# PARECER DA 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 protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (COM (2005) 475 final)**

(2006/C 47/12)

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,

Tendo em conta o pedido de parecer segundo o n.º 2 do artigo 28.º 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.

ADOPTOU O SEGUINTE PARECER:

## I. OBSERVAÇÕES PRELIMINARES

*Consulta da AEPD*

1. A proposta de decisão-quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal foi transmitida pela Comissão à AEPD por carta de 4 de Outubro de 2005. A AEPD interpreta essa carta como um pedido de aconselhamento das instituições e órgãos comunitários, como prevê o n.º 2 do artigo 28.º do Regulamento 45/2001/CE. Segundo a AEPD, o presente parecer deve ser referido no preâmbulo da decisão-quadro.

*A importância da presente proposta*

2. A AEPD sublinha a importância da presente proposta, na óptica dos direitos e liberdades fundamentais das pessoas singulares, nos quais se inclui que os seus dados pessoais sejam protegidos. A adopção desta proposta representaria um importante passo em frente para protecção dos dados pessoais, num domínio importante que exige concretamente um mecanismo coerente e eficaz para a protecção dos dados pessoais ao nível da União Europeia.

3. Neste contexto, a AEPD salienta que a cooperação policial e judiciária entre os Estados-Membros tem uma importância crescente, enquanto elemento da criação gradual dum espaço de liberdade, segurança e justiça. O Programa da Haia introduziu o princípio da disponibilidade a fim de melhorar o intercâmbio transfronteiras de informações policiais. Segundo esse Programa ([1]), o mero facto de a informação atravessar fronteiras deveria deixar de ser relevante. A introdução do princípio da disponibilidade reflecte uma tendência mais geral para facilitar o intercâmbio de informações em matéria de aplicação da lei (ver por exemplo a chamada Convenção de Prüm ([2]) assinada por sete Estados-Membros e a proposta da Suécia de decisão-quadro relativa à simplificação do intercâmbio de dados e informações entre serviços responsáveis pela aplicação da lei ([3])). A recente aprovação pelo Parlamento Europeu da directiva do Parlamento Europeu e do Conselho relativa à conservação de dados de comunicação ([4]) pode ser vista sob o mesmo ângulo. Esta evolução exige a adopção de um instrumento jurídico que garanta uma protecção eficaz dos dados pessoais em todos os Estados-Membros da União Europeia, assente em normas comuns.

([1]) P. 18 do programa.

([2]) Convenção entre o Reino da Bélgica, a República Federal da Alemanha, o Reino da Espanha, a República Francesa, o Grão-Ducado do Luxemburgo, o Reino dos Países Baixos e a República da Áustria relativa à intensificação da cooperação transfronteiras, especialmente na luta contra o terrorismo, a criminalidade transfronteiras e a emigração ilegal. Prüm (Alemanha) 27 de Maio de 2005.

([3]) Iniciativa do Reino da Suécia tendo em vista a adopção da decisão-quadro relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia, nomeadamente no que respeita a infracções graves, incluindo actos terroristas (JO C 281).

([4]) Com base na proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação dos dados tratados em ligação com a oferta de serviços de comunicações electrónicas públicos e que altera a Directiva 2002/58/CE (COM (2005) 438 final

4. A AEPD salienta que o actual quadro geral da protecção de dados nesse domínio é insuficiente. Em primeiro lugar, a Directiva 95/46/CE excluiu do seu âmbito de aplicação o tratamento de dados pessoais efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas no Título VI do Tratado da União Europeia (n.º 2 do artigo 3.º da Directiva). Conquanto na maioria dos Estados-Membros o âmbito de aplicação da legislação de execução seja mais amplo que o exigido pela própria directiva, e não exclua o tratamento de dados para efeitos da acção policial, existem significativas diferenças no direito nacional. Em segundo lugar, a Convenção n.º 108 do Conselho da Europa ([1]), a que todos os Estados-Membros estão vinculados, não confere o rigor necessário à protecção como foi reconhecido já ao tempo da adopção da Directiva 95/46/CE. Em terceiro lugar, nenhum desses instrumentos jurídicos tem em conta as características específicas do intercâmbio de dados pelas autoridades policiais e judiciárias ([2]).

*Um contributo para o êxito da própria cooperação*

5. A protecção eficaz dos dados pessoais não só é importante para as pessoas a quem os dados dizem respeito mas contribui também para o êxito da própria cooperação policial e judiciária. Em muitos aspectos, os dois interesses públicos estão em perfeita sintonia.

6. Há que ter presente que os dados pessoais em causa são muitas vezes de natureza sensível e foram obtidos pelas autoridades policiais e judiciárias em consequência de uma investigação sobre pessoas. A vontade de trocar esses dados com autoridades de outros Estados-Membros será maior se a autoridade tiver garantias do nível de protecção nesse outro Estado-Membro. A AEPD refere enquanto elementos pertinentes da protecção de dados a confidencialidade e segurança dos dados e as restrições em matéria de acesso e ulterior utilização.

7. Acresce que um nível de protecção elevado pode assegurar a exactidão e a fiabilidade dos dados pessoais. Efectuado o intercâmbio de dados entre as autoridades policiais e/ou judiciárias, a exactidão e fiabilidade desses dados adquirem ainda maior importância, sobretudo porque, após sucessivos intercâmbios e retransmissões de dados entre as autoridades incumbidas da aplicação da lei, os dados são eventualmente tratados longe da respectiva fonte e fora do contexto em que foram originalmente recolhidos e utilizados. Em regra, as autoridades destinatárias nada sabem acerca das circunstâncias suplementares e têm que confiar plenamente nos próprios dados.

8. A harmonização das regulamentações nacionais em matéria de dados pessoais na esfera da polícia e da justiça — incluindo garantias adequadas para a protecção desses dados — pode pois estimular a confiança mútua, assim como a própria eficácia do intercâmbio.

*Observância dos princípios da protecção de dados aliada a um conjunto de regras suplementar*

9. A necessidade e a importância da presente proposta têm sido salientadas em diversas ocasiões. Durante a Conferência da Primavera em Cracóvia de Abril de 2005, as Autoridades Europeias para a Protecção de Dados adoptaram uma declaração e uma posição escrita em que apelavam para a adopção de um novo quadro jurídico em matéria de protecção de dados aplicável às actividades do terceiro pilar. Esse novo quadro deveria não só respeitar os princípios relativos à protecção de dados estabelecidos na Directiva 95/46/CE — importa assegurar a coerência da protecção de dados na União Europeia — mas também prever um conjunto de regras suplementar que tivesse em conta a especificidade do domínio da aplicação da lei ([3]). A AEPD acolhe com agrado o facto de a presente proposta ter em conta estes ponto de partida: respeita os princípios relativos à protecção de dados estabelecidos na Directiva 95/46/CE e prevê um conjunto de regras suplementar.

10. O presente parecer analisará até que ponto o resultado é aceitável na perspectiva da protecção de dados, com o devido respeito pelo contexto específico da protecção dos dados no domínio da aplicação da lei. Por um lado, os dados em causa são frequentemente de natureza muito sensível (ver ponto 6 do presente parecer) e, por outro lado, há uma forte pressão para o acesso a tais dados, na óptica de um desempenho eficaz da acção policial, que pode incluir a protecção da vida e da segurança física das pessoas. Segundo a AEPD, as regras em matéria de protecção de dados deverão responder às necessidades legítimas dos serviços responsáveis pela aplicação da lei, mas deverá também proteger a pessoa a quem os dados dizem respeito contra o tratamento e o acesso injustificados. Para se coadunar com o princípio da proporcionalidade, o resultado das considerações do legislador europeu tem de reflectir o respeito pelos dois interesse públicos potencialmente opostos. Neste contexto, a AEPD refere uma vez mais que os dois interesses estão frequentemente em sintonia.

*O contexto do Título VI do Tratado da União Europeia*

11. Por último, cabe referir que a presente proposta se insere no Título VI do Tratado da União Europeia, o chamado terceiro pilar. A intervenção do legislador comunitário está circunscrita por limitações claras: limitação das competências legislativas da União às matérias referidas nos artigos 30.º e 31.º, limitações quanto ao processo legislativo, que não compreende a participação plena do Parlamento Europeu, e limitações quanto ao controlo judicial uma vez que as competências do Tribunal de Justiça das Comunidades Europeias por força do artigo 35.º do TUE são incompletas. Estas limitações exigem uma análise ainda mais cuidada do texto da proposta.

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

([2]) Em 1987 o Conselho da Europa emitiu a Recomendação n.º R (87) 15, para a Regulamentação da Utilização de Dados Pessoais no Sector da Polícia, mas essa recomendação não é por natureza vinculativa para os Estados-Membros.

([3]) Ver no mesmo sentido «A AEPD aconselha as instituições comunitárias sobre propostas legislativas, assim como sobre documentos conexos» , 18 de Março de 2005, publicada em www.edps.eu.int.

## II. O CONTEXTO: INTERCÂMBIO DE INFORMAÇÕES AO ABRIGO DO PRINCIPIO DA DISPONIBILIDADE, CONSERVAÇÃO DE DADOS E QUADROS ESPECÍFICOS DO SIS II E DO VIS

### II.1 O princípio da disponibilidade

12. A proposta está intimamente ligada à proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade (COM(2005) 490 final). Esta última proposta visa implementar o princípio da disponibilidade e, ao fazê-lo, assegurar que a informação ao dispor das autoridades de um Estado-Membro competentes para a luta contra o crime seja fornecida às autoridades equivalentes de outros Estados-Membros. Deveria levar à supressão das fronteiras internas para o intercâmbio dessa informação, subordinando o intercâmbio de informações a condições uniformes em toda a União.

13. A estreita ligação entre as duas propostas resulta do facto de as informações policiais envolverem em grande medida dados pessoais. Não se pode adoptar legislação sobre o intercâmbio de informações em matéria de aplicação da lei sem se garantir uma protecção adequada dos dados pessoais. Quando uma intervenção ao nível da União Europeia conduz à supressão das fronteiras internas para o intercâmbio desses dados, a protecção dos dados pessoais deixa de poder ser tratada unicamente pelo direito nacional. Passou a ser atribuição das instituições europeias garantir a protecção dos dados pessoais em todo o território da União sem fronteiras internas. Essa atribuição está explicitamente enunciada na alínea b) do n.º 1 do artigo 30.º do TUE e é uma consequência da obrigação da União de respeitar os direitos fundamentais (artigo 6.º do TUE). Ademais:

— o n.º 2 do artigo 1.º da presente proposta declara explicitamente que os Estados-Membros já não podem restringir ou proibir o fluxo transfronteiras de informação por razões de protecção de dados pessoais.

— a proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade contém várias referências à presente proposta.

14. A AEPD salienta que uma decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade só deveria ser adoptada na condição de também ser adoptada uma decisão-quadro relativa à protecção dos dados pessoais. Todavia, a presente proposta de decisão-quadro do Conselho relativa à protecção dos dados tem os seus méritos e é necessária mesmo não havendo um instrumento jurídico sobre a disponibilidade. Este ponto foi salientado na Secção I do presente parecer.

15. Assim sendo, a AEPD analisará as duas propostas em dois pareceres distintos. Existe também uma razão de ordem prática: nada garante que as propostas sejam tratadas conjuntamente e com a mesma celeridade pelo Conselho e pelo Parlamento Europeu.

### II.2 Conservação de dados

16. Em 26 de Setembro de 2005, a AEPD apresentou o seu parecer sobre a proposta de directiva relativa à conservação de dados de comunicação [1]. Nesse parecer, apontou algumas lacunas importantes da proposta e sugeriu que se aditassem à directiva disposições específicas sobre o acesso das autoridades competentes aos dados relativos ao tráfego e à localização e sobre a ulterior utilização dos dados, e também que se aditassem outras garantias suplementares para efeitos de protecção de dados. O texto da directiva adoptado pelo Parlamento Europeu e o Conselho contém uma disposição limitada — mas de forma alguma suficiente — sobre protecção de dados e segurança de dados e contém uma disposição ainda mais insuficiente em matéria de acesso, que remete a formulação de medidas em matéria de acesso para o direito nacional, sob reserva das disposições pertinentes do direito da União Europeia ou do direito internacional público.

17. A aprovação da Directiva relativa à conservação de dados de comunicação torna ainda mais urgente que se estabeleça um quadro jurídico para a protecção de dados no terceiro pilar. Ao adoptar a directiva, o legislador comunitário obriga os prestadores de serviços de telecomunicações e de Internet a conservar dados para efeitos de aplicação da lei, sem as garantias necessárias e adequadas para a protecção da pessoa a quem os dados dizem respeito. Subsiste uma lacuna na protecção, uma vez que a directiva não aborda (suficientemente) o acesso aos dados, nem a sua ulterior utilização depois de as autoridades competentes no domínio da aplicação da lei terem tido acesso a esses dados.

18. A presente proposta vem colmatar uma parte importante dessa lacuna, já que se aplica à utilização ulterior dos dados, após o acesso aos mesmos pelas autoridades incumbidas de fazer cumprir a lei. A AEPD lamenta todavia que também a presente proposta não trate do acesso a esses dados. Ao contrário do que se prevê para os sistemas SIS II e VIS (ver II.3 do presente parecer), esta questão é deixada ao critério do legislador nacional.

### II.3 Tratamento no quadro do SIS II e do VIS

19. A União Europeia utiliza ou desenvolve actualmente vários sistemas de informação em larga escala (Eurodac, SIS II, VIS) e procura desenvolver sinergias entre esses sistemas. Há também uma tendência crescente para conceder um acesso mais amplo a esses sistemas para fins de aplicação da lei. Esta evolução tem enormes consequências e deve ter em conta, segundo o Programa da Haia, a «necessidade de obter o devido equilíbrio entre os fins da aplicação da lei e a garantia dos direitos fundamentais dos cidadãos».

[1] Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação dos dados tratados em ligação com a oferta de serviços de comunicações electrónicas públicos e que altera a Directiva 2002/58/CE (COM(2005) 438 final), publicado em www.edps.eu.int

20. No seu parecer de 19 de Outubro de 2005 sobre as propostas de Sistema de Informação Schengen de segunda geração (SIS-II) [1], a AEPD sublinhou certos elementos respeitantes à aplicação simultânea de regras gerais (*lex generalis* e regras mais específicas (*lex specialis)* em matéria de protecção de dados. A presente proposta pode ser vista como uma *lex generalis*, que substitui a Convenção n.º 108 no quadro do terceiro pilar [2].

21. A AEPD sublinha neste contexto que a proposta prevê também um quadro geral de protecção de dados para instrumentos específicos como a vertente de terceiro pilar do SIS II e o acesso dos serviços responsáveis pela aplicação da lei ao Sistema de Informação sobre Vistos. [3]

## III. **CERNE DA PROPOSTA**

### III.1 **Normas comuns aplicáveis a todo o tratamento de dados**

*Ponto de partida*

22. De acordo com o n.º 1 do artigo 1.º, a proposta destina-se a determinar normas comuns para garantir a protecção dos dados pessoais no decurso de actividades de cooperação policial e judiciária em matéria penal. O n.º 1 do artigo 1.º deve ser lido em conjugação com o n.º 1 do artigo 3.º, que estipula que a proposta é aplicável ao tratamento de dados pessoais (…) por uma autoridade competente para efeitos de prevenção, investigação, detecção e perseguição de infracções penais.

23. Destas disposições decorre que a decisão-quadro proposta tem duas características principais: estabelece normas comuns e aplica-se a todo o tratamento de dados pessoais para efeitos de aplicação do direito penal, mesmo que os dados em causa não tenham sido transmitidos ou disponibilizados pelas autoridades competentes de outros Estados-Membros.

24. A AEPD salienta a importância destas duas características principais. A presente proposta deveria ter por ambição estabelecer para a protecção de dados um enquadramento que complete inteiramente o quadro jurídico já existente no primeiro pilar. Só nesta condição poderá a União Europeia cumprir plenamente a sua obrigação, consignada no n.º 2 do artigo 6.º do TUE, de respeitar os direitos fundamentais tal como os garante a Convenção Europeia dos Direitos do Homem.

*Normas comuns*

25. Quanto à primeira característica: a presente proposta tem por objectivo assegurar que os princípios existentes em matéria de protecção de dados sejam aplicados na área do terceiro pilar. Além disso, prevê normas comuns que especificam esses princípios, tendo em vista a sua aplicação nesta área. A AEPD salienta a importância destes aspectos da proposta, que reflectem o carácter específico e sensível do tratamento de dados neste domínio. A AEPD aprecia, em particular, a introdução do princípio da distinção entre dados pessoais relativos a diferentes categorias de pessoas, como princípio específico de protecção de dados no domínio da cooperação policial e judiciária em matéria penal, para além dos princípios já existentes em matéria de protecção de dados (n.º 4 do artigo 4.º). No entender da AEPD, haverá que especificar *melhor* ainda o próprio princípio e as suas consequências jurídicas para a pessoa em causa (ver pontos 88-92 do presente parecer).

26. As regras devem aplicar-se a situações diversas, pelo que não podem ser demasiado pormenorizadas. Por outro lado, devem dar ao cidadão a necessária certeza jurídica e também uma protecção adequada dos seus dados pessoais. A AEPD considera que a proposta consegue em geral respeitar o equilíbrio entre estes dois requisitos jurídicos potencialmente incompatíveis. As disposições dão uma margem de flexibilidade nos aspectos em que tal é necessário, mas são na maior parte dos domínios suficientemente precisas para proteger o cidadão.

27. Em certos pontos, porém, a proposta é demasiado flexível e não oferece as garantias necessárias. No n.º 1 do artigo 7.º, por exemplo, a proposta estabelece uma derrogação geral em relação às garantias aí previstas, ao estipular que as mesmas se aplicam «salvo disposição em contrário da legislação nacional». Conceder um tão amplo poder discricionário no que se refere à manutenção dos dados por um período superior ao necessário para os fins previstos não só seria incompatível com o direito fundamental à protecção de dados, mas também prejudicaria contra a necessidade básica de harmonização da protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal.

28. As derrogações, nos casos em que sejam necessárias, deveriam limitar-se às disposições jurídicas — nacionais ou europeias — decretadas para proteger interesses públicos específicos. O n.º 1 do artigo 7.º deveria mencionar esses interesses públicos.

29. Estas considerações conduzem-nos a outro aspecto. Sempre que qualquer outro instrumento jurídico específico adoptado ao abrigo do Título VI do TUE preveja condições ou restrições mais precisas para o tratamento dos dados ou o acesso a eles, essa legislação mais específica deverá aplicar-se como sendo uma *lex specialis*. O artigo 17.º da presente proposta prevê derrogações aos artigos 12.º, 13.º, 14.º e 15.º se um acto legislativo específico adoptado ao abrigo do Título VI estabelecer condições específicas para a protecção dos dados. Esta

[1] § 2.2.4 do parecer.

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

[3] *Proposal for a Council Decision concerning the access for consultation to the Visa Information System to authorities in Member States responsible for internal security and to Europol for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences* (COM (2005) 600 final), emitida em 24 de Novembro de 2005. A AEPD tenciona formular um parecer sobre esta proposta no início de 2006.

disposição ilustra o carácter geral da proposta (tal como explicado mais acima) mas não abrange todas as hipóteses. No entender da AEPD, o artigo 17.º deveria:

— ser redigido de uma forma mais geral: se existirem actos legislativos mais específicos que rejam qualquer dos aspectos do tratamento de dados (e não apenas a transmissão de dados), esses actos legislativos são aplicáveis;

— incluir a ressalva de que as derrogações não podem fazer baixar o nível de protecção.

*Aplicável a todo o tratamento de dados pessoais*

30. Quanto à segunda característica: o resultado ideal seria que ficasse abrangida a totalidade da recolha e do tratamento dos dados pessoais no âmbito do terceiro pilar.

31. Para alcançar este objectivo, é essencial que a decisão-quadro abranja todos os dados policiais e judiciários, mesmo que estes não sejam transmitidos ou disponibilizados pelas autoridades competentes de outros Estados-Membros.

32. Esta condição é tanto mais importante quanto o facto de prever qualquer limitação aos dados transmitidos ou disponibilizados às autoridades competentes de outros Estados-Membros tornaria o campo de aplicação da decisão-quadro demasiado inseguro e incerto, o que seria contrário ao seu objectivo essencial ([1]) e prejudicaria a segurança jurídica das pessoas. Em circunstâncias normais, nunca se sabe de antemão — no momento da recolha ou do tratamento de dados pessoais — se esses dados serão relevantes para um intercâmbio de informações com as autoridades competentes de outros Estados-Membros. A AEPD refere, neste contexto, o princípio da disponibilidade e a supressão das fronteiras internas para o intercâmbio de dados relativos à aplicação da lei.

33. Por último, a AEPD faz notar que a proposta não se aplica aos seguintes aspectos:

— tratamento de dados no âmbito do segundo pilar do TUE (política estrangeira e de segurança comum);

— tratamento de dados pelos serviços de informações e acesso por parte desses serviços a tais dados quando estes são tratados pelas autoridades competentes ou por outras partes (o que decorre do artigo 33.º do TUE).

Nestes domínios, a legislação nacional deve prever uma adequada protecção das pessoas a quem os dados se referem. Esta lacuna na protecção a nível da UE deve ser tida em conta ao ponderar a proposta: ([2]) uma vez que nem todo o tratamento é possível no domínio da aplicação da lei, o legislador tem de assegurar uma protecção ainda mais eficaz nos domínios que são efectivamente abrangidos pela proposta.

III.2 **Base jurídica**

34. Os considerandos da proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade referem uma base jurídica específica, a saber, a alínea b) do n.º 1 do artigo 30.º. Em contraste, a presente proposta não especifica quais são, de entre as disposições do artigo 30.º ou do artigo 31.º, aquelas que constituem a sua base jurídica.

35. Embora não caiba à AEPD, nas suas funções de aconselhamento sobre a legislação da União Europeia, escolher a base jurídica de uma proposta, não deixa de ser útil supor que a presente proposta também poderia ter por base a alínea b) do n.º 1 do artigo 30.º. Poderia basear-se ainda na alínea c) do n.º 1 do artigo 31.º do TUE e aplicar-se, na sua totalidade, a situações existentes a nível nacional, na medida em que tal fosse necessário para melhorar a cooperação policial e judiciária entre Estados-Membros. Neste contexto, a AEPD salienta mais uma vez que todos os dados pessoais recolhidos, armazenados, tratados ou analisados para efeitos de aplicação da lei podem, em especial ao abrigo do princípio da disponibilidade, ser objecto de intercâmbio com as autoridades competentes de outro Estado-Membro.

36. A AEPD partilha a opinião de que a alínea b) do n.º 1 do artigo 30.º e a alínea c) do n.º 1 do artigo 31.º constituem uma base jurídica para regras em matéria de protecção de dados que não se limitem à protecção dos dados pessoais efectivamente trocados entre as autoridades competentes dos Estados-Membros mas sejam também aplicáveis a situações existentes a nível nacional. Em especial:

— A alínea b) do n.º 1 do artigo 30.º, que pode servir de base jurídica para as regras em matéria de recolha, armazenamento, tratamento, análise e intercâmbio das informações pertinentes não se limita às informações disponibilizadas ou transmitidas a outros Estados-Membros. A única limitação imposta pela alínea b) do n.º 1 do artigo 30.º reside na pertinência das informações para a cooperação policial.

— No que respeita à cooperação judiciária, a alínea c) do n.º 1 do artigo 31.º é ainda mais explícita, uma vez que a acção em comum incluirá o objectivo de «assegurar a compatibilidade das normas aplicáveis nos Estados-Membros, na medida do necessário para melhorar a referida cooperação».

— Do Processo Pupino14 decorre que o Tribunal de Justiça aplica princípios do direito comunitário a assuntos do terceiro pilar. Este processo reflecte a evolução de uma mera cooperação entre autoridades dos Estados-Membros no âmbito do terceiro pilar para a criação de um espaço de liberdade, segurança e justiça comparável ao mercado interno instituído pelo Tratado CE.

([1]) A AEPD remete para o mesmo raciocínio por parte do Tribunal de Justiça, nomeadamente no acórdão proferido in Österreichischer Rundfunk e Outros, Processos conjuntos C-465/00, C-138/01 e C-139/01 [Colectânea do Tribunal de Justiça Europeu, 2003, Página I-4989].

([2]) Neste mesmo sentido, ver parecer da AEPD de 26 de Setembro de 2005 sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE, ponto 33.

— No entender da AEPD, o princípio da eficácia implica que o Tratado não seja interpretado de uma forma que impeça as instituições da União Europeia de desempenharem eficazmente as suas funções, entre as quais se conta a protecção dos direitos fundamentais.

— Tal como atrás ficou dito, uma limitação às situações transfronteiras não respeitaria as consequências do princípio da disponibilidade e prejudicaria a segurança jurídica das pessoas.

37. A AEPD chama agora a atenção para uma questão a abordar separadamente: o *intercâmbio de dados com países terceiros*. Os Estados-Membros utilizam os dados pessoais recolhidos e tratados em países terceiros e transferidos para os Estados-Membros para efeitos de aplicação da lei, e transferem dados pessoais que eles próprios recolheram e/ou trataram para autoridades competentes de países terceiros e para organismos internacionais.

38. Os artigos 30.º e 31.º do TUE não exigem que os dados recolhidos por autoridades de países terceiros tenham um tratamento diferente do aplicado aos dados inicialmente recolhidos pelas autoridades competentes dos Estados-Membros. Uma vez recebidos, os dados provenientes de países terceiros devem respeitar os mesmos padrões que os dados recolhidos num Estado-Membro. No entanto, a qualidade dos dados nem sempre pode ser assegurada com facilidade (este aspecto será abordado no próximo capítulo do presente parecer).

39. A transmissão, pelas autoridades competentes dos Estados-Membros, de dados pessoais para países terceiros está, em sentido estrito, fora do âmbito do Título VI do TUE. No entanto, se os dados pudessem ser transmitidos para países terceiros sem assegurar a protecção da pessoa em causa, ficaria seriamente afectada a protecção dentro do território da União Europeia tal como prevista na presente proposta, pelas razões mencionadas na Secção III.4 do presente parecer. Ou seja:

— Os direitos da pessoa em causa tal como assegurados pela presente proposta ficariam directamente afectados se a transmissão para os países terceiros não estivesse sujeita às normas da protecção de dados.

— Existiria o risco de as autoridades competentes dos Estados-Membros contornarem as normas estritas em matéria de protecção de dados.

40. Em resumo, a aplicabilidade de regras comuns em matéria de protecção dos dados pessoais trocados pelas autoridades competentes dos Estados-Membros com as autoridades de países terceiros e as organizações internacionais é necessária para assegurar a eficácia das regras comuns em matéria de protecção de dados entre as autoridades competentes dos Estados-Membros e é, pois, necessária para melhorar a cooperação entre os Estados-Membros. Os artigos 30.º e 31.º do TUE constituem a base jurídica necessária.

### III.3 **Observações específicas sobre o âmbito da proposta**

*Dados pessoais tratados pelas autoridades judiciárias*

41. Os dados pessoais são objecto de tratamento e intercâmbio não só pelas forças de polícia mas também pelas autoridades judiciárias. A proposta, baseada nos artigos 30.º e 31.º do TUE, aplica-se à cooperação entre forças policiais e à cooperação entre autoridades judiciárias. Neste aspecto, a proposta tem um âmbito mais vasto que a decisão-quadro do Conselho relativa ao intercâmbio de informações, a qual se limita à cooperação policial e se aplica apenas às informações anteriores à instauração de um processo.

42. A AEPD congratula-se por a proposta ser extensiva aos dados pessoais tratados pelas autoridades judiciárias. Há muito boas razões para abordar numa mesma proposta dados policiais e dados das autoridades judiciárias tratados para efeitos de aplicação da lei. Em primeiro lugar, a organização da cadeia da investigação penal/instauração de processo penal varia entre Estados-Membros. A participação das autoridades judiciárias tem início em fases diferentes nos vários Estados-Membros. Em segundo lugar, todos os dados pessoais desta cadeia podem ter por destino um ficheiro judiciário. Não tem lógica prever regimes diferentes aplicáveis à protecção de dados nas fases anteriores.

43. Porém, no que se refere à fiscalização do tratamento de dados, é necessário seguir uma abordagem diferente. O artigo 30.º da proposta enumera as funções das autoridades de controlo. O n.º 9 do artigo 30.º estipula que os poderes da autoridade de controlo não afectam a independência do poder judicial. A AEPD recomenda que se esclareça na proposta que as autoridades de controlo não fiscalizam o tratamento de dados pelas autoridades judiciárias no exercício das suas funções judiciárias. ([1])

*Tratamento pela Europol e pela Eurojust (e pelo Sistema de Informação Aduaneiro)*

44. Nos termos do n.º 2 do artigo 3.º da proposta, a decisão-quadro não é aplicável ao tratamento de dados pessoais por parte da Europol, da Eurojust e do Sistema de Informação Aduaneiro ([2]).

([1]) Acórdão do Tribunal de Justiça de 16 de Junho de 2005, Pupino, Processo C-105/03.

([2]) Esta disposição poderia ser semelhante ao disposto no artigo 46.º do Regulamento 45/2001/CE.

45. Estritamente falando, esta disposição é supérflua, em todo o caso no que diz respeito à Europol e à Eurojust. Uma decisão-quadro ao abrigo da alínea b) do artigo 34.º do TUE só pode ser adoptada para efeitos de aproximação das disposições legislativas e regulamentares dos Estados-Membros, não podendo ser dirigida à Europol e à Eurojust.

46. Quanto ao fundo, o texto do n.º 2 do artigo 3.º conduz às seguintes observações:

— a presente proposta proporciona um quadro geral, que deverá em princípio ser aplicável a todas as situações abrangidas pelo terceiro pilar. A coerência do quadro jurídico da protecção de dados é em si mesma um elemento que reforça a eficácia da protecção de dados;

— actualmente, a Europol e a Eurojust têm ao seu dispor sistemas de protecção de dados bem definidos, incluindo um sistema de supervisão. Por este motivo, não há urgência imediata em adaptar ao texto da presente proposta as regras aplicáveis;

— todavia, a mais longo prazo, as regras de protecção de dados aplicáveis à Europol e à Eurojust deverão ser plenamente ajustadas à presente decisão-quadro;

— isso é tanto mais importante quanto a presente proposta de decisão-quadro — com excepção do seu Capítulo III — é aplicável à recolha e ao tratamento dos dados pessoais transmitidos à Europol e à Eurojust pelos Estados-Membros.

### III.4 **Estrutura da proposta**

47. A AEPD analisou a proposta e conclui que globalmente está prevista uma protecção estratificada. As normas comuns estabelecidas no Capítulo II da proposta (e as relativas a matérias específicas, nos Capítulos IV a VII) prevêem dois estratos de protecção:

— Transposição para o terceiro pilar de princípios gerais da protecção de dados estabelecidos na Directiva 95/46/CE e noutros instrumentos jurídicos das Comunidades Europeias, bem como na Convenção 108 do Conselho da Europa.

— Regras suplementares de protecção de dados aplicáveis a todo o tipo de tratamento de dados pessoais no âmbito do terceiro pilar, nomeadamente as disposições dos n.ºs 3 e 4 do artigo 4.º da proposta.

48. O Capítulo III acrescenta um terceiro estrato de protecção para formas específicas de tratamento de dados. Os títulos das duas secções deste capítulo e a formulação de diversas disposições da proposta limitam aparentemente a sua aplicação aos dados transmitidos ou disponibilizados pelas autoridades competentes noutros Estados-Membros. Como consequência, algumas disposições importantes para a protecção de dados pessoais apenas seriam aplicáveis se os dados fossem trocados entre Estados-Membros. Posto isto, o texto é ambíguo, uma vez que as próprias disposições parecem exceder as actividades directamente ligadas aos dados trocados. Seja como for, esta limitação do âmbito não é explicada explicitamente nem justificada quer no memorando explicativo, quer na avaliação do impacto.

49. A AEPD sublinha a mais-valia inerente a esta estrutura estratificada, que já de per si pode garantir uma grande protecção ao interessado, tendo com conta as exigências específicas da aplicação da lei. Por outro lado, corresponde à necessidade de uma protecção adequada de dados sublinhada na Conferência da Primavera em Cracóvia, em Abril de 2005 e, em princípio, está em conformidade com o artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e da Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais, nomeadamente o seu artigo 8.º.

50. Todavia, a análise do texto da proposta suscita as seguintes observações.

51. Em primeiro lugar, convém assegurar que as regras suplementares de protecção de dados constantes do Capítulo II (segundo estrato mencionado no ponto 47) não derroguem dos princípios gerais da protecção. No entender da AEPD, as regras suplementares do Capítulo II devem oferecer uma protecção suplementar aos interessados no contexto específico do terceiro pilar (informações policiais e judiciais). Por outras palavras, estas regras não devem diminuir o nível de protecção.

52. Além disso, o Capítulo III sobre formas específicas de tratamento (que inclui o terceiro estrato de protecção) não deveria derrogar do Capítulo II. No entender da AEPD, as disposições do Capítulo III devem oferecer uma protecção suplementar aos interessados em situações que envolvam as autoridades competentes de mais do que um Estado-Membro, não devendo em caso algum diminuir o nível de protecção.

53. Em segundo lugar, não deveriam ser integradas no Capítulo III regras de natureza genérica. A AEPD recomenda que essas disposições sejam transferidas para o Capítulo II. No Capítulo III, apenas devem ser incluídas disposições estritamente relacionadas com a protecção de dados pessoais no âmbito do intercâmbio de dados entre Estados-Membros. Isto é tanto mais importante quanto o Capítulo contém disposições importantes que visam um elevado nível de protecção dos interessados no âmbito da aplicação da lei (cf. ponto VI.1 do presente parecer).

## IV. **ANÁLISE DA PROPOSTA NA ESPECIALIDADE**

### IV.1 **Pontos de referência da análise**

54. A AEPD terá em conta a especificidade da estrutura e do conteúdo da proposta ao analisar os vários elementos constitutivos, mas não comentará cada um dos artigos da proposta.

55. Em primeiro lugar, a maioria das disposições reflecte outros instrumentos jurídicos da UE relativos à protecção de dados pessoais. Estas disposições são consentâneas com o quadro jurídico da protecção de dados da UE e fornecem garantias adequadas nesta matéria no âmbito do terceiro pilar.

56. Todavia, a AEPD regista que certas disposições do Capítulo III da proposta — relativas a pontos específicos de tratamento e geralmente aplicáveis (cf. ponto 48 do presente parecer) apenas a dados trocados com outros Estados-Membros — integram princípios gerais e essenciais da legislação da UE em matéria de protecção de dados. Por conseguinte, estas disposições deveriam ser transferidas para o Capítulo II e ser aplicáveis a todo o tipo de tratamento de dados pelas autoridades responsáveis pela aplicação da lei. Trata-se nomeadamente das disposições relativas à verificação da qualidade dos dados (n.os 1 e 6 do artigo 9.º) e ao tratamento posterior de dados pessoais (n.º 1 do artigo 11.º).

57. Certos outros artigos do Capítulo III da proposta não distinguem entre condições suplementares especificamente relacionadas com o intercâmbio de dados com outros Estados-Membros — como o consentimento da autoridade competente do Estado-Membro que transmite os dados — e as salvaguardas que são importantes e necessárias também no contexto dos dados tratados num Estado-Membro. Nestes casos, a AEPD recomenda que estas salvaguardas passem a ser geralmente aplicáveis, mesmo aos dados pessoais que não tenham sido transmitidas ou postos à disposições de outro Estado-Membro. Esta recomendação diz respeito:

— à transmissão de dados a particulares e a autoridades que não as autoridades de aplicação da lei (alíneas a) e b) dos artigos 13.º e 14.º) e

— à transferência de dados para países terceiros ou organismos internacionais ( artigo 15.º com excepção da alínea c)).

58. Nesta parte do parecer, chama-se a atenção do legislador para algumas salvaguardas não estipuladas na presente proposta. No entender da AEPD, estas salvaguardas suplementares devem ser previstas no que respeita a decisões individuais automáticas, aos dados pessoais recebidos de países terceiros, ao acesso a bases de dados privadas, ao tratamento de dados biométricos e aos perfis de ADN.

59. Além disso, a análise que se segue inclui recomendações no intuito de melhorar o actual texto, a fim de assegurar a eficácia das disposições, a coerência do texto e a adequação ao actual quadro jurídico em matéria de protecção de dados.

### IV.2 **Limitação da finalidade e tratamento posterior**

60. A alínea b) do n.º1 do artigo 4.º estipula que os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não devem ser posteriormente tratados de forma incompatível com essas finalidades. Regra geral, os dados serão recolhidos no contexto de um crime específico (ou, em certas circunstâncias, para investigar uma associação ou rede criminosa, etc.). Podem ser utilizados para esta finalidade primeira e posteriormente tratados para outros fins desde que estes sejam compatíveis com a finalidade primeira (por exemplo, dados recolhidos sobre um indivíduo condenado por tráfico de droga podem ser utilizados no quadro de uma investigação de uma rede de traficantes). Esta abordagem reflecte bem o princípio da limitação da finalidade, tal como se encontra consagrado no artigo 8.º da Convenção Europeia dos Direitos do Homem e corresponde, pois, à legislação sobre protecção de dados em vigor.

*Tratamento posterior para fins abrangidos pelo âmbito da decisão-quadro*

61. A AEPD observa que a proposta não contempla de modo totalmente satisfatório uma situação que pode surgir no âmbito do trabalho policial, nomeadamente, a necessidade de utilização posterior dos dados para fins considerados incompatíveis com a finalidade para a qual foram recolhidos. Uma vez recolhidos pela polícia, os dados podem ser necessários para resolver um crime totalmente diferente. A título de exemplo, podem referir-se os dados recolhidos no âmbito da sanção de infracções rodoviárias que são posteriormente utilizados para localizar e perseguir o autor do roubo de um veículo. A segunda finalidade, por muito legítima que seja, não pode ser considerada como totalmente compatível com a finalidade da recolha de dados. Se as autoridades responsáveis pela aplicação da lei não puderem utilizar os dados para esta segunda finalidade, podem tender a recolher dados para fins alargados ou mal definidos e, nesse caso, o princípio da limitação da finalidade perderia o seu valor para efeitos de recolha. Além disso, seria dificultada a aplicação de outros princípios, designadamente a proporcionalidade, a exactidão e a fiabilidade (cf. alíneas c) e d) do n.º 1 do artigo 4.º)

62. Segundo a legislação da UE em matéria de protecção de dados, os dados pessoais devem ser recolhidos para finalidades determinadas e explícitas e não ser posteriormente tratados de forma incompatível com essas finalidades. Todavia, a AEPD é de parecer que deve ser permitida alguma flexibilidade para utilizações posteriores. A limitação da recolha será provavelmente mais respeitada pelas autoridades encarregadas pela segurança interna se puderem contar, com as devidas salvaguardas, com derrogações da limitação da utilização posterior.

63. Convém recordar que esta necessidade de tratamento posterior é reconhecida no artigo 11.º da proposta, embora de forma bastante insuficiente. Com efeito, o artigo 11.º apenas se aplica a dados recebidos ou disponibilizados pela autoridade competente de outro Estado-Membro e não prevê salvaguardas suficientes.

64. A AEPD recomenda que o n.º1 do artigo 11.º seja aplicável a todos os dados quer tenham sido recebidos de outro Estado-Membro quer não. Além disso, devem ser acrescentadas salvaguardas mais rigorosas ao disposto na alínea b) do n.º1 do artigo 11.º. A utilização posterior de dados para fins considerados incompatíveis com a finalidade primeira deve ser permitida apenas quando for estritamente necessária, num caso específico, para efeitos de prevenção, investigação, detecção e repressão de infracções penais ou de protecção dos interesses ou direitos fundamentais de uma pessoa. Em termos práticos, a AEPD sugere que esta disposição seja incluída num novo artigo 4.º-A ( em todo o caso, no Capítulo II da proposta).

65. Os n.ºs2 e 3 do artigo 11.º mantêm o seu campo de aplicação. Neles se prevêem salvaguardas adicionais para dados recebidos de outros Estados-Membros. A AEPD assinala que o n.º3 do artigo 11.º se aplicará ao intercâmbio de dados através do SIS II. No seu parecer sobre o SIS II a AEPD já referiu que se deve assegurar que os dados do SIS não possam ser utilizados para fins alheios ao sistema.

*Tratamento posterior para fins fora do âmbito da cooperação policial e judiciária*

66. Em certos casos, os dados devem ser tratados para salvaguardar outros interesses importantes, podendo mesmo ser tratados por outras autoridades que não as autoridades competentes no âmbito da presente decisão-quadro. Estas competências dos Estados-Membros podem implicar um tratamento de dados que constitui uma ingerência na vida privada (por exemplo, o controlo de uma pessoa que não é suspeita), devendo, por conseguinte, estar sujeito a condições muito rigorosas, nomeadamente obrigando os Estados-Membros a adoptar legislação específica se pretenderem recorrer a esta derrogação. No âmbito do primeiro pilar, esta questão foi abordada no artigo 13.º da Directiva 95/46/CE que estipula que, em determinados casos, são permitidas restrições a algumas disposições da directiva. Os Estados-Membros que apliquem estas restrições devem fazê-lo no respeito do artigo 8.º da CEDH.

67. Seguindo o mesmo raciocínio, a presente decisão-quadro deveria estipular no Capítulo II que os Estados-Membros devem poder tomar medidas legislativas destinadas a permitir o tratamento posterior sempre que essas medidas sejam necessárias para efeitos de:

— prevenção de ameaças à segurança pública, defesa ou segurança do Estado;

— protecção de um interesse económico ou financeiro importante de um Estado-membro ou da União Europeia

— protecção do interessado.

### IV.3 **Critérios que legitimam o tratamento de dados**

68. O artigo 5.º da proposta estipula que os dados devem ser tratados pelas autoridades competentes apenas por força de uma lei que estabeleça que esse tratamento é necessário para o cumprimento da missão legítima da autoridade em causa e para efeitos de prevenção, investigação, detecção e repressão de infracções penais. A AEPD subscreve os requisitos rigorosos do artigo 5.º.

69. Todavia, o texto do artigo 5.º subestima a necessidade de legitimar, em determinadas circunstâncias, o tratamento de dados por outros motivos legais. Trata-se de uma disposição importante, que não deveria obstar, por exemplo, ao cumprimento por parte da polícia das obrigações legais que lhe incumbem por força do direito interno de divulgar informações aos serviços de imigração ou autoridades fiscais. Por conseguinte, a AEPD sugere que o artigo 5.º contemple outros motivos legais que justifiquem o tratamento de dados pessoais, nomeadamente a necessidade de cumprimento de uma obrigação legal imposta ao controlador, o consentimento inequívoco do interessado, desde que o tratamento seja efectuado no seu interesse ou ainda a necessidade de proteger um interesse vital seu.

70. A AEPD observa que o cumprimento dos critérios que legitimam o tratamento de dados se reveste de importância especial no âmbito da cooperação policial e judiciária, se tivermos em conta que a recolha ilegal de dados pessoais pelas forças policiais pode implicar que esses dados não possam ser utilizados como meios de prova em tribunal.

### IV.4 **Necessidade e proporcionalidade**

71. Os artigos 4.º e 5.º da proposta destinam-se igualmente a assegurar — de um modo globalmente satisfatório — que as restrições à protecção de dados pessoais sejam necessárias e proporcionais, em conformidade com a legislação da União Europeia e com a jurisprudência do Tribunal Europeu dos Direitos do Homem sobre o artigo 8.º da CEDH:

— a alínea c) do n.º 1 do artigo 4.º enuncia a regra geral de que os dados devem ser exactos, pertinentes e não excessivos relativamente às finalidades para que são recolhidas e/ou tratados posteriormente.

— O artigo 5.º especifica que o tratamento deve ser *necessário* para o cumprimento da missão legítima da autoridade em causa e para efeitos de prevenção, investigação, detecção e repressão de infracções penais.

— O n.º 4 do artigo 4.º estipula que o tratamento de dados só é necessário se estiverem preenchidas determinadas condições específicas.

72. A AEPD observa que, tal como está formulado, o n.º 4 do artigo 4.º não preenche os critérios estabelecidos pela jurisprudência do Tribunal Europeu dos Direitos do Homem sobre o artigo 8.º da CEDH que estipula que numa sociedade democrática só pode haver ingerência na vida privada se for necessária. Nos termos da proposta, o tratamento de dados será considerado necessário não só quando *permite* às autoridades policiais e às autoridades judiciárias cumprir as suas missões, mas também quando existirem *boas razões para crer* que os dados pessoais em causa simplesmente *facilitariam ou acelerariam* a prevenção, a investigação, a detecção e a repressão de infracções penais.

73. Estes critérios não obedecem aos requisitos do artigo 8.º da CEDH uma vez que praticamente todo o tratamento de dados pode ser considerado como facilitante das actividades das autoridades policiais ou judiciárias, mesmo que os dados em causa não sejam realmente necessárias ao cumprimento dessas missões.

74. Na sua formulação actual, o n.º 4 do artigo 4 abre caminho para uma vasta e inaceitável recolha de dados pessoais, unicamente com base na convicção de que os dados pessoais possam *simplificar* a prevenção, a investigação, a detecção e a repressão de infracções penais. Pelo contrário, o tratamento de dados pessoais deve ser considerado necessário exclusivamente quando as autoridades competentes puderem comprovar claramente essa necessidade e desde que não estejam disponíveis outras medidas que impliquem menor ingerência na vida privada.

75. Por conseguinte, a AEPD recomenda que o primeiro travessão do n.º 4 do artigo 4.º seja reformulado por forma a garantir o respeito pela jurisprudência sobre o artigo 8.º da CEDH. Além disso, para sistematizar, a AEPD sugere que esta disposição seja transferida para o fim do artigo 5.º.

### IV.5 **Tratamento de categorias específicas de dados**

76. O artigo 6.º estabelece uma proibição de princípio do tratamento de dados sensíveis, isto é, de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual. Esta proibição não é aplicável quando o tratamento estiver previsto por lei e for absolutamente necessário para o cumprimento da missão legítima da autoridade em causa para efeitos da prevenção, investigação, detecção e repressão de infracções penais. Os dados sensíveis poderão igualmente ser tratados se a pessoa em questão der expressamente o seu consentimento. Em ambos os casos, haverá que prever garantias específicas adequadas .

77. O texto do artigo 6.º impõe duas observações. Em primeiro lugar, assenta demasiado no consentimento da pessoa em causa. A AEPD salienta que o tratamento de dados sensíveis com base no consentimento expresso da pessoa só deverá ser permitido desde que seja efectuado no interesse dessa mesma pessoa, não devendo da recusa de consentimento advir consequências negativas para a pessoa em causa. A AEPD recomenda que se altere o artigo 6.º nesse sentido, por forma a torná-lo coerente com a legislação actual da UE em matéria de protecção de dados.

78. Em segundo lugar, a AEPD considera que poderão ser também tidos em conta outros fundamentos jurídicos para o tratamento de dados, como sejam a necessidade de proteger os interesses vitais da pessoa em causa ou de outra pessoa (se a pessoa em causa não tiver capacidade física ou jurídica para dar o seu consentimento).

79. No domínio da cooperação policial e judiciária, o tratamento de outras categorias de dados pessoais potencialmente sensíveis, como os dados biométricos e os perfis de ADN, assume uma importância crescente. Esses dados não são explicitamente contemplados no artigo 6.º da proposta. A AEPD solicita ao legislador da UE que preste especial atenção ao implementar os princípios gerais da protecção de dados estabelecidos na proposta em futura legislação que implique o tratamento de categorias específicas de dados. Exemplo disso é a actual proposta de decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade (ver pontos 12-15), que prevê explicitamente o tratamento e o intercâmbio de dados biométricos e de perfis de ADN (ver Anexo II da proposta), mas não aborda a sensibilidade e as especificidades desses dados do ponto de vista da sua protecção.

80. A AEPD recomenda que sejam previstas garantias específicas, especialmente a fim de garantir que:

— os dados biométricos e os perfis de ADN só sejam utilizados com base em normas técnicas bem estabelecidas e interoperáveis;

— o seu nível de exactidão seja cuidadosamente tido em conta e possa ser contestado pela pessoa em causa através de meios prontamente disponíveis; e

— o respeito pela dignidade das pessoas seja plenamente garantido.

Compete ao legislador decidir se estas garantias adicionais deverão ser previstas na presente decisão-quadro ou nos instrumentos jurídicos específicos que regulamentam a recolha e intercâmbio dessas categorias específicas de dados.

### IV.6 **Exactidão e fiabilidade**

81. A alínea d) do n.º 1 do artigo 4.º estabelece as regras gerais aplicáveis à qualidade dos dados. Nos termos deste artigo, o responsável pelo tratamento dos dados deverá garantir que estes sejam exactos e, se necessário, actualizados. Deverá tomar todas as medidas razoáveis para assegurar que os dados inexactos ou incompletos sejam apagados ou rectificados, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente. Esta disposição é consentânea com os princípios gerais da legislação da UE em matéria de protecção de dados.

82. A terceira frase da alínea d) do n.º 1 do artigo 4.º estabelece a possibilidade de os Estados-Membros preverem um tratamento dos dados com diversos graus de exactidão e de fiabilidade. A AEPD entende que esta disposição constitui uma derrogação do princípio geral de exactidão e recomenda que se clarifique a natureza derrogatória da disposição, mediante o aditamento de «contudo» ou «não obstante» no início do n.º 1, terceira frase da alínea d), do artigo 4.º. Em tais casos, quando a exactidão dos dados não pode ser plenamente garantida, o responsável pelo tratamento terá por obrigação distinguir os dados em função do seu grau de exactidão e fiabilidade, frisando em particular a distinção fundamental entre dados baseados em factos e dados baseados em opiniões ou apreciações pessoais. A AEPD salienta a importância desta obrigação, tanto no que respeita às pessoas implicadas como às autoridades responsáveis pela aplicação da lei, especialmente nos casos em que o tratamento dos dados ocorra longe da sua fonte (ver ponto 7 do presente parecer).

*Verificação da qualidade dos dados*

83. O princípio geral estabelecido na alínea d) do n.º 1 do artigo 4.º é complementado pelas garantias mais específicas previstas no artigo 9.º quanto à verificação da qualidade dos dados. Este artigo estabelece, em particular, que:

1. a qualidade dos dados pessoais seja verificada o mais tardar antes de estes serem transmitidos ou disponibilizados. Além disso, a qualidade dos dados disponibilizados por acesso automatizado directo deverá ser periodicamente verificada (n.ºs 1 e 2 do artigo 9.º);

2. em todas as transmissões de dados, as decisões judiciais e as decisões de arquivamento sejam indicadas e os dados baseados em opiniões pessoais verificados na fonte antes de serem transmitidos, com indicação do seu grau de exactidão ou fiabilidade (n.º 1 do artigo 9.º);

3. os dados pessoais sejam «anotados» a pedido da pessoa em causa, se a sua exactidão for contestada por essa pessoa e a sua exactidão ou inexactidão não puder ser apurada (n.º 6 do artigo 9.º).

84. Assim sendo, se aplicados em conjunto, o n.º 1 do artigo 4.º e o artigo 9.º garantem a que qualidade dos dados pessoais seja devidamente verificada, tanto pela pessoa em causa como pelas autoridades mais próximas das fontes dos dados tratados e, como tal, em melhor posição para os verificarem.

85. A AEPD congratula-se com estas disposições, uma vez que, embora se centrem nas necessidades das autoridades responsáveis pela aplicação da lei, garantem que todos os dados sejam devidamente tidos em conta e utilizados consoante a sua exactidão e fiabilidade, evitando, assim, que a pessoa em causa seja desnecessariamente afectada pela eventual falta de exactidão de alguns dos dados que lhe digam respeito.

86. A verificação da qualidade dos dados constitui um elemento essencial de protecção das pessoas, especialmente no que diz respeito aos dados pessoais tratados pelas autoridades pessoais e judiciárias. Assim, a AEPD lamenta que a aplicabilidade do artigo 9.º, relativo à verificação da qualidade dos dados, se limite aos dados transmitidos ou facultados a outros Estados-Membros. É uma solução infeliz, pois implica que a qualidade dos dados pessoais, essencial também para efeitos de aplicação da lei, só seja plenamente garantida quando esses dados são transmitidos ou facultado a outros Estados-Membros, mas não quando são tratados dentro de um Estado-Membro ([1]). Em vez disso, é essencial — tanto no interesse das pessoas envolvidas como no das autoridades competentes — garantir que a verificação da qualidade diz respeito a todos os dados pessoais, incluindo aqueles que não são transmitidos ou facultados por outro Estado-Membro.

87. Por conseguinte, a AEPD recomenda que, em todo o caso se suprimam as limitações ao âmbito de aplicação dos n.ºs 1 e 6 do artigo 9.º, transferindo essas disposições para o capítulo II da proposta.

*Distinção entre categorias de dados diferentes*

88. O n.º 3 do artigo 4.º prevê a obrigação de o responsável pelo tratamento estabelecer uma distinção clara dos dados pessoais respeitantes a diferentes categorias de pessoas (suspeitos, condenados, testemunhas, vítimas, informadores, contactos, outros). A AEPD congratula-se com esta abordagem. Embora seja certo que as autoridades judiciárias e as demais autoridades responsáveis pela aplicação da lei possam ter necessidade de tratar dados respeitantes a categorias muito diferentes de pessoas, é essencial que esses dados sejam distinguidos consoante o seu grau de envolvimento num crime. Em especial, as condições respeitantes à recolha de dados, prazos, condições de recusa de acesso ou de prestação de informações às pessoas em causa e as modalidades de acesso aos dados pelas autoridades competentes deverão reflectir as especificidades das diferentes categorias de dados tratados e as diferentes finalidades com que esses dados são recolhidos pelas autoridades judiciárias e demais autoridades responsáveis pela aplicação da lei.

89. Neste contexto, a AEPD solicita que se preste especial atenção aos dados respeitantes a pessoas não suspeitas. Haverá que estabelecer condições e garantias específicas por forma a garantir a proporcionalidade e evitar que se lesem as pessoas que não estejam activamente envolvidas num crime. No que respeita a esta categoria de pessoas, a proposta deverá prever disposições suplementares que restrinjam a finalidade do tratamento, que estabeleçam prazos específicos e limitem o acesso aos dados. A AEPD recomenda que se altere a proposta em conformidade.

([1]) O Sistema de Informação Aduaneiro é um sistema pequeno mas complicado, constituído por elementos nacionais e supranacionais, comparável ao Sistema de Informação de Schengen. Atendendo à importância relativamente limitada da presente proposta para o Sistema de Informação Aduaneiro, bem como à complexidade do próprio sistema, não o evocaremos no presente parecer. A AEPD abordará o Sistema de Informação Aduaneiro noutro contexto.

90. O actual texto da proposta contém uma garantia específica relativa às pessoas não suspeitas, o n.º 1 do artigo 7.º. Segundo a AEPD, trata-se de uma garantia importante, principalmente pelo facto de os Estados-Membros não poderem prever derrogações. Infelizmente, o n.º 1 do artigo 7.º estabelece garantias específicas unicamente no que respeita aos prazos de conservação e a sua aplicabilidade limita-se à categoria de pessoas mencionadas no último travessão do n.º 3 do artigo 4.º da proposta. Por conseguinte, não prevê garantias suficientes e não abrange todo o grupo de pessoas não suspeitas. ([1])

91. Também os dados relativos às pessoas condenadas merecem especial atenção. Com efeito, no que respeita a esses dados, haverá que ter devidamente em conta as iniciativas recentes e futuras sobre o intercâmbio de registos criminais e garantir uma certa coerência. ([2])

92. Tendo em conta as observações acima feitas a AEPD recomenda que se adite ao artigo 4.º um novo número que contenha os seguintes elementos:

— disposições adicionais, no que respeita às pessoas não suspeitas, que restrinjam a finalidade do tratamento, estabeleçam prazos exactos e limitem o acesso aos dados;

— a obrigação de os Estados-Membros determinarem as consequências jurídicas das distinções a fazer entre dados pessoais de diferentes categorias de pessoas, por forma a reflectir as especificidades das diferentes categorias de dados tratados e os diferentes fins para os quais esses dados são recolhidos pelas autoridades judiciárias e demais autoridades responsáveis pela aplicação da lei.

— as consequências jurídicas deverão dizer respeito às condições de recolha de dados pessoais, prazos, posterior transferência e utilização dos dados e condições de recusa de acesso ou de prestação de informações às pessoas envolvidas.

### IV.7 **Prazos para a conservação de dados pessoais**

93. Os princípios gerais aplicáveis aos prazos para a conservação de dados pessoais estão estabelecidos na alínea e) do n.º 1 do artigo 4.º e no n.º 1 do artigo 7.º da proposta. Em regra, os dados pessoais só deverão ser conservados durante o período estritamente necessário para os efeitos para que foram recolhidos, o que é consentâneo com a legislação da UE em matéria de protecção de dados. ([3])

94. No entanto, a disposição geral que constitui o n.º 1 do artigo 7.º só é aplicável «salvo disposição em contrário da legislação nacional». A AEPD salienta que esta excepção é muito geral e vai além das derrogações admissíveis nos termos da alínea e) do n.º 1 do artigo 4.º. A AEPD propõe que se suprima a derrogação geral prevista no n.º 1 do artigo 7.º ou, pelo menos, se restrinja explicitamente o interesse público que justifica o recurso a esta derrogação por parte dos Estados-Membros ([4]).

95. O n.º 2 do artigo 7.º estabelece que o cumprimento dos prazos de conservação deverá ser garantido através de medidas processuais e técnicas adequadas e periodicamente controlado. A AEPD congratula-se com esta disposição, mas recomenda que se refira explicitamente que as medidas processuais e técnicas adequadas deverão prever a supressão automática e periódica dos dados pessoais depois de decorrido um certo tempo.

### IV.8 **Intercâmbio de dados pessoais com países terceiros**

96. Uma cooperação policial e judiciária eficaz dentro das fronteiras da UE depende cada vez mais da cooperação com os países terceiros e as organizações internacionais. Está a ser debatido ou projectado um grande número de acções destinadas a melhorar a cooperação judiciária e no domínio da aplicação da lei com países terceiros ou organizações internacionais, tanto a nível nacional como da UE ([5]). É muito provável que o desenvolvimento desta cooperação internacional dependa, em grande medida, do intercâmbio de dados pessoais.

97. Assim sendo, é essencial que os princípios do tratamento legal e equitativo, bem como os da equidade do processo em geral, se apliquem também à recolha e ao intercâmbio de dados pessoais para além das fronteiras da União e que esses dados só sejam transferidos para países terceiros ou organizações internacionais se as terceiras partes envolvidas assegurarem o devido nível de protecção ou garantias adequadas.

---

([1]) Além disso, tal não é consentâneo com a Recomendação n.º R (87) 15 para a regulamentação da utilização de dados pessoais no sector da polícia, dirigida pelo Comité de Ministros do Conselho da Europa aos Estados-Membros. O princípio 7.2 nela enunciado prevê, em particular, que deverão ser estabelecidas «verificações regulares» da qualidade dos dados pessoais, de acordo com a autoridade de controlo ou nos termos da legislação interna.

([2]) Ver, mais especificamente, o ponto 94 do presente parecer.

([3]) A decisão 2005/876/JAI do Conselho relativa ao intercâmbio de informações extraídas do registo criminal, entrou em vigor a 9 de Dezembro. A decisão completa e facilita o uso dos mecanismos existentes para a transmissão de informações sobre condenações com base em Convenções em vigor, como a Convenção Europeia de auxílio judiciário mútuo em matéria penal de 1959 e a Convenção de 2000 relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia. Este texto será posteriormente substituído por uma decisão-quadro mais específica do Conselho. A Comissão tenciona propor uma nova decisão-quadro nesta matéria.

([4]) Para além da disposição geral relativa aos prazos para a conservação de dados pessoais, estabelecida no artigo 7.º, a proposta prevê outras disposições específicas respeitantes aos dados pessoais objecto de intercâmbio com outros Estados-Membros. O n.º 7 do artigo 9.º, em especial, estabelece que os dados pessoais deverão ser suprimidos quando:
1. Não devessem ter sido transmitidos, disponibilizados ou recebidos;
2. Decorrido um prazo comunicado pela autoridade que o transmitiu, a menos que ainda sejam necessários para uma acção judicial;
3. Não sejam ou tenham deixado de ser necessários para os efeitos para os quais foram transmitidos.

([5]) Poder-se-á considerar como limitação a luta contra o terrorismo e/ /ou interesses públicos específicos referidos na alínea e) do n.º 1 do artigo 4.º: fins históricos, estatísticos ou científicos.

*Transferências de dados pessoais para países terceiros*

98. Nesta perspectiva, a AEPD congratula-se com o artigo 15.º da proposta, que prevê formas de protecção em caso de transferência para as autoridades competentes de países terceiros ou organismos internacionais. Porém, esta disposição, incluída no capítulo III da proposta, só se aplica aos dados recebidos das autoridades competentes de outros Estados-Membros ou por elas disponibilizados. Como consequência desta limitação, continua a haver uma falha no sistema de protecção de dados a nível da União Europeia no que respeita aos dados não recebidos das autoridades competentes de outros Estados-Membros. Segundo a AEPD, esta falha é inaceitável pelas razões que seguidamente se apontam.

99. Em primeiro lugar, o nível de protecção proporcionado pela legislação da EU em caso de transferência para países terceiros não deverá ser determinado pela fonte dos dados, ou seja, por uma polícia do Estado-Membro que transfere os dados para um país terceiro ou uma polícia de outro Estado-Membro.

100. Em segundo lugar, saliente-se que as regras aplicáveis às transferências de dados pessoais para países terceiros constituem um princípio fundamental da legislação em matéria de protecção de dados. Esta princípio representa, não só uma das disposições fundamentais da Directiva 95/46/CE, mas está também consagrado no Protocolo Adicional à Convenção n. [1] 108 [2]. Não poderá ser garantido o estabelecimento de normas comuns de protecção dos dados pessoais, conforme refere o artigo 1.º da proposta, se as regras comuns aplicáveis à transferência de dados pessoais para países terceiros não englobarem todas as operações de tratamento. Por conseguinte, os direitos das pessoas envolvidas garantidos pela presente proposta serão directamente afectados se os dados pessoais puderem ser transmitidos a países terceiros que não proporcionem um nível de protecção adequado.

101. Em terceiro lugar, limitar o âmbito de aplicação destas regras aos «dados objecto de intercâmbio» implicará que, no que respeita aos dados tratados unicamente dentro de um país, não haja garantias: paradoxalmente, os dados pessoais poderão ser transferidos para países terceiros, independentemente de qualquer protecção adequada, mais «facilmente» do que para outros Estados-Membros, o que poderá dar azo ao «branqueamento de informações». As autoridades competentes dos Estados-Membros poderão contornar as estritas normas em matéria de protecção de dados transmitindo aos países terceiros ou organizações internacionais dados a que a autoridade competente de outro Estado-Membro possa ter acesso ou que possam mesmo ser-lhe restituídos.

102. A AEPD recomenda, pois, que se altere a presente proposta de molde a garantir que o artigo 15.º se aplique ao intercâmbio de *todos* os dados pessoais com países terceiros. Esta recomendação não engloba a alínea c) do n.º 1 do artigo 15.º, que, por natureza, só diz respeito aos dados pessoais que sejam objecto de intercâmbio com outros Estados-Membros.

*Transferências que não assegurem o nível de protecção adequado*

103. O artigo 15.º estabelece uma série de condições aplicáveis às transferências para autoridades competentes de países terceiros com organizações internacionais e comparáveis com as condições estabelecidas no artigo 25.º da Directiva 95/46/CE. O n.º 6 do artigo 15.º prevê, contudo, a possibilidade de transferir dados para países terceiros ou organismos internacionais que não assegurem um nível adequado de protecção, desde que a transferência seja absolutamente necessária para salvaguardar os interesses essenciais de um Estado-Membro ou prevenir um perigo grave iminente que ameace a segurança pública ou uma ou várias pessoas em especial.

104. Haverá que clarificar a aplicabilidade da derrogação prevista no n.º 6. A AEPD recomenda, pois, que:

— se esclareça que esta excepção estabelece apenas uma derrogação da condição da «protecção adequada», e que não se sobrepõe às demais condições estabelecidas no n.º 1 do artigo 15.º;

— se acrescente que as transferências de dados efectuadas nos termos desta derrogação deverão ficar sujeitas a determinadas condições (como a condição explícita de que os dados só sejam tratados temporariamente e com finalidades específicas) e deverão ser comunicadas à autoridade de controlo competente.

*Tratamento de dados pessoais recebidos de países terceiros*

105. No âmbito do crescente intercâmbio de dados pessoais com as autoridades policiais e judiciárias de países terceiros, haverá também que prestar especial atenção aos dados pessoais «importados» de países onde não estejam garantidos padrões adequados de respeito pelos direitos humanos — e, em especial, de protecção dos dados pessoais.

---

[1] Ver, por exemplo, a recente comunicação da Comissão intitulada «Uma Estratégia relativa à dimensão externa do espaço de liberdade, segurança e justiça» (COM(2005) 491 final).

[2] O Protocolo Adicional à Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, relativo às autoridades de controlo e aos fluxos de dados transfronteiriços, foi assinado em 8.11.2001 e entrou em vigor em 1.7.2004. Este instrumento jurídico internacional, de carácter vinculativo, foi até agora assinado por 11 Estados (9 dos quais Estados-Membros da UE). O n.º 1 do artigo 2.º do Protocolo estabelece, com o princípio geral, que cada uma das Partes só deverá prever a transferência de dados pessoais para um destinatário sujeito à jurisdição de um Estado ou organização que não seja Parte na Convenção se este Estado ou organização garantir um nível de protecção adequado da transferência de dados pretendida.

106. Numa perspectiva mais ampla, a AEPD considera que o legislador deverá assegurar que os dados pessoais recebidos de países terceiros cumpram, no mínimo, as normas internacionais em matéria de respeito pelos direitos humanos. Por exemplo, os dados recolhidos mediante tortura ou violações dos direitos humanos, as «listas negras» meramente baseadas em convicções políticas ou preferências sexuais não deverão ser objecto de tratamento nem as autoridades judiciárias e demais autoridades responsáveis pela aplicação da lei neles deverão fazer fé, a não ser que o interesse da pessoa envolvida o justifique. A AEPD recomenda, pois, que este aspecto seja clarificado, pelo menos num considerando da proposta, eventualmente mediante uma referência aos instrumentos internacionais relevantes. ([1])

107. No que respeita, mais especificamente, à protecção de dados pessoais, a AEPD salienta que, quando os dados são transmitidos por países em que não existem normas e garantias adequadas de protecção dos dados pessoais, a eventual falta de qualidade dos dados deverá ser devidamente avaliada, a fim de evitar que as autoridades da UE responsáveis pela aplicação da lei se baseiem erroneamente nessas informações e que as pessoas envolvidas sejam, prejudicadas.

108. A AEPD recomenda, por conseguinte, que se adite ao artigo 9.º da proposta uma disposição no sentido de a qualidade dos dados pessoais transmitidos por países terceiros ser especificamente avaliada logo que esses dados sejam recebidos e ser indicado o seu grau de exactidão e fiabilidade.

### IV.9 **Intercâmbio de dados pessoais com particulares e autoridades não responsáveis pela aplicação da lei**

109. Os artigos 13.º e 14.º da proposta estabelecem uma série de requisitos a preencher no caso de os dados pessoais serem posteriormente transmitidos a particulares e a autoridades não responsáveis pela aplicação da lei. Tal como acima referido, estes artigos complementam as regras mais gerais estabelecidas no Capítulo II, que deverão ser sempre observadas.

110. A AEPD considera que, embora a transferência para particulares e outros organismos públicos possa ser necessária em determinados casos, para prevenir e combater o crime, haverá que impor condições estritas e específicas, o que é consentâneo com o parecer expresso pelos Comissários Europeus para a Protecção de Dados na posição escrita de Cracóvia ([2]).

111. Nesta perspectiva, a AEPD entende que podem ser consideradas satisfatórias as condições adicionais estabelecidas nos artigos 13.º e 14.º, desde que aplicadas em conjunto com as regras gerais previstas no Capítulo II, inclusive com a aplicação geral das regras em matéria de tratamento posterior (ver ponto, IV.2). A presente proposta limita, contudo, a aplicabilidade dos artigos 13.º e 14.º aos dados pessoais recebidos das autoridades competentes de outro Estado-Membro ou por elas disponibilizados.

112. A aplicabilidade geral destas últimas condições torna-se ainda mais importante se considerarmos o crescente intercâmbio de dados entre as autoridades responsáveis pela aplicação da lei e outras autoridades ou particulares dentro dos Estados-Membros. Exemplo disso é a parceria público/privado no âmbito das actividades de aplicação da lei ([3]).

113. Por conseguinte, a AEPD recomenda que se altere a presente proposta por forma a garantir que os artigos 13.º e 14.º se apliquem ao intercâmbio de *todos* os dados pessoais, incluindo aqueles que não são transmitidos ou facultados por outro Estado-Membro. Esta recomendação não se aplica à alínea c) do artigo 13.º nem à alínea c) do artigo 14.º.

*Acesso aos dados pessoais controlados por particulares e sua posterior utilização*

114. O intercâmbio de dados pessoais com particulares processa-se de forma bidireccional, uma vez que implica que sejam também transmitidos ou facultados por particulares às autoridades judiciárias e demais autoridades responsáveis pela aplicação da lei.

115. Neste caso, as autoridades públicas terão acesso e poderão utilizar posteriormente os dados pessoais recolhidos para fins comerciais (transacções comerciais, comercialização, prestação de serviços, etc.) e geridos por particulares responsáveis pelo seu tratamento com uma finalidade diversa, como seja a da prevenção, investigação, detecção e repressão de infracções penais. Além disso, a exactidão e a fidelidade dos dados tratados para fins comerciais serão cuidadosamente avaliadas quando esses dados forem utilizados para efeitos de aplicação da lei ([4]).

([1]) A Convenção das Nações Unidas contra a tortura e outras penas ou tratamentos cruéis, desumanos ou degradantes, assinada por todos os Estados-Membros da UE e em vigor desde 26 de Junho de 1987, estabelece, nomeadamente no seu artigo 15.º, que «os Estados partes deverão providenciar para que qualquer declaração que se prove ter sido obtida pela tortura não possa ser invocada como elemento de prova num processo, salvo se for utilizada contra a pessoa acusada da prática de tortura para provar que a declaração foi feita».

([2]) *A posição escrita sobre a aplicação da lei e o intercâmbio de informações na UE*, adoptada na Conferência da Primavera das Autoridades Europeias para a Protecção de Dados, Cracóvia, 25-26 de Abril de 2005.

([3]) Ver Programa Legislativo e de Trabalho da Comissão para 2006 COM(2005) 531 final.

([4]) Por exemplo, uma factura de telefone só poderá ser considerada credível para fins comerciais, desde que especifique correctamente as chamadas telefónicas efectuadas; mas essa mesma factura poderá, para as autoridades responsáveis pela aplicação da lei, não fazer inteiramente fé como prova conclusiva quanto à pessoa que efectuou uma chamada telefónica específica.

116. Como exemplo — aliás bastante recente e importante — de acesso às bases de dados privadas para efeitos de aplicação da lei, refira-se o texto, já aprovado, da directiva relativa à conservação dos dados de comunicação (ver pontos 16-18), nos termos da qual os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações deverão conservar, durante um período máximo de dois anos, determinados dados respeitantes a comunicações efectuadas, por forma a garantir que estes sejam facultados para efeitos de investigação, detecção e repressão de crimes graves. Segundo o texto aprovado, certas questões relativas ao acesso a esses dados vão além do direito comunitário, não podendo ser reguladas pela própria directiva. Em vez disso, essas importantes questões poderão ficar sujeitas à legislação nacional ou a acções desenvolvidas ao abrigo do Título VI do TUE ([1]).

117. No parecer que emitiu sobre a proposta de directiva referida, a AEPD defendeu uma interpretação mais lata do Tratado CE, uma vez que é necessário impor limitações ao acesso para garantir a devida protecção das pessoas cujos dados de comunicação tenham de ser conservados. Infelizmente, o legislador europeu não incluiu regras em matéria de acesso na directiva acima mencionada.

118. No presente parecer, a AEPD manifesta, uma vez mais, a sua marcada preferência por que a legislação da UE preveja normas comuns em matéria de acesso e posterior utilização pelas autoridades responsáveis pela aplicação da lei. Uma vez que este aspecto não é contemplado no âmbito do primeiro pilar, um instrumento do terceiro pilar poderá estabelecer a protecção necessária. Esta posição da AEPD justifica-se também pelo aumento generalizado do intercâmbio de dados entre Estados-Membros e pela recente proposta relativa ao princípio da disponibilidade. Prever regras nacionais diferentes em matéria de acesso e utilização posterior não seria compatível com a «livre circulação» em toda a UE de informações policiais proposta, que inclui também dados provenientes de bases privadas.

119. A AEPD considera, pois, que deverão ser aplicadas normas comuns ao acesso das autoridades responsáveis pela aplicação da lei aos dados pessoais detidos por particulares, por forma a garantir que o acesso só é permitido com base em condições e limitações bem definidas. Em particular, o acesso das autoridades competentes só deverá ser autorizado caso a caso, em determinadas circunstâncias e para fins específicos, ficando sujeito a controlo judicial nos Estados-Membros.

([1]) Nos termos dos considerandos da directiva «As questões que se prendem com o acesso das autoridades nacionais aos dados conservados de acordo com a presente directiva no contexto das actividades enumeradas no primeiro travessão do n.º 2 do artigo 3.º da Directiva 95/46/CE não são abrangidas pelo direito comunitário. Todavia, podem estar sujeitas à legislação nacional ou a acções desenvolvidas ao abrigo do Título VI do Tratado da União Europeia, no pressuposto de que estas leis ou acções respeitam plenamente os direitos fundamentais consagrados nas tradições constitucionais dos Estados-Membros e garantidos pela CETH. O artigo 8.º desta Convenção, na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem,….».

## IV.10 **Direitos da pessoa a quem os dados dizem respeito**

120. O Capítulo IV trata dos direitos da pessoa envolvida de uma forma que é, de um modo geral, consentânea com a actual legislação em matéria de protecção de dados e com o artigo 8.º da Carta dos Direitos Fundamentais da UE.

121. A AEPD congratula-se com estas disposições, que estabelecem um conjunto harmonizado de direitos, tendo simultaneamente em conta as especificidades do tratamento de dados pelas autoridades judiciárias e policiais. Este aspecto constitui uma melhoria significativa, uma vez que a situação actual se caracteriza por uma grande diversidade de regras e práticas, especialmente no que respeita ao direito de acesso. Certos Estados-Membros não permitem que as pessoas envolvidas tenham acesso aos dados que lhes dizem respeito, mas dispõem de um sistema «acesso indirecto» (neste caso, o direito de acesso é exercido pela autoridade nacional para a protecção de dados, em nome da pessoa envolvida).

122. A proposta harmoniza as eventuais derrogações ao direito de acesso directo. Este aspecto assume especial importância pelo facto de permitir que os cidadãos, cujos dados são cada vez mais objecto de tratamento e intercâmbio pelas autoridades competentes de diferentes Estados-Membros da UE, exerçam um conjunto harmonizado de direitos enquanto pessoas envolvidas, independentemente do Estado-Membro em que os dados são recolhidos ou tratados. ([2]).

123. A AEPD reconhece que importa restringir os direitos das pessoas envolvidas nos casos em que tal se afigure necessário para efeitos de prevenção, investigação, detecção ou repressão de infracções penais. Em todo o caso, uma vez que tais limitações devem ser consideradas excepções aos direitos básicos das pessoas, haverá que aplicar um estrito teste de proporcionalidade. Significa isto que as excepções deverão ser limitadas e bem definidas e as restrições, sempre que possível, imparciais e limitadas no tempo.

124. Nesta perspectiva, a AEPD gostaria de chamar a especial atenção do legislador para a alínea a) do n.º 2 dos artigos 19.º, 20.º e 21.º, que prevê uma excepção demasiado lata e indefinida dos direitos das pessoas envolvidas, estabelecendo que estes direitos podem ser limitados se isso for necessário para «permitir que o responsável pelo

([2]) O capítulo IV contempla, em especial, o direito de informação (Artigos 19.º e 20.º) e o direito de acesso, rectificação, apagamento ou bloqueio (Artigo 21.º). De um modo geral, estes artigos conferem às pessoas em causa todos os direitos habitualmente garantidos pela legislação da UE em matéria de protecção de dados, estabelecendo simultaneamente uma série de excepções destinadas a ter em conta as especificidades do terceiro pilar. Em particular, são previstas restrições aos direitos das pessoas em causa mediante disposições praticamente idênticas tanto em relação ao direito de informação (n.º 2 do artigo 19.º e n.º 2 do artigo 20.º) como o direito ao acesso (n.º 2 do artigo 21.º).

tratamento compra as suas funções legais de forma adequada». Além disso, esta excepção sobrepõe-se à disposição constante da alínea b), que permite estabelecer restrições aos direitos das pessoas em causa se isso for necessário «para evitar prejudicar investigações, inquéritos ou processos em curso ou o cumprimento pelas autoridades competentes das suas funções legais». Embora se possa considerar que esta última excepção é justificada, a primeira parece impor uma restrição desproporcionada aos direitos das pessoas. Por conseguinte, a AEPD recomenda que seja suprimida a alínea a) do n.º 2.º dos artigos 19.º, 20.º e 21.º.

125. A AEPD recomenda ainda que se introduzam as seguintes melhorias nos artigos 19.º, 20.º e 21.º:

— especificar que as restrições aos direitos das pessoas não são obrigatórias, não se aplicam por um período indefinido e «só» são permitidas nos casos específicos enunciados nos artigos;

— ter em conta que as informações deverão ser fornecidas, de forma autónoma, pelo responsável pelo tratamento de dados, e não com base num pedido apresentado pela pessoa em causa;

— acrescentar, na alínea c) do n.º 1 do artigo 19.º, que deverão também ser fornecidas informações sobre «os prazos de conservação dos dados»;

— garantir, mediante alteração do n.º 1 do artigo 20.º consentânea com as disposições de outros instrumentos da UE em matéria de protecção de dados, que, se os dados não tiverem sido recolhidos junto da pessoa em causa ou tiverem sido obtidos sem o seu conhecimento, lhe serão fornecidas informações «o mais tardar quando os dados forem divulgados pela primeira vez»;

— garantir que o mecanismo de recurso contra a recusa ou restrição dos direitos da pessoa em causa seja aplicável aos casos de restrição do direito a ser informado, e alterar o último período do n.º 4 do artigo 19.º em conformidade.

*Decisões individuais automatizadas*

126. A AEPD lamenta que a proposta não aborde de todo a importante questão das decisões individuais automatizadas. Com efeito, a experiência prática demonstra que as autoridades responsáveis pela aplicação da lei recorrem cada vez mais ao tratamento automatizado de dados com o fim de avaliar determinados aspectos pessoais dos indivíduos, especialmente a fim de avaliar a sua fiabilidade e conduta.

127. Reconhecendo embora que estes sistemas possam ser necessários em determinados casos para aumentar a eficácia das acções policiais, a AEPD salienta que as decisões unicamente baseadas no tratamento automatizado de dados deverão ser sujeitas a condições e garantias muito estritas quando produzem efeitos legais que digam respeito a uma pessoa ou possam afectá-la de forma significativa. Este aspecto assume ainda maior relevância no contexto do terceiro pilar, uma vez que, neste caso, as autoridades competentes dispõem de poderes coercivos e, como tal, as suas acções ou decisões podem afectar uma pessoa ou ser mais intrusivas do que normalmente aconteceria se essas acções ou decisões proviessem de uma entidade privada.

128. Refira-se em especial — e de acordo com os princípios gerais em matéria de protecção de dados — que tais decisões ou acções só deverão ser permitidas se tal for expressamente autorizado por lei ou por uma autoridade de controlo competente, devendo ficar sujeitas a medidas especificamente destinadas a salvaguardar os legítimos interesses das pessoas envolvidas. Além disso, a pessoa em causa deverá dispor prontamente de meios que lhe permitam expor o seu ponto de vista e tomar conhecimento dos motivos que presidiram à decisão; caso contrário, esta será incompatível com a finalidade para a qual os dados são tratados.

129. A AEPD recomenda, pois, que se introduza uma disposição específica sobre as decisões individuais automatizadas, consentânea com a actual legislação da UE em matéria de protecção de dados.

### IV.11 **Segurança do tratamento de dados**

130. No que respeita à segurança do tratamento, o artigo 24.º prevê a obrigação de o responsável pelo tratamento de dados pôr em prática medidas técnicas e organizativas adequadas consentâneas com as disposições previstas noutros instrumentos da UE em matéria de protecção de dados. Além disso, o n.º 2 apresenta uma lista pormenorizada e exaustiva de medidas a aplicar no que respeita ao tratamento automatizado de dados.

131. A AEPD congratula-se com esta disposição, mas sugere que, para facilitar um controlo eficaz por parte das autoridades competentes, se acrescente à lista de medidas enunciadas no n.º 2 a seguinte medida complementar: «*k) assegurar um acompanhamento e informação sistemáticas sobre a eficácia das medidas de segurança anteriormente mencionadas (auto-auditoria sistemática das medidas de segurança)*» [1].

*Registo de dados*

132. O artigo 10.º estabelece que cada transmissão ou recepção automatizada de dados pessoais deve ser registada (em caso de transmissão automatizada) ou documentada (em caso de transmissão não automatizada), a fim de garantir a posterior verificação da licitude da transmissão e do tratamento dos dados. Essas informações deverão ser prestadas à autoridade de controlo competente, se esta o solicitar.

[1] Ver, a este respeito, o parecer da AEPD sobre a 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) 835 final), publicado no *site* www.edps.eu.int

133. A AEPD congratula-se com este disposição. Salienta, no entanto, a fim de garantir um controlo exaustivo dos dados pessoais e verificar se estes forma devidamente utilizados, também o «acesso» aos dados deverá ser registado ou documentado. Estas informações são essenciais, uma vez que um controlo eficaz do correcto tratamento dos dados pessoais deverá incidir, não só na licitude da transmissão dos dados pessoais entre autoridades, mas também na licitude do acesso por parte dessas mesmas autoridades ([1]). A AEPD recomenda, pois, que se altere o artigo 10.º de molde a prever que o acesso aos dados seja também registado ou documentado.

### IV.12 **Recursos judiciais, responsabilidade e sanções**

134. O capítulo 6.º da proposta trata dos recursos judiciais (artigo 27.º), da responsabilidade (artigo 28.º) e das sanções (artigo 29.º). As disposições previstas são, de um modo geral, consentâneas com a actual legislação da UE em matéria de protecção de dados.

135. Especialmente no que respeita às sanções, a AEPD congratula-se por ter sido especificado que, em caso de violação das disposições adoptadas nos termos da decisão-quadro, as sanções a aplicar deverão ser eficazes, proporcionadas e dissuasivas. Além disso, as sanções penais a aplicar a infracções cometidas intencionalmente que impliquem graves violações — especialmente no que respeita à confidencialidade e à segurança do tratamento — terão um efeito tanto mais dissuasor quanto mais graves forem as violações da legislação em matéria de protecção de dados.

### IV.13 **Funções de controlo e aconselhamento**

136. As disposições da proposta aplicáveis ao controlo do tratamento dos dados, bem como à consulta sobre questões com ele relacionadas, assemelham-se, em larga medida, às da Directiva 95/46/CE. A AEPD congratula-se por a Comissão ter optado, na sua proposta, por mecanismos que deram já provas de funcionar bem e destaca, em particular a introdução de um sistema (obrigatório) de controlo prévio. Tanto a Directiva 95/46/CE como o Regulamento 45/2001/CE prevêem já um sistema desse tipo que demonstrou já ser um instrumento eficaz de que a AEPD poderá dispor para proceder ao controlo do tratamento de dados pelas instituições e órgãos das Comunidades Europeias.

137. A nomeação, por um responsável pelo tratamento de dados, de responsáveis pela protecção dos mesmos constitui outro instrumento de controlo do tratamento de dados que demonstrou já a sua eficácia. Este instrumento, utilizado em vários Estados-Membros e instituído, com carácter obrigatório, pelo Regulamento 45/2001/CE, desempenha um papel fundamental a nível das Comunidades Europeias. Os responsáveis pela protecção de dados são administradores dentro de uma organização a quem compete garantir, de forma independente, a aplicação interna das disposições sobre protecção de dados.

138. A AEPD recomenda que se aditem à proposta disposições em matéria de responsáveis pela protecção de dados, que poderão ser idênticas às dos artigos 24.º a 26.º do Regulamento 45/2001/CE.

139. Os Estados-Membros são os destinatários da proposta de decisão-quadro. Por conseguinte, é lógico que o artigo 30.º da proposta preveja que o controlo seja efectuado por autoridades independentes. O texto deste artigo é muito semelhante ao do artigo 28.º da Directiva 95/46/CE. As autoridades nacionais de controlo deverão cooperar entre si, com as autoridades comuns de controlo criadas ao abrigo do Título VI do Tratado da UE e com a AEPD. Além disso, o artigo 31.º da proposta prevê a criação de um grupo cujo papel deverá ser semelhante ao que o grupo do artigo 29.º desempenha nas matérias do primeiro pilar. Todos os intervenientes relevantes na área da protecção de dados são mencionados no artigo 31.º da proposta.

140. Escusado será dizer que, numa proposta que tem por objectivo melhorar a cooperação policial e judiciária entre Estados-Membros, a cooperação entre todos os intervenientes relevantes na área da protecção de dados desempenha um papel importante. A AEPD congratula-se, pois, com o destaque dado na proposta à cooperação entre as autoridades de controlo.

141. A AEPD, salienta ainda que importa seguir uma abordagem coerente no que respeita às questões atinentes à protecção de dados, promovendo nomeadamente a comunicação entre o actual Grupo do Artigo 29.º e o grupo criado ao abrigo da presente proposta de decisão-quadro. A AEPD recomenda que se altere o n.º 2 do artigo 31.º da proposta de molde a permitir que o presidente do Grupo do Artigo 29.º participe ou se faça representar nas reuniões do novo grupo.

142. O texto do artigo 31.º da presente proposta contêm uma diferença significativa em relação ao artigo 29.º da Directiva 95/46/CE. A AEPD é membro efectivo do Grupo do Artigo 29.º, o que lhe confere o direito de voto. A proposta em apreço designa também a AEPD como membro do grupo (com base no artigo 31.º), mas não lhe confere direito de voto. As razões pelas quais a presente proposta se afasta do texto do artigo 29.º da Directiva 95/46/CE não são claras. No entender da AEPD, o texto proposto é ambíguo no que respeita ao papel que lhe cabe, o que poderá prejudicar a eficácia do seu envolvimento nos trabalhos do grupo. A AEPD recomenda, pois, que o texto da decisão-quadro seja coerente com o da directiva.

([1]) Este requisito é consentâneo com o disposto no artigo 18.º da proposta, nos termos da qual a autoridade que transmite os dados deverá ser informada, a seu pedido, do tratamento posterior dos dados pessoais transmitidos ou disponibilizados, e no artigo 24.º, respeitante à aplicação das medidas de segurança, sem deixar de ter em conta a auto-auditoria sistemática dessas medidas ora proposta.

### IV.14 **Outras disposições**

143. O Capítulo VIII da proposta inclui algumas disposições finais que alteram a Convenção de Schengen e outros instrumentos relativos ao tratamento e à protecção dos dados pessoais.

*Convenção de Schengen*

144. O artigo 33.º da proposta estipula que, para efeitos das questões abrangidas pelo âmbito do TUE, os artigos 126.º a 130.º da Convenção de Aplicação do Acordo de Schengen serão substituídos pela presente decisão. Os artigos 126.º a 130.º da Convenção de Schengen contêm as normas gerais em matéria de protecção de dados aplicáveis ao tratamento de dados comunicados ao abrigo da Convenção (mas fora do âmbito do Sistema de Informação de Schengen).

145. A AEPD congratula-se com a substituição acima referida, por esta vir melhorar a coerência do regime de protecção de dados no terceiro pilar e representar, nalguns aspectos, uma melhoria significativa para a protecção dos dados pessoais, dando por exemplo mais poderes às autoridades de controlo. Nalguns pontos, contudo, tem o resultado involuntário — e pouco feliz — de fazer baixar o nível da protecção de dados. Certas disposições da Convenção de Schengen são efectivamente mais rigorosas do que as da decisão-quadro.

146. A AEPD refere, em particular, a alínea b) do n.º 3 do artigo 126.º da Convenção, que estabelece que os dados só podem ser utilizados pelas autoridades judiciárias, e pelos serviços e entidades que asseguram uma tarefa ou que cumprem uma função no âmbito dos fins estipulados pela Convenção. Esta disposição exclui aparentemente a transmissão a particulares, que seria permitida nos termos da decisão-quadro proposta. Outro ponto a referir é que na Convenção de Schengen as disposições em matéria de protecção de dados se aplicam também a *todos* os dados comunicados a partir de um ficheiro *não automatizado* ou inseridos num ficheiro do mesmo tipo (artigo 127.º), ao passo que os ficheiros não estruturados são excluídos do âmbito de aplicação da decisão-quadro proposta.

*Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia*

147. O artigo 34.º estipula que o artigo 23.º da Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia é substituído pela decisão-quadro. A AEPD observa que, embora esta substituição proporcione uma melhor protecção dos dados pessoais transmitidos no âmbito da Convenção, poderá também dar lugar a alguns problemas de compatibilidade entre os dois instrumentos.

148. Em especial, a Convenção trata também do auxílio mútuo na intercepção de comunicações. Neste caso, o Estado-Membro requerido pode dar o seu consentimento — à intercepção ou à transmissão da gravação de telecomunicações — sob reserva das condições que teriam de ser cumpridas num caso nacional semelhante. Segundo o n.º 4 do artigo 23.º da Convenção, se essas condições adicionais disserem respeito à utilização de dados pessoais, as mesmas prevalecerão sobre as regras de protecção de dados previstas no artigo 23.º. Analogamente, o n.º 5 do artigo 23.º determina a precedência das regras adicionais relativas à segurança das informações recolhidas pelas equipas de investigação conjuntas. A AEPD observa que, se o artigo 23.º for substituído pela actual proposta, não se saberá com clareza se as referidas regras adicionais continuarão a ser aplicáveis. Por conseguinte, a AEPD recomenda que se esclareça este ponto, a fim de poder avaliar devidamente as consequências de uma total substituição do artigo 23.º da Convenção pela presente decisão-quadro.

*Convenção n.º 108 do Conselho da Europa relativa à protecção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais*

149. O n.º 2 do artigo 34.º estabelece que qualquer referência à Convenção n.º 108 deve entender-se como uma referência à presente decisão-quadro. A interpretação e a aplicabilidade concreta desta disposição estão longe de ser claras. De qualquer forma, a AEPD parte do princípio de que esta disposição se aplica apenas no âmbito de aplicação *ratione materiae* da presente decisão-quadro.

*Questões finais*

150. No que se refere à coerência sistemática do texto, a AEPD faz notar que alguns artigos poderiam ter uma melhor localização no texto da proposta.

Por conseguinte, a AEPD sugere:

1. que o artigo 16.º («Comité») seja transferido do Capítulo III («Formas específicas de tratamento») para um novo capítulo;

2. que os artigos 25.º («Registo») e 26.º («Controlo prévio») sejam transferidos do Capítulo V («Confidencialidade e segurança do tratamento») para um novo capítulo.

## V. **CONCLUSÕES**

*Um progresso considerável*

a) A adopção da presente proposta representaria um progresso considerável para a protecção dos dados pessoais, num domínio importante que requer, em especial, um mecanismo coerente e eficaz para a protecção dos dados pessoais a nível da União Europeia.

b) Uma protecção eficaz dos dados pessoais não só é importante para as pessoas em causa mas também contribui para o êxito da própria cooperação policial e judiciária. Em muitos aspectos, trata-se em ambos os casos de interesses públicos que estão interligados.

*Normas comuns*

c) No entender da AEPD, o novo enquadramento para a protecção de dados deverá não só respeitar os princípios da protecção de dados — importa garantir a coerência da protecção de dados na União Europeia — mas também proporcionar um conjunto adicional de regras que tenham em conta o carácter específico do domínio da aplicação da lei.

d) A presente proposta preenche essas condições: assegura que os princípios existentes em matéria de protecção de dados, tal como enunciados na Directiva 95/46/CE, venham a ser aplicados no domínio do terceiro pilar, já que a maior parte das disposições da proposta reflecte outros instrumentos jurídicos da UE relativos à protecção dos dados pessoais e é consentânea com esses instrumentos jurídicos. Além disso, prevê normas comuns que especificam esses princípios, tendo em vista a sua aplicação neste domínio, as quais são geralmente suficientes para assegurar a existência de garantias adequadas em matéria de protecção de dados no âmbito do terceiro pilar.

*Aplicável a todo o tratamento*

e) Para alcançar o seu objectivo, é essencial que a decisão-quadro abranja todos os dados policiais e judiciários, ainda que estes não sejam transmitidos ou disponibilizados pelas autoridades competentes de outros Estados-Membros.

f) A alínea b) do n.º 1 do artigo 30.º e a alínea c) do n.º 1 do artigo 31.º do TUE constituem um fundamento jurídico para as regras de protecção de dados que não se limitem à protecção dos dados pessoais efectivamente trocados entre as autoridades competentes dos Estados-Membros mas sejam também aplicáveis às situações a nível nacional.

g) A proposta não se aplica ao tratamento no âmbito do segundo pilar da UE (política externa e de segurança comum), nem ao tratamento de dados pelos serviços de informações e ao acesso a esses dados por parte desses serviços quando os dados sejam tratados por autoridades competentes ou outras partes (o que decorre do artigo 33.º do TUE). Nestes domínios, a legislação nacional deve prever uma protecção adequada das pessoas em causa. Esta lacuna na protecção a nível da UE requer uma protecção ainda mais eficaz nos domínios efectivamente abrangidos pela proposta.

h) A AEPD congratula-se por a proposta ser extensiva aos dados pessoais tratados pelas autoridades judiciárias.

*Relação com outros instrumentos jurídicos*

i) Sempre que qualquer outro instrumento jurídico específico adoptado ao abrigo do Título VI do TUE preveja condições ou restrições mais precisas para o tratamento dos dados ou o acesso a eles, o instrumento jurídico específico deverá aplicar-se como sendo uma *lex specialis*.

j) A presente proposta de decisão-quadro do Conselho relativa à protecção dos dados vale por si só e é necessária mesmo que não seja adoptado um instrumento jurídico sobre a disponibilidade (tal como proposto pela Comissão em 12 de Outubro de 2005).

k) A aprovação, pelo Parlamento Europeu, da directiva relativa à conservação dos dados relacionados com a oferta de serviços de comunicações electrónicas torna ainda mais urgente a instituição de um quadro jurídico para a protecção dos dados no âmbito do terceiro pilar.

*Estrutura da proposta*

l) As normas adicionais constantes do Capítulo II (para além dos princípios gerais da Directiva 95/46/CE) deverão oferecer às pessoas em causa uma protecção adicional relacionada com o contexto específico do terceiro pilar, mas não pode conduzir a uma descida do nível de protecção.

m) O Capítulo III relativo às formas específicas de tratamento (no qual é incorporada o terceiro estrato de protecção) não pode derrogar ao Capítulo II: as disposições do Capítulo III deverão oferecer às pessoas em causa uma protecção adicional em situações em que estejam envolvidas autoridades competentes de mais do que um Estado-Membro, mas essas disposições não poderão conduzir a um nível de protecção mais baixo.

n) As disposições relativas à verificação da qualidade dos dados (n.ºs 1 e 6 do artigo 9.º) e as que regulam o tratamento posterior dos dados pessoais (n.º 1 do artigo 11.º) deverão ser transferidas para o Capítulo II e tornar-se aplicáveis a todo o tratamento de dados por parte das autoridades de aplicação da lei, mesmo que os dados pessoais não tenham sido transmitidos ou disponibilizados por outro Estado-Membro. Em particular, é essencial — no interesse não só das pessoas em causa mas também das autoridades competentes — assegurar que a verificação adequada da qualidade se aplique a todos os dados pessoais.

*Limitação da finalidade*

o) A proposta não aborda de uma forma inteiramente satisfatória uma situação que pode ocorrer no decurso do trabalho policial: a necessidade de utilizar posteriormente os dados para uma finalidade considerada incompatível com aquela para a qual foram recolhidos.

p) Nos termos do direito comunitário em matéria de protecção de dados, os dados pessoais devem ser recolhidos para fins especificados e explícitos e não devem ser tratados posteriormente de uma forma incompatível com esses fins. No que se refere à utilização posterior, há que permitir uma certa flexibilidade. É mais provável que a limitação da recolha seja cumprida se as autoridades encarregadas da segurança interna souberem que, mediante as garantias adequadas, podem contar com uma derrogação à limitação da utilização posterior.

q) A decisão-quadro deveria estipular no Capítulo II que os Estados-Membros devem ser autorizados a adoptar medidas legislativas que permitam o tratamento posterior nos casos em que tais medidas sejam necessárias para garantir:

— a prevenção das ameaças à segurança pública, à defesa ou à segurança nacional;

— a protecção de um interesse económico ou financeiro importante para um Estado-Membro;

— a protecção da pessoa em causa.

Estas competências dos Estados-Membros poderão implicar um tratamento intrusivo para a vida privada, pelo que deverão ser acompanhadas de condições muito estritas.

*Necessidade e proporcionalidade*

r) Os princípios da necessidade e da proporcionalidade da proposta deverão reflectir plenamente a jurisprudência do Tribunal Europeu dos Direitos do Homem, assegurando que o tratamento dos dados pessoais seja considerado necessário apenas nos casos em que as autoridades competentes possam demonstrar que existe para tal uma necessidade evidente, e desde que não se disponha de medidas menos intrusivas para a vida privada.

*Intercâmbio de dados pessoais com países terceiros*

s) Se os dados pudessem ser transmitidos a países terceiros sem que estivesse assegurada a protecção das pessoas em causa, ficaria seriamente comprometida a protecção prevista na presente proposta parra o território da União Europeia. A AEPD recomenda que se altere a proposta por forma a assegurar que o artigo 15.º se aplica ao intercâmbio de *todos* os dados pessoais com os países terceiros. Esta recomendação não é extensiva à alínea c) do n.º 1 do artigo 15.º.

t) Quando os dados transmitidos sejam provenientes de países terceiros, haverá que ponderar criteriosamente a sua qualidade em termos de respeito pelos direitos humanos e pelas normas de protecção de dados, antes de os utilizar.

*Intercâmbio de dados pessoais com particulares e com autoridades não implicadas na aplicação da lei*

u) A transferência de dados para particulares e para outros organismos públicos pode revelar-se necessária em casos específicos para fins de prevenção e luta contra a criminalidade, mas haverá que aplicar condições estritas. A AEPD recomenda que a presente proposta seja alterada de modo a assegurar que os artigos 13.º e 14.º se apliquem ao intercâmbio de *todos* os dados pessoais, incluindo os que não sejam recebidos ou disponibilizados por outro Estado-Membro. Esta recomendação não é extensiva à alínea c) do artigo 13.º nem à alínea c) do artigo 14.º.

v) Deverão ser aplicadas normas comuns ao acesso por parte das autoridades de aplicação da lei aos dados detidos por particulares, de forma a assegurar que o acesso só seja permitido com base em condições e restrições bem definidas.

*Categorias específicas de dados*

w) Haverá que prever salvaguardas específicas, em especial para garantir que:

— os dados biométricos e os perfis de ADN sejam utilizados apenas com base em normas técnicas comprovadas e interoperáveis,

— o nível de exactidão dos dados seja tido cuidadosamente em conta e possa ser contestado pela pessoa em causa através de meios rapidamente disponíveis, e que

— esteja plenamente assegurado o respeito pela dignidade das pessoas.

*Distinção entre as diferentes categorias de dados*

x) Os dados pessoais relativos a diferentes categorias de pessoas (suspeitos, condenados, vítimas, testemunhas, etc.) deverão ser tratados de acordo com condições e garantias diferentes e adequadas. Por conseguinte, a AEPD propõe que se adite no artigo 4.º um novo número que contenha os seguintes elementos:

— a obrigação, para os Estados-Membros, de estipular as consequências jurídicas decorrentes das distinções a estabelecer entre os dados pessoais das diferentes categorias de pessoas;

— disposições adicionais para restringir a finalidade do tratamento, fixar prazos exactos e limitar o acesso aos dados, no que se refere às pessoas não suspeitas.

*Decisões individuais automatizadas*

y) As decisões baseadas apenas no processamento automatizado de dados deverão ficar sujeitas a condições muito estritas quando produzirem efeitos que digam respeito a uma pessoa ou que afectem significativamente uma pessoa. Por conseguinte, a AEPD recomenda que sejam introduzidas disposições específicas sobre as decisões individuais automatizadas, à semelhança das previstas na Directiva 95/46/CE.

*Selecção de outras recomendações*

z) A AEPD recomenda que:

— o primeiro travessão do n.º 4 do artigo 4.º seja reformulado de modo a assegurar o respeito pela jurisprudência relativa ao artigo 8.º da CEDH (Convenção Europeia dos Direitos do Homem), uma vez que a formulação proposta para o n.º 4 do artigo 4.º não preenche os critérios estabelecidos pela jurisprudência do Tribunal Europeu dos Direitos do Homem no que se refere ao artigo 8.º da CEDH;

— a ampla derrogação prevista no n.º 1 do artigo 7.º seja suprimida ou, pelo menos, limitada explicitamente aos interesses públicos que justifiquem o recurso a ela pelos Estados-Membros;

— o artigo 10.º seja alterado de forma a prever que o acesso aos dados também seja registado e documentado;

— seja suprimida a alínea a) do n.º 2 dos artigos 19.º, 20.º e 21.º;

— sejam aditadas à proposta disposições relativas aos Responsáveis pela Protecção de Dados. Essas disposições poderiam ser formuladas inspirando-se nos artigos 24.º--26.º do Regulamento 45/2001/CE;

— se altere o n.º 2 do artigo 31.º da proposta de forma a que o presidente do Grupo do Artigo 29.º fique também habilitado a participar ou a fazer-se representar nas reuniões do novo Grupo.

Feito em Bruxelas, em 19 de Dezembro de 2005,

Peter HUSTINX

*Autoridade Europeia para a Protecção de Dados*