Parecer da Autoridade Europeia para a Protecção de Dados 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

(2011/C 181/02)

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 [1],

Tendo em conta o pedido de parecer apresentado nos termos do artigo 28.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 [2],

ADOPTOU O SEGUINTE PARECER:

I. **INTRODUÇÃO**

I.1. *Consulta da AEPD*

1. Em 2 de Fevereiro de 2011, a Comissão adoptou uma 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 (a seguir designada «a Proposta») [3]. A Proposta foi enviada à AEPD para consulta no mesmo dia.

2. A AEPD congratula-se com o facto de ter sido consultada pela Comissão. Ainda antes da adopção da Proposta, já lhe tinha sido oferecida a possibilidade de formular observações informais. Algumas dessas observações foram tidas em conta na Proposta, e a AEPD constata que, em termos globais, as garantias de protecção de dados nela incluídas foram reforçadas. Subsistem, todavia, algumas preocupações a respeito de várias questões, nomeadamente em relação à escala e aos objectivos da recolha de dados pessoais.

I.2. *A proposta no seu contexto*

3. Os debates sobre um eventual sistema PNR na União Europeia têm vindo a desenvolver-se desde 2007, ano em que a Comissão adoptou uma proposta de decisão-quadro do Conselho sobre esta questão [4]. O objectivo principal de um sistema PNR da UE é obrigar as transportadoras aéreas que operam voos internacionais entre a União Europeia e países terceiros a transmitir dados PNR de todos os passageiros às autoridades competentes para efeitos de prevenção, detecção, investigação e repressão das infracções terroristas e da criminalidade grave. Os dados seriam centralizados e analisados por unidades de informações de passageiros e os resultados da análise transmitidos às autoridades nacionais competentes de cada Estado-Membro.

4. Desde 2007 que a AEPD tem vindo a acompanhar atentamente a evolução relativa a um possível sistema PNR da UE, em paralelo com a dos sistemas PNR de países terceiros. Em 20 de Dezembro de 2007, a AEPD adoptou um parecer sobre essa proposta da Comissão [5]. Em muitas outras ocasiões, foram formuladas observações consistentes, não só pela AEPD mas também pelo Grupo de Trabalho do Artigo 29.º [6], sobre a questão da conformidade do tratamento de dados PNR para efeitos de aplicação da lei com os princípios da necessidade e da proporcionalidade, bem como com outras garantias essenciais de protecção de dados.

5. A principal questão persistentemente levantada pela AEPD centra-se na justificação da necessidade de um sistema PNR europeu adicionalmente a vários outros instrumentos que permitem o tratamento de dados pessoais para efeitos de aplicação da lei.

6. A AEPD reconhece que na proposta em apreço há visíveis melhorias em termos de protecção de dados, comparativamente à versão que foi objecto dos seus pareceres anteriores. Essas melhorias estão, designadamente, relacionadas com o âmbito de aplicação da Proposta, a definição do papel dos diversos intervenientes (unidades de informações de passageiros), a exclusão do tratamento de dados sensíveis, a mudança para um sistema «push» sem um período de transição [7] e a limitação da conservação de dados.

---

[1] JO L 281 de 23.11.1995, p. 31.
[2] JO L 8 de 12.1.2001, p. 1.
[3] COM(2011) 32 final.
[4] COM(2007) 654 final.
[5] Parecer da AEPD de 20 de Dezembro de 2007 sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (Passenger Name Record — PNR) para efeitos de aplicação da lei, (JO C 110 de 1.5.2008, p. 1).
[6] — Parecer 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, disponível no endereço: http://www.edps.europa.eu/EDPSWEB/edps/Consultation/OpinionsC/OC2010
— Os pareceres do Grupo de Trabalho do Artigo 29.º estão disponíveis no seguinte endereço: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm#data_transfers
[7] Isto significa que os dados PNR serão activamente transmitidos pelas companhias aéreas e não «extraídos» pelas autoridades públicas através de um acesso directo à base de dados das companhias aéreas.

7. A AEPD também se congratula com os progressos adicionais registados na avaliação de impacto em relação às razões da existência de um sistema PNR da UE. Todavia, apesar de existir uma clara vontade de clarificar a necessidade do sistema, a AEPD continua a não considerar que essas novas justificações constituem uma base convincente para o desenvolvimento do sistema, sobretudo no que diz respeito à «avaliação prévia» em larga escala de todos os passageiros. A necessidade e a proporcionalidade serão a seguir analisadas no capítulo II. O capítulo III concentrar-se-á em aspectos mais específicos da proposta.

II. **NECESSIDADE E PROPORCIONALIDADE DA PROPOSTA**

II.1. *Observações preliminares sobre a necessidade e a proporcionalidade*

8. A demonstração da necessidade e da proporcionalidade do tratamento de dados é um requisito absoluto para o desenvolvimento do sistema PNR. A AEPD já insistiu em ocasiões anteriores, nomeadamente no contexto da eventual revisão da Directiva 2006/24/CE (a «Directiva relativa à conservação de dados»), no facto de a necessidade de tratar ou armazenar quantidades maciças de informações dever assentar numa demonstração clara da relação entre *utilização* e *resultado*, e permitir a avaliação *sine qua non* da possibilidade de se obterem resultados comparáveis com meios alternativos, menos invasivos da privacidade ([1]).

9. A fim de justificar o sistema, a Proposta e, sobretudo, a avaliação do seu impacto incluem uma vasta documentação e argumentos jurídicos para justificar que o sistema é necessário e que cumpre os requisitos de protecção de dados. A proposta vai, aliás, mais longe ao afirmar que ele traz valor acrescentado em termos de harmonização das normas relativas à protecção de dados.

10. Depois de analisar estes elementos, a AEPD considera que a Proposta, com o seu conteúdo actual, *não* cumpre os requisitos de necessidade e proporcionalidade impostos pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, o artigo 8.º da CEDH e o artigo 16.º do TFUE. O raciocínio subjacente a esta consideração é a seguir desenvolvido.

II.2. *Documentos e estatísticas fornecidos pela Comissão*

11. A AEPD constata que a avaliação de impacto inclui amplas explicações e estatísticas para justificar a Proposta. Todavia, esses elementos não são convincentes. A título ilustrativo, a descrição da ameaça de terrorismo e criminalidade grave na avaliação de impacto e na exposição de motivos da Proposta ([2]) cita o número de 14 000 crimes por 100 000 habitantes nos Estados-Membros. em 2007. Embora este número se possa considerar impressionante, diz respeito a tipos de crimes indiferenciados e não pode servir para justificar uma proposta que visa combater apenas um tipo limitado de criminalidade transnacional grave e o terrorismo. Também a título de exemplo, a citação de um relatório sobre os «problemas» de droga sem ligar os dados estatísticos ao tipo de tráfico de droga visado pela proposta não constitui, no entender da AEPD, uma referência válida. O mesmo se aplica às indicações das consequências de crimes, referindo o «valor dos bens roubados» e o impacto psicológico e físico nas vítimas, que não são dados directamente relacionados com a finalidade da Proposta.

12. Como último exemplo, a avaliação de impacto afirma que a «Bélgica comunicou que 95 % de todas as apreensões de droga em 2009 foi exclusiva ou predominantemente devido ao tratamento de dados PNR». Convém salientar, todavia, que a Bélgica (ainda) não aplica sistematicamente um sistema PNR comparável ao que é previsto na Proposta. Esse exemplo pode indicar a utilidade dos dados PNR em casos específicos, o que a AEPD não contesta. O que suscita graves problemas de protecção de dados é antes a sua ampla recolha com o objectivo de fazer uma avaliação sistemática de todos os passageiros.

13. A AEPD considera que não há suficiente documentação relevante e precisa que demonstre a necessidade do instrumento.

II.3. *Condições para limitar um direito fundamental*

14. Embora o documento note a ingerência das medidas de tratamento de dados nos direitos consagrados na Carta, na CEDH e no artigo 16.º do TFUE, refere-se directamente às possíveis limitações desses direitos e manifesta satisfação com a conclusão de que «como as acções propostas se destinariam a combater o terrorismo e outros crimes graves, previstos num diploma legislativo, cumpririam claramente tais requisitos, desde que sejam necessárias numa sociedade democrática e cumpram o princípio da proporcionalidade ([3])». Falta, contudo, uma demonstração clara de que as medidas são essenciais e de que não existem alternativas menos invasivas.

15. Nesse sentido, o facto de objectivos adicionais, como a aplicação da lei no domínio da imigração, das «listas negras» e da segurança sanitária, terem sido previstos mas, finalmente, não incluídos por motivos de proporcionalidade não significa que «limitar» o tratamento de dados PNR à criminalidade grave e ao terrorismo seja *de facto* proporcionado por ser menos invasivo. A opção de limitar o sistema à luta contra o terrorismo, sem incluir outros crimes, tal como se previa em sistemas PNR anteriores, nomeadamente no anterior sistema PNR australiano, também não foi avaliada. A AEPD salienta que, nesse sistema anterior, sobre o

([1]) Ver «The moment of truth for the Data Retention Directive» (O momento da verdade para a Directiva relativa à conservação de dados), discurso de Peter Hustinx na conferência «Taking on the Data Retention Directive» (Assumir a Directiva relativa à conservação de dados), Bruxelas, 3 de Dezembro de 2010, disponível em: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

([2]) Avaliação de impacto, Capítulo 2.1.1, e Exposição de Motivos, Capítulo 1, primeiro parágrafo.

([3]) Avaliação de impacto, capítulo 3.2, n. 2.

qual o Grupo de Trabalho do Artigo 29.º adoptou um parecer favorável em 2004, os objectivos restringiam-se à «identificação dos passageiros que possam constituir uma ameaça de terrorismo ou actividade criminosa afim» [1]. O sistema australiano também não previa qualquer conservação de dados PNR, excepto de passageiros específicos, identificados como constituindo uma ameaça específica [2].

16. Além disso, no que diz respeito à previsibilidade da vigilância das pessoas em causa, é duvidoso que a Proposta da Comissão preencha os requisitos de uma base jurídica sólida nos termos do direito da UE: a «avaliação» dos passageiros (anteriormente designada «avaliação dos riscos») será realizada com base em critérios que estão em constante evolução e não são transparentes. Como se afirma explicitamente no texto, o principal objectivo do sistema não é o controlo fronteiriço tradicional, mas sim a obtenção de informações [3] e a detenção de pessoas que não são suspeitas, antes da prática de um crime. O desenvolvimento de um tal sistema à escala europeia, envolvendo a recolha de dados sobre todos os passageiros e a tomada de decisões com base em critérios de avaliação desconhecidos e em evolução, suscita sérias questões de transparência e proporcionalidade.

17. A única finalidade que, no entender da AEPD, estaria conforme com os requisitos de transparência e proporcionalidade, seria a utilização de dados PNR caso a caso, como é mencionado no artigo 4.º, n.º 2, alínea c), mas apenas se houver uma ameaça grave e concreta determinada por indicadores concretos.

II.4. *O risco de desvirtuamento da função*

18. O artigo 4.º, n.º 2, alínea b), prevê que uma unidade de informações de passageiros pode proceder a uma avaliação do risco representado pelos passageiros e que, nessa actividade, pode comparar os dados PNR com «bases de dados pertinentes», como é referido no artigo 4.º, n.º 2, alínea b). Esta disposição não indica quais são as bases de dados pertinentes. Em consequência, a medida não é previsível, o que também constitui um requisito da Carta e da CEDH. A disposição levanta, além do mais, a questão da sua compatibilidade com o princípio de limitação da finalidade: no entender da AEPD, deve ser excluída, por exemplo, em relação a uma base de dados como a do Eurodac, que foi desenvolvida para fins diferentes [4]. Além disso, só deve ser possível caso haja uma necessidade específica, num caso específico em que exista uma suspeita prévia em relação a uma pessoa, depois de um crime ter sido cometido. A verificação, por exemplo, da base de dados do Sistema de Informação sobre Vistos [5] de forma sistemática comparando-a com todos os dados PNR seria excessiva e desproporcionada.

II.5. *O valor acrescentado da proposta em termos de protecção de dados*

19. A ideia de que a proposta reforçaria a protecção de dados ao criar condições uniformes no que diz respeito aos direitos das pessoas é questionável. A AEPD reconhece que, caso a necessidade e a proporcionalidade do sistema sejam estabelecidas, a existência de normas uniformes na UE, incluindo em relação à protecção de dados, reforçaria a segurança jurídica. No entanto, a actual redacção da proposta, no seu considerando 28, menciona que a «directiva não obsta a que os Estados-Membros possam prever, ao abrigo do direito nacional, um sistema de recolha e tratamento dos dados PNR para objectivos diferentes dos previstos na presente directiva, ou recolher, junto de outros transportadores para além dos especificados na directiva, dados relativos aos voos internos (…)».

20. A harmonização efectuada pela proposta é, por conseguinte, limitada. Pode abranger os direitos das pessoas em causa, mas não a limitação da finalidade, e pode presumir-se que, de acordo com esta redacção, os sistemas PNR já utilizados para combater, por exemplo, a imigração ilegal podem continuar a fazê-lo ao abrigo da Directiva.

21. Isto significa que, por um lado, subsistiriam algumas diferenças entre os Estados-Membros que já desenvolveram um sistema PNR e que, por outro lado, a grande maioria dos Estados-Membros que não recolhem sistematicamente dados PNR (21 dos 27 Estados-Membros) seria obrigada a fazê-lo. A AEPD considera que, deste ponto de vista, qualquer valor acrescentado em termos de protecção de dados é muito questionável.

---

[1] Parecer 1/2004, de 16 de Janeiro de 2004, sobre o nível de protecção assegurado na Austrália à transmissão de dados dos registos de identificação dos passageiros das companhias aéreas, WP85.

[2] O parecer do Grupo de Trabalho do Artigo 29.º explica ainda que «no que respeita à conservação de dados PNR, não é imposta às autoridades aduaneiras uma obrigação legal de conservação desses dados. Do mesmo modo, também não há uma proibição legal que impeça as autoridades aduaneiras de os conservar. Os dados PNR dos passageiros avaliados através do *software* automático de análise de perfis e considerados de baixo risco (95 % a 97 % dos passageiros) não são conservados, nem se mantém um registo das suas informações PNR. Assim, as autoridades aduaneiras aplicam uma política geral de não conservação desses dados. Em relação aos 0,05 % a 0,1 % dos passageiros que são encaminhados para as autoridades aduaneiras para uma avaliação mais aprofundada, os dados PNR das companhias aéreas são temporariamente conservados, mas não armazenados, enquanto aguardam a avaliação fronteiriça. Subsequentemente, os seus dados PNR são apagados do PC do funcionário aduaneiro em causa e não são introduzidos nas bases de dados australianas».

[3] Exposição de Motivos, Capítulo 1. Contexto da proposta, Coerência com outras políticas e objectivos da União Europeia.

[4] O objectivo do Eurodac «consiste em ajudar a determinar o Estado-Membro responsável, nos termos da Convenção de Dublim, pela análise de um pedido de asilo apresentado num Estado-Membro e em facilitar noutros aspectos a aplicação da Convenção de Dublim nos termos do presente regulamento», nos termos do artigo 1.º, n.º 1, do Regulamento (CE) n. 2725/2000 do Conselho, de 11 de Dezembro de 2000, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efectiva da Convenção de Dublim,(JO L 316 de 15.12.2000, p. 1).

[5] «O VIS tem por objectivo melhorar a aplicação da política comum em matéria de vistos, a cooperação consular e a consulta entre as autoridades centrais responsáveis pelos vistos ao facilitar o intercâmbio de dados entre Estados-Membros sobre os pedidos de vistos e as decisões relativas aos mesmos», nos termos do artigo 2.º do Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de Julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (Regulamento VIS), (JO L 218 de 13.8.2008, p. 60).

22. Pelo contrário, as consequências do considerando 28 constituem uma grave violação do princípio de limitação da proporcionalidade. No entender da AEPD, a proposta deveria dispor explicitamente que os dados PNR não podem ser utilizados para outros fins.

23. A AEPD chega a uma conclusão semelhante à que foi extraída da avaliação da Directiva relativa à conservação de dados: em ambos os contextos, a ausência de uma harmonização efectiva faz-se acompanhar pela ausência de segurança jurídica. Além disso, a recolha e o tratamento adicionais de dados pessoais tornam-se obrigatórios para todos os Estados-Membros, onde a real necessidade do sistema não foi demonstrada.

II.6. *Ligação com a Comunicação sobre a gestão da informação no domínio da liberdade, da segurança e justiça*

24. A AEPD constata ainda que a evolução em relação ao sistema PNR está ligada à avaliação geral em curso de todos os instrumentos da UE no domínio da gestão do intercâmbio de informações, lançada pela Comissão em Janeiro de 2010 e desenvolvida na recente Comunicação intitulada «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça» [1]. Existe, nomeadamente, uma ligação clara com o presente debate sobre a Estratégia Europeia de Gestão da Informação. A AEPD considera, a este respeito, que os resultados do actual trabalho sobre o modelo europeu de intercâmbio de informações, previstos para 2012, devem ser tidos em conta na avaliação da necessidade de um sistema PNR da União Europeia.

25. Neste contexto, e atendendo às insuficiências da Proposta e sobretudo da sua avaliação de impacto, a AEPD considera ser necessário avaliar especificamente o impacto em matéria de privacidade e de protecção de dados em casos como este, em que a substância da Proposta afecta os direitos fundamentais à privacidade e à protecção de dados. Uma avaliação de impacto genérica não é suficiente.

III. **OBSERVAÇÕES ESPECÍFICAS**

III.1. *Âmbito de aplicação*

26. Os termos «infracções terroristas», «criminalidade grave» e «criminalidade transnacional grave» são definidos no artigo 2.º, alíneas g), h) e i), da Proposta. A AEPD congratula-se com o facto de as definições — e o seu âmbito — terem sido explicitadas, fazendo-se uma diferenciação entre a criminalidade grave e a criminalidade transnacional grave. Esta distinção é bem-vinda, sobretudo por implicar um tratamento diferente dos dados pessoais, excluindo a avaliação com base em critérios pré-determinados no caso da criminalidade grave que não seja transnacional.

27. A definição de criminalidade grave ainda é, todavia, demasiado ampla, no entender da AEPD. Este facto é reconhecido pela Proposta, onde se diz que os Estados-Membros podem excluir *infracções menores* abrangidas pela definição de criminalidade grave [2] mas cujo tratamento seria contrário ao princípio da proporcionalidade. Esta redacção implica que a definição contida na Proposta pode incluir infracções menores, cujo tratamento seria desproporcionado. Aquilo que ficaria exactamente abrangido pelo conceito de infracções menores não é claro. Em lugar de se deixar aos Estados-Membros a faculdade de reduzir o âmbito de aplicação, a AEPD considera que a Proposta deveria enumerar explicitamente as infracções que devem ser incluídas no seu âmbito e aquelas que devem ser excluídas por serem consideradas menores e não preencherem o critério da proporcionalidade.

28. A mesma preocupação se aplica à possibilidade deixada em aberto no artigo 5.º, n.º 5, de se tratarem dados relacionados com quaisquer outros tipos de infracções que sejam detectadas no decurso de acções repressivas, bem como à possibilidade mencionada no considerando 28 de alargar o âmbito de aplicação a outros objectivos diferentes dos previstos na Proposta, ou a outros transportadores.

29. A AEPD também está preocupada com a possibilidade prevista no artigo 17.º de incluir os voos internos no âmbito de aplicação da directiva, à luz da experiência adquirida pelos Estados-Membros que já recolhem dados PNR. Um tal alargamento do âmbito do sistema PNR ameaçaria ainda mais os direitos fundamentais das pessoas e não deveria ser previsto antes de uma análise adequada, incluindo uma avaliação de impacto exaustiva.

30. Para concluir, deixar o âmbito de aplicação em aberto e conceder aos Estados-Membros a possibilidade de alargarem a finalidade é algo que contraria o requisito de que os dados só devem ser recolhidos para finalidades determinadas e explícitas.

III.2. *Unidades de informações de passageiros*

31. O papel das unidades de informações de passageiros (UIP) e as garantias que rodeiam o tratamento de dados PNR levantam questões específicas, principalmente tendo em conta que essas unidades recebem dados de todos os passageiros das transportadoras aéreas e possuem — nos termos da Proposta — amplas competências para tratar esses dados. Isto inclui a avaliação do comportamento de passageiros que não são suspeitos de qualquer crime e a possibilidade de comparar os dados PNR com bases de dados indeterminadas [3]. A AEPD observa que na Proposta estão previstas condições de «acesso restritivo», mas considera que tais condições não são, só por si, suficientes, tendo em conta as amplas competências das UIP.

32. Em primeiro lugar, a natureza da autoridade designada como unidade de informações de passageiros e a sua composição continuam a não ser claras. A Proposta menciona a possibilidade de os membros do pessoal poderem «ser agentes destacados pelas autoridades competentes», mas

[1] COM(2010) 385 final.

[2] A que se referem as Decisões-quadro 2008/841/JAI e 2002/584/JAI do Conselho.

[3] Sobre as unidades de informações de passageiros, ver também o parecer da AEPD de 20 de Dezembro de 2007.

não oferece quaisquer garantias em termos de competência e de integridade do pessoal da UIP. A AEPD recomenda que se incluam tais requisitos no texto da directiva, tendo em conta o carácter sensível do tratamento efectuado por essas unidades.

33. Em segundo lugar, a proposta prevê a possibilidade de se designar uma UIP para vários Estados-Membros, o que abre as portas a riscos de utilização abusiva dos dados e da sua transmissão em condições diferentes das previstas na Proposta. A AEPD reconhece que podem existir razões de eficiência para essa união de esforços, sobretudo no caso dos Estados-Membros mais pequenos, mas recomenda que se incluam no texto condições aplicáveis a esta opção. Essas condições devem visar a cooperação com as autoridades competentes e a supervisão, nomeadamente no que diz respeito à autoridade em matéria de protecção de dados responsável pela mesma e ao exercício dos direitos das pessoas em causa, uma vez que várias autoridades podem ser competentes para supervisionar uma UIP.

34. Há um risco de desvirtuamento da função associado aos elementos acima mencionados e, em especial, no que se refere à qualidade do pessoal competente para analisar os dados e à «partilha» de uma unidade de informações de passageiros entre vários Estados-Membros.

35. Em terceiro lugar, a AEPD questiona as garantias previstas contra os abusos. As obrigações de registo são bem-vindas, mas não suficientes. O autocontrolo deve ser complementado por um controlo externo, de forma mais estruturada. A AEPD sugere que as auditorias sejam organizadas de forma sistemática de quatro em quatro anos. Há que desenvolver e aplicar um vasto conjunto de normas de segurança horizontalmente a todas as unidades de informações de passageiros.

III.3. *Intercâmbio de dados entre Estados-Membros*

36. O artigo 7.º da Proposta prevê vários cenários que permitem o intercâmbio de dados entre as unidades de informações de passageiros — que é a situação normal — ou entre as autoridades competentes de um Estado-Membro e as UIP, em situações excepcionais. As condições também são mais rigorosas consoante o acesso seja solicitado à base de dados prevista no artigo 9.º, n.º 1, onde os dados são conservados durante os primeiros 30 dias, ou à base de dados mencionada no artigo 9.º, n.º 1 onde os dados são conservados durante um período adicional de cinco anos.

37. As condições de acesso são definidas de forma mais rigorosa quando o pedido de acesso vai além do procedimento normal. A AEPD observa, todavia, que a redacção utilizada suscita confusão: o artigo 7.º, n.º 2, é aplicável num «caso específico de prevenção, detecção, investigação ou repressão de infracções terroristas ou de criminalidade grave»; o n.º 3 do mesmo artigo menciona «circunstâncias excepcionais para dar resposta a uma ameaça específica ou a uma investigação ou repressão concreta relacionada com infracções terroristas ou a criminalidade grave», enquanto o n.º 4, se refere a «uma ameaça imediata e grave para a segurança pública» e o n.º 5 menciona «uma ameaça específica e real relacionada com infracções terroristas ou com a criminalidade grave». As condições de acesso às bases de dados por parte dos diversos interessados variam em função desses critérios. Contudo, a diferença entre uma ameaça específica, uma ameaça imediata e grave e uma ameaça específica e real não é clara. A AEPD sublinha a necessidade de especificar melhor as condições exactas em que as transferências de dados serão permitidas.

III.4. *Legislação aplicável*

38. A proposta indica como base jurídica geral para os princípios de protecção de dados a Decisão-Quadro 2008/977/JAI do Conselho, e alarga o seu âmbito ao tratamento de dados a nível interno.

39. A AEPD já tinha destacado, em 2007 [1], as lacunas da decisão-quadro no que respeita aos direitos das pessoas em causa. Entre os elementos em falta na decisão-quadro, figuram, nomeadamente, alguns requisitos de informação da pessoa em causa, em caso de pedido de acesso aos seus dados: as informações devem ser dadas de forma inteligível, a finalidade do tratamento deve ser indicada e são necessárias garantias mais desenvolvidas em caso de recurso à autoridade responsável pela protecção de dados, se o acesso directo tiver sido recusado.

40. A referência à decisão-quadro também tem consequências no que diz respeito à identificação da autoridade responsável pela protecção de dados competente para controlar a aplicação da futura directiva, pois pode não coincidir necessariamente com a autoridade competente nas matérias do (ex) primeiro pilar. A AEPD considera que não é satisfatório tomar-se exclusivamente por base a decisão-quadro no contexto pós-Lisboa, quando um dos principais objectivos é adaptar o quadro jurídico de modo a garantir um nível elevado e harmonizado de protecção em todos os (ex) pilares. Considera necessário introduzir disposições adicionais na Proposta para completar a referência à decisão-quadro do Conselho onde foram identificadas lacunas, nomeadamente em relação às condições de acesso aos dados pessoais.

41. Estas preocupações também são totalmente válidas no tocante às disposições relativas às transferências de dados para países terceiros. A Proposta refere o artigo 13.º, n.º 3, alínea ii), da decisão-quadro, que inclui amplas derrogações às garantias de protecção de dados: derroga, em especial, do requisito de adequação em caso de «interesses superiores legítimos, especialmente interesses públicos importantes». Esta derrogação tem uma redacção imprecisa, potencialmente aplicável em muitos casos de tratamento de dados PNR, se fosse interpretada de forma lata. A AEPD considera que a Proposta deve impedir explicitamente a aplicação das derrogações previstas na decisão-quadro no contexto do tratamento de dados PNR e manter a exigência de uma rigorosa avaliação da adequação.

[1] Terceiro parecer da Autoridade Europeia para a Protecção de Dados, de 27 de Abril de 2007, sobre a proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, (JO C 139 de 23.6.2007, p. 1).

III.5. *Conservação de dados*

42. A proposta prevê um período de 30 dias de conservação, com um período adicional de cinco anos em arquivo. Este período de conservação é consideravelmente reduzido em comparação com as versões anteriores do documento, em que a retenção se prolongava por cinco mais oito anos.

43. A AEPD congratula-se com a redução do primeiro período de conservação para trinta dias. Questiona, todavia, o período de conservação adicional de cinco anos: não se lhe afigura claro que haja necessidade de conservar esses dados por mais tempo numa forma que ainda possibilita a identificação das pessoas.

44. Salienta igualmente uma questão terminológica do texto que tem consequências jurídicas importantes: o artigo 9.º, n.º 2, refere que os dados dos passageiros serão «ocultados» e, por conseguinte, «tornados anónimos». No entanto, mais adiante, o texto menciona que continua a ser possível aceder à «integralidade dos dados PNR». Se isto for possível, significa que os dados PNR nunca foram totalmente tornados anónimos: embora sejam ocultados, continuam a ser identificáveis. Em consequência, o quadro de protecção de dados continua a ser totalmente aplicável, o que suscita a questão fundamental da necessidade e da proporcionalidade da conservação de dados identificáveis de todos os passageiros durante cinco anos.

45. A AEPD recomenda que a Proposta seja reformulada, mantendo o princípio de uma efectiva anonimização sem possibilidade de voltar a aceder a dados identificáveis, o que significa que não deve ser permitida qualquer investigação retroactiva. Esses dados poderão ser ainda — e unicamente — utilizados para efeitos de aplicação geral da lei com base na identificação de padrões de terrorismo e de criminalidade com ele relacionada nos fluxos migratórios. Isto deve ser distinguido da conservação de dados numa forma identificável — sujeita a determinadas garantias — em casos que tenham suscitado uma suspeita concreta.

III.6. *Lista de dados PNR*

46. A AEPD congratula-se com o facto de os dados sensíveis não estarem incluídos na lista de dados a tratar. Salienta, todavia, que a Proposta ainda prevê a possibilidade de esses dados serem enviados à unidade de informações de passageiros, que tem posteriormente a obrigação de os apagar (artigo 4.º, n.º 1, artigo 11.º). Desta redacção não se entende claramente se as unidades de informações de passageiros ainda têm a obrigação de filtrar e apagar, por rotina, os dados sensíveis transmitidos pelas companhias aéreas, ou se apenas deverão fazê-lo no caso excepcional de as companhias aéreas os terem transmitido por engano. A AEPD recomenda que o texto seja alterado de modo a deixar claro que as companhias aéreas não devem transmitir dados sensíveis, na própria origem do tratamento de dados.

47. Para além dos dados sensíveis, a lista de dados que podem ser transferidos corresponde em grande medida à lista PNR dos EUA, que foi criticada por ser demasiado ampla, em vários pareceres do Grupo de Trabalho do Artigo 29.º ([1]). A AEPD considera que essa lista deve ser reduzida em conformidade com o parecer do Grupo de Trabalho e qualquer adição à mesma deve ser devidamente justificada. É o caso, em especial, do campo «observações gerais», que deve ser excluído da lista.

III.7. *Decisões individuais automatizadas*

48. Nos termos do artigo 4.º, n.º 2, alíneas a) e b), a avaliação das pessoas em função de critérios pré-definidos ou da comparação com bases de dados pertinentes pode envolver um tratamento automatizado, mas este deve ser controlado individualmente por meios não automatizados.

49. A AEPD congratula-se com os esclarecimentos introduzidos nesta nova versão do texto. A ambiguidade do anterior âmbito de aplicação da disposição, em relação a decisões automatizadas susceptíveis de produzir «efeitos jurídicos *adversos* contra uma pessoa ou que *a afecte significativamente* (…)», foi substituída por uma redacção mais explícita. Fica agora claro que qualquer correspondência positiva será controlada individualmente.

50. Fica igualmente claro, na nova versão, que uma avaliação nunca pode ser baseada na origem racial ou étnica de uma pessoa, nas suas convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, situação médica ou vida sexual. Por outras palavras, a AEPD entende desta nova redacção que não se pode tomar nenhuma decisão, nem mesmo parcialmente, com base em dados sensíveis. Isto é compatível com a disposição segundo a qual as unidades de informações de passageiros não podem tratar dados sensíveis, o que também é de louvar.

III.8. *Reexame e dados estatísticos*

51. A AEPD considera extremamente importante que se realize uma avaliação minuciosa da aplicação da directiva, como se prevê no artigo 17.º. Considera que o reexame deve avaliar não só o respeito dos níveis de protecção de dados em geral, mas de forma mais fundamental e específica, se os sistemas PNR constituem ou não uma medida necessária. Os dados estatísticos mencionados no artigo 18.º desempenham um papel importante deste ponto de vista. A AEPD considera que nestas informações se deve incluir o número de acções repressivas, como se previa no projecto de texto, mas também o número de condenações efectivas que resultaram, ou não, dessas acções. Tais dados são essenciais para que o resultado do reexame seja conclusivo.

III.9. *Relação com outros instrumentos*

52. A proposta não prejudica os acordos já existentes com países terceiros (artigo 19.º). A AEPD considera que esta disposição deve referir mais explicitamente o objectivo de um quadro global que preveja garantias harmonizadas de protecção dos dados PNR, dentro e fora da UE, como foi solicitado pelo Parlamento Europeu e desenvolvido pela

([1]) Parecer de 23 de Junho de 2003 sobre o nível de protecção assegurado nos Estados Unidos à transferência de dados dos passageiros, WP78. Este parecer e os pareceres seguintes do Grupo de Trabalho sobre esta questão estão disponíveis no endereço: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

Comissão na sua Comunicação 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.

53. Nesse sentido, os acordos com países terceiros não devem incluir disposições com um limiar de protecção de dados inferior ao da directiva. Isto reveste-se de particular importância neste momento em que os acordos com os Estados Unidos, a Austrália e o Canadá estão a ser renegociados nessa perspectiva de um quadro global e harmonizado.

IV. **CONCLUSÃO**

54. O desenvolvimento de um sistema PNR da UE, juntamente com a negociação de acordos PNR com países terceiros, tem sido um projecto moroso. A AEPD reconhece que, em comparação com a Proposta de decisão-quadro do Conselho relativa ao sistema PNR da UE de 2007, o projecto de texto foi visivelmente melhorado. Foram acrescentadas garantias de protecção de dados, para as quais contribuíram os debates e pareceres das diversas partes interessadas, incluindo, nomeadamente, o Grupo de Trabalho do Artigo 29.º, a AEPD e o Parlamento Europeu.

55. A AEPD congratula-se com estas melhorias e, em especial, com os esforços para restringir o âmbito de aplicação da Proposta e as condições de tratamento de dados PNR. Sente-se, todavia, na obrigação de observar que o requisito essencial para qualquer desenvolvimento de um sistema PNR — isto é, a conformidade com os princípios da necessidade e da proporcionalidade — não se encontra preenchido na Proposta. A AEPD lembra que, no seu entender, os dados PNR podem, certamente, ser necessários para efeitos de aplicação da lei em casos *específicos* e respeitar os requisitos de protecção de dados. É a sua utilização de forma sistemática e indiscriminada, em relação a todos os passageiros, que suscita preocupações específicas.

56. A avaliação de impacto apresenta elementos que procuram justificar a necessidade de dados PNR para combater a criminalidade, mas a natureza dessas informações é demasiado geral e não justifica o tratamento em larga escala de dados PNR para efeitos de aplicação da lei. No entender da AEPD, a única medida conforme com os requisitos de protecção de dados seria a utilização de dados PNR caso a caso, quando exista uma ameaça grave, confirmada por indicadores concretos.

57. Para além desta lacuna fundamental, as observações da AEPD dizem respeito aos seguintes aspectos:

— o âmbito de aplicação deve ser muito mais limitado no tocante ao tipo de crimes envolvidos. A AEPD questiona a inclusão na Proposta da criminalidade grave que não tenha ligações com o terrorismo. Em todo o caso, as infracções menores devem ser explicitamente definidas e excluídas. A AEPD recomenda que se exclua a possibilidade de os Estados-Membros alargarem o âmbito de aplicação,

— a natureza das diversas ameaças que permitem um intercâmbio de dados entre unidades de informações de passageiros ou com os Estados-Membros não foi suficientemente definida,

— os princípios de protecção de dados aplicáveis não se devem basear apenas na Decisão-quadro 2008/977/JAI do Conselho, que contém lacunas, nomeadamente em termos dos direitos das pessoas em causa e das transferências para países terceiros. A Proposta deve conter um nível de garantias mais elevado, assente nos princípios da Directiva 95/46/CE,

— os dados não devem ser conservados durante mais de 30 dias sob uma forma identificável, excepto em casos que exijam investigações posteriores,

— a lista de dados PNR a tratar deve ser reduzida, em conformidade com as anteriores recomendações do Grupo de Trabalho do Artigo 29.º e da AEPD. Em especial, o campo «observações gerais» não deve ser incluído,

— a avaliação da directiva deve ser baseada em dados exaustivos, incluindo o número de pessoas efectivamente condenadas — e não apenas objecto de acções judiciais — com base no tratamento dos seus dados.

58. A AEPD recomenda ainda que a evolução relativa ao sistema PNR da UE seja avaliada numa perspectiva mais ampla, incluindo a avaliação geral em curso de todos os instrumentos da UE no domínio da gestão do intercâmbio de informações, lançada pela Comissão em Janeiro de 2010. Em especial, os resultados do actual trabalho sobre o modelo europeu de intercâmbio de informações, previstos para 2012, devem ser tidos em conta na avaliação da necessidade de um sistema PNR da União Europeia.

Feito em Bruxelas, em 25 de Março de 2011.

Peter HUSTINX

Supervisor Europeu para a Protecção de Dados