Parecer da Autoridade Europeia para a Protecção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho «Um espaço de liberdade, de segurança e de justiça ao serviço dos cidadãos»

(2009/C 276/02)

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, designadamente 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 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, nomeadamente o artigo 41.º,

EMITIU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 10 de Junho de 2009, a Comissão aprovou a Comunicação ao Parlamento Europeu e ao Conselho «Um espaço de liberdade, de segurança e de justiça ao serviço dos cidadãos» [1]. A AEPD apresenta o presente parecer nos termos do artigo 41.º do Regulamento (CE) n.º 45/2001.

2. Antes de aprovar a Comunicação, a Comissão consultou informalmente a AEPD, por carta de 19 de Maio de 2009. A 20 de Maio de 2009, respondendo a essa consulta, a AEPD enviou observações informais destinadas a melhorar o texto da Comunicação. Além disso, a AEPD deu o seu contributo activo para a carta de 14 de Janeiro de 2009 do Grupo da Polícia e Justiça acerca do programa plurianual no domínio da liberdade, segurança e justiça [2].

3. A Comunicação realça, no ponto 1, que a União se deve dotar «de um novo programa plurianual que, a partir dos progressos e dos ensinamentos retirados das deficiências actuais, se projecta no futuro com ambição. Este novo programa deverá definir prioridades para os próximos cinco anos». Este programa plurianual (já conhecido por «programa de Estocolmo») dará seguimento aos programas de Tampere e da Haia, que imprimiram um forte impulso político à área da liberdade, segurança e justiça.

4. A Comunicação deverá servir de base ao novo programa plurianual. A este respeito, a AEPD regista que, embora os programas plurianuais não sejam, em si mesmos, vinculativos, têm um impacto considerável na política a ser definida pelas instituições no sector em causa, pois muitas das medidas concretas, legislativas e outras, decorrerão do programa.

5. É desta perspectiva que a própria Comunicação deve ser encarada. É a próxima etapa de um debate que começou sensivelmente em Junho de 2008, com a apresentação de dois relatórios dos chamados «Grupos do Futuro» criados pela Presidência do Conselho para apresentar sugestões: «Liberdade, Segurança, Privacidade — os Assuntos Internos Europeus num mundo aberto» [3] e «Proposta de soluções para o futuro Programa da UE no domínio da Justiça» [4].

II. PRINCIPAIS ELEMENTOS DO PRESENTE PARECER

6. O presente parecer, além de exprimir uma reacção à Comunicação, é também um contributo da AEPD para o debate mais vasto sobre o futuro do espaço de liberdade, segurança e justiça que terá de conduzir à adopção de um novo programa de trabalho estratégico (programa de Estocolmo), conforme anunciado pela Presidência sueca da UE [5]; o parecer debruçar-se-á ainda sobre determinadas consequências da eventual entrada em vigor do Tratado de Lisboa.

7. Depois de na Parte III especificarmos as grandes perspectivas do parecer, passaremos na Parte IV a uma avaliação geral da Comunicação.

8. Na Parte V abordaremos a questão da resposta à necessidade de respeitar permanentemente a protecção da vida privada e dos dados pessoais num contexto de crescente intercâmbio destes dados. Centrar-nos-emos no ponto 2.3 da Comunicação, relativo à protecção dos dados pessoais e da vida privada, e de um modo geral na necessidade de continuar a adoptar novas medidas, legislativas e outras, para melhorar o quadro da protecção de dados.

[1] COM(2009) 262 final (adiante designada por «Comunicação»).

[2] Não publicada. O Grupo da Polícia e Justiça foi criado pela Conferência Europeia dos Comissários para a Protecção de Dados para preparar as posições da Conferência no domínio da aplicação da lei e agir em seu nome nos casos urgentes.

[3] Documento do Conselho n.º 11657/08 (adiante designado por «relatório sobre os Assuntos Internos»).

[4] Documento do Conselho n.º 11549/08 (adiante designado por «relatório sobre a Justiça»).

[5] Programa de trabalho da UE elaborado pelo Governo, http://www.regeringen.se

9. Na Parte VI são debatidas as necessidades e possibilidades de conservação, acesso e intercâmbio de informações para efeitos de aplicação da lei ou, como se diz na Comunicação, para «uma Europa que protege». O ponto 4 da Comunicação enuncia uma série de objectivos em termos de fluxo de informação e ferramentas tecnológicas, designadamente nos pontos 4.1.2 (Dominar a informação), 4.1.3 (Mobilizar as ferramentas tecnológicas necessárias) e 4.2.3.2 (Sistemas de informação). Neste contexto, pode dizer-se que a proposta que levanta o maior desafio é a da definição de um modelo europeu de informação (*in* ponto 4.1.2). O presente parecer da AEPD faz uma análise aprofundada dessa proposta.

10. Quanto à Parte VII, afora um tópico específico do espaço de liberdade, segurança e justiça que é pertinente para a protecção de dados, a saber, o acesso à justiça e a justiça electrónica (ou *e-Justice*).

III. **PERSPECTIVAS DO PARECER**

11. No presente parecer a necessidade de proteger os direitos fundamentais será o principal ângulo do qual perspectivaremos a análise da Comunicação e o futuro do espaço de liberdade, segurança e justiça em geral, concebido por um novo programa plurianual. Além disso, o parecer basear-se-á nos contributos da AEPD para a definição da política da UE neste domínio, sobretudo no exercício das suas funções consultivas. Até à data a AEPD aprovou mais de trinta pareceres e observações (acessíveis no seu sítio internet) sobre iniciativas decorrentes do programa da Haia.

12. No seu parecer sobre a Comunicação, a AEPD terá designadamente em conta as quatro perspectivas adiante enunciadas, que são relevantes para o futuro do espaço de liberdade, segurança e justiça e que também ocupam um lugar preponderante na própria Comunicação.

13. A primeira perspectiva é o crescimento exponencial da informação digital sobre os cidadãos em consequência da evolução das tecnologias da informação e da comunicação ([6]). A sociedade está a evoluir para o que muitas vezes se chama uma «sociedade da vigilância», em que todas as operações e quase todos os movimentos dos cidadãos são passíveis de registo digital. Tanto a «Internet das coisas» como a «inteligência ambiente» já estão em rápido desenvolvimento graças à utilização das etiquetas RFID. Recorre-se cada vez mais à digitalização das características do corpo humano (biométrica). Tudo isto nos leva a um mundo cada vez mais interligado, em que os organismos de segurança pública têm acesso a enormes volumes de informação potencialmente útil, o que pode afectar directamente a vida das pessoas em causa.

14. A segunda perspectiva é a internacionalização. Por um lado, nesta era digital o intercâmbio de dados não está circunscrito às fronteiras externas da União e, por outro lado, cada vez se torna mais necessária a cooperação internacional em todo o leque de actividades da UE no espaço de liberdade, segurança e justiça — das quais a luta antiterrorista, a cooperação policial e judiciária, a justiça em matéria civil e o controlo das fronteiras constituem tão-só alguns exemplos.

15. A terceira perspectiva é a utilização dos dados para efeitos de aplicação da lei: as recentes ameaças à sociedade, relacionadas ou não com o terrorismo, fizeram com que surgissem (pedidos no sentido de) mais possibilidades de recolha, armazenamento e intercâmbio de dados pessoais por parte das autoridades de aplicação da lei. Em muitos casos os particulares são activamente implicados, como acontece, entre outros, com a directiva sobre conservação de dados ([7]) e com os vários instrumentos sobre PNR ([8]).

16. A quarta perspectiva é a livre circulação. O desenvolvimento progressivo de um espaço de liberdade, segurança e justiça implica que as fronteiras internas e os eventuais obstáculos à livre circulação nesse espaço continuem a ser eliminados. De modo algum os novos instrumentos neste domínio devem voltar a erguer esses obstáculos. No contexto actual a livre circulação compreende, por um lado, a livre circulação de pessoas e, por outro, a livre circulação de dados (pessoais).

17. Estas quatro perspectivas demonstram a rápida mudança que se está a operar na conjuntura em que a informação é utilizada. Em tais circunstâncias, é indubitável a importância de se dispor de um mecanismo forte para proteger os direitos fundamentais do cidadão, designadamente a protecção dos dados e da vida privada. São estes os motivos que levam a AEPD a escolher a necessidade de protecção como principal ângulo de análise, conforme referido no ponto 11.

([6]) O relatório sobre os Assuntos Internos fala mesmo, neste contexto, de «tsunami digital».

([7]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE, JO L 105 de 13.4.2006, p. 54.

([8]) Veja-se, p. ex., o Acordo entre a União Europeia e os Estados Unidos da América sobre a transferência de dados contidos nos registos de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Departamento da Segurança Interna dos Estados Unidos e sobre o tratamento dos dados em causa pelo mesmo departamento (Acordo PNR de 2007), JO L 204 de 4.8.2007, p. 18, e a proposta de decisão-quadro do Conselho relativa à utilização dos Registos de Identificação dos Passageiros (PNR) para efeitos de aplicação da lei [COM(2007) 654 final].

IV. **AVALIAÇÃO GERAL**

18. Tanto a Comunicação como o programa de Estocolmo visam especificar as intenções da UE para os próximos cinco anos, possivelmente com efeitos ainda mais longínquos. A AEPD constata que a Comunicação está redigida em termos neutrais relativamente ao Tratado de Lisboa. Embora compreenda perfeitamente os motivos que levaram a Comissão a adoptar esta abordagem, a AEPD lamenta que a Comunicação não tenha tirado o melhor partido das possibilidades adicionais oferecidas pelo Tratado de Lisboa. No presente parecer será dado maior realce à perspectiva do Tratado de Lisboa.

19. A Comunicação baseia-se nos resultados da acção que a UE tem vindo a desenvolver, ao longo dos últimos anos, no espaço de liberdade, segurança e justiça. Pode dizer-se que esses resultados são desencadeados por acontecimentos específicos, com destaque para medidas que alargam as competências das autoridades de aplicação da lei e são invasivas para o cidadão. Isto é óbvio nos domínios em que são intensivamente usados e trocados dados pessoais e que por isso se revestem da maior importância para a protecção de dados. Os resultados são induzidos pelos acontecimentos na medida em que certos eventos externos, como o 11 de Setembro e os atentados à bomba de Madrid e Londres, deram um forte impulso às actividades legislativas. Por exemplo, a transferência de dados sobre os passageiros para os Estados Unidos pode ser vista como consequência do 11 de Setembro ([9]), ao passo que os atentados à bomba em Londres conduziram à aprovação da Directiva 2006/24/CE, relativa à conservação de dados ([10]). Procurou-se uma acção mais invasiva, já que o legislador comunitário se centrou em medidas destinadas a facilitar a utilização e o intercâmbio de dados, e que foi dada menor urgência ao debate de medidas de protecção dos dados pessoais. A principal medida de protecção existente foi aprovada após três anos de debates no Conselho — trata-se da Decisão-Quadro 2008/977/JAI do Conselho relativa à protecção de dados pessoais tratados no quadro da cooperação policial e judiciária em matéria penal ([11]). O que se obteve foi uma decisão-quadro do Conselho não inteiramente satisfatória (ver pontos 29-30).

20. A experiência dos últimos anos demonstra que, antes de se adoptarem novos instrumentos, é necessário reflectir nas consequências que estes terão para as autoridades de aplicação da lei e para os cidadãos europeus. Tanto o sacrifício da vida privada como a eficácia na aplicação da lei devem ser devidamente ponderados nessa reflexão — primeiro nas fases de proposta e discussão de novos instrumentos, e depois, em revisões periódicas, quando já tiverem sido implementados. Essa mesma reflexão também é essencial antes de se lançar um novo programa plurianual com iniciativas importantes para o futuro próximo.

21. A AEPD saúda o facto de a Comunicação reconhecer que a protecção dos direitos fundamentais, designadamente a protecção dos dados pessoais, é uma das problemáticas mais relevantes para o futuro do espaço de liberdade, segurança e justiça. O ponto 2 da Comunicação qualifica a UE como um espaço singular para a protecção dos direitos fundamentais, baseado em valores comuns. Também é positivo que a adesão à Convenção Europeia dos Direitos do Homem seja mencionada como questão prioritária — é mesmo a primeira orientação prioritária formulada na Comunicação. Essa adesão representa um passo importante no sentido da criação de um sistema harmonioso e coerente para a protecção dos direitos fundamentais. Por último, mas não menos importante, há o facto de a Comunicação ter reservado um lugar de relevo à protecção de dados.

22. Esse destaque dado na Comunicação traduz a firme intenção de assegurar a protecção dos direitos dos cidadãos e de adoptar, assim, uma abordagem mais equilibrada. Os governos precisam de instrumentos adequados para garantirem a segurança dos cidadãos; por outro lado, na nossa sociedade europeia, têm de respeitar inteiramente os direitos fundamentais desses mesmos cidadãos. Para estar ao serviço dos cidadãos ([12]), a União Europeia tem de preservar este equilíbrio.

23. A AEPD considera que a Comunicação tem na devida conta a necessidade de manter esse equilíbrio, e inclusive a necessidade de proteger os dados pessoais, e reconhece que a tónica deve ser inflectida. Este aspecto é importante, na medida em que as políticas adoptadas para o espaço de liberdade, segurança e justiça não devem fomentar a mudança gradual para uma sociedade da vigilância. A AEPD espera que o Conselho adopte a mesma abordagem no programa de Estocolmo, nomeadamente subscrevendo as orientações formuladas no ponto 25 *infra*.

24. Tudo isto é tanto mais importante quanto o espaço de liberdade, segurança e justiça é um espaço que «molda as circunstâncias em que os cidadãos vivem, e em especial o espaço privado de sua responsabilidade e de segurança política e social, protegido pelos direitos fundamentais», conforme sublinhado pelo Tribunal Constitucional alemão no seu recentíssimo acórdão (de 30 de Junho de 2009) relativo ao Tratado de Lisboa ([13]).

([9]) Acordo PNR de 2007, mencionado na nota anterior, e seus predecessores.

([10]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE, JO L 105 de 13.4.2006, p. 54. Embora a base jurídica seja o artigo 95.º do TCE, esta directiva foi uma reacção imediata aos atentados de Londres.

([11]) Decisão-Quadro 2008/977/JAI do Conselho, de 27 de Novembro de 2008, relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, JO L 350 de 30.12.2008, p. 60.

([12]) Cf. título da Comunicação.

([13]) Comunicado de Imprensa n.º 72/2009, de 30 de Junho de 2009, do Tribunal Constitucional Federal da Alemanha, ponto 2.c).

25. A AEPD salienta que, num espaço com tais características:

— a troca de informações entre as autoridades dos Estados-Membros, incluindo os organismos ou bases de dados europeus pertinentes, se for o caso, deve ser efectuada com base em mecanismos adequados e eficazes, que respeitem inteiramente os direitos fundamentais do cidadão e garantam a confiança recíproca,

— para tal é necessário, não só que a informação esteja disponível e que exista um reconhecimento mútuo dos sistemas jurídicos dos Estados-Membros (e da UE), mas também que haja uma harmonização das normas de protecção dessas informações graças por exemplo, mas não só, à criação de um quadro comum para a protecção de dados,

— as normas comuns assim criadas não devem aplicar-se apenas a situações de dimensão transnacional. A confiança mútua só pode existir se as normas forem sólidas — e sempre respeitadas, sem que se corra o risco de deixarem de se aplicar quando a dimensão transnacional não é, ou deixa de ser, manifesta. Para além disto, especialmente no que toca à utilização das informações, as diferenças entre «dados internos» e «dados transfronteiriços» não podem funcionar na prática ([14]).

V. INSTRUMENTOS DE PROTECÇÃO DE DADOS

V.1. Rumo a um regime completo de protecção dos dados

26. A AEPD subscreve a abordagem estratégica da Comunicação que reserva um lugar de relevo, ao tema da protecção de dados. Com efeito, muitas das iniciativas tomadas no espaço de liberdade, segurança e justiça recorrem à utilização de dados pessoais e, para serem bem sucedidas, têm absoluta necessidade de uma boa protecção desses dados. O respeito pela vida privada e a protecção dos dados representam, não apenas uma obrigação jurídica cada vez mais reconhecida ao nível da UE, mas igualmente uma questão crucial para os cidadãos europeus, como mostram os resultados do Eurobarómetro ([15]). Além disso, para assegurar a confiança dos serviços de aplicação da lei também é fundamental que o acesso aos dados pessoais seja restringido.

27. No ponto 2.3 da Comunicação afirma-se ser necessário um regime completo de protecção de dados que abranja o conjunto das competências da União ([16]). A AEPD subscreve totalmente este objectivo, independentemente da entrada em vigor do Tratado de Lisboa. Observa ainda que esse regime pode não corresponder necessariamente a uma moldura jurídica única, aplicável a todos os tipos de tratamento. À luz dos tratados em vigor, são poucas as possibilidades de adoptar um quadro jurídico único e abrangente que seja aplicável a todos os tipos de tratamento, devido à estrutura de pilares e ao facto de que — pelo menos no primeiro pilar — a protecção dos dados tratados pelas instituições europeias assenta numa base jurídica separada (o artigo 286.º do TCE). A AEPD assinala, contudo, que se podem introduzir alguns melhoramentos se as possibilidades oferecidas pelos actuais tratados forem plenamente aproveitadas, conforme já salientado pela Comissão na sua comunicação «Aplicação do programa da Haia: O rumo a seguir» ([17]). Depois de o Tratado de Lisboa entrar em vigor, o artigo 16.º do TFUE proporcionará a base jurídica necessária à adopção de um quadro jurídico único e abrangente que seja aplicável a todos os tipos de tratamento.

28. A AEPD regista que — seja como for — importa assegurar a coerência do quadro jurídico da protecção de dados, se necessário harmonizando e consolidando os diferentes instrumentos jurídicos aplicáveis ao espaço de liberdade, segurança e justiça.

À luz dos tratados em vigor

29. O primeiro passo foi dado recentemente, com a aprovação da Decisão-Quadro 2008/977/JAI do Conselho ([18]). Este instrumento não pode, todavia, ser qualificado de quadro jurídico abrangente, sobretudo porque as suas disposições não têm aplicação geral; de facto, não se aplicam às situações internas, em que os dados pessoais provêm do próprio Estado-Membro que os utiliza. Esta limitação diminui forçosamente o valor acrescentado da decisão-quadro do Conselho, a não ser que todos os Estados-Membros decidam incluir as situações internas na legislação nacional de aplicação — o que não é provável.

30. A segunda razão pela qual a AEPD considera que, a longo prazo, a Decisão-Quadro 2008/977/JAI do Conselho não oferece um quadro jurídico satisfatório para a protecção de dados num espaço de liberdade, segurança e justiça, é o facto de muitas das suas disposições essenciais não serem consentâneas com a Directiva 95/46/CE. À luz dos tratados em vigor, poder-se-ia dar um segundo passo: alargar o âmbito de aplicação da decisão-quadro do Conselho e alinhá-la pela Directiva 95/46/CE.

31. Também se poderia contribuir para a concretização de um regime completo de protecção de dados definindo uma visão clara e a longo prazo. Esta visão poderia incluir uma abordagem global e coerente para definir a recolha e o intercâmbio de dados — bem como a forma de utilizar as bases de dados existentes — e, simultaneamente, as

([14]) A AEPD desenvolveu esta última ideia no seu parecer de 19 de Dezembro de 2005 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], JO C 47 de 25.2.2006, p. 27, pontos 30-32.

([15]) Data Protection in the European Union — Citizens' perceptions — Analytical report, Flash Eurobarometer Series 225, Jan. 2008, http://www.ec.europa.eu/public_opinion/flash/fl_225_en.pdf

([16]) Cf. também as orientações prioritárias da Comunicação.

([17]) COM(2006) 331 final, de 28 de Junho de 2006.

([18]) Cf. nota 11.

garantias de protecção de dados; deveria evitar a sobreposição e a duplicação desnecessárias de instrumentos (e, por conseguinte, do tratamento de dados pessoais); deveria igualmente fomentar a coerência das políticas comunitárias nesta matéria e a confiança na forma como as autoridades oficiais tratam os dados dos cidadãos. A AEPD recomenda ao Conselho que, no programa de Estocolmo, anuncie a necessidade de uma visão clara e a longo prazo.

32. A AEPD recomenda ainda que sejam avaliadas e perspectivadas as medidas já adoptadas nesta matéria, bem como a sua aplicação concreta e a sua eficácia. Devem, avaliar-se, nesse contexto, o sacrifício da vida privada e a eficácia da aplicação da lei. Caso estas avaliações demonstrem que determinadas medidas não dão os resultados esperados ou são desproporcionadas em relação aos objectivos em vista, ponderar-se-á a possibilidade de adoptar a seguinte abordagem faseada:

— na primeira etapa, alterar ou revogar as medidas que pareçam não se justificar por não representarem uma mais-valia concreta para as autoridades de aplicação da lei e para os cidadãos europeus,

— na segunda etapa, avaliar as possibilidades de melhorar a aplicação das medidas já existentes,

— só propor novas medidas legislativas numa terceira etapa, e se for provável que essas novas medidas sejam necessárias para atingir os objectivos em vista. Só deverão aprovar-se novos instrumentos que tragam uma mais-valia clara e concreta às autoridades de aplicação da lei e aos cidadãos europeus.

A AEPD recomenda que o programa de Estocolmo faça referência a um sistema de avaliação das medidas em vigor.

33. Por último, mas não menos importante, deve ser dada especial importância à necessidade de aplicar melhor as garantias existentes, em conformidade com a comunicação da Comissão sobre o acompanhamento do programa de trabalho para uma melhor aplicação da directiva relativa à protecção de dados ([19]) e com as sugestões formuladas pela AEPD no seu parecer sobre essa comunicação ([20]). Infelizmente, no âmbito do terceiro pilar a Comissão não tem possibilidade de iniciar processos por incumprimento.

À luz do Tratado de Lisboa

34. O Tratado de Lisboa abre caminho à criação de um quadro verdadeiramente abrangente para a protecção de dados. O n.º 2 do artigo 16.º do Tratado relativo ao Funcionamento da União Europeia prevê que o Conselho e o Parlamento Europeu estabeleçam as normas relativas à protecção de dados pelas instituições, órgãos e organismos da União, pelos Estados-Membros no exercício de actividades relativas à aplicação do direito da União, e por entidades do sector privado.

35. No entender da AEPD, o destaque dado na Comunicação à concretização de um regime completo de protecção de dados traduz a vontade da Comissão de propor uma moldura legal aplicável a todas as actividades de tratamento de dados. A AEPD subscreve inteiramente esta ambição, que visa reforçar a coerência do sistema, garantir a segurança jurídica e melhorar, deste modo, a protecção. Mais concretamente, deixariam de existir as dificuldades criadas pela existência de uma linha divisória entre os pilares nas situações em que os dados recolhidos no sector privado para efeitos comerciais são posteriormente utilizados para fins repressivos. Esta linha divisória entre os pilares não reflecte totalmente a realidade, conforme demonstrado pelos importantes acórdãos do Tribunal de Justiça sobre os PNR ([21]) e a conservação de dados ([22]).

36. A AEPD sugere que o programa de Estocolmo dê lugar de destaque a esta argumentação a favor de um regime completo de protecção de dados, que revela que este é mais do que uma simples preferência: é uma necessidade criada pela evolução das práticas na utilização de dados. A AEPD recomenda que o programa de Estocolmo aponte como prioridade a criação de um novo enquadramento jurídico que venha, nomeadamente, substituir a Decisão-Quadro 2008/977/JAI do Conselho.

37. A AEPD sublinha que a ideia de um regime completo de protecção de dados baseado num quadro jurídico geral não exclui a adopção de regras adicionais sobre protecção de dados para os sectores policial e judiciário. Essas regras adicionais poderão ter em conta as necessidades específicas dos serviços de aplicação da lei, como se prevê na Declaração n.º 21, anexada ao Tratado de Lisboa ([23]).

V.2. **Reafirmar os princípios em matéria de protecção de dados**

38. A Comunicação toma nota das mudanças tecnológicas que estão a transformar a comunicação entre as pessoas singulares e as organizações públicas e privadas. Torna-se assim necessário, no entender da Comissão, reafirmar um certo número de princípios fundamentais da protecção de dados.

([19]) COM(2007) 87 final, de 7 de Março de 2007.

([20]) Parecer de 25 de Julho de 2007, JO C 255 de 27.10.2007, p. 1, designadamente ponto 30.

([21]) Acórdão do Tribunal de 30 de Maio de 2006, Parlamento Europeu c/Conselho da União Europeia (C-317/04) e Comissão Europeia (C-318/04), Processos apensos C-317/04 e C-318/04, Col. [2006], p. I-4721.

([22]) Acórdão do Tribunal de 10 de Fevereiro de 2009, Irlanda c/Parlamento Europeu e Conselho da União Europeia, Processo C-301/06, ainda não publicado.

([23]) Cf. Declaração n.º 21, sobre a protecção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial, anexada à Acta Final da Conferência Intergovernamental que aprovou o Tratado de Lisboa, JO C 115 de 9.5.2008, p. 345.

39. A AEPD saúda estas intenções da Comissão. É, de facto, da maior pertinência que se proceda a uma avaliação, para verificar se aqueles princípios são efectivamente aplicados na perspectiva da evolução tecnológica. Em primeiro lugar, importa referir que essa reafirmação dos princípios da protecção de dados não tem forçosamente uma ligação directa com a evolução tecnológica, podendo também tornar-se necessária de outros pontos de vista (mencionados na parte III supra), como a internacionalização, a crescente utilização dos dados para efeitos de aplicação da lei e a livre circulação.

40. Acresce que, no entender da AEPD, essa avaliação pode ser incluída na consulta pública anunciada pela Comissão na conferência «*Personal data — more use, more protection?*», de 19 e 20 de Maio de 2009. Esta consulta pública poderá dar um contributo valioso neste contexto ([24]). A AEPD sugere que a articulação entre as intenções da Comissão (afirmadas no ponto 2.3), por um lado, e a consulta pública sobre o futuro da protecção de dados, por outro, seja destacada pelo Conselho — no texto do programa de Estocolmo — e pela Comissão — nas suas declarações públicas sobre a consulta.

41. A referida avaliação poderá abranger, por exemplo, os seguintes aspectos:

— os dados pessoais no espaço de liberdade, segurança e justiça podem ser extremamente sensíveis, sendo esse o caso dos dados relativos a condenações penais, dos dados policiais e dos dados biométricos (impressões digitais, perfis de ADN),

— o tratamento dos dados em causa pode ter consequências negativas para as pessoas a que dizem respeito, especialmente se atendermos aos poderes coercivos das autoridades de aplicação da lei. Além disso, as operações de acompanhamento e análise dos dados são cada vez mais efectuadas por sistemas automáticos, muitos deles sem intervenção humana. A tecnologia permite que as bases que incluem dados pessoais sejam utilizadas para pesquisas gerais (prospecção de dados, caracterização, etc.). Devem ser claramente definidas as obrigações legais ligadas ao tratamento de dados,

— um dos princípios fundamentais da legislação em matéria de protecção de dados é o de que os dados pessoais devem ser recolhidos para fins específicos e não podem ser utilizados de forma incompatível com esses fins. A sua utilização para fins incompatíveis só deve ser permitida se estiver prevista por lei, e se for motivada por interesses específicos de ordem pública como os estabelecidos no n.º 2 do artigo 8.º da CEDH,

— a necessidade de respeitar o princípio da limitação da finalidade poderá repercutir-se nas actuais tendências da utilização de dados. Os serviços de aplicação da lei utilizam dados recolhidos por empresas privadas para fins comerciais, nos sectores das telecomunicações e dos transportes e no sector financeiro. Além disso, já estão instituídos sistemas de informação de grande escala, por exemplo, nos domínios da imigração e do controlo de fronteiras. São ainda permitidas interligações e acessos a bases de dados, o que vem ampliar a finalidade inicial da recolha dos dados. É necessário reflectir sobre estas actuais tendências e introduzir os ajustamentos e/ou garantias adicionais que se afigurem pertinentes,

— para além dos princípios da protecção de dados que são referidos na Comunicação, a avaliação atenderá à necessidade de transparência no tratamento, de modo a que a pessoa a quem os dados dizem respeito possa exercer os seus direitos. A transparência é uma problemática dificílima no sector da aplicação da lei, sobretudo porque tem de ser contrabalançada com os riscos para as investigações,

— importa procurar soluções para os intercâmbios com países terceiros.

42. A avaliação de que falamos deverá também incidir sobre as possibilidades de tornar mais eficaz a aplicação dos princípios da protecção de dados. Neste contexto, haveria vantagem em examinar os instrumentos susceptíveis de reforçar as responsabilidades das entidades responsáveis pelo tratamento dos dados. Esses instrumentos devem permitir que os responsáveis pelo tratamento prestem contas da gestão dos dados. «Administração dos dados» é, neste contexto, um conceito pertinente que abarca todos os meios jurídicos, técnicos e organizativos a que as organizações recorrem para garantir a plena responsabilidade pela forma como os dados são tratados, a saber, planeamento e controlo, utilização de tecnologias sólidas, boa formação dos efectivos, auditorias do cumprimento das regras, etc.

V.3. **Tecnologias respeitadoras da vida privada**

43. A AEPD saúda a alusão, feita na Comunicação, a uma certificação para as tecnologias respeitadoras da vida privada. Além desta, poder-se-ia também falar de uma «privacidade na concepção» e na necessidade de encontrar as «melhores técnicas disponíveis» que sejam consentâneas com o enquadramento comunitário da protecção de dados.

44. A AEPD considera que tanto a «privacidade na concepção» como as tecnologias respeitadoras da vida privada poderão contribuir para uma melhor protecção e uma utilização mais eficaz das informações. A AEPD sugere duas vias, que não se excluem mutuamente:

— um regime de certificação da protecção dos dados e da vida privada ([25]), como opção para os criadores e os utilizadores de sistemas de informação, com ou sem apoio financeiro ou legislativo da UE,

([24]) O Grupo do Artigo 29.º para a Protecção da Dados, que conta com a participação da AEPD, decidiu trabalhar intensivamente no seu contributo para esta consulta pública.

([25]) Como exemplo deste regime, temos o EuroPriSe (*European Privacy Seal* — rótulo europeu de protecção da vida privada).

— uma obrigação legal, imposta aos criadores e aos utilizadores de sistemas de informação, de utilizar sistemas conformes com o princípio da privacidade na concepção. Para seguir esta via, poderá ser necessário alargar o actual âmbito da legislação sobre protecção de dados por forma a responsabilizar os criadores pelos sistemas de informação que concebem ([26]).

a AEPD sugere que estas (possíveis) vias sejam mencionadas no programa de Estocolmo.

V.4. **Aspectos externos**

45. Outro dos assuntos mencionados na Comunicação é o desenvolvimento e a promoção de normas internacionais em matéria de protecção de dados pessoais. Neste momento estão a ser desenvolvidas muitas actividades que visam a definição de normas viáveis de aplicação universal, como por exemplo a Conferência Internacional dos Comissários para a Protecção dos Dados e da Vida Privada. Esta conferência poderá levar, no futuro próximo, à celebração de um acordo internacional. A AEPD sugere que o programa de Estocolmo apoie estas actividades.

46. A Comunicação alude ainda à celebração de acordos bilaterais, tomando como ponto de partida os progressos já feitos com os Estados Unidos. A AEPD concorda com a necessidade de um enquadramento jurídico claro para a transferência de dados para países terceiros, tendo por isso saudado a colaboração desenvolvida pelas autoridades da UE e dos EUA, no Grupo de Contacto de Alto Nível, a respeito de um eventual instrumento transatlântico em matéria de protecção de dados e, simultaneamente, preconizado mais clareza e cuidado com determinados aspectos ([27]). Nesta perspectiva, interessa também registar as ideias formuladas no relatório sobre os Assuntos Internos a favor da realização de um espaço euro-atlântico de cooperação no domínio da liberdade, segurança e justiça, a cujo respeito, segundo o relatório, a UE deverá tomar posição até 2014. A criação desse espaço não será possível sem que existam garantias apropriadas em matéria de protecção de dados.

47. Na opinião da AEPD, as normas europeias de protecção de dados — baseadas na Convenção 108 do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal ([28]) e na jurisprudência do Tribunal de Justiça Europeu e do Tribunal Europeu dos Direitos do Homem — deverão determinar o nível de protecção a estabelecer num acordo geral com os Estados Unidos em matéria de protecção e intercâmbio de dados. Esse acordo geral poderá servir de base à celebração de convénios específicos aplicáveis ao intercâmbio de dados pessoais. Este aspecto assume ainda maior importância se tivermos em conta a intenção, formulada no ponto 4.2.1 da Comunicação, de que a União deverá concluir acordos de cooperação policial quando tal se justificar.

48. A AEPD compreende perfeitamente a necessidade de reforçar a cooperação internacional, inclusive, em certos casos, com países que não protegem os direitos fundamentais. Não obstante ([29]), importa ter em conta que esta cooperação internacional pode provocar um grande acréscimo na recolha e na transferência internacional de dados. Assim sendo, é essencial que os princípios do tratamento legal e equitativo, bem como os da equidade do processo em geral, se apliquem à recolha e à transferência de dados pessoais através das fronteiras da União e que esses dados só sejam transferidos para países terceiros ou organizações internacionais se os terceiros envolvidos assegurarem o devido nível de protecção ou derem outras garantias adequadas.

49. A concluir, a AEPD recomenda que o programa de Estocolmo realce que devem ser celebrados acordos gerais com os Estados Unidos e outros países terceiros, no domínio da protecção e do intercâmbio de dados, tendo por base o nível de protecção garantido no território da UE. Numa perspectiva mais vasta, a AEPD assinala que importa promover activamente o respeito pelos direitos fundamentais, e em especial o direito à protecção de dados, nas relações com países terceiros e organizações internacionais ([30]). Além disso, o programa de Estocolmo poderia fazer alusão à ideia geral de que o intercâmbio de dados pessoais com países terceiros requer que estes assegurem o devido nível de protecção ou dêem outras garantias adequadas.

VI. **UTILIZAÇÃO DAS INFORMAÇÕES**

VI.1. **Rumo a um modelo europeu de informação**

50. Um dos grandes objectivos políticos da União Europeia, no espaço de liberdade, segurança e justiça, é melhorar o intercâmbio de informações. O ponto 4.1.2 da Comunicação salienta que a segurança na União Europeia depende de mecanismos eficientes para o intercâmbio de informações entre as autoridades nacionais e outros intervenientes europeus. É lógico que o intercâmbio de informações mereça este destaque, na medida em que não dispomos de uma força de polícia, de um sistema de justiça penal, de um

([26]) Os utilizadores da informação são abrangidos pela legislação sobre protecção de dados, assim como os responsáveis pelo tratamento e os subcontratantes.

([27]) Parecer da AEPD, de 11 de Novembro de 2008, sobre o relatório final do Grupo de Contacto de Alto Nível UE-EUA sobre o intercâmbio de informações e a protecção da vida privada e dos dados pessoais, JO C 128 de 6.6.2009, p. 1.

([28]) STCE 108 de 28.1.1981.

([29]) Ver carta da AEPD, de 28 de Novembro de 2005, sobre a comunicação da Comissão relativa à dimensão externa do espaço de liberdade, segurança e justiça, disponível no sítio internet da AEPD.

([30]) A recente jurisprudência sobre as listas de terroristas confirma que são necessárias garantias — inclusive nas relações com os Estados Unidos — de que as medidas antiterroristas obedecem às normas da UE sobre os direitos fundamentais (Acórdão de 3 de Setembro de 2008 nos Processos apensos C-402/05 P e C-415/05 P, Kadi e Al Barakaat Foundation c/ Conselho, ainda não publicado).

controlo de fronteiras, à escala europeia. Daí que as medidas relativas a informações são contributos essenciais da União Europeia que permitem às autoridades dos Estados-Membros combater eficazmente a criminalidade transfronteiras e proteger as fronteiras externas com a mesma eficácia. No entanto, essas medidas não contribuem apenas para a segurança dos cidadãos, contribuem também para a sua liberdade — a livre circulação de pessoas foi atrás mencionada como perspectiva do presente parecer — e para a justiça.

51. Foram estes, precisamente, os motivos que levaram à introdução do princípio da disponibilidade no programa da Haia. Este princípio implica que as informações necessárias para combater a criminalidade devem transpor as fronteiras internas da UE sem encontrar obstáculos. Diversas experiências recentes vieram comprovar a dificuldade de traduzir este princípio em medidas legislativas. O Conselho não aceitou a proposta da Comissão, de 12 de Outubro de 2005, tendo em vista a aprovação de uma decisão-quadro do Conselho relativa ao intercâmbio de informações com base no princípio da disponibilidade ([31]). Os Estados-Membros não estavam, com efeito, dispostos a aceitar as consequências do princípio da disponibilidade em toda a sua extensão. Foram, em vez disso, adoptados instrumentos mais limitados ([32]), como a Decisão 2008/615/JAI do Conselho, de 23 de Junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (adiante designada por «Decisão de Prüm») ([33]).

52. Embora o princípio da disponibilidade estivesse no cerne do programa da Haia, a Comissão parece ter agora ambições mais modestas; tenciona estimular mais ainda o intercâmbio de informações entre as autoridades dos Estados-Membros, graças à introdução do modelo europeu de informação. A Presidência sueca da UE, que segue a mesma linha de pensamento ([34]), irá apresentar uma proposta de estratégia de intercâmbio de informações. O Conselho já começou a trabalhar neste ambicioso projecto de definição de uma Estratégia de Gestão de Informação da União Europeia, que está estreitamente ligado ao do modelo europeu de informação. A AEPD regista estes desenvolvimentos com o maior interesse e salienta que nestes projectos deve ser dada a maior atenção à vertente da protecção de dados.

Modelo europeu de informação e protecção de dados

53. Em primeiro lugar, deve-se partir do princípio de que o futuro do espaço de liberdade, segurança e justiça não pode ir «a reboque» das tecnologias, querendo isto dizer que as oportunidades quase ilimitadas oferecidas pelas novas tecnologias têm sempre de ser contrabalançadas com os princípios da protecção de dados e só devem ser utilizadas se obedecerem a esses princípios.

54. A AEPD regista que a Comunicação apresenta o modelo de informação, não só como um modelo técnico, mas como uma poderosa capacidade de análise estratégica e uma melhor recolha e tratamento das informações operacionais. Reconhece igualmente que determinados aspectos estratégicos — como os critérios de recolha, partilha e tratamento das informações — devem ser tidos em conta, no respeito pelos princípios da protecção de dados.

55. Tanto as tecnologias da informação como as condições jurídicas são — e continuarão a ser — essenciais. A AEPD saúda o facto de a Comunicação partir do princípio de que o modelo europeu de informação não pode ser visto com base em considerações técnicas. É essencial que as informações só sejam recolhidas, partilhadas e tratadas caso existam necessidades concretas e se forem respeitados os princípios da protecção de dados. A AEDP também concorda inteiramente com a necessidade de criar um mecanismo de acompanhamento que permita avaliar o funcionamento dos intercâmbios de informações. A AEPS sugere ao Conselho que aprofunde estes aspectos no programa de Estocolmo.

56. Neste contexto, a AEPD sublinha que a protecção de dados, que visa proteger os cidadãos, não deve ser encarada como um obstáculo à gestão efectiva dos dados. Com efeito, a protecção de dados oferece ferramentas úteis para melhorar a conservação, o acesso e o intercâmbio de informações; além disso, os direitos da pessoa em causa (a saber que informações a seu respeito são tratadas, bem como a rectificar as informações incorrectas) podem contribuir para a exactidão dos dados existentes nos sistemas de gestão de dados.

57. A legislação sobre protecção de dados tem, no essencial, as seguintes consequências: se os dados forem necessários para uma finalidade específica e legítima, podem ser utilizados; se não forem necessários para um fim bem definido, os dados pessoais não devem ser utilizados. No primeiro caso, poderão ser necessárias medidas adicionais que ofereçam as devidas garantias.

58. A AEPD não está, contudo, de acordo com a Comunicação quando esta refere a «identificação das necessidades futuras» como fazendo parte do modelo de informação. A AEPD salienta que, também no futuro, o princípio da limitação da finalidade deverá orientar a criação de sistemas de informação ([35]). Este princípio é uma das principais garantias que o sistema de protecção de dados oferece ao cidadão: este tem de poder saber, com antecedência, para que efeito são recolhidos dados a seu respeito, e que tais dados só serão utilizados para esse efeito, designadamente no futuro. Esta garantia está mesmo consagrada no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. O princípio da limitação da finalidade pode ter excepções — especialmente pertinentes no espaço de liberdade, segurança e justiça — mas estas não podem determinar a arquitectura de um sistema.

([31]) COM(2005) 490 final.

([32]) Na perspectiva da disponibilidade; a Decisão de Prüm compreende disposições de longo alcance em matéria de utilização de dados biométricos (ADN e impressões digitais).

([33]) JO L 210 de 6.8.2008, p. 1.

([34]) Cf. programa de trabalho da UE elaborado pelo Governo, citado na nota 5, p. 23.

([35]) Cf. igualmente ponto 41 *supra*.

Escolher a arquitectura certa

59. Tudo deve partir da escolha da arquitectura adequada. A Comunicação reconhece a importância de uma verdadeira arquitectura dos sistemas de informação (ponto 4.1.3), mas, infelizmente, apenas para efeitos de interoperabilidade.

60. A AEPD destaca outro aspecto: no modelo europeu de informação, os requisitos de protecção de dados não devem ser vistos unicamente como uma condição necessária à legalidade dos sistemas, devem antes fazer parte integrante de todo o processo de desenvolvimento de qualquer sistema ([36]). Há que utilizar os conceitos da «privacidade na concepção» e da necessidade de encontrar as «melhores técnicas disponíveis» ([37]), como se afirma no ponto 43 *supra*, e o modelo europeu de informação deverá assentar nestes mesmos conceitos. Significa isto, em concreto, que a arquitectura dos sistemas de informação concebidos para efeitos de segurança pública deve sempre obedecer ao princípio da «privacidade na concepção». A AEPD recomenda ao Conselho que inclua estes elementos no programa de Estocolmo.

Interoperabilidade dos sistemas

61. A AEPD realça que a interoperabilidade não é uma mera questão técnica, mas também tem consequências para a protecção dos cidadãos, e em particular para a protecção de dados. Na perspectiva da protecção de dados, a interoperabilidade dos sistemas, se for bem realizada, apresenta a vantagem manifesta de evitar o duplo armazenamento. Todavia, também é óbvio que a viabilização técnica do acesso/ /intercâmbio de dados se torna, muitas vezes, num poderoso incentivo para aceder/trocar efectivamente esses dados. Por outras palavras, a interoperabilidade apresenta riscos especiais de interligação de bases de dados com finalidades diferentes ([38]), podendo afectar as estritas limitações à finalidade das bases.

62. Resumindo, o simples facto de ser tecnicamente possível trocar informações digitais entre bases de dados interoperáveis, ou fundir essas bases de dados, não é motivo para abrir excepção ao princípio da limitação da finalidade. A interoperabilidade deve, em cada caso concreto, assentar em opções políticas claras e cuidadosas. A AEPD sugere que este conceito seja especificado no programa de Estocolmo.

VI.2. **Utilização das informações recolhidas para outros fins**

63. A Comunicação não se debruça explicitamente sobre uma das mais importantes tendências dos últimos anos, a saber, a utilização para fins de aplicação da lei dos dados recolhidos no sector privado para efeitos comerciais. Esta tendência não diz respeito apenas aos dados de tráfego das comunicações electrónicas e às informações sobre os passageiros dos voos para (determinados) países terceiros ([39]), estando também presente no sector financeiro. Exemplo disso é a Directiva 2005/60/CE do Parlamento Europeu e do Conselho, de 26 de Outubro de 2005, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo ([40]). Outro exemplo, bem conhecido e amplamente debatido, é o tratamento, pela Sociedade Mundial de Telecomunicações Financeiras Interbancárias (SWIFT) ([41]), de dados pessoais necessários para efeitos do programa do Departamento do Tesouro dos Estados Unidos para detecção do financiamento do terrorismo.

64. A AEPD considera que o programa de Estocolmo deve consagrar especial atenção a estas tendências — que podem ser encaradas como derrogações ao princípio da limitação da finalidade e constituem com frequência uma forte invasão da vida privada, pois a utilização desses dados pode ser muito reveladora dos comportamentos individuais. Para cada caso específico em que se proponha a sua adopção, tem de haver provas muito fortes que justifiquem uma medida de natureza tão invasiva. Se forem apresentadas essas provas, importa garantir o pleno respeito pelos direitos das pessoas singulares.

65. No entender da AEPD, a utilização para efeitos de aplicação da lei de dados pessoais recolhidos para fins comerciais só deve ser autorizada em condições rigorosas, tais como:

— os dados apenas são utilizados para finalidades especificamente definidas (como o combate ao terrorismo ou às formas graves de criminalidade) e a determinar caso a caso,

— os dados são transferidos através de um sistema de «exportação», e não pelo método de «extracção» ([42]),

([36]) Cf. as directrizes e critérios para desenvolver, implementar e utilizar tecnologias de segurança destinadas a proteger a vida privada («*Guidelines and criteria for the development, implementation and use of Privacy Enhancing Security Technologies*»), elaborados no âmbito do projecto PRISE (http://www.prise.oeaw.ac.at).

([37]) Por «melhores técnicas disponíveis» entende-se o estádio de desenvolvimento mais eficaz e avançado das actividades e dos seus métodos de operação que demonstre a aptidão prática de técnicas específicas para servir de base, em princípio, a aplicações e sistemas consentâneos com os requisitos do quadro regulamentar da UE em matéria de segurança e de protecção dos dados e da vida privada.

([38]) Cf. as observações da AEPD sobre a comunicação da Comissão relativa à interoperabilidade das bases de dados europeias, 10 de Março de 2006, disponível em http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

([39]) Cf., por exemplo, ponto 15 *supra*.

([40]) JO L 309 de 25.11.2005, p. 15.

([41]) Cf. parecer 10/2006 do Grupo do Artigo 29.º sobre o tratamento de dados pessoais pela Sociedade Mundial de Telecomunicações Financeiras Interbancárias (SWIFT).

([42]) Segundo o sistema de transferência por exportação, o responsável pelo tratamento transmite os dados ao serviço de aplicação da lei, a pedido desta. Segundo o sistema de transferência por «extracção», o serviço de aplicação da lei tem acesso à base de dados do responsável pelo tratamento e «extrai» informações dessa base. Com este último sistema («extracção»), o responsável pelo tratamento tem mais dificuldade em reassumir a responsabilidade.

— os pedidos de dados devem ser proporcionados, centrados em fins muito específicos e, em princípio, baseados em suspeitas a respeito de pessoas concretas,

— são de evitar as pesquisas de rotina, a prospecção de dados e a caracterização,

— todos os casos de utilização de dados para efeitos de aplicação da lei devem ficar registados, para que essa utilização possa ser efectivamente controlada pela pessoa em causa, no exercício dos seus direitos, bem como pelas autoridades para a protecção de dados e pelos serviços judiciários.

VI.3. **Sistemas de informação e organismos da UE**

Sistemas de informação com ou sem armazenamento centralizado ([43])

66. Ao longo dos últimos anos, o espaço de liberdade, segurança e justiça registou um aumento significativo do número de sistemas de informação baseados na legislação da UE. Umas vezes decide-se criar um sistema que implica o armazenamento centralizado dos dados a nível europeu, outras vezes a legislação prevê unicamente o intercâmbio de informações entre as bases de dados nacionais. O Sistema de Informação de Schengen é, provavelmente, o melhor exemplo de sistema com armazenamento centralizado. A Decisão 2008/615/JAI do Conselho (Decisão de Prüm) ([44]) é, do ponto de vista da protecção de dados, o exemplo mais significativo de sistema sem armazenamento centralizado, já que prevê um intercâmbio maciço de dados biométricos entre as autoridades dos Estados-Membros.

67. A Comunicação mostra que esta tendência para criar novos sistemas se irá prolongar. O primeiro exemplo, apresentado no ponto 4.2.2, é o de um sistema de informação que vem ampliar o sistema europeu de informação sobre os registos criminais (ECRIS) de modo a abranger os nacionais de países terceiros. A Comissão já encomendou um estudo sobre o registo europeu de pessoas nacionais de países terceiros condenadas (*European Index for Convicted Third Country Nationals* — EICTCN), que poderá levar à criação de uma base de dados centralizada. Um segundo exemplo é o intercâmbio de informações sobre pessoas singulares contidas em registos de insolvência de outros Estados-Membros, no quadro da justiça electrónica (ponto 3.4.1 da Comunicação), sem armazenamento centralizado.

68. A opção por um sistema descentralizado teria certas vantagens em termos de protecção de dados. De facto, a descentralização evita o duplo armazenamento dos dados — pela autoridade do Estado-Membro e pelo sistema centralizado —, a responsabilidade pelos dados é clara porque a autoridade do Estado-Membro será responsável pelo tratamento, e o controlo por parte dos serviços judiciários e das autoridades de protecção de dados pode ser efectuado ao nível dos Estados-Membros. Não obstante, este sistema revela deficiências no intercâmbio de dados com outras autoridades, por exemplo no que toca à actualização das informações, tanto no país de origem como no país de destino, e ao controlo efectivo de ambas as partes. Ainda é mais complicado garantir a responsabilidade do sistema técnico pelo intercâmbio. Estas lacunas podem ser colmatadas se se optar por um sistema centralizado em que os organismos da União Europeia sejam responsáveis, pelo menos, por determinadas partes do sistema (por exemplo, a infra-estrutura técnica).

69. Neste contexto, haveria vantagem em definir critérios de base para optar entre sistemas centralizados e descentralizados, assegurando-se assim a realização de opções políticas claras e cuidadosas em cada caso concreto. Os critérios assim definidos podem contribuir para o funcionamento dos próprios sistemas, e bem assim para a protecção dos dados dos cidadãos. A AEPD sugere que o programa de Estocolmo inclua a intenção de definir estes critérios.

Sistemas de informação de grande escala

70. No ponto 4.2.3.2 da Comunicação é feita uma breve reflexão sobre o futuro dos sistemas de informação de grande escala, com destaque para o Sistema de Informação de Schengen (SIS) e o Sistema de Informação sobre Vistos (VIS).

71. Nesse mesmo ponto 4.2.3.2 faz-se ainda referência à criação de um sistema de registo electrónico das entradas e saídas do território dos Estados-Membros, bem como de programas de viajantes registados. Este sistema fora anunciado anteriormente pela Comissão, no âmbito do pacote de propostas sobre as fronteiras, por iniciativa do Vice-Presidente Franco Frattini ([45]). Nas suas observações preliminares ([46]), a AEPD mostrou-se bastante crítica em relação a esta proposta, considerando não estar suficientemente demonstrada a necessidade de criar esse sistema, de natureza invasiva, em acréscimo aos sistemas de grande escala já existentes. A AEPD não tem conhecimento de novos elementos que comprovem a necessidade de tal sistema, sugerindo pois ao Conselho que não faça referência a esta ideia no programa de Estocolmo.

72. Neste contexto, a AEPD gostaria de remeter para os seus pareceres sobre várias iniciativas no domínio do intercâmbio de informações na UE ([47]), nos quais formulou muitas sugestões e comentários acerca das consequências que a utilização das grandes bases de dados a nível da UE pode

([43]) Entende-se neste contexto, por «armazenamento centralizado», o armazenamento a nível central europeu e, por «armazenamento descentralizado», o armazenamento ao nível dos Estados-Membros.

([44]) Cf. nota 33.

([45]) Comunicação da Comissão «Preparar as próximas etapas da gestão das fronteiras na União Europeia», de 13.2.2008, COM(2008) 69 final.

([46]) Observações preliminares da AEPD sobre três comunicações da Comissão no domínio da gestão de fronteiras [COM(2008) 69, COM(2008) 68 e COM(2008) 67], de 3 de Março de 2008. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf

([47]) Em particular: Parecer de 23 de Março de 2005 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, JO C 181 de 23.7.2005, p. 13, e parecer de 19 de Outubro de 2005 sobre três propostas relativas ao Sistema de Informação de Schengen de segunda geração (SIS II), JO C 91 de 19.4.2006, p. 38.

ter em termos de protecção de dados. Entre outros aspectos, a AEPD consagrou especial atenção à necessidade de criar garantias fortes e bem adaptadas, bem como à proporcionalidade e à necessidade de efectuar estudos de impacto antes de serem propostas ou tomadas quaisquer medidas nesta matéria. A AEPD sempre preconizou um equilíbrio correcto e consentâneo com a protecção de dados entre, por um lado, os requisitos de segurança e, por outro, a protecção da vida privada das pessoas singulares abrangidas pelos sistemas. Foi também essa a posição que tomou enquanto autoridade de controlo das partes centrais dos sistemas.

73. A AEPD aproveita ainda esta oportunidade para salientar que é necessário adoptar uma abordagem coerente para todos os intercâmbios de informações na UE — isto é, deve haver coerência, nos aspectos jurídicos, técnicos e de controlo, entre os sistemas já implantados e os que estão a ser desenvolvidos. De facto, hoje mais do que antes, é manifesta a necessidade de uma visão corajosa e abrangente de como deveria ser o intercâmbio de informações na UE, e de qual deveria ser o futuro dos sistemas de informação de grande escala. Só com base nessa visão poderia, talvez, ser reanalisada a criação de um sistema de registo electrónico das entradas e saídas do território dos Estados-Membros.

74. A AEPD sugere que o programa de Estocolmo faça referência à intenção de elaborar essa visão, devendo-se neste contexto reflectir sobre a eventual entrada em vigor do Tratado de Lisboa e sobre as consequências que daí advirão para os sistemas com base jurídica dos primeiro e terceiro pilares.

75. Por último, a Comunicação refere a instituição de uma nova agência que, também segundo a Comunicação, terá igualmente competência em relação ao sistema de registo electrónico das entradas e saídas. A Comissão aprovou, entretanto, uma proposta de criação da referida agência ([48]). A AEPD apoia em princípio esta proposta, na medida em que pode tornar mais eficaz o funcionamento dos sistemas em causa, inclusive no que toca à protecção de dados; no momento oportuno apresentará um parecer sobre a mesma proposta.

Europol e Eurojust

76. O papel da Europol é mencionado em diversos pontos da Comunicação, segundo a qual é prioritário que a Europol desempenhe um papel preponderante na coordenação, intercâmbio de informações e formação dos profissionais. Além disso, o ponto 4.2.2 da Comunicação faz referência às recentes mudanças do quadro jurídico da cooperação entre a Eurojust e a Europol e anuncia que vão prosseguir os trabalhos no sentido do reforço da Eurojust, nomeadamente em matéria de investigação nos domínios da criminalidade organizada transfronteiras. A AEPD apoia inteiramente estes objectivos, desde que sejam devidamente respeitadas as garantias de protecção de dados.

77. A este respeito, a AEPD saúda o novo projecto de acordo recentemente alcançado entre a Europol e a Eurojust ([49]), que visa melhorar e intensificar a cooperação entre os dois organismos e estabelecer entre eles um intercâmbio de informações eficiente. Para este trabalho é fundamental uma protecção de dados eficiente.

VI.4. **Utilização de dados biométricos**

78. A AEPD observa que a Comunicação não analisa o tema da crescente utilização de dados biométricos em diversos instrumentos jurídicos da União Europeia relativos ao recurso ao intercâmbio de informações, incluindo os instrumentos que criam os sistemas de informação de grande escala. Ora, isso é lamentável por se tratar de uma questão extremamente importante e sensível do ponto de vista da protecção de dados e da vida privada.

79. Embora reconheça as vantagens, em termos gerais, do recurso à biometria, a AEPD tem insistentemente salientado o grande impacto da utilização desse tipo de dados sobre os direitos individuais, e tem sugerido, portanto, a inserção de salvaguardas rigorosas para a utilização da biometria em cada sistema específico. O recente acórdão do Tribunal Europeu dos Direitos do Homem no processo *S. e Marper contra Reino Unido* ([50]) dá indicações úteis a este respeito, designadamente sobre a justificação e os limites da utilização de dados biométricos. Mais concretamente, a utilização de dados relativos ao ADN pode revelar informações sensíveis sobre as pessoas singulares, tendo designadamente em conta que continuam em expansão as possibilidades técnicas de extrair informações do ADN. Também é problemática a utilização em grande escala de dados biométricos constantes de sistemas informáticos, devido às inexactidões associadas à recolha e comparação desses dados. Por todos estes motivos, o legislador da UE deve mostrar contenção relativamente ao uso de tais dados.

80. Outro tema recorrente nos últimos anos tem sido a utilização de impressões digitais de crianças e idosos, devido às imperfeições inerentes aos sistemas biométricos nestas faixas etárias. A AEPD preconizou a realização de um estudo aprofundado que identificasse devidamente a exactidão dos sistemas ([51]) e propôs um limite de idade (14 anos) para as crianças, sob reserva de prova em contrário decorrente desse estudo. A AEPD recomenda que esta questão seja referida no programa de Estocolmo.

([48]) Proposta da Comissão, de 24 de Junho de 2009, com vista à aprovação de um regulamento do Parlamento Europeu e do Conselho que cria uma Agência para a gestão operacional do Sistema de Informação de Schengen (SIS II), do Sistema de Informação sobre Vistos (VIS), do EURODAC e de outros sistemas informáticos de grande escala no domínio da liberdade, da segurança e da justiça [COM(2009) 293/2].

([49]) Projecto de acordo aprovado pelo Conselho e que terá ainda de ser assinado por ambas as partes. Ver registo do Conselho:
http://register.consilium.europa.eu/pdf/en/09/st10/st10019.pt09.pdf
http://register.consilium.europa.eu/pdf/en/09/st10/st10107.pt09.pdf

([50]) Req. apensos 30562/04 e 30566/04, S. e Marper contra Reino Unido, acórdão de 4 de Dezembro de 2008 do TEDH, ainda não publicado.

([51]) Parecer de 26 de Março de 2008 sobre a proposta de regulamento que altera o Regulamento (CE) n.º 2252/2004 do Conselho que estabelece normas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem emitidos pelos Estados-Membros, JO C 200 de 6.8.2008, p. 1.

81. Dito isto, a AEPD sugere que sejam definidos critérios de base para a utilização de dados biométricos. Esses critérios deverão assegurar que os dados apenas sejam utilizados em caso de necessidade, de forma adequada e proporcionada, e se o legislador mostrar que a utilização tem finalidades determinadas, explícitas e legítimas. Mais concretamente, significa isto que os dados biométricos, e em particular o ADN, não devem ser utilizados caso seja possível chegar ao resultado pretendido usando informações menos sensíveis.

VII. **ACESSO À JUSTIÇA E JUSTIÇA ELECTRÓNICA**

82. As tecnologias também servirão para melhorar a cooperação judiciária. No ponto 3.4.1 da Comunicação, a justiça electrónica é-nos apresentada como um meio de facilitar o acesso dos cidadãos à Justiça; consiste num portal com informações e videoconferências como parte integrante do procedimento legal; abre ainda caminho aos procedimentos legais em linha e anuncia a interligação dos registos nacionais, como os registos de insolvência. A AEPD regista que a Comunicação não faz referência a novas iniciativas ligadas à justiça electrónica, mas consolida as acções que já estão a ser desenvolvidas. A AEPD intervém em algumas destas acções, no seguimento do seu parecer de 19 de Dezembro de 2008 sobre a comunicação da Comissão «Rumo a uma estratégia europeia em matéria de *e-Justice*» ([52]).

83. A justiça electrónica é um projecto ambicioso, que merece todo o apoio: pode, de facto, melhorar o sistema de justiça na Europa e a protecção judicial dos cidadãos, e representa um avanço importante para a realização de um espaço europeu da justiça. Tendo presente esta apreciação positiva, cabe fazer as seguintes observações:

— os sistemas tecnológicos para a e-Justice devem ser concebidos em conformidade com o princípio da «privacidade na concepção». Como atrás se afirmou a propósito do modelo europeu de informação, tudo deve partir da escolha da arquitectura adequada,

— a interligação e a interoperabilidade dos sistemas devem obedecer ao princípio da limitação da finalidade,

— é necessário definir com precisão as responsabilidades dos diversos intervenientes,

— devem ser previamente analisadas as consequências que pode ter para as pessoas singulares a interligação de registos nacionais com dados pessoais delicados, como os registos de insolvência.

VIII. **CONCLUSÕES**

84. A AEPD subscreve o destaque dado na Comunicação à protecção dos direitos fundamentais, designadamente à protecção dos dados pessoais, como sendo uma das problemáticas mais relevantes para o futuro do espaço de liberdade, segurança e justiça. Na opinião da AEPD, a Comunicação está certa ao defender o equilíbrio entre a necessidade de dispor de instrumentos adequados para garantir a segurança dos cidadãos, por um lado, e a necessidade de proteger os direitos fundamentais desses mesmos cidadãos, por outro; a Comunicação reconhece, além disso, que deve ser dada maior importância à protecção dos dados pessoais.

85. A AEPD subscreve totalmente o ponto 2.3 da Comunicação, segundo o qual deve ser instituído um regime completo de protecção de dados que abranja o conjunto das competências da União, independentemente da entrada em vigor do Tratado de Lisboa. Para o efeito, a AEPD recomenda que:

— no programa de Estocolmo seja anunciada a necessidade de uma visão clara e a longo prazo para esse regime completo,

— sejam avaliadas as medidas já adoptadas nesta matéria, bem como a sua aplicação concreta e a sua eficácia, ponderando tanto o sacrifício da vida privada como a eficácia da aplicação da lei,

— o programa de Estocolmo aponte como prioridade a criação de um novo enquadramento legislativo que venha, nomeadamente, substituir a Decisão-Quadro 2008/977/JAI do Conselho.

86. A AEPD saúda a intenção da Comissão de reafirmar os princípios da protecção de dados, que deve estar ligada à consulta pública anunciada pela Comissão na conferência «*Personal data — more use, more protection?*», que teve lugar em 19 e 20 de Maio de 2009. No essencial, a AEPD realça que importa respeitar o princípio da limitação da finalidade, fundamento da legislação em matéria de protecção de dados, e examinar as possibilidades de tornar mais eficaz a aplicação dos princípios nessa matéria graças a instrumentos destinados a reforçar as competências dos responsáveis pelo tratamento dos dados.

87. Tanto a «privacidade na concepção» como as tecnologias respeitadoras da vida privada poderão ser promovidas mediante

— um regime de certificação da protecção dos dados e da vida privada, como opção para os criadores e os utilizadores de sistemas de informação,

— uma obrigação legal, imposta aos criadores e aos utilizadores de sistemas de informação, de utilizar sistemas conformes com o princípio da privacidade na concepção.

88. No que toca aos aspectos externos da protecção de dados, a AEPD recomenda que:

— o programa de Estocolmo assinale que devem ser celebrados acordos gerais com os Estados Unidos e outros países terceiros, no domínio da protecção e do intercâmbio de dados,

([52]) Parecer da AEPD, de 19 de Dezembro de 2008, sobre a comunicação da Comissão «Rumo a uma estratégia europeia em matéria de *e-Justice*», JO C 128 de 6.6.2009, p. 13.

— seja activamente promovido o respeito pelos direitos fundamentais, e em especial o direito à protecção de dados, nas relações com países terceiros e organizações internacionais,

— o programa de Estocolmo afirme que o intercâmbio de dados pessoais com países terceiros requer que estes assegurem o devido nível de protecção ou dêem outras garantias adequadas.

89. A AEPD toma nota, com o maior interesse, do avanço registado no sentido de uma Estratégia de Gestão de Informação da União Europeia e de um modelo europeu de informação, e salienta que nestes projectos deve ser dada a maior atenção à vertente da protecção de dados, a aprofundar no programa de Estocolmo. A arquitectura do intercâmbio de informações deve basear-se na «privacidade na concepção» e nas «melhores técnicas disponíveis».

90. O simples facto de ser tecnicamente possível trocar informações digitais entre bases de dados interoperáveis, ou fundir essas bases de dados, não é motivo para abrir excepção ao princípio da limitação da finalidade. A interoperabilidade deve, em cada caso concreto, assentar em opções políticas claras e cuidadosas. A AEPD sugere que este conceito seja especificado no programa de Estocolmo.

91. No entender da AEPD, a utilização para efeitos de aplicação da lei de dados pessoais recolhidos para fins comerciais só deve ser autorizada em condições rigorosas, que são especificadas no ponto 65 do presente parecer.

92. Eis algumas sugestões para a utilização de informações de carácter pessoal:

— definir critérios de base para a opção entre sistemas centralizados e descentralizados e afirmar, no programa de Estocolmo, a intenção de elaborar esses critérios,

— não mencionar no programa de Estocolmo a criação de um sistema de registo electrónico das entradas e saídas do território dos Estados-Membros, nem a instituição de programas de viajantes registados,

— apoiar o reforço da Europol e da Eurojust, bem como o novo acordo a que os dois órgãos chegaram recentemente,

— definir critérios de base para a utilização de dados biométricos, de modo a assegurar que estes apenas sejam utilizados em caso de necessidade, de forma adequada e proporcionada, e se o legislador mostrar que a utilização tem finalidades determinadas, explícitas e legítimas; os dados relativos ao ADN não devem ser utilizados caso seja possível chegar ao resultado pretendido usando informações menos sensíveis.

93. A AEPD, que apoia a justiça electrónica, formulou algumas observações sobre a forma de melhorar este projecto (cf. ponto 83).

Feito em Bruxelas, em 10 de Julho de 2009.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados