagem geral que procura harmonizar as garantias de protecção de dados nos vários acordos PNR com países terceiros. Ainda é, todavia, necessário formular algumas observações.
9. Uma observação constantemente reiterada nos pareceres da AEPD e nos pareceres do Grupo de Trabalho do artigo 29.º é igualmente aplicável à proposta relativa ao PNR australiano: a necessidade e a proporcionalidade dos sistemas PNR têm de ser demonstradas.
10. Estes dois requisitos fundamentais são aspectos essenciais da legislação em matéria de protecção de dados, nos termos

<sup>(1)</sup> — Parecer da AEPD, de 25 de Março de 2011, sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave;

— Parecer da AEPD, de 19 de Outubro de 2010, sobre a abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros.

Os dois pareceres estão disponíveis no endereço Internet: <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation>

<sup>(2)</sup> Parecer 10/2011 do Grupo de Trabalho do artigo 29.º, de 5 de Abril de 2011, sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave: [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm)

<sup>(3)</sup> Parecer do Comité Económico e Social Europeu, de 5 de Maio de 2011, sobre a «proposta de directiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave», COM(2011) 32 final.

<sup>(4)</sup> *Opinion of the European Union Agency for Fundamental Rights of 14 June 2011 on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime* [COM(2011) 32 final] [Parecer da Agência dos Direitos Fundamentais da União Europeia, de 14 de Junho de 2011, sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave [COM(2011) 32 final]].

dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais e do artigo 16.º do TFUE. A União Europeia deve garantir que os requisitos dessa legislação também são cumpridos nos casos em que são tratados e transferidos dados de cidadãos europeus do território da UE para o território de um país terceiro. Nesses casos, a necessidade e a proporcionalidade devem ser avaliadas e demonstradas, antes de se poder assinar qualquer acordo. Complementarmente aos elementos que justificam a necessidade do sistema PNR, a proporcionalidade exige um equilíbrio adequado entre a finalidade prosseguida e o tratamento de quantidades enormes de dados que implique uma invasão grave da vida privada das pessoas.

11. No caso dos sistemas PNR, a finalidade é combater o terrorismo e a criminalidade (transnacional) grave, utilizando a recolha de quantidades maciças de dados relativos a todos os passageiros para realizar uma avaliação dos riscos referente a esses passageiros. Até agora, a AEPD não considerou existirem elementos convincentes nas justificações apresentadas para os sistemas PNR existentes ou previstos, como o sistema PNR da UE que analisou em pormenor no seu parecer de Março de 2011 <sup>(5)</sup>.

12. Além disso, ainda que a necessidade seja demonstrada, a AEPD sublinha que é necessário preencher o critério da proporcionalidade. Questiona, assim, o equilíbrio entre o tratamento de dados pessoais em larga escala e a finalidade prosseguida, sobretudo tendo em conta a diversidade de crimes incluídos no âmbito de aplicação do projecto de acordo. Tem em conta que há outros instrumentos eficazes disponíveis para combater o terrorismo e a criminalidade grave.

13. As observações específicas a seguir apresentadas não prejudicam esta observação preliminar e fundamental. A AEPD congratula-se com as disposições que prevêm garantias específicas, como as relativas à segurança dos dados, à aplicação da lei e à fiscalização, bem como as relativas às transferências ulteriores. Simultaneamente, manifesta preocupação, adicionalmente à questão da necessidade e da proporcionalidade do sistema, a respeito do âmbito das definições e das condições de conservação dos dados.

## 2. ANÁLISE DA PROPOSTA

### 2.1. Base jurídica

14. A AEPD observa que o acordo se baseia no artigo 82.º, n.º 1, alínea d), no artigo 87.º, n.º 2, alínea a), e no artigo 218.º, n.º 6, alínea a), do Tratado sobre o Funcionamento da União Europeia. Recorda que entre os elementos objectivos a considerar na escolha da base jurídica figuram, designadamente, a finalidade e o conteúdo do

<sup>(5)</sup> Parecer da AEPD, de 25 de Março de 2011, sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave; ver também o parecer do Grupo de Trabalho do artigo 29.º, mencionado *supra*.

- acto<sup>(1)</sup>. Se a análise de um acto da UE revelar que ele prossegue uma dupla finalidade ou que tem uma dupla componente e se uma destas for identificável como principal ou preponderante, enquanto a outra é apenas acessória, o acto deve ter por base um único fundamento jurídico, nomeadamente o que for exigido pela finalidade ou componente principal ou preponderante<sup>(2)</sup>. Excepcionalmente, quando se provar que o acto prossegue ao mesmo tempo vários objectivos, que se encontram ligados de forma indissociável, sem que um seja secundário e indirecto relativamente ao outro, esse acto pode assentar nos fundamentos jurídicos correspondentes<sup>(3)</sup>.
15. No contexto da jurisprudência assente, tal como foi sucintamente resumida, e para além do artigo 218.º, n.º 6, alínea a), a AEPD defende que o acordo não deverá ser baseado no artigo 82.º, n.º 1, alínea d), e no artigo 87.º, n.º 2, alínea a), mas sim no artigo 16.º do TFUE.
16. No que respeita à finalidade, importa recordar que os acordos PNR que a UE está a negociar foram todos suscitados pela necessidade de conciliar a obrigação que as transportadoras aéreas têm de fornecer dados PNR a autoridades de países terceiros com o direito fundamental à protecção de dados<sup>(4)</sup>. Além disso, o texto da proposta refere-se por diversas vezes à finalidade da protecção de dados pessoais<sup>(5)</sup>.
17. Quanto ao conteúdo, o predomínio das disposições relativas à protecção de dados é evidente no acordo. Para além
- dos artigos 3.º, 4.º e 6.º, a protecção de dados parece estar presente em quase todas as suas disposições. Ela está presente no artigo 1.º (objectivo), no artigo 2.º (definições), no artigo 5.º (adequação) e nos artigos 7.º a 19.º (garantias aplicáveis ao tratamento de dados PNR).
18. Quanto às cláusulas relativas às garantias (artigos 7.º a 19.º), importa notar que contêm disposições características da legislação em matéria de protecção de dados<sup>(6)</sup>. O facto de um acto conter disposições que pertencem caracteristicamente a um domínio jurídico específico foi considerado pelo Tribunal como um elemento justificativo de um fundamento jurídico específico<sup>(7)</sup>.
19. Em suma, a AEPD considera que o acordo tem a finalidade, não de melhorar a cooperação policial, mas sim de mandar e autorizar a transferência de dados pessoais por operadores privados face ao pedido de um país terceiro. Embora essa transferência não fosse, em princípio, possível segundo as regras da UE, o acordo PNR visa permitir a transferência de dados pessoais em conformidade com os requisitos de protecção de dados da União através da adopção de garantias específicas.
20. Por estes motivos, a AEPD considera que o acordo deverá ser baseado — em todo o caso, principalmente — no artigo 16.º do TFUE<sup>(8)</sup>.

## 2.2. Finalidade e definições

21. A AEPD constata que os fins para os quais os dados PNR podem ser tratados são definidos de forma precisa no artigo 3.º da proposta. Lamenta, todavia, que as actuais definições sejam mais amplas do que as da proposta de directiva relativa ao PNR da UE, cujo âmbito já deveria ter sido, ele próprio, restringido, sobretudo no que respeita às infracções menores.
22. Embora as definições da proposta relativa ao PNR da UE tenham em conta as consequências das actividades definidas como «terroristas», como os danos concretos causados a pessoas ou a poderes públicos (morte, ofensas graves à integridade física, destruição dos sistemas de transporte, de infra-estruturas, etc.), a presente proposta é menos específica e mais orientada para os objectivos quando se refere a intimidar as pessoas e a coagir os poderes públicos, ou a desestabilizar gravemente as estruturas políticas ou económicas fundamentais.

(1) Processo C-491/01, *British American tobacco*, em especial os n.ºs 92-93.

(2) Processo C-42/97, *Parlamento Europeu contra Conselho da União Europeia*, n.ºs 39 e 40.

(3) Ver, neste sentido, o Processo C-491/01, *British American tobacco*, n.ºs 92-93 [n.º 94], Processo C-42/97, *Parlamento Europeu contra Conselho da União Europeia*, n.º 38.

(4) Esta necessidade é reconhecida pelo Tribunal na parte relativa aos factos dos acórdãos PNR, processos apensos C-317/04 e C-318/04, n.º 33.

(5) — A exposição de motivos reconhece que a legislação da UE em matéria de protecção de dados não autoriza que as transportadoras aéreas transmitam os dados PNR para países terceiros que não assegurem um nível de protecção adequado. Por conseguinte, é «necessária uma solução que forneça a base jurídica para a transferência [...] a fim de assegurar [...] o respeito do direito dos indivíduos à protecção dos dados pessoais».

— O objectivo de assegurar o respeito do direito à protecção dos dados pessoais também surge muito claramente no preâmbulo, nomeadamente do considerando que cita o artigo 6.º do Tratado da União Europeia, o artigo 16.º do Tratado sobre o Funcionamento da União Europeia, o artigo 8.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades fundamentais, a Convenção 108.º do Conselho da Europa, etc.

— O preâmbulo também cita as disposições pertinentes em matéria de protecção de dados da legislação australiana, reconhecendo que prevêem a protecção dos dados, direitos de acesso e de reparação, de correcção e de anotação, bem como de recurso e sanções contra a utilização abusiva dos dados pessoais.

— O artigo 1.º do Acordo — intitulado «Objectivo do Acordo» — dispõe que o acordo prevê a transferência de dados PNR. Acrescenta que «estabelece as condições de transferência e utilização desses dados e as respectivas modalidades de protecção» (italico acrescentado).

(6) Como as disposições relativas aos dados sensíveis, à segurança dos dados, à responsabilização, à transparência, ao direito de acesso, de rectificação e de supressão, ao direito de recurso, ao tratamento automático, etc.

(7) Parecer 2/2000, Protocolo de Cartagena, n.º 33.

(8) Neste contexto, importa referir também a Declaração 21 «sobre a protecção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial», anexada ao Tratado de Lisboa. A redacção clara da Declaração 21 confirma que, mesmo nos casos em que existam elementos de cooperação policial, um instrumento de protecção de dados neste domínio continuará a ser baseado no artigo 16.º do TFUE (se necessário, em conjunto com outras disposições). Esta análise em nada prejudicaria a repartição de competências a nível da Comissão Europeia.

23. A AEPD considera que é necessário usar de maior precisão em relação aos conceitos de «intimidar, constranger e coagir», bem como aos de «estruturas políticas, constitucionais, económicas, ou (sobretudo) sociais fundamentais de um país ou de uma organização internacional». Impedir-se-ia, desta forma, a aplicação do sistema PNR em casos para os quais ele não deve estar, de qualquer modo, direccionado, como as actividades legítimas (por exemplo, manifestações pacíficas) exercidas num contexto social, cultural ou político <sup>(1)</sup>.
24. A possibilidade de tratamento dos dados noutros casos excepcionais suscita questões adicionais, em especial por se alargar à «ameaça para a saúde». A AEPD considera que esse alargamento da finalidade é desproporcionado, sobretudo tendo em conta que podem estar disponíveis procedimentos alternativos e mais específicos para fazer face a ameaças importantes para a saúde, sempre que necessário e numa base casuística. Além disso, os dados PNR não constituem a ferramenta mais adequada para identificar os passageiros: na verdade, existem dados mais fiáveis, designadamente os dados API.
25. A AEPD faz notar ainda que a lista de dados PNR anexada à proposta ultrapassa o que as autoridades responsáveis pela protecção de dados consideraram ser proporcionado nos pareceres do Grupo de Trabalho do artigo 29.º <sup>(2)</sup>. Essa lista deve ser reduzida. Designadamente, a inclusão do domínio «Observações gerais», que pode conter dados irrelevantes — e potencialmente sensíveis — não se justifica e deve ser suprimida.

### 2.3. Dados sensíveis

26. A AEPD congratula-se com a exclusão do tratamento de dados sensíveis do âmbito de aplicação, como dispõe o artigo 8.º da proposta. No entanto, a forma como esta disposição está redigida ainda sugere que os dados sensíveis podem ser «tratados». Esse artigo permite que estes dados sejam enviados, numa primeira fase, pelas transportadoras aéreas e, depois, suprimidos pelas autoridades públicas, numa segunda fase. O envio pelas transportadoras aéreas é um acto de tratamento. A AEPD considera que as transportadoras aéreas deveriam ser obrigadas a filtrar e apagar os dados sensíveis na origem do tratamento.

### 2.4. Segurança dos dados

27. A proposta inclui, no artigo 9.º, uma disposição global relativa à segurança e integridade dos dados, o que é positivo. A AEPD apoia, em especial, a obrigação de comunicar as violações da segurança ao gabinete do Comissário para a protecção de dados e informação australiano. No que respeita à comunicação subsequente dessa informação à Comissão Europeia, será necessário explicar melhor o procedimento a seguir. Além disso, a AEPD considera que as autoridades responsáveis pela protecção de dados também

são destinatárias relevantes deste tipo de informações e deveriam ser explicitamente mencionadas na proposta.

### 2.5. Supervisão e aplicação da lei

28. O sistema de supervisão, incluindo as medidas de fiscalização e responsabilização e a insistência na ausência de discriminação baseada na nacionalidade ou no lugar de residência, é bem-vindo. A AEPD também apoia fortemente o direito fundamental de cada indivíduo à possibilidade de recurso administrativo e a uma protecção judicial eficaz. Considera que a função desempenhada pelo gabinete do Comissário para a protecção de dados e informação australiano constitui uma garantia importante no que respeita às possibilidades de recurso e ao exercício dos direitos das pessoas em causa.

### 2.6. Decisões individuais automatizadas

29. Segundo o artigo 15.º, interpretado *a contrario*, uma decisão automatizada que não seja susceptível de produzir «efeitos jurídicos adversos para um passageiro ou afectá-lo gravemente» pode ser tomada com base no tratamento automático de dados. As garantias só são aplicáveis quando a decisão possa afectar gravemente o passageiro. Considerando o vasto âmbito do tratamento automático de dados pessoais previsto no sistema PNR, esta restrição é questionável no entender da AEPD. Para evitar uma interpretação flexível desta disposição, recomenda, por isso, que o termo «gravemente» seja suprimido e que se garanta a proibição total de qualquer decisão automatizada que possa ter efeitos adversos numa pessoa.

### 2.7. Conservação de dados

30. A AEPD considera que a duração do período de conservação de dados prevista no artigo 16.º é uma das principais dificuldades da proposta. Um período de conservação de cinco anos e meio, incluindo três anos sem qualquer ocultação dos dados, é claramente desproporcionado, sobretudo se este período de conservação for comparado com o anterior sistema PNR australiano, que não previa o armazenamento dos dados excepto numa base casuística <sup>(3)</sup>. A razão por que é agora previsto um período de conservação tão longo, que não foi considerado necessário no primeiro sistema PNR australiano, deverá ser explicada e devidamente justificada.
31. De acordo com a posição defendida no seu parecer sobre a proposta de directiva relativa a um PNR da UE, a AEPD considera que se deve proceder à anonimização completa (isto é, irreversível) de todos os dados, se não imediatamente após a análise, no máximo 30 dias depois.

<sup>(1)</sup> Neste aspecto, por exemplo, o direito fundamental à liberdade de reunião (artigo 12.º da Carta dos Direitos Fundamentais) não deve ser comprometido por uma formulação excessivamente lata.

<sup>(2)</sup> Parecer de 23 de Junho de 2003 sobre o nível de protecção assegurado nos Estados Unidos para a transferência de dados dos passageiros, WP78.

<sup>(3)</sup> Ver, a este respeito, o parecer favorável do Grupo de Trabalho do artigo 29.º: Parecer 1/2004, de 16 de Janeiro de 2004, «sobre o nível de protecção conferido pela Austrália à transmissão de dados dos passageiros contidos no *Passenger Name Record* (PNR) das companhias aéreas», WP85. O parecer tem em conta o facto de que «(...) as alfândegas aplicam uma política geral de não-conservação destes dados. Em relação aos 0,05 % a 0,1 % dos passageiros seleccionados para exame complementar pelas alfândegas, os dados dos PNR das companhias aéreas são temporariamente conservados, mas não armazenados, até à decisão tomada na fronteira. Após esta decisão, os dados dos PNR são apagados do computador do funcionário da PAU das alfândegas, não sendo introduzidos nas bases de dados australianas».

## 2.8. Transferências ulteriores

32. As garantias fornecidas nos artigos 18.º e 19.º são bem-vindas, nomeadamente porque estabelecem uma lista de destinatários dos dados transferidos na Austrália, além de preverem que as transferências sejam efectuadas numa base casuística e que a sua necessidade seja avaliada em todos os casos. A AEPD observa, todavia, que esta disposição pode ser contornada pela derrogação prevista no artigo 18.º, n.º 1, alínea c), que permite a partilha de dados tornados anónimos, mesmo que não seja numa base casuística. Contudo, o acto de tornar os dados anónimos não implica o apagamento dos elementos identificativos que permitem aceder aos dados completos quando isso é necessário, mas apenas a sua ocultação, continuando a ser possível um acesso total aos dados. Por este motivo, a AEPD recomenda que não seja permitida qualquer derrogação ao princípio das transferências «caso a caso». A título de garantia adicional, a AEPD sugere que as transferências sejam limitadas às autoridades que têm a função de «combater o terrorismo e a criminalidade transnacional», em lugar das autoridades «cujas funções estejam directamente relacionadas com a prevenção» dessa criminalidade.
33. A AEPD concorda que as transferências para países terceiros estejam sujeitas à condição de fornecerem as «mesmas» garantias que o acordo inicial. Considerando, todavia, que as novas transferências implicam uma perda de controlo sobre a forma como os dados podem ser tratados, e na ausência de um acordo internacional que garanta que os novos destinatários aplicam eficazmente as ditas garantias, a AEPD sugere, além disso, que essas transferências estejam sujeitas a uma autorização judicial prévia.
34. A proposta prevê que, sempre que o Serviço Aduaneiro e de Protecção das Fronteiras australiano tiver conhecimento de que os dados de um residente de um Estado-Membro da UE são objecto de transferência para um país terceiro, o Estado-Membro em causa deve ser informado dessa situação [artigo 19.º, n.º 1, alínea f)]. A AEPD considera que devem ser incluídos outros elementos que expliquem a finalidade de uma tal transmissão para um Estado-Membro. Caso a transmissão de informações afecte a pessoa em causa, devem ser incluídas justificações e garantias adicionais.
35. Por último, no que respeita às transferências dentro da Austrália e para países terceiros, tanto o artigo 18.º como o artigo 19.º prevêem uma disposição geral segundo a qual nenhuma disposição deve obstar à divulgação de dados PNR sempre que necessário para efeitos da aplicação do artigo 3.º, n.º 4<sup>(1)</sup>, por outras palavras, caso existam circunstâncias excepcionais e se trate de proteger os interesses vitais de uma pessoa, incluindo o risco de ameaça para a saúde. A AEPD já questionou o risco de uma interpretação lata desta derrogação. Além disso, não entende por que razão uma transferência em circunstâncias excep-

cionais não há-de estar sujeita às garantias previstas no artigo 18.º e no artigo 19.º, sobretudo no que respeita à limitação da finalidade ou à minimização de dados, bem como à protecção da identidade dos destinatários e ao nível de protecção concedida aos dados pessoais.

## 2.9. Transferências efectuadas pelas transportadoras aéreas

36. Nos termos do artigo 21.º, n.º 3, as transferências de dados PNR para as autoridades podem ter lugar mais de cinco vezes por voo em circunstâncias excepcionais, caso exista uma ameaça específica. Para aumentar a segurança jurídica, as condições dessas transferências adicionais devem ser explicitadas de forma mais pormenorizada e incluir, nomeadamente, o requisito adicional da existência de uma ameaça imediata.

## 2.10. Revisão do acordo

37. A AEPD considera que as condições da revisão devem ser descritas de forma mais pormenorizada em relação a vários aspectos. A frequência das revisões, após a revisão inicial deve ser especificada. Além disso, as autoridades responsáveis pela protecção de dados devem ser explicitamente incluídas na equipa encarregada da revisão, e não apenas de forma condicional.
38. A AEPD sugere que a revisão se concentre também na avaliação da necessidade e da proporcionalidade das medidas, recolhendo dados estatísticos sobre o número de pessoas afectadas e efectivamente condenadas com base em dados PNR, e sobre o exercício efectivo dos direitos das pessoas em causa: nessa avaliação deverá incluir-se a verificação da forma como os pedidos das pessoas em causa estão a ser tratados na prática, sobretudo nos casos em que o acesso directo não foi permitido.

## 3. CONCLUSÃO

39. A AEPD congratula-se com as garantias previstas nas propostas, sobretudo no que diz respeito à aplicação concreta do acordo. Em especial, os aspectos relativos à segurança dos dados, bem como as disposições referentes à supervisão e à aplicação da lei, são desenvolvidos de forma satisfatória. A AEPD salienta que qualquer pessoa tem acesso à autoridade australiana responsável pela protecção de dados, bem como às autoridades judiciais australianas. Estas são duas das garantias essenciais fornecidas pelas propostas.
40. No entanto, a AEPD também identificou algumas melhorias significativas que podem ser introduzidas, sobretudo em relação ao âmbito do acordo, à definição de terrorismo e à inclusão de algumas finalidades excepcionais, bem como ao período de conservação dos dados PNR. Em comparação com o sistema PNR australiano anterior, e também com a proposta relativa ao PNR da UE, esse período de conservação é desproporcionado.

<sup>(1)</sup> Bem como para efeitos do artigo 10.º quando os dados forem transferidos dentro da Austrália.

41. A base jurídica do acordo deverá ser reconsiderada. Face à jurisprudência assente, e para além do artigo 218.º, n.º 6, alínea a), a AEPD considera que o acordo se deverá basear — em todo o caso, principalmente — no artigo 16.º do TFUE e não no artigo 82.º, n.º 1, alínea d), e no artigo 87.º, n.º 2, alínea a), do TFUE. Esta sugestão é totalmente consentânea com a Declaração 21 anexada ao Tratado de Lisboa.
42. Estas observações devem ser inseridas no contexto mais vasto da legitimidade de qualquer sistema PNR, entendido como a recolha sistemática de dados de passageiros para fins de avaliação dos riscos. Só se o sistema respeitar os requisitos fundamentais da necessidade e da proporcionalidade, nos termos dos artigos 7.º e 8.º da Carta dos Direitos

Fundamentais e do artigo 16.º do TFUE, poderá a respectiva proposta satisfazer os restantes requisitos do quadro de protecção de dados.

43. A AEPD também conclui, assim, que se deve prestar mais atenção a estes requisitos fundamentais nas avaliações finais que antecederão a conclusão do acordo.

Feito em Bruxelas, em 15 de Julho de 2011.

Peter HUSTINX

*Supervisor Europeu para a Protecção de Dados*

---