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-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (Passenger Name Record — PNR) para efeitos de aplicação da lei

(2008/C 110/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado que institui a Comunidade Europeia, nomeadamente o artigo 286.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 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 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]), designadamente o artigo 41.º,

Tendo em conta o pedido de parecer nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, recebido em 13 de Novembro de 2007 da Comissão Europeia,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

Consulta da AEPD

1. 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 foi transmitida pela Comissão à AEPD para consulta, nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001 (a seguir designada por «proposta»).

2. A proposta diz respeito ao tratamento de dados PNR na UE e está estreitamente relacionada com outros regimes de recolha e utilização de dados sobre passageiros, nomeadamente o acordo UE-EUA de Julho de 2007. Estes regimes são de grande interesse para a AEPD, que já teve a oportunidade de transmitir certas observações preliminares sobre o questionário da Comissão relativo ao pretendido sistema PNR da UE, enviado em Dezembro de 2006 às partes interessadas ([3]). A AEPD congratula-se com a consulta da Comissão. Segundo a AEPD, o presente parecer deve ser referido no preâmbulo da decisão do Conselho.

A proposta no seu contexto

3. A proposta destina-se a harmonizar as disposições dos Estados-Membros relativas à obrigação de as transportadoras aéreas que operam voos com destino ou partida do território de pelo menos um Estado-Membro transmitirem os dados PNR às autoridades competentes no contexto da prevenção e luta contra infracções terroristas e a criminalidade organizada.

4. A UE concluiu com os Estados Unidos e o Canadá acordos relativos à transferência dos dados PNR, para efeitos similares. Um primeiro acordo celebrado com os EUA em Maio de 2004 foi substituído por um novo acordo em

([1]) JO L 281 de 23.11.1995, p. 31.
([2]) JO L 8 de 12.1.2001, p. 1.

([3]) Incluindo os Estados-Membros, as autoridades de protecção de dados e as associações de transportadoras aéreas. Esse questionário foi elaborado tendo em vista a preparação de uma avaliação do impacto da presente proposta pela Comissão Europeia.

Julho de 2007 ([1]). Foi celebrado um acordo semelhante com o Canadá em Julho de 2005 ([2]). Além disso, estão previstas negociações entre a UE e a Austrália com vista a um acordo sobre o intercâmbio de dados PNR e a Coreia do Sul também passou a requerer dados PNR relativos a voos com destino ao seu território, embora de momento não estejam previstas negociações a nível europeu.

5. A nível da UE, a proposta em apreço vem-se juntar à Directiva 2004/82/CE do Conselho ([3]), relativa à obrigação de comunicação de dados dos passageiros (dados API) pelas transportadoras, e destinada a melhorar os controlos nas fronteiras e a lutar contra a imigração ilegal. Essa directiva devia ter sido transposta para a legislação nacional dos Estados-Membros até 5 de Setembro de 2006. No entanto, a sua implementação ainda não está assegurada em todos os Estados-Membros.

6. Ao contrário dos dados API (Informações Antecipadas sobre os Passageiros), que servem para identificar pessoas, os dados PNR mencionados na proposta contribuiriam para efectuar avaliações de risco de pessoas, obter informações e estabelecer associações entre pessoas conhecidas e não conhecidas.

7. Os principais elementos dessa proposta são:

— a colocação de dados PNR à disposição das autoridades competentes dos Estados-Membros, por parte das transportadoras aéreas, para efeitos de prevenção e luta contra as infracções terroristas e a criminalidade organizada,

— a designação de uma Unidade de Informações de Passageiros (UIP), em princípio em cada Estado-Membro, que seja responsável pela recolha de dados PNR junto das transportadoras aéreas (ou intermediários designados) e pela avaliação de risco dos passageiros,

— a informação assim avaliada será transmitida às autoridades competentes de cada Estado-Membro. Essa informação será objecto de intercâmbio com outros Estados-Membros, caso a caso e para os fins acima referidos,

— a transferência para países fora da União Europeia está sujeita a condições adicionais,

— os dados serão conservados durante treze anos, oito dos quais numa base de dados passiva,

— o tratamento será regido pelo (projecto de) decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (a seguir designada por «decisão-quadro de protecção de dados») ([4]),

— a Comissão será assistida por um Comité composto por representantes dos Estados-Membros, no que respeita a protocolos e questões de cifragem, bem como critérios e práticas de avaliação de risco,

— a decisão será objecto de revisão no prazo de três anos a contar da sua entrada em vigor.

Conteúdo essencial do parecer

8. A proposta apresentada à AEPD para consulta representa mais um passo em direcção a uma recolha rotineira de dados sobre pessoas que, em princípio, não são suspeitas de nenhum crime. Tal como acima referido, esta evolução ocorre tanto a nível internacional como a nível europeu.

9. A AEPD nota ainda que o Grupo do artigo 29.º e o Grupo «Polícia e Justiça» apresentaram um parecer conjunto sobre a proposta em apreço ([5]). A AEPD subscreve esse parecer. O presente parecer salienta e desenvolve um certo número de questões adicionais.

10. Se bem que o parecer da AEPD analise todos os aspectos pertinentes da proposta, focará sobretudo quatro questões principais:

— a primeira destas questões é a legitimidade das medidas pretendidas. A questão da finalidade, necessidade e da proporcionalidade será avaliada por referência aos critérios do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia,

— o parecer analisará também a questão da lei aplicável ao tratamento ou tratamentos projectados. Em especial, merece uma atenção específica o âmbito de aplicação da decisão-quadro de protecção de dados relativamente à aplicação da legislação do primeiro pilar em matéria de protecção de dados. Serão também examinadas as consequências do regime aplicável de protecção de dados para o exercício dos direitos das pessoas em causa,

([1]) Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento (Acordo PNR 2007) (JO L 204 de 4.8.2007, p. 18).

([2]) Acordo entre a Comunidade Europeia e o Governo do Canadá sobre o tratamento dos dados relativos às informações antecipadas sobre os passageiros e aos registos de identificação dos passageiros (JO L 82 de 21.3.2006, p. 15).

([3]) Directiva 2004/82/CE do Conselho, de 29 de Abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras (JO L 261 de 6.8.2004, p. 24).

([4]) A última versão deste projecto consta do documento n.º 16397/07 do Conselho.

([5]) Parecer conjunto sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (PNR) para efeitos de aplicação da lei, apresentada pela Comissão em 6 de Novembro de 2007, aprovado pelo Grupo do artigo 29.º em 5 de Dezembro de 2007 e pelo Grupo «Polícia e Justiça» em 18 de Dezembro de 2007, WP 145, WPPJ 01/07.

— em seguida, o parecer focará a qualidade dos destinatários de dados a nível nacional. Em especial a qualidade das UIP, dos intermediários e das autoridades competentes designadas para a realização de avaliações de risco e a análise dos dados sobre passageiros levanta preocupações específicas, dado que a proposta não adianta nenhuma precisão a este respeito,

— a quarta questão diz respeito às condições em que é efectuada a transferência de dados para países terceiros. Não resulta claro em que condições se realizam tais transferências, perante a existência de conjuntos de regras: as condições de transferência estabelecidas na presente proposta, a par das definidas pela decisão-quadro de protecção de dados e dos acordos internacionais existentes (com os EUA e o Canadá).

11. Por fim, serão focados outros pontos substantivos, incluindo os passos positivos em matéria de protecção de dados e certos motivos de preocupação suscitados pela proposta.

II. LEGITIMIDADE DAS MEDIDAS PROPOSTAS

12. Para analisar a legitimidade das medidas propostas segundo os princípios fundamentais da protecção de dados, nomeadamente o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e os artigos 5.º a 8.º da Convenção n.º 108 do Conselho da Europa ([1]), é necessário determinar claramente a finalidade do tratamento previsto de dados pessoais, bem como avaliar a sua necessidade e proporcionalidade. Deverá ser assegurado que não se dispõe de outros meios, menos invasivos, para alcançar a mesma finalidade.

Determinação da finalidade

13. A redacção da proposta e a avaliação do seu impacto indicam que o objectivo não é simplesmente identificar terroristas conhecidos ou criminosos conhecidos envolvidos no crime organizado, comparando os seus nomes com os nomes constantes das listas geridas pelas autoridades de aplicação da lei. A finalidade é recolher informações relativas ao terrorismo ou crime organizado, mais concretamente «efectuar avaliações de risco de pessoas, obter informações e estabelecer associações entre pessoas conhecidas e não conhecidas» ([2]). Na mesma ordem de ideias, o n.º 5 do artigo 3.º estabelece em primeiro lugar como finalidade: «Identificar pessoas implicadas *ou susceptíveis de estarem* implicadas numa infracção terrorista ou de criminalidade organizada, *bem como os seus associados*».

14. Esta a razão invocada para explicar que os dados API não são suficientes para alcançar a finalidade pretendida. De facto, tal como já foi acima referido, ao passo que os dados API que servem para identificar pessoas, os dados PNR não se destinam a fins de identificação, mas os seus pormenores contribuiriam para efectuar avaliações de risco de pessoas, obter informações e estabelecer associações entre pessoas conhecidas e não conhecidas.

15. As medidas previstas têm por finalidade não só a captura de pessoas *conhecidas* como também a localização de pessoas que *podem* ser abrangidas pelos critérios da proposta.

A fim de identificar tais pessoas, a análise de risco e a identificação de padrões constituem o cerne do projecto. O considerando n.º 9 da proposta afirma explicitamente que os dados devem ser conservados «durante um período suficientemente longo a fim de servirem para estabelecer indicadores de risco e padrões de viagem e de comportamento».

16. A finalidade é, pois, descrita em dois estratos: o primeiro consiste no objectivo geral de lutar contra o terrorismo e a criminalidade organizada, ao passo que o segundo inclui os meios e as medidas inerentes à consecução deste objectivo. Se bem que a finalidade de lutar contra o terrorismo e a criminalidade organizada pareça ser suficientemente clara e legítima, os meios utilizados para a alcançar são susceptíveis de discussão.

Definição de padrões e avaliação de riscos

17. A proposta não dá nenhuma indicação quanto à forma como serão definidos os padrões e efectuada a avaliação de riscos. A avaliação de impacto especifica do seguinte modo a utilização que será feita dos dados PNR: comparar os dados dos passageiros «com uma combinação de características e padrões comportamentais, com o objectivo de realizar uma avaliação de risco. Quando um passageiro corresponde a uma determinada categoria de risco, pode ser identificado como um passageiro de alto risco» ([3]).

18. As pessoas suspeitas podem ser seleccionadas segundo elementos concretos de suspeição incluídos nos seus dados PNR (p.ex. contacto com uma agência de viagens suspeita, referência de um cartão de crédito roubado) ou com base em «padrões» ou um perfil abstracto. Podem até ser constituídos diferentes perfis normalizados com base nos padrões de viagem, para «passageiros normais» ou «passageiros suspeitos». Tais perfis permitiriam aprofundar a investigação dos passageiros que não entram na «categoria de passageiro normal», por maioria de razão se o seu perfil estivar associado a outros elementos suspeitos, tais como um cartão de crédito roubado.

19. Embora não se possa presumir que os passageiros serão visados conforme a sua religião ou outros dados sensíveis, afigura-se que seriam sujeitos a investigação com base numa mescla de informações *concretas* e *abstractas, incluindo* padrões normalizados e perfis abstractos.

([1]) Convenção do Conselho da Europa de 28 de Janeiro de 1981 para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal.

([2]) Exposição de motivos da proposta, capítulo I.

([3]) Avaliação de impacto, capítulo 2.1, «Definição do problema».

20. É passível de debate considerar se este tipo de investigação pode ser qualificado de caracterização. A caracterização é definida como «um método informatizado que utiliza a prospecção de dados num armazém de dados, que permite ou visa permitir a classificação — com uma certa probabilidade, e portanto com uma certa margem de erro — de uma pessoa numa determinada categoria, a fim de tomar decisões específicas sobre essa pessoa» ([1]).

21. A AEPD está ciente de que a definição de caracterização ainda é objecto de debate. Quer seja ou não reconhecido oficialmente que a proposta se destina a *caracterizar* passageiros, não estamos perante uma questão de definições. O que está em questão é o impacto nas pessoas.

22. Para a AEPD, é sobretudo motivo de preocupação o facto de as decisões relativas a pessoas serem tomadas com base em padrões e critérios estabelecidos utilizando os dados sobre passageiros em geral. Assim sendo, as decisões relativas a uma pessoa poderão ser tomadas, tomando como referência (pelo menos parcialmente) padrões derivados dos dados de *outras* pessoas. É portanto com referência a um contexto abstracto que serão tomadas decisões que podem afectar grandemente as pessoas em causa. É extremamente difícil para um indivíduo defender-se contra tais decisões.

23. Além disso, a avaliação de risco é efectuada num contexto de falta de normas uniformes de identificação de suspeitos. A AEPD tem sérias reservas sobre a certeza jurídica de todo o processo de filtragem, tendo em conta que são definidos de modo tão insuficiente os critérios subjacentes à verificação de cada passageiro.

24. A AEPD recorda a jurisprudência do Tribunal Europeu dos Direitos do Homem, segundo a qual a legislação nacional tem de ser suficientemente precisa para indicar aos cidadãos em que circunstâncias e em que termos as autoridades públicas são habilitadas a registar informações sobre a sua vida privada e a fazer uso das mesmas. A informação «deve ser acessível à pessoa em causa e previsível nos seus efeitos». Uma regra é «previsível» se for «formulada com suficiente previsão para permitir a qualquer pessoa, se necessário com o aconselhamento adequado, regular a sua conduta» ([2]).

25. Em conclusão, é nomeadamente devido a estes tipos de riscos que a presente proposta precisa de uma cuidadosa ponderação. Se bem que o objectivo geral de lutar contra o terrorismo e a criminalidade organizada seja por si próprio claro e legítimo, o cerne do processo de tratamento a criar não parece estar suficientemente delimitado e justificado. Por conseguinte, a AEPD insta o legislador da UE a abordar claramente esta questão, antes de ser aprovada a decisão-quadro.

Necessidade

26. É evidente o carácter intrusivo das medidas, como acima ficou indicado. Por outro lado, não está de todo demonstrada a sua utilidade.

27. A avaliação de impacto da proposta centra-se mais na melhor forma de estabelecer um registo PNR na UE que na necessidade do mesmo. É feita referência à avaliação ([3]) dos sistemas PNR já existentes noutros países, nomeadamente os EUA e o Reino Unido. No entanto, é deplorável a falta de factos e números precisos no que respeita a esses sistemas. No sistema semafórico do Reino Unido, são assinaladas «numerosas detenções» relacionadas com «vários crimes», mas sem especificar a conexão com o terrorismo ou a criminalidade organizada. Não são dados pormenores relativos ao programa dos EUA, a não ser que a UE pôde «apreciar o valor dos dados PNR e as suas potencialidades para efeitos de aplicação da lei».

28. Não só há uma falta de informação precisa *na proposta* sobre os resultados concretos de tais sistemas PNR, como os relatórios publicados *por outros serviços*, p. ex. o GAO dos Estados Unidos, não confirmam nesta fase a eficácia das medidas ([4]).

([1]) Esta definição provém de um estudo recente do Conselho da Europa sobre caracterização: L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD), Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, Novembro de 2007 (ainda não publicado). Ver também a definição de Lee Bygrave: «De um modo geral, a caracterização é o processo de inferir um conjunto de características (normalmente comportamentais) de uma determinada pessoa ou entidade colectiva e em seguida tratar essa pessoa/ /entidade (ou outras pessoas/entidades) à luz dessas características. O processo de caracterização tem duas componentes principais: i) criação do perfil — o processo de inferir um perfil, ii) aplicação do perfil — o processo de tratar pessoas/entidades à luz deste perfil» (Tradução oficiosa do Secretariado-Geral do Conselho). L. A. BYGRAVE, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, 2001, vol. 17, pp. 17-24: http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Ver *Rotaru v. Romania*, n.º 28341/95, pontos 50, 52 e 55 (Tradução oficiosa do Secretariado-Geral do Conselho). Ver também *Amann v. Switzerland*, n.º 27798/95, pontos 50 e segs.

([3]) Capítulo 2.1, «Definição do problema».

([4]) Ver p. ex. o relatório do «Accountability Office» do Governo dos Estados Unidos a membros do Congresso, Maio de 2007, «Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain»: http://www.gao.gov/new.items/d07346.pdf

29. A AEPD considera que deve ser aprofundada a avaliação das técnicas que consistem em avaliar o risco produzido por pessoas mediante instrumentos de prospecção de dados e padrões de comportamento, e que deve ser claramente estabelecida a sua utilidade no âmbito da luta contra o terrorismo, antes de serem utilizadas em tão grande escala.

Proporcionalidade

30. Para apreciar o equilíbrio entre a ingerência na vida privada das pessoas e a necessidade das medidas ([1]), são tidos em consideração os seguintes elementos:

— as medidas aplicam-se a todos os passageiros, estejam ou não sob investigação das autoridades de aplicação da lei, e constituem uma investigação antecipatória, numa escala sem precedentes,

— as decisões sobre pessoas singulares podem ser baseadas em perfis abstractos, incluindo assim uma margem de erro significativa,

— as medidas a tomar contra a pessoa são de natureza policial: as consequências em termos de exclusão ou coerção são, por conseguinte, muito mais intrusivas que noutros contextos, como sejam a fraude relacionada com cartões de crédito ou as técnicas de comercialização.

31. O cumprimento do princípio da proporcionalidade implica não só que a medida proposta seja eficiente, mas também que a finalidade prevista pela proposta não possa ser atingida com instrumentos menos invasivos da privacidade. Não ficou demonstrada a eficiência das medidas propostas. Deve ser cuidadosamente ponderada a existência de alternativas antes de criar medidas adicionais/ /novas para tratamento da informação de carácter pessoal. No entender da AEPD, não foi feita essa avaliação circunstanciada.

32. A AEPD chama a atenção para os outros sistemas de grande dimensão para controlo das deslocações de pessoas nas fronteiras da UE ou no seu interior, quer estejam já em funcionamento ou em fase de implementação, nomeadamente o Sistema de Informação sobre Vistos ([2]) e o Sistema de Informação Schengen ([3]). Se bem que estes instrumentos não tenham como objectivo principal a luta contra o terrorismo ou a criminalidade organizada, são até certo ponto acessíveis às autoridades de aplicação da lei para a finalidade mais lata de combate ao crime ([4]).

33. Um outro exemplo é a disponibilização a todos os Estados-Membros da União Europeia dos dados pessoais contidos nas bases de dados das polícias nacionais, sobretudo no que respeita à informação biométrica, no âmbito do Tratado de Prüm assinado em Maio de 2005 ([5]).

34. Todos estes diferentes instrumentos têm em comum permitir um controlo um controlo global das deslocações de pessoas, se bem que com diferentes perspectivas. A forma como já contribuem para a luta contra determinadas formas de criminalidade, incluindo o terrorismo, deverá ser objecto de uma análise profunda e circunstanciada, antes de ser decidido criar uma nova forma de verificação sistemática de todas as pessoas que entram ou saem da UE de avião. A AEPD recomenda que a Comissão efectue tal análise, como passo necessário no processo legislativo.

Conclusão

35. Tendo em conta o que precede, a AEPD conclui o seguinte sobre a legitimidade das medidas propostas. A utilização de diferentes bases de dados, sem uma visão global dos resultados concretos e das deficiências:

— é contrária a uma política legislativa racional, em que não devem ser adoptados novos instrumentos antes de os já existentes terem sido plenamente aplicados e se ter constatado que são insuficientes ([6]),

— poderia, caso contrário, conduzir a uma viragem para uma sociedade de vigilância total.

36. A luta contra o terrorismo é certamente um motivo legítimo para aplicar excepções aos direitos fundamentais da privacidade e da protecção de dados. Contudo, para ser válida, a necessidade da ingerência deve fundamentar-se em elementos claros e inegáveis, e deve ser demonstrada a

([1]) Segundo o artigo 9.º da Convenção n.º 108, «é possível derrogar as disposições dos artigos 5.º, 6.º e 8.º da presente Convenção quando tal derrogação, prevista pela lei da Parte, constitua medida necessária numa sociedade democrática:
1. para protecção da segurança do Estado, da segurança pública, dos interesses monetários do Estado ou para repressão das infracções penais;
2. para protecção do titular dos dados e dos direitos e liberdades de outrem.».

([2]) Decisão 2004/512/CE do Conselho, de 8 de Junho de 2004, que estabelece o Sistema de Informação sobre Vistos (VIS) (JO L 213 de 15.6.2004, p. 5); Proposta de regulamento do Parlamento Europeu e do Conselho relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração, COM(2004) 0835 final; Proposta de decisão do Conselho relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades dos Estados-Membros responsáveis pela segurança interna e da Europol para efeitos de prevenção, detecção e investigação de infracções terroristas e outras infracções penais graves, COM(2005) 0600 final.

([3]) Ver nomeadamente a Decisão 2007/533/JAI do Conselho, de 12 de Junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (SIS II) (JO L 205 de 7.8.2007).

([4]) Proposta de decisão do Conselho relativa ao acesso para consulta ao Sistema de Informação sobre Vistos (VIS) por parte das autoridades dos Estados-Membros responsáveis pela segurança interna e da Europol para efeitos de prevenção, detecção e investigação de infracções terroristas e outras infracções penais graves [COM(2005) 600 final] (JO C 97 de 25.4.2006, p. 6).

([5]) Ver os pareceres da AEPD sobre as decisões de Prüm: Parecer de 4 de Abril de 2007 sobre a iniciativa de 15 Estados-Membros com vista a adoptar uma decisão do Conselho relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras (JO C 169 de 21.7.2007, p. 2) e Parecer de 19 de Dezembro de 2007 sobre a iniciativa da República Federal da Alemanha com vista a adoptar uma decisão do Conselho respeitante à implementação da Decisão 2007/…/JAI relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras, disponível em: http://www.edps.europa.eu

([6]) A AEPD já insistiu várias vezes nesta questão, que considera importante, mais recentemente no seu parecer de 25 de Julho de 2007 sobre a melhor aplicação da directiva relativa à protecção de dados (JO C 255 de 27.10.2007, p. 1).

proporcionalidade da medida. Isso é ainda mais necessário no caso de ampla ingerência na vida privada das pessoas, tal como prevê a proposta em apreço.

37. Ora o que se verifica é que a proposta não contém tais elementos de justificação e não são satisfeitos os testes da necessidade e da proporcionalidade.

38. A AEPD insiste em que os testes de necessidade e proporcionalidade acima referidos são de natureza essencial. Constituem mesmo uma condição *sine qua non* para a entrada em vigor da presente proposta. Todas as posteriores considerações da AEPD no presente parecer devem ser vistas à luz desta condição prévia.

III. LEGISLAÇÃO APLICÁVEL — EXERCÍCIO DOS DIREITOS DAS PESSOAS EM CAUSA

Legislação aplicável

39. A análise deste tópico será articulada em torno de três elementos:

— uma descrição das diversas fases do tratamento previsto na proposta, a fim de identificar a legislação aplicável em cada fase,

— as restrições da proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, em termos de âmbito de aplicação e direitos das pessoas em causa,

— uma análise mais geral para determinar até que ponto um instrumento do terceiro pilar pode ser aplicado a intervenientes privados que procedem a tratamento de dados no âmbito do primeiro pilar.

Legislação aplicável nas diferentes fases do tratamento

40. O artigo 11.º da proposta diz que «os Estados-Membros devem assegurar que a decisão-quadro (…) do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal é aplicada ao tratamento dos dados pessoais ao abrigo da presente decisão-quadro».

41. No entanto, apesar desta disposição, não resulta claro até que ponto a decisão-quadro de protecção de dados — que é um instrumento do terceiro pilar do Tratado UE — será aplicável aos dados tratados pelas companhias aéreas, recolhidos pelas UIP e posteriormente tratados por outras autoridades competentes.

42. A primeira fase do tratamento de dados pessoais previsto na proposta é o tratamento pelas transportadoras aéreas, que são obrigadas a facultar os dados PNR às UIP nacionais, usando em princípio um sistema de exportação («push»). A redacção da proposta e da avaliação de impacto ([1]) parece implicar que os dados também poderiam ser transmitidos pelas companhias aéreas aos intermediários por atacado. As companhias aéreas dedicam-se principalmente a uma actividade comercial, sujeitas à legislação nacional de protecção de dados que transpõe a Directiva 95/46/CE ([2]). As questões sobre a legislação aplicável surgirão quando os dados recolhidos forem utilizados para fins policiais ([3]).

43. Em seguida, os dados serão filtrados por um intermediário (para os formatar e excluir os dados PNR não incluídos na lista dos dados requeridos pela proposta) ou enviados directamente às UIP. Os intermediários podem também ser agentes do sector privado, como sucede com a SITA, que opera nesse sentido no quadro do acordo PNR com o Canadá.

44. No que respeita às UIP, que são responsáveis pela avaliação de risco de todo o volume de dados, não é claro quem será responsável pelo tratamento. Poderão ser autoridades aduaneiras e serviços de fronteiras, e não necessariamente autoridades policiais.

45. A transmissão subsequente de dados filtrados às autoridades «competentes» seria provavelmente feita num contexto policial, pois a proposta diz que «as autoridades competentes incluem apenas autoridades responsáveis em matéria de prevenção e luta contra as infracções terroristas e a criminalidade organizada».

46. À medida que se sucedem as diferentes fases do tratamento, os intervenientes e as finalidades adquirem um elo mais estrito com a cooperação policial e judiciária em matéria penal. No entanto, a proposta não menciona explicitamente em que momento é aplicável a decisão-quadro de protecção de dados. A própria redacção da proposta leva a pensar que seria aplicável a todo o processo de tratamento, inclusive às companhias aéreas ([4]). Contudo, a decisão-quadro de protecção de dados contém em si certas restrições.

([1]) N.º 3 do artigo 6.º proposta e anexo A da avaliação de impacto «Método de transmissão dos dados pelas transportadoras aéreas».

([2]) 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 (JO L 281 de 23.11.1995, p. 31).

([3]) Ver a este respeito as consequências do acórdão PNR: Acórdão do Tribunal de Justiça de 30 de Maio de 2006, Parlamento Europeu/Conselho (C-317/04) e Comissão (C-318/04), processos apensos C-317/04 e C-318/04, Col. [2006], ponto 56.

([4]) Art. 11.º da proposta: Ver igualmente o considerando n.º 10 no preâmbulo: «A decisão-quadro (…) do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal deve ser aplicada a todos os dados tratados em conformidade com a presente decisão-quadro. Os direitos das pessoas abrangidas em relação ao tratamento dos dados, como o direito de informação, acesso, rectificação, apagamento ou bloqueio, bem como os direitos a compensação e recursos judiciais, devem ser os previstos nessa decisão-quadro».

47. Perante este pano de fundo, a AEPD questiona seriamente que o Título VI do Tratado UE possa servir de base jurídica para obrigações legais de intervenientes do sector privado, numa base de rotina e para fins policiais. Acresce que é pertinente a questão de saber se o Título VI do Tratado UE pode servir de base jurídica para obrigações legais de autoridades públicas que, em princípio, não recaem no âmbito da cooperação policial. Estas questões serão aprofundadas mais adiante no presente parecer.

Restrições da decisão-quadro de protecção de dados

48. A proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal contém pelo menos duas restrições que são pertinentes em termos de âmbito de aplicação.

49. Em primeiro lugar, o âmbito de aplicação da decisão-quadro de protecção de dados está bem definido na própria decisão-quadro: aplica-se «unicamente aos dados recolhidos ou tratados pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou de execução de sanções penais» ([1]).

50. Em segundo lugar, a decisão-quadro de protecção de dados não é aplicável aos dados tratados puramente a nível nacional, antes se limita aos dados trocados entre os Estados-Membros e à sua transferência para países terceiros ([2]).

51. A decisão-quadro de protecção de dados também contém alguns retrocessos em comparação com a Directiva 95/46/CE, em especial uma ampla excepção ao princípio da limitação da finalidade. No que toca a este princípio, a proposta limita claramente a finalidade do tratamento à luta contra o terrorismo e a criminalidade organizada. Porém, a decisão-quadro de protecção de dados permite o tratamento para fins mais amplos. Numa situação como esta, a *lex specialis* (a proposta) deve prevalecer sobre a *lex generalis* (a decisão-quadro de protecção de dados) ([3]). Isso mesmo deverá ser explicitado no texto da proposta.

52. Por conseguinte, a AEPD recomenda que seja aditada na proposta a seguinte disposição: «Os dados pessoais transmitidos pelas companhias aéreas de acordo com a presente decisão-quadro não podem ser tratados para outros fins além da luta contra o terrorismo e a criminalidade organizada. Não se aplicam as excepções ao princípio da finalidade previstas na decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal».

53. Em conclusão, a AEPD faz notar que há uma séria carência de certeza jurídica no que respeita ao regime de protecção de dados aplicável aos diversos intervenientes no projecto, em especial às companhias aéreas e outros agentes do primeiro pilar: a saber, as regras da proposta, as regras da decisão-quadro de protecção de dados ou a legislação nacional que transpõe a Directiva 95/46/CE. O legislador deverá clarificar em que preciso momento do processo de tratamento serão aplicáveis estas diferentes regras.

Condições de aplicação das regras do primeiro e do terceiro pilares

54. A AEPD questiona seriamente o facto de um instrumento do terceiro pilar criar obrigações legais, numa base de rotina e para fins policiais, a intervenientes do sector privado ou do sector público que, em princípio, não recaem no âmbito da cooperação policial.

55. Neste contexto, pode ser feita a comparação com outros dois casos em que o sector privado estava envolvido na conservação ou transferência de dados numa perspectiva policial:

— *o caso do acordo PNR com os EUA, que previa uma transferência sistemática de dados PNR às autoridades policiais pelas companhias aéreas.* O acórdão do Tribunal de Justiça no processo PNR excluiu a competência comunitária para celebrar o acordo PNR. Uma das motivações foi o facto de a transferência de dados para o CBP dos EUA constituir um tratamento que tem como objectivo a segurança pública e as actividades do Estado no domínio do direito penal ([4]). Neste caso, tratava-se de uma operação de transferência de dados para o CBP *de forma sistemática*, o que a torna diferente do caso seguinte:

— *a conservação geral de dados pelos operadores de comunicações electrónicas.* No que respeita à competência comunitária para estabelecer tal período de conservação, verifica-se que há uma diferença em relação ao acordo PNR com os EUA, dado que a Directiva 2006/24/CE ([5]) apenas prevê uma obrigação de conservação, ficando os dados sob o controlo dos operadores. Não está prevista a transferência sistemática para as autoridades de aplicação da lei. Pode-se, pois, concluir que, na medida em que os dados ficam sob o controlo dos prestadores de serviços, esses prestadores também ficam responsáveis, relativamente às pessoas em causa, pelo cumprimento das obrigações de protecção dos dados pessoais.

([1]) Considerando 5-A, versão de 11 de Dezembro de 2007 da decisão-quadro de protecção de dados.
([2]) Artigo 1.º.
([3]) No que respeita a este ponto, deve ser cuidadosamente ponderado e debatido o texto do artigo 27.º-B da última versão da decisão-quadro de protecção de dados no terceiro pilar.
([4]) Decisão do Tribunal de 30 de Maio de 2006, Parlamento Europeu/Conselho da União Europeia (C-317/04) e Comissão (C-318/04), processos apensos C-317/04 e C-318/04, Col. [2006], p. 56.
([5]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE (JO L 105 de 13.4.2006, p. 54).

56. Na proposta ora em apreço, as companhias aéreas têm de facultar os dados PNR de todos os passageiros de forma sistemática. No entanto, estes dados não são transferidos directamente por atacado às autoridades policiais: podem ser enviados a um intermediário e são avaliados por uma terceira parte, cujo estatuto ainda não é claro, antes de a informação seleccionada ser enviada às autoridades competentes.

57. A maior parte do tratamento decorre numa zona «cinzenta», que tem ligações materiais tanto com o primeiro como com o terceiro pilar. Como veremos com mais pormenor no Capítulo IV, não é clara a qualidade das partes intervenientes que procedem ao tratamento de dados. As companhias não são obviamente autoridades de aplicação da lei e os intermediários podem ser entidades do sector privado. Mesmo em relação às UIP, que seriam autoridades públicas, não é demais sublinhar que nem todas as autoridades públicas têm a qualidade e a competência para desempenhar funções policiais numa base de rotina.

58. Tradicionalmente, tem havido uma clara separação entre as actividades policiais e as do sector privado, sendo as funções policiais desempenhadas por serviços especificamente dedicados, em particular as forças de polícia, e sendo os intervenientes privados solicitados, caso a caso, a comunicar dados pessoais a esses serviços de aplicação da lei. Presentemente, a tendência é para impor a cooperação dos intervenientes privados para fins policiais de forma sistemática, o que levanta a questão de saber qual enquadramento de protecção de dados (primeiro ou terceiro pilar) se aplica às condições desta cooperação: deverão as regras ser baseadas na qualidade do responsável pelo tratamento dos dados (sector privado) ou na finalidade prosseguida (aplicação da lei)?

59. A AEPD já chamou a atenção para o risco de vazio jurídico entre as actividades do primeiro e do terceiro pilares ([1]). Na verdade, não é possível determinar com clareza se as actividades de empresas privadas, de algum modo relacionadas com a aplicação da lei penal, são abrangidas pelo campo de acção do legislador da União Europeia com fundamento nos artigos 30.º, 31.º e 34.º do Tratado UE.

60. Se não for aplicável o enquadramento geral (primeiro pilar), o prestador de serviços terá de proceder a difíceis distinções nas suas bases de dados. Com o regime actual, resulta claro que o responsável pelo tratamento de dados tem de assegurar a mesma protecção de dados às pessoas em causa, independentemente da finalidade que justifica a conservação dos dados. Deve ser evitada, portanto, uma situação em que o tratamento de dados pelos prestadores de serviços para diferentes finalidades seja sujeito a diferentes regimes de protecção.

([1]) Ver Parecer da Autoridade Europeia para a Protecção de Dados respeitante à Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados (JO C 255 de 27.10.2007, p. 1). Ver também Relatório Anual de 2006, p. 47.

Exercício dos direitos das pessoas em causa

61. Os diferentes regimes jurídicos que seriam aplicáveis a nível nacional teriam um enorme impacto, sobretudo no exercício dos direitos das pessoas em causa.

62. O preâmbulo da proposta diz que «o direito de informação, acesso, rectificação, apagamento ou bloqueio, bem como os direitos a compensação e recursos judiciais, devem ser os previstos na decisão-quadro [de protecção de dados]». Contudo, esta afirmação não responde à questão de saber qual é o responsável pelo tratamento que tem o encargo de responder aos pedidos das pessoas em causa.

63. Se bem que a informação sobre o tratamento possa ser comunicada pelas companhias aéreas, a questão torna-se mais complicada quando se tratar do acesso aos dados ou da sua rectificação. De facto, estes direitos estão sujeitos a restrições na decisão-quadro de protecção de dados. Tal como acima referimos, é duvidoso que o prestador de serviços, no caso vertente uma companhia aérea, possa ser obrigado a conceder direitos diferenciados de acesso e rectificação, conforme a finalidade prosseguida (comercial ou policial). Poder-se-á argumentar que tais direitos deverão ser exercidos perante a UIP ou as autoridade competentes designadas. No entanto, a proposta não dá mais nenhuma indicação a este respeito e, tal como já foi referido, também não resulta claro que essas autoridades (pelo menos as UIP) serão autoridades policiais normalmente sujeitas a procedimentos de acesso restrito (que pode ser indirecto).

64. A pessoa em causa corre também o risco de se ver confrontada com diversos destinatários dos dados, no que toca às UIP: os dados são de facto transmitidos à UIP do país de partida/destino dos voos, mas eventualmente também às UIP de outros Estados-Membros, numa base casuística. Além disso, é possível que vários Estados-Membros criem ou designem uma única UIP comum. Nesse caso, a pessoa em causa poderia ter de exercer o direito de recurso perante uma autoridade de outro Estado-Membro. Mais uma vez, não resulta claro se serão aplicáveis as regras nacionais de protecção de dados (em princípio, estarão harmonizadas na UE), ou se terá que ser tida em conta legislação policial específica (dada a falta de plena harmonização no terceiro pilar a nível nacional).

65. Põe-se a mesma questão a respeito do acesso aos dados tratados por intermediários, cujo estatuto é nebuloso e que poderão ser comuns a companhias aéreas de diversos Estados-Membros da UE.

66. A AEPD deplora a incerteza que subsiste quanto ao exercício destes direitos fundamentais da pessoa em causa. Salienta igualmente que esta situação se deve principalmente ao facto de se confiarem responsabilidades a intervenientes que não têm a aplicação da lei como missão principal.

Conclusão

67. A AEPD considera que a proposta deverá indicar claramente qual é o regime jurídico aplicável em tal ou tal fase do tratamento e especificar perante qual interveniente ou autoridade serão exercidos os direitos de acesso e de recurso. A AEPD recorda que, em conformidade com o n.º 1, alínea b), do artigo 30.º do Tratado UE, as disposições em matéria de protecção de dados devem ser apropriadas e cobrir toda a gama de operações de tratamento determinada pela proposta. Não é suficiente uma simples referência à decisão-quadro de protecção de dados, em virtude do âmbito limitado dessa decisão-quadro e das restrições de direitos que contém. Na medida em que estejam envolvidas autoridades policiais, as regras da decisão-quadro de protecção de dados deverão, pelo menos, aplicar-se a todo o processo de tratamento previsto na proposta, a fim de garantir que os princípios de protecção de dados são aplicados com coerência.

IV. QUALIDADE DOS DESTINATÁRIOS

68. A AEPD regista que a proposta não prevê nenhum requisito para a qualidade dos destinatários dos dados pessoais recolhidos pelas companhias aéreas, quer sejam intermediários, quer Unidades de Informações de Passageiros, quer autoridades competentes. Há que salientar que a qualidade do destinatário tem uma relação directa com o tipo de garantia de protecção de dados que se aplica a esse mesmo destinatário. Já foi referida a diferença entre as garantias prestadas, nomeadamente, pelas regras do primeiro e do terceiro pilares. É essencial que o regime aplicável seja claro para todas as partes envolvidas, incluindo os governos nacionais, os serviços de aplicação da lei, as autoridades de protecção de dados, bem como os responsáveis pelo tratamento de dados e as próprias pessoas em causa.

Intermediários

69. A proposta não dá indicações sobre a qualidade dos intermediários ([1]). Também não é especificado o papel dos intermediários enquanto responsáveis pelo tratamento ou subcontratantes. A experiência mostra que uma entidade do sector privado, seja ela um Sistema Informatizado de Reserva ou outra, pode perfeitamente ser encarregada da tarefa de recolher dados PNR directamente das companhias aéreas e de os transmitir às UIP. É precisamente dessa forma que os dados são tratados no âmbito do Acordo PNR com o Canadá. A SITA ([2]) é a empresa responsável pelo tratamento da informação. O papel do intermediário é crucial, já que pode ser responsável pela filtragem/reformatação dos dados que são transmitidos por atacado pelas companhias aéreas ([3]). Mesmo que os intermediários sejam obrigados a apagar a informação tratada logo que tenha sido transmitida às UIP, o tratamento é por si mesmo uma actividade altamente sensível: uma das consequências da intervenção dos intermediários é a criação de uma base de dados adicional que contém enormes quantidades de dados e inclusive, segundo a proposta, dados sensíveis (embora os intermediários sejam obrigados a apagar esses dados sensíveis). Por este motivo, a AEPD recomenda que não haja intermediários envolvidos no tratamento de dados de passageiros, a menos que haja requisitos estritos de qualidade e definição de tarefas.

Unidades de informações de passageiros

70. As UIP desempenham um papel crucial na identificação de pessoas que estão ou podem estar envolvidas ou associadas ao terrorismo ou à criminalidade organizada. Nos termos da proposta, serão responsáveis pela criação de indicadores de risco e por prestar informação sobre padrões de viagem ([4]). Quando a avaliação de risco se baseia em padrões de viagem normalizados e não em provas materiais relacionadas com um caso concreto, pode-se considerar que a análise constitui uma investigação antecipatória. A AEPD sublinha que este tipo de tratamento é, em princípio, estritamente regulado na legislação dos Estados-Membros (se não mesmo proibido) e que o mesmo é atribuído a autoridades públicas específicas, cujo funcionamento também é estritamente regulado.

71. Por conseguinte, é confiado às UIP um tratamento muito sensível de informação sem que a proposta dê quaisquer pormenores sobre a sua qualidade e sobre as condições em que exercerão tal competência. Embora seja provável que esta competência será exercida por uma autoridade estatal, eventualmente a alfândega ou o serviço de fronteiras, a proposta não impede explicitamente os Estados-Membros de confiar o seu exercício aos serviços de informações ou mesmo a um tipo qualquer de subcontratante. A AEPD chama a atenção para o facto de a transparência e as garantias aplicáveis aos serviços de informações nem sempre serem idênticas às que se aplicam às autoridades tradicionais de aplicação da lei. Os pormenores sobre a qualidade das UIP são essenciais, já que isso terá consequências directas no quadro jurídico aplicável e nas condições de fiscalização. A AEPD considera que a proposta tem de incluir uma disposição adicional que especifique os requisitos para as UIP.

([1]) Artigo 6.º da proposta.

([2]) A SITA foi criada em 1949 por 11 companhias aéreas, seus membros. A indústria de transporte aéreo recebe soluções de valor acrescentado por intermédio da empresa comercial SITA INC (Information, Networking, Computing) e serviços de rede por intermédio da SITA SC numa base cooperativa.

([3]) Avaliação de impacto, anexo A, «Método de transmissão dos dados pelas companhias aéreas».

([4]) Artigo 3.º da proposta.

Autoridades competentes

72. Depreende-se do artigo 4.º da proposta que qualquer autoridade responsável pela prevenção ou luta contra as infracções terroristas e a criminalidade organizada pode ser destinatária de dados. Se bem que esteja claramente definida a finalidade, nada é dito sobre a qualidade da autoridade. A proposta não prevê nenhuma limitação dos destinatários às autoridades de aplicação da lei.

Tal como acima referimos a propósito das UIP, é essencial que a informação sensível em questão seja tratada num ambiente dotado de um claro enquadramento jurídico. Isso verifica-se muito mais claramente com as autoridades de aplicação da lei, por exemplo, que com os serviços de informações. Tendo em conta os elementos de prospecção de dados e a investigação antecipatória que a proposta contém, não se pode excluir que tais serviços de informações sejam envolvidos no tratamento de dados, sem exclusão de qualquer outro tipo de autoridades.

Conclusão

73. A título geral, a AEDP observa que a implementação de um sistema PNR da UE ainda se torna mais difícil se tivermos presente que as autoridades de aplicação da lei têm competências diferentes conforme a legislação nacional dos Estados-Membros, podendo incluir ou não as informações, os impostos, a imigração ou a polícia. Esta é, no entanto, uma razão suplementar para recomendar que a proposta seja redigida como muito mais precisão relativamente à qualidade dos referidos intervenientes e às garantias de controlo da execução das suas tarefas. A proposta deveria conter disposições adicionais, que especifiquem de forma estrita as competências e as obrigações legais dos intermediários, das UIP e de outras autoridades competentes.

V. **CONDIÇÕES DE TRANSFERÊNCIA PARA PAÍSES TERCEIROS**

74. A proposta contém certas salvaguardas quanto à transferência de dados PNR para países terceiros ([1]). Nomeadamente, prevê em termos explícitos a aplicação da decisão-quadro de protecção de dados às transferências de dados, estabelece uma limitação específica da finalidade e estipula que é necessário o consentimento do Estado-Membro em questão em caso de transferências subsequentes. A transferência deve também ser consentânea com a legislação do Estado-Membro em questão, bem como com os acordos internacionais aplicáveis.

75. Subsistem, porém, muitas questões, em especial no que respeita à qualidade do consentimento, às condições em que é aplicável a decisão-quadro de protecção de dados e à questão da «reciprocidade» na transmissão de dados a países terceiros.

([1]) Artigo 8.º da proposta.

Qualidade do consentimento

76. O Estado-Membro de origem tem de consentir expressamente nas transferências subsequentes de dados de um país terceiro para outro. A proposta não especifica em que condições e por quem será dado tal consentimento, nem se as autoridades nacionais de protecção de dados serão envolvidas nessa decisão. A AEPD considera que a forma como é dado o consentimento deverá, pelo menos, ser conforme com a legislação nacional sobre transferência de dados pessoais para países terceiros.

77. Além disso, o consentimento de um Estado-Membro não deverá prevalecer sobre o princípio de que o país destinatário deve prever um nível adequado de protecção para o tratamento pretendido. Estas condições deverão ser cumulativas, tal como sucede na decisão-quadro de protecção de dados (artigo 14.º). A AEPD sugere, portanto, o aditamento de uma alínea c) ao n.º 1 do artigo 8.º com a seguinte redacção: «e c) o Estado terceiro assegura um nível adequado de protecção para o tratamento de dados pretendido». A este respeito, a AEPD recorda que devem ser estabelecidos mecanismos que assegurem normas comuns e decisões coordenadas relativas à adequação ([2]).

Aplicação da decisão-quadro de protecção de dados

78. A proposta remete para as condições e salvaguardas contidas na decisão-quadro de protecção de dados e ao mesmo tempo estabelece expressamente certas condições, nomeadamente o acima mencionado consentimento do Estado-Membro em questão, e uma limitação da finalidade à prevenção e luta contra as infracções terroristas e a criminalidade organizada.

79. A decisão-quadro de protecção de dados, por seu turno, estabelece as condições em que é feita a transferência de dados para países terceiros, nomeadamente no que toca à limitação de finalidade, a qualidade dos destinatários, o consentimento do Estado-Membro e o princípio da adequação. Contudo, também prevê derrogações a estas condições de transferência: interesses superiores legítimos, especialmente interesses públicos importantes podem constituir um motivo suficiente para a transferência, mesmo que não estejam preenchidas as condições acima referidas.

80. Como já teve ocasião de referir no capítulo III do presente parecer, a AEPD considera que o texto da proposta deve indicar claramente que as garantias mais concretas da proposta prevalecem sobre as condições gerais — e as excepções — da decisão-quadro de protecção de dados, quando esta for aplicável.

([2]) Parece da AEPD de 26 de Junho 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, pontos 27 a 30 (JO C 139 de 23.6.2007, p. 1).

Reciprocidade

81. A proposta foca a questão dos eventuais «pedidos retaliativos» por parte de países que poderão solicitar à UE dados PNR relativos a voos da UE para o seu território. Se a UE solicita dados provenientes das bases de dados das companhias aéreas desses países terceiros, porque estas operam um voo com partida ou destino na UE, esse mesmo país terceiro poderá solicitar o mesmo às companhias aéreas estabelecidas na UE, incluindo dados sobre cidadãos da UE. A Comissão admite essa eventualidade, embora a considere «muito remota». A este respeito, a proposta refere que o acordo com os Estados Unidos e o Canadá prevê tal tratamento recíproco «que pode ser aplicado automaticamente» ([1]). A AEPD questiona a importância de tal reciprocidade automática, bem como a aplicação de salvaguardas a essas transferências, nomeadamente tendo em conta a existência de um nível adequado de protecção no país em questão.

82. Há que fazer a distinção entre países terceiros que já celebraram um acordo com a UE e aqueles que não têm tal acordo.

Países que não têm acordo com a UE

83. A AEPD observa que a reciprocidade poderá conduzir à transferência de dados pessoais para países que não podem dar garantias em termos de padrões democráticos e nível adequado de protecção de dados.

84. A avaliação de impacto aduz mais alguns elementos relativamente às condições em que se efectua a transferência de dados para países terceiros e salienta a vantagem do sistema PNR da UE, em que os dados são filtrados pelas UIP. Apenas seriam transferidos dados seleccionados de indivíduos suspeitos (e não dados a granel) para as autoridades competentes dos Estados-Membros e, presumivelmente, também para países terceiros ([2]). A AEPD recomenda que este ponto seja clarificado no texto da proposta. Uma simples afirmação na avaliação de impacto não confere a protecção necessária.

85. Se bem que a selecção de dados contribua para minimizar o impacto na vida privada dos passageiros, cabe recordar que os princípios da protecção de dados vão muito mais além da minimização de dados, pois incluem princípios tais como a necessidade, a transparência e o exercício dos direitos que assistem às pessoas em causa, devendo todos eles ser tidos em conta ao determinar se um país terceiro oferece um adequado nível de protecção.

Países que têm acordo bilateral com a UE

86. A avaliação de impacto indica que esta eventualidade permitirá à UE «insistir em determinados padrões e assegurar a coerência nesses acordos bilaterais com países terceiros. Dará também a possibilidade de solicitar uma atitude recíproca por parte de países terceiros com os quais a UE venha a ter um acordo, coisa que não é possível actualmente» ([3]).

87. Destas observações decorre a questão de saber qual o impacto da proposta nos acordos existentes com o Canadá e os EUA. De facto, as condições de acesso aos dados previstas nesses acordos são muito mais latas, já que os dados não são sujeitos a uma selecção similar antes de ser transferidos para esses dois países terceiros.

88. A avaliação de impacto indica que «nos casos em que a UE tenha um acordo internacional com um país terceiro para o intercâmbio/transmissão de dados PNR com esse mesmo país terceiro, tais acordos deverão ser tidos na devida conta. As transportadoras deverão enviar os dados PNR às Unidades de Informações de Passageiros segundo a prática normal ao abrigo da presente medida. A UIP destinatária desses dados envia-os depois à autoridade competente do país terceiros com o qual exista um acordo desse tipo» ([4]).

89. Se por um lado a proposta parece ter como objectivo a transferência de *apenas dados seleccionados* para uma autoridade competente, quer dentro quer fora da UE, por outro lado a avaliação de impacto, o preâmbulo da proposta (considerando 21) e o próprio artigo 11.º recordam que devem ser tidos na devida os acordos existentes. Daí se poderá concluir que a filtragem apenas seria uma medida válida para os acordos a celebrar futuramente. Nesta perspectiva, é previsível que o acesso por grosso continue a ser a regra geral para o acesso aos dados PNR, p. ex. pelas autoridades dos EUA, em conformidade com o acordo UE-EUA, mas que, em paralelo e numa base caso-a-caso, ocorra uma transferência de dados para os EUA relativa a dados específicos identificados pelas UIP, que incluam mas não se limitem aos dados relativos a voos para os EUA.

90. A AEPD deplora a falta de clareza nesta ponto crucial da proposta. Considera ser da maior importância que as condições de transferência de dados PNR para países terceiros sejam coerentes e sujeitos a um nível harmonizado de protecção. Acresce que, por razões de certeza jurídica, as especificações relativas às garantias aplicáveis à transferência de dados devem ser incluídas na própria proposta e não apenas na avaliação de impacto, como sucede agora.

([1]) Exposição de motivos da proposta, capítulo 2.
([2]) Avaliação de impacto, capítulo 5.2, «Protecção da privacidade».
([3]) Avaliação de impacto, capítulo 5.2, «Relações com países terceiros».
([4]) Avaliação de impacto, anexo A, «Entidades a quem as Unidades de Informações de Passageiros transmitem dados».

VI. OUTROS PONTOS SUBSTANTIVOS

Tratamento automático

91. A AEPD faz notar que a proposta exclui expressamente que as unidades de informações de passageiros e as autoridades competentes dos Estados-Membros tomem medidas coercivas apenas devido ao tratamento automático de dados PNR ou em razão da origem racial ou étnica, crenças religiosas ou filosóficas, opiniões políticas ou orientação sexual da pessoa em causa ([1]).

92. Congratulamo-nos com essa especificação, dado que limita o risco de medidas arbitrárias contras pessoas singulares. Contudo, a AEPD verifica que o âmbito fica limitado a *medidas coercivas* das UIP ou autoridades competentes. Não exclui, na sua versão actual, a filtragem automática de pessoas segundo perfis padrão, nem evita a constituição automática de listas de pessoas suspeitas e a tomada de medidas como a vigilância alargada, enquanto tais medidas não forem consideradas coercivas.

93. A AEPD considera que a noção de *medidas coercivas* é demasiado vaga e que, em princípio, *nenhuma decisão* deve ser tomada a respeito de pessoas *apenas* em resultado do tratamento automático dos seus dados ([2]). A AEPD recomenda que se altere a proposta em conformidade.

Natureza dos dados

94. A proposta contém uma importante precisão no n.º 2 do artigo 5.º, ao estipular que as companhias aéreas não têm obrigação de recolher ou conservar dados além daqueles que foram recolhidos para a finalidade comercial inicial.

95. Porém, vários aspectos do tratamento destes dados merecem ainda uma observação:

— os dados a facultar, tal como enumerados no anexo 1 da proposta, são muito extensos, e a lista é semelhante à lista facultada às autoridades dos EUA segundo o acordo UE-EUA. A natureza dos dados requeridos já foi questionada várias vezes por Autoridades de Protecção de Dados, nomeadamente pelo Grupo do artigo 29.º ([3]),

— a redacção da avaliação de impacto ([4]) e do n.º 3 do artigo 6.º parece implicar que os dados também poderiam ser transmitidos pelas companhias aéreas aos intermediários por atacado. Numa primeira fase, os dados transmitidos a terceiros não ficariam sequer limitados à lista de dados PNR constante do anexo 1 da proposta,

— no que respeita ao tratamento de dados sensíveis, mesmo que tais dados possam ser filtrados na fase em que intervêm os intermediários, mantém-se a questão de saber se é estritamente necessário que as companhias aéreas transfiram o campo aberto.

A este respeito, a AEPD apoia as observações feitas no parecer do Grupo do artigo 29.º.

Método de transferência de dados PNR

96. As transportadoras aéreas estabelecidas fora da UE deverão transferir os dados às UIP ou aos intermediários pelo método de *exportação*, desde que possuam a estrutura técnica para o fazer. Caso contrário, deverão permitir o acesso aos dados para efectuar a sua *extracção*.

97. Permitir diferentes métodos de comunicação de dados conforme as capacidades das companhias aéreas apenas levantará mais dificuldades à acção de controlar se a transferência de dados PNR é feita segundo as regras de protecção de dados. Além disso, implica riscos de distorção de concorrência entre as companhias aéreas dentro e fora da UE.

98. A AEPD recorda que o método de «exportação», que permite às companhias aéreas manter o controlo da qualidade dos dados transferidos e das condições em que é feita a transferência, é o único método admissível à luz da proporcionalidade do tratamento. Por outro lado, deve consistir de facto numa «exportação», ou seja, os dados não deverão ser enviados a granel para o intermediário, mas sim filtrados logo na primeira fase do tratamento. Não é admissível que sejam enviados a terceiros os dados não necessários, assim como os dados não incluídos no anexo 1 da proposta, mesmo que tais dados venham a ser apagados imediatamente por esses terceiros.

Conservação de dados

99. O artigo 9.º da proposta prevê um prazo de conservação de 5 anos para os dados PNR, acrescido de um período de 8 anos em que os dados são conservados numa base dados «passiva», acessível em condições restritas.

([1]) Considerando n.º 20 e artigo 3.º, n.ºs 3 e 5, da proposta.

([2]) Ver a este respeito o n.º 1 do artigo 15.º da Directiva 95/46/CE. Essa directiva proíbe tais decisões automáticas nos casos em que possam afectar a pessoa em causa. Atendendo ao contexto da proposta, as decisões de natureza policial podem, em todo o caso, afectar gravemente a pessoa em causa. Também o facto de ser sujeita a controlos secundários pode afectar a pessoa em causa, especialmente se tais acções ocorrerem repetidas vezes.

([3]) Ver em especial o Parecer n.º 5/2007, de 17 de Agosto de 2007, sobre o Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento, celebrado em Julho de 2007, WP 138.

([4]) Avaliação de impacto, anexo A, «Método de transmissão dos dados pelas companhias aéreas».

100. A AEPD questiona a diferença entre estes dois tipos de bases de dados, pois é duvidoso que a base de dados passiva constitua realmente um arquivo, com diferentes métodos de armazenamento e recuperação de dados. Na realidade, a maioria das condições estabelecidas para o acesso à base de dados passiva consiste em requisitos de segurança que também podem ser aplicados à «base de dados de conservação por cinco anos».

101. Em todo o caso, o período total de armazenamento — isto é, 13 anos — é excessivo. A avaliação de impacto dá como justificação a necessidade de estabelecer indicadores de risco e padrões de viagem e comportamento ([1]), cuja eficácia carece ainda de melhor demonstração. Se bem que seja óbvio que os dados possam ser conservados por tanto tempo quanto necessário no caso de estar em curso uma investigação, não há justificação para conservar os dados de todos os passageiros durante 13 anos, em total ausência de suspeita.

102. A AEPD faz ainda notar que este período de conservação não é apoiado pelas respostas dos Estados-Membros ao questionário da Comissão, segundo o qual a duração média da armazenagem necessária seria de 3,5 anos ([2]).

103. Acresce que o período de 13 anos é comparável ao período de conservação de 15 anos no mais recente acordo com os Estados Unidos. A AEPD sempre depreendeu que este longo período de conservação apenas foi acordado em virtude da forte pressão do Governo dos EUA no sentido de dispor de um período muito mais amplo que 3,5 anos, e não porque tivesse sido defendido a qualquer momento pelo Conselho ou pela Comissão. Não há motivo para transpor tal compromisso — que apenas se justificou como resultado necessário das negociações — para um instrumento jurídico da própria UE.

Papel do Comité de Estados-Membros

104. O Comité de Estados-Membros estipulado pelo artigo 14.º da proposta seria competente por questões de segurança, incluindo protocolos e cifragem de dados PNR, e também em matéria de orientações para critérios gerais comuns, métodos e práticas de avaliação de risco.

105. Além destas indicações, a proposta não inclui nenhum elemento ou critério relativo às condições concretas e ao enquadramento do processo de avaliação de risco. A avaliação de impacto menciona que os critérios dependerão em última análise das informações detidas por cada Etado-Membro, que estão em constante evolução. Além disso, a avaliação de risco é efectuada num contexto de falta de normas uniformes de identificação de suspeitos. Parece, portanto, discutível em que medida o Comité de Estados-Membros poderá desempenhar um papel a este respeito.

Segurança

106. A proposta especifica uma série de medidas de segurança ([3]) a tomar pelas UIP, pelos intermediários e por outras autoridades competentes, a fim de proteger os dados. Dada a importância da base de dados e a sensibilidade do tratamento, a AEPD considera que, além das medidas previstas, a entidade que procede ao processo de tratamento dos dados deverá ser obrigada a notificar oficialmente qualquer violação da segurança.

107. A AEPD tem conhecimento do projecto de estabelecer tal procedimento de notificação no sector das comunicações electrónicas a nível europeu. Aconselha que essa salvaguarda seja incluída na presente proposta, e remete a este respeito para o sistema anti-quebras de segurança criado nos Estados Unidos relativamente às agências estatais ([4]). Na verdade, podem suceder incidentes de segurança em qualquer sector de actividade, tanto no privado como no público, como demonstrou a recente perda de toda uma base de dados de cidadãos pela administração britânica ([5]). As bases de dados de grande dimensão, como é a prevista na proposta em apreço, deveriam estar no topo das prioridades para beneficiar de tal sistema de alerta.

Cláusula de revisão e caducidade

108. A AEPD regista que será feita uma revisão no prazo de três a contar da entrada em vigor da decisão-quadro, com base num relatório da Comissão. A AEPD regista que esta revisão, baseada na informação prestada pelos Estados-Membros, prestará uma atenção específica às salvaguardas da protecção de dados, e incluirá a implementação do método de «exportação», a conservação de dados e a qualidade da avaliação de risco. Para ser completa, essa revisão deveria incluir os resultados de uma análise das estatísticas produzidas com base no tratamento dos dados PNR. Essas estatísticas deveriam incluir, além dos elementos mencionados no artigo 18.º da proposta, pormenores estatísticos relativos à identificação de pessoas de alto risco, tais como os critérios para essa identificação e os resultados concretos de qualquer acção policial decorrente da identificação.

([1]) Avaliação de impacto, anexo A, «Período de conservação de dados».
([2]) Avaliação de impacto, anexo B.
([3]) Artigo 12.º da proposta.
([4]) Ver em especial os trabalhos da «Identity Theft Task Force» americana: http://idtheft.gov/
([5]) Ver ao sitio Web do Serviço Britânico das Alfândegas e Impostos: http://www.hmrc.gov.uk/childbenefit/update-faqs.htm Ver também: http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. A AEPD já insistiu no presente parecer na falta de elementos concretos que estabeleçam a necessidade do sistema proposto. No entanto, considera que, no caso de a decisão-quadro entrar em vigor, deverá no mínimo ser complementada com uma cláusula de caducidade. No final do período de três anos, a decisão-quadro deverá ser revogada se não houver elementos que justifiquem a sua continuação.

Impacto noutros instrumentos jurídicos

110. Nas suas disposições finais, a proposta condiciona a aplicação subsequente de acordos ou convénios bilaterais ou multilaterais já existentes. Tais instrumentos só podem ser aplicados na medida em que sejam compatíveis com os objectivos da decisão-quadro proposta.

111. A AEPD põe em questão o âmbito desta disposição. Tal como já referimos no Capítulo V, secção «Reciprocidade», não é claro qual vai ser o impacto desta disposição no conteúdo dos acordos celebrados com países terceiros, como seja o acordo com os EUA. Por outro lado, não se sabe ao certo se a disposição terá impacto nas condições de aplicação de instrumentos com âmbito de aplicação mais lato, como a Convenção n.º 108 do Conselho da Europa. Embora isso se afigure improvável, dada a diferença de contexto institucional e de partes envolvidas, deverá ser evitado qualquer risco de interpretação errada, pelo que a proposta deverá clarificar que não tem qualquer impacto em instrumentos de âmbito mais lato, nomeadamente aqueles que têm como objecto a protecção de direitos fundamentais.

VII. **CONCLUSÕES**

112. A AEPD salienta o enorme impacto que a proposta em apreço terá em termos de protecção de dados. A AEPD centrou a sua análise em quatro questões fundamentais suscitadas pela proposta e insiste em que as questões levantadas têm de ser resolvidas de forma exaustiva. Tal como se apresenta, a proposta não é conforme com certos direitos fundamentais, nomeadamente o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, pelo que não deverá ser aprovada.

113. No caso de serem atendidas as observações acima expostas, em especial o teste da legitimidade, o presente parecer adianta certas propostas de redacção a ter em consideração pelo legislador. Para o efeito, refiram-se em especial os pontos 67, 73, 77, 80, 90, 93, 106, 109 e 111 do presente parecer.

Legitimidade das medidas propostas

114. Se bem que o objectivo geral de lutar contra o terrorismo e a criminalidade organizada seja por si próprio claro e legítimo, o cerne do processo de tratamento a criar não está suficientemente delimitado e justificado.

115. A AEPD considera que devem ser objecto de maior ponderação as técnicas que consistem em avaliar o risco de certas pessoas mediante instrumentos de prospecção de dados e padrões de comportamento, e que deve ser claramente estabelecida a sua utilidade no âmbito da luta contra o terrorismo, antes de serem utilizadas em tão grande escala.

116. A utilização de diferentes bases de dados, sem uma visão global dos resultados concretos e das deficiências:

— é contrária a uma política legislativa racional, em que não devem ser adoptados novos instrumentos antes de os já existentes terem sido plenamente aplicados e se ter constatado que são insuficientes,

— poderia, caso contrário, conduzir a uma viragem para uma sociedade de vigilância total.

117. A luta contra o terrorismo é certamente um motivo legítimo para aplicar excepções aos direitos fundamentais da privacidade e da protecção de dados. Contudo, para ser válida, a necessidade da ingerência deve fundamentar-se em elementos claros e inegáveis, e deve ser demonstrada a proporcionalidade da medida. Isso é ainda mais necessário no caso de ampla ingerência na vida privada das pessoas, tal como prevê a proposta em apreço.

118. A proposta não contém tais elementos de justificação e não são satisfeitos os testes da necessidade e da proporcionalidade.

119. A AEPD insiste em que os testes de necessidade e proporcionalidade acima referidos são de natureza essencial. Constituem uma condição *sine qua non* para a entrada em vigor da proposta.

Quadro jurídico aplicável

120. Em conclusão, a AEPD faz notar que há uma séria carência de certeza jurídica no que respeita ao regime aplicável aos diversos intervenientes no projecto, em especial às companhias aéreas e outros agentes do primeiro pilar: a saber, as regras da proposta, as regras da decisão-quadro de protecção de dados ou a legislação nacional que transpõe a Directiva 95/46/CE. O legislador deverá clarificar em que fase do processo de tratamento serão aplicáveis estas diferentes regras.

121. A actual tendência para impor a cooperação dos intervenientes privados para fins policiais de forma sistemática levanta a questão de saber qual enquadramento de protecção de dados (primeiro ou terceiro pilar) se aplica às condições desta cooperação: não está determinado se as regras deverão ser baseadas na qualidade do responsável pelo tratamento dos dados (sector privado) ou na finalidade prosseguida (aplicação da lei).

122. A AEPD já chamou a atenção para o risco de vazio jurídico entre as actividades do primeiro e do terceiro pilares ([1]). Na verdade, não é possível determinar com clareza se as actividades de empresas privadas, de algum modo relacionadas com a aplicação da lei penal, são abrangidas pelo campo de acção do legislador da União Europeia com fundamento nos artigos 30.º, 31.º e 34.º do Tratado UE.

123. Deve ser evitada uma situação em que o tratamento de dados pelos prestadores de serviços para diferentes finalidades seja sujeito a diferentes regimes de protecção, sobretudo perante as dificuldades que daí resultariam em matéria de exercício dos direitos das pessoas em causa.

Qualidade dos destinatários

124. A proposta deverá prever requisitos para a qualidade dos destinatários dos dados pessoais recolhidos pelas companhias aéreas, quer sejam intermediários, quer Unidades de Informações de Passageiros, quer autoridades competentes.

125. A qualidade do destinatário, que em certos casos pode ser um interveniente do sector privado, tem uma relação directa com o tipo de garantia de protecção de dados que se aplica a esse mesmo destinatário. É essencial que o regime aplicável seja claro para todas as partes envolvidas, incluindo o legislador, as autoridades de protecção de dados, os responsáveis pelo tratamento de dados e as próprias pessoas em causa.

Transferência de dados para países terceiros

126. A AEPD sublinha a necessidade de assegurar haja um nível de protecção adequado no país destinatário. Questiona também a importância do princípio da «reciprocidade» mencionado na proposta, bem como a sua aplicação a países já vinculados por um acordo com a UE, como o Canadá e os EUA. Considera ser da maior importância que as condições de transferência de dados PNR para países terceiros sejam coerentes e sujeitos a um nível harmonizado de protecção.

Outros pontos substantivos,

127. A AEPD chama a atenção do legislador para aspectos específicos da proposta que devem ser mais precisos ou que deverão atender melhor aos princípios da protecção de dados. Trata-se nomeadamente dos seguintes aspectos:

— devem ser restringidas as condições em que podem ser tomadas decisões automáticas,

— deve ser reduzido o volume de dados a tratar,

— o método de transferência de dados deve assentar apenas na exportação,

— o período de conservação de dados é considerado excessivo e injustificado,

— o papel do comité de Estados-Membros poderá ser mais preciso no que respeita às suas orientações sobre «avaliação de risco»,

— as medidas de segurança deverão incluir um processo de «notificação de quebra de segurança»,

— a revisão da decisão deverá incluir uma cláusula de caducidade,

— a proposta deverá especificar que não terá qualquer impacto em instrumentos com âmbito de aplicação mais lato que tenham como objectivo a protecção de direitos fundamentais.

Observações finais

128. A AEPD observa que a presente proposta é apresentada num momento em que o contexto institucional da União Europeia está prestes a sofrer uma alteração fundamental. As consequências do Tratado de Lisboa em termos de processo de decisão serão fundamentais, especialmente no que respeita ao papel do Parlamento.

129. Tendo em consideração o impacto sem precedentes que a proposta tem em termos de direitos fundamentais, a AEPD aconselha a que não seja adoptada no quadro dos Tratados actuais, antes se assegure que seguirá o processo de co-decisão previsto no novo Tratado. Isso reforçaria os fundamentos jurídicos com que serão tomadas as medidas essenciais previstas na proposta.

([1]) Ver Parecer da Autoridade Europeia para a Protecção de Dados respeitante à Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados (JO C 255 de 27.10.2007, p. 1). Ver também Relatório Anual de 2006, p. 47.