I

(Comunicações)

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

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 relacionados com a oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE [COM(2005) 438 final)]

(2005/C 298/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia e, 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 [1] e a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (directiva relativa à privacidade e às comunicações electrónicas) [2],

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 [3] e, designadamente, o artigo 41.º,

Tendo em conta o pedido de parecer de harmonia com o n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, recebido em 23 de Setembro de 2005 da Comissão;

ADOPTOU O SEGUINTE PARECER:

I **Introdução**

1. A AEPD acolhe com agrado o facto de ser consultada com base no n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001. Todavia, atento o carácter obrigatório do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, o presente parecer deve ser referido no preâmbulo da Directiva.

2. A AEPD reconhece a importância de os serviços repressivos dos Estados-Membros disporem de todos os instrumentos jurídicos necessários, em especial no combate

[1] JO L 281 de 23.11.1995, p. 31.

[2] JO L 201 de 31.7.2002, p. 37.

[3] JO L 8 de 12.1.2001, p. 1.

ao terrorismo e outros crimes graves. Uma disponibilidade adequada de certos dados dos serviços públicos electrónicos relativos ao tráfego e à localização pode ser um instrumento crucial para esses órgãos repressivos e pode contribuir para a segurança física das pessoas. Assinale-se que tal não implica automaticamente a necessidade dos novos instrumentos previstos na presente proposta.

3. É igualmente óbvio que a proposta tem um impacto considerável sobre a protecção dos dados de carácter pessoal. Considerando-se a proposta exclusivamente na óptica da protecção dos dados, os dados relativos ao tráfego e à localização não deveriam ser de todo conservados para efeitos da acção repressiva. É por razões de protecção de dados que a Directiva 2002/58/CE estabelece como princípio de direito que os dados relativos ao tráfego têm de ser apagados assim que o armazenamento deixe de ser necessário para fins relacionados com a comunicação em si (incluindo para fins de facturação). As excepções a este princípio de direito subordinam-se a condições rigorosas.

4. No presente parecer, a AEPD deverá salientar o impacto da proposta sobre a protecção dos dados de carácter pessoal. A AEPD deverá além disso ter em conta que, mau grado a importância da proposta para a acção repressiva, não pode ter por consequência que alguém seja destituído do direito fundamental a que a sua privacidade seja protegida.

5. O presente parecer da EDPS tem de ser visto à luz dessas considerações. A AEPD preconiza uma abordagem equilibrada, em que a necessidade e a proporcionalidade da ingerência na protecção de dados desempenham um papel central.

6. Quanto à proposta em si, deve ser encarada como uma reacção à iniciativa da República Francesa, Irlanda, Reino da Suécia e Reino Unido com vista a uma decisão-quadro relativa à conservação dos dados tratados e armazenados em ligação com a oferta de serviços de comunicações electrónicas publicamente disponíveis ou dos dados em redes de comunicações públicas para efeitos de prevenção, investigação, detecção e instauração de acções penais por crimes e infracções penais, incluindo terrorismo («o projecto de decisão-quadro»), que foi rejeitada pelo Parlamento Europeu (no processo de consulta).

7. A AEPD não foi consultada acerca do projecto de decisão-quadro, nem deu parecer por iniciativa própria. A AEPD não tenciona dar para já parecer sobre o projecto de decisão-quadro, mas referir-se-á no presente parecer a esse projecto sempre que o considere útil.

II **Observações de ordem geral**

O impacto da proposta sobre a protecção dos dados de carácter pessoal

8. É essencial para a AEPD que a proposta respeite os direitos fundamentais. Uma medida legislativa susceptível de lesar a protecção garantida pelo direito comunitário e, mais concretamente, pela jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem não só é inaceitável como ilegal. As circunstâncias na sociedade podem ter mudado devido aos atentados terroristas, mas isso não pode ter por efeito que os elevados padrões de protecção que o direito consigna sejam postos em causa. A protecção é conferida por lei independentemente das necessidades reais dos órgãos repressivos. Acresce que a própria jurisprudência permite excepções, se necessárias numa sociedade democrática.

9. A proposta tem um impacto directo sobre a protecção conferida pelo artigo 8.º da Convenção Europeia de Protecção dos Direitos do Homem e das Liberdades Fundamentais (a «CEDH»). Segundo a jurisprudência do Tribunal Europeu dos Direitos do Homem:

— O armazenamento de informações sobre um indivíduo foi considerado uma ingerência na vida privada, muito embora não contivesse quaisquer dados sensíveis (Amann ([1])).

— O mesmo se verifica em relação à prática da «contagem» das chamadas telefónicas, que envolve a utilização de um dispositivo que regista automaticamente os números marcados num telefone e a hora e a duração de cada chamada (Malone ([2])).

— A justificação da ingerência deve sobrepor-se ao efeito prejudicial que a própria existência das disposições legislativas em causa poderá ter para os sujeitos (Dudgeon ([3])).

10. Dispõe o n.º 2 do artigo 6.º do Tratado da UE que a União respeitará os direitos fundamentais, tal como os garante a CEDH. Ficou demonstrado no ponto anterior que, segundo a jurisprudência do Tribunal Europeu dos Direitos do Homem, a obrigação de reter dados se insere no âmbito de aplicação do artigo 8.º da CEDH e que é necessária uma justificação premente que respeite o critério do acórdão Dudgeon. A

([1]) Acórdão do TEDH de 16 de Fevereiro de 2000, Amann, 2000-II, Req. 27798/95.

([2]) Acórdão do TEDH de 2 de Agosto de 1984, Malone, A82, Req. 8691/79.

([3]) Acórdão do TEDH de 22 de Outubro de 1981, Dudgeon, A45, Req. 7525.

necessidade e proporcionalidade da obrigação de conservar dados — na sua acepção plena — têm de ser provadas.

11. Além disso, a proposta tem um enorme impacto sobre os princípios da protecção de dados reconhecidos pelo direito comunitário:

— Os dados têm de ser conservados por um prazo muito mais longo do que os prazos de conservação habituais pelos prestadores de serviços de comunicações electrónicas publicamente disponíveis ou por uma rede pública de comunicações (ambos os serviços são adiante designados por «prestadores»).

— Nos termos da Directiva 2002/58/CE e, mais concretamente, do seu artigo 6.º, os dados só podem ser recolhidos e armazenados por motivos directamente relacionados com a própria comunicação, incluindo para fins de facturação ([1]). Seguidamente, os dados têm de ser apagados (com ressalvas). Nos termos da presente proposta, a conservação para fins de aplicação do direito penal é obrigatória. O ponto de partida é por conseguinte inverso.

— A Directiva 2002/58/CE é garante de segurança e confidencialidade. A presente proposta não pode levar a lacunas nesse domínio; são necessárias salvaguardas rigorosas e a restrição às finalidades deve ser elucidada.

— A introdução da obrigação de conservar dados, prevista pela proposta, gera bases de dados substanciais e induz especiais riscos para a pessoa a quem os dados dizem respeito. Seria o caso da utilização comercial dos dados, assim como da utilização dos dados para «operações de pesca» e/ou prospecção de dados por parte das autoridades competentes para a aplicação da lei ou dos serviços de segurança nacionais.

12. Por último, tanto a protecção da vida privada como a protecção dos dados pessoais foram reconhecidas na Carta dos Direitos Fundamentais, como se referiu na exposição de motivos.

13. O impacto da proposta sobre a protecção dos dados de carácter pessoal carece de uma análise exaustiva. Nessa análise, a AEPD terá em conta os elementos a seguir enunciados e concluirá que são necessárias mais salvaguardas. Não basta uma mera referência ao quadro jurídico vigente em matéria de protecção de dados (a saber, as directivas 95/46/CE e 2002/58/CE).

A necessidade de conservar os dados relativos ao tráfego e à localização

14. A AEPD evoca a conclusão de 9 de Novembro de 2004 do Grupo da Protecção de Dados (Grupo do Artigo 29.º) sobre o projecto de decisão-quadro. O Grupo declarou que a conservação obrigatória dos dados relativos ao tráfego, nas condições previstas no projecto de decisão-quadro, não é aceitável. Esta conclusão baseou-se designadamente na não produção de qualquer prova da necessidade da conservação para fins de ordem pública, devido ao facto de a análise ter revelado que a parte mais significativa dos dados relativos ao tráfego solicitados pelos órgãos repressivos não tinha mais de seis meses.

15. Para a AEPD, as considerações do referido Grupo da Protecção de Dados (Grupo do Artigo 29.º) devem ser o ponto de partida para a apreciação da presente proposta. Todavia, o resultado dessas considerações não pode ser meramente transposto para a presente proposta. Há que ter em conta que as circunstâncias podem mudar. Segundo a AEPD, os elementos seguintes poderiam ser pertinentes para a apreciação.

16. Em primeiro lugar, foram apresentados alguns números para provar que, na prática, os órgãos repressivos procuravam dados relativos ao tráfego com menos de um ano. A Comissão e a Presidência do Conselho salientam um estudo da polícia do Reino Unido ([2]) que revela que, embora 85% dos dados relativos ao tráfego solicitados pela polícia tivessem menos de seis meses, os dados com 6 meses a 1 ano eram utilizados em investigações mais complexas de crimes mais graves. Foram também apresentados alguns casos exemplares. O prazo de conservação da proposta — 1 ano para os dados telefónicos — reflecte essas práticas dos órgãos repressivos.

17. A AEPD não está convencida de que estes números provem a necessidade de conservar por um ano os dados relativos ao tráfego. O facto de nalguns casos a disponibilidade de dados relativos ao tráfego e/ou à localização ter ajudado a solucionar um crime não significa automaticamente que esses dados sejam necessários (em geral) como ferramenta da acção repressiva. Porém, os números não podem ser ignorados. Constituem pelo menos uma tentativa séria de provar a necessidade da conservação. Acresce que os números indicam nitidamente que na óptica das práticas actuais da acção repressiva não é necessário um prazo de conservação superior a um ano.

18. Em segundo lugar, as possibilidades existentes ao abrigo da Directiva 2002/58/CE de os prestadores conservarem dados relativos ao tráfego para efeitos de facturação não são sempre utilizadas, uma vez que, num crescente número de casos, a conservação dos dados para efeitos de facturação não tem de todo lugar (cartões pré-pagos para comunicações

([1]) Ver também ponto 3 do presente parecer.

([2]) «Liberdade e segurança, obter o devido equilíbrio». Documento da Presidência UK da União Europeia de 7 de Setembro de 2005.

móveis, assinaturas de tarifa fixa, etc.). Nesses casos — que na prática se tornaram mais frequentes — os dados relativos ao tráfego ou à localização não serão de todo armazenados, mas apagados imediatamente após a comunicação. O mesmo se aplica às chamadas não respondidas. Esta situação pode ter consequências para a eficácia da acção repressiva.

19. Acresce que esta evolução dos serviços de telecomunicações pode gerar perturbações no funcionamento do mercado interno, devidas designadamente à adopção (iminente) de medidas legislativas nos Estados-Membros nos termos do artigo 15.º da Directiva 2002/58/CE. Por exemplo, o Governo Italiano publicou recentemente um decreto que obriga os prestadores a armazenar os dados telefónicos durante 4 anos. Essa obrigação induzirá encargos consideráveis em determinados Estados-Membros, como a Itália.

20. Em terceiro lugar, os métodos de trabalho dos órgãos repressivos evoluíram também: as investigações pró-activas e a utilização de apoio técnico adquiriram maior relevo. Esta evolução exige que as autoridades disponham de ferramentas adequadas e formuladas rigorosamente para poderem fazer o seu trabalho com o devido respeito pelos princípios da protecção dos dados. Uma das ferramentas de que as autoridades dos Estados-Membros habitualmente dispõem é a preservação dos dados, ou congelamento de dados de comunicações solicitados numa investigação concreta. Afirmou-se que esta ferramenta, que em si mesma tem menos impacto sobre esses princípios do que a ferramenta ora proposta (conservação de dados), pode não ser sempre suficiente, designadamente para detectar o rasto de pessoas implicadas em terrorismo ou noutros crimes graves que anteriormente não eram suspeitas de qualquer actividade criminosa. Porém, são necessárias mais provas para apurar se assim é efectivamente.

21. Em quarto lugar, as preocupações com os atentados terroristas aumentaram. A AEPD comunga do ponto de vista exprimido no contexto das propostas em matéria de conservação dos dados, que a segurança física é, em si mesma, de extrema importância. A sociedade precisa de ser protegida. Por esse motivo os Governos, em caso de atentado contra a sociedade, são obrigados a provar que têm em sério apreço essa necessidade de protecção e a averiguar se têm de reagir introduzindo novas medidas legislativas. Escusado será dizer que a AEPD subscreve inteiramente o esforço dos Governos — tanto a nível nacional como europeu — para proteger a sociedade e provar que fazem todo o necessário para oferecer protecção, incluindo a adopção de medidas novas, legítimas e eficazes em consequência das suas investigações.

22. A AEPD reconhece que as circunstâncias mudaram, mas ainda não está convencida da necessidade de conservar dados relativos ao tráfego e à localização para fins repressivos, como definida na proposta. Salienta a importância do princípio de direito estabelecido pela Directiva 2002/58/CE segundo o qual os dados têm de ser apagados assim que o armazenamento deixe de ser necessário para fins que não se relacionem com a própria comunicação. Além disso, os números fornecidos não provam que o quadro jurídico vigente não ofereça os instrumentos necessários para proteger a segurança física, nem que os Estados-Membros exerçam plenamente as suas competências para cooperarem que o direito comunitário lhes outorgou no quadro jurídico vigente (mas sem os resultados necessários).

23. Todavia, se o Parlamento Europeu e o Conselho — após terem sopesado cuidadosamente os interesses em jogo — chegarem à conclusão de que a necessidade de conservar dados relativos ao tráfego e à localização está suficientemente provada, a AEPD defende que a conservação só é justificável nos termos do direito comunitário na medida em que seja observado o princípio da proporcionalidade e providenciadas salvaguardas adequadas, em conformidade com o presente parecer.

A proporcionalidade

24. A proporcionalidade da nova medida legislativa proposta depende ela própria da substância das disposições que compreende: compreende a resposta adequada e proporcionada às necessidades da sociedade?

25. A primeira consideração tem a ver com a adequação da proposta: pode-se esperar que a proposta aumente a segurança física dos habitantes da União Europeia? Um motivo para duvidar da adequação, frequentemente evocado no debate público, é que os dados relativos ao tráfego e os dados relativos à localização nem sempre dizem respeito a um determinado indivíduo, pelo que o conhecimento de um número de telefone (ou um número de acesso à Internet) não revela necessariamente a identidade de um indivíduo. Outro motivo — ainda mais grave — para dúvidas é se a existência de bases de dados gigantescas permite ou não aos órgãos repressivos encontrar aquilo de que precisam num dado caso.

26. A AEPD defende que a simples conservação dos dados relativos ao tráfego e à localização não constitui por si só uma resposta adequada ou eficaz. São necessárias medidas suplementares, por forma a assegurar às autoridades um acesso direccionado e rápido aos dados necessários num caso concreto. A conservação de dados só é adequada e eficaz na medida em que existam motores de busca eficazes.

27. A segunda consideração tem a ver com a proporcionalidade da resposta. Para ser proporcionada, a proposta deve:

— Limitar os prazos de conservação. Os prazos têm de reflectir as necessidades provadas dos órgãos repressivos.

— Limitar o número de dados a armazenar. Esse número tem de reflectir as necessidades provadas dos órgãos repressivos, tendo de se assegurar que o acesso a dados de conteúdo não é possível.

— Conter medidas de segurança adequadas, por forma a restringir o acesso e ulterior utilização, garantir a segurança dos dados e assegurar que as próprias pessoas a quem os dados dizem respeito possam exercer os seus direitos.

28. A AEPD frisa a importância dessas restrições rigorosas, com salvaguardas adequadas na óptica de um acesso restrito. Opina que, na óptica da importância dos três elementos referidos no próximo ponto, os Estados-Membros podem — no que respeita a esses três elementos — não tomar medidas suplementares que prejudiquem a proporcionalidade. Essa necessidade de harmonização será aprofundada na secção IV.

Medidas de segurança adequadas

29. O efeito da proposta será que os prestadores disporão de bases de dados em que se encontrará armazenada uma quantidade significativa de dados relativos ao tráfego e à localização.

30. Em primeiro lugar, a proposta terá de assegurar que o acesso aos dados e a sua ulterior utilização são restringidos a circunstâncias especificadas e para um número restrito de fins especificados.

31. Em segundo lugar, as bases de dados terão de estar devidamente protegidas (segurança dos dados). Para o efeito, há que assegurar que no termo dos prazos de conservação os dados são efectivamente apagados. Não deve haver *dumping* ou exploração dos dados. Em suma, exige-se um nível elevado de segurança dos dados e medidas técnicas e orgânicas de segurança adequadas.

32. Uma protecção elevada dos dados é tanto mais importante quanto a mera existência dos dados poderá levar a pedidos de acesso e utilização, por pelo menos três grupos de partes interessadas:

— Os próprios prestadores. Poderiam ser tentados a utilizar os dados para os seus próprios fins comerciais. São necessárias garantias que impeçam a reprodução desses ficheiros;

— Autoridades responsáveis pela aplicação da lei: a proposta faculta-lhes direito de acesso, mas só em casos específicos e nos termos da legislação nacional (n.º 2 do artigo 3.º da proposta). Não deve haver acesso para fins de prospecção de dados ou «operações de pesca». O intercâmbio de dados com autoridades de outros Estados-Membros deve ser regulado de forma clara;

— Serviços de informações (com responsabilidade pela segurança interna).

33. Quanto ao acesso por parte dos serviços de informações, a AEPD observa que, nos termos do artigo 33.º do TUE e do artigo 64.º CE, as intervenções na esfera do terceiro e do primeiro pilares não afectam o exercício das responsabilidades que incubem aos Estados-Membros em matéria de manutenção da ordem pública e de garantia da segurança interna. Segundo a AEPD, resulta destas disposições que a União Europeia carece de competência para controlar o acesso dos serviços de segurança ou de informações aos dados conservados pelos prestadores. Por outras palavras, nem o acesso desses serviços aos dados dos prestadores relativo ao tráfego e à localização, nem a utilização ulterior das informações adquiridas por esses serviços são afectados pelo direito da União Europeia. É um elemento que tem de ser tido em conta na apreciação da proposta. Devem ser os Estados-Membros a tomar as medidas necessárias para regular o acesso por parte dos serviços de informações.

34. Em terceiro lugar, os efeitos descritos nos pontos anteriores têm implicações potenciais para a pessoa a quem os dados dizem respeito. São necessárias salvaguardas suplementares por forma a assegurar que pode exercer singela e celeremente os seus direitos enquanto pessoa a quem os dados dizem respeito. A AEPD aponta a necessidade de um controlo eficaz do acesso e da ulterior utilização, de preferência pelas autoridades judiciais dos Estados-Membros. As salvaguardas devem igualmente aplicar-se em caso de acesso aos dados relativos ao tráfego e sua ulterior utilização por autoridades de outros Estados-Membros.

35. Neste contexto, a AEPD remete para iniciativas com vista a um novo quadro jurídico em matéria de protecção de dados aplicável à repressão (no terceiro pilar do TUE). Em sua opinião, esse quadro jurídico exige salvaguardas complementares e não poderá restringir-se à reafirmação dos princípios gerais de protecção dos dados do primeiro pilar ([1]).

36. Em quarto lugar, existe uma relação directa entre a adequação das medidas de segurança e os custos dessas medidas. Uma lei adequada em matéria de conservação de dados tem por conseguinte de conter incentivos a que os prestadores invistam na infra-estrutura técnica. Esse incentivo poderia consistir em indemnizar os prestadores pelos encargos suplementares das medidas de segurança adequadas.

37. Resumidamente, as medidas de segurança adequadas devem:

— Restringir o acesso aos dados e sua ulterior utilização;

— Prever medidas técnicas e orgânicas de segurança adequadas à protecção das bases de dados. Trata-se de apagar correctamente os dados no termo do prazo de

([1]) Ver, no mesmo sentido, o Documento de Posição sobre a repressão e o intercâmbio de informações na UE da Conferência da Primavera das autoridades nacionais encarregadas da protecção de dados, Cracóvia, 25-26 de Abril de 2005.

conservação e acusar a recepção dos pedidos de acesso e utilização de diversos grupos de partes interessadas;

— Assegurar o exercício dos direitos das pessoas a quem os dados dizem respeito, não apenas reafirmando os princípios gerais de protecção dos dados;

— Conter incentivos a que os prestadores invistam nas infra-estruturas técnicas.

III A base jurídica e o projecto de decisão-quadro

38. A proposta funda-se no Tratado CE e, designadamente, no artigo 95.º, e tem em vista, segundo o seu artigo 1.º, harmonizar as obrigações dos prestadores no tocante ao tratamento e conservação dos dados de tráfego ou de localização. Declara que os dados só serão fornecidos às entidades nacionais competentes em casos individuais, relacionados com infracções penais, mas deixa ao critério dos Estados-Membros a definição mais exacta da finalidade, e bem assim do acesso aos dados e sua ulterior utilização, sob reserva das salvaguardas do quadro comunitário vigente em matéria de protecção de dados.

39. Nessa perspectiva, a proposta possui um âmbito de aplicação mais restrito que o projecto de decisão-quadro, que se funda na alínea c) do n.º 1 do artigo 31.º do TUE e contém disposições suplementares sobre o acesso aos dados conservados bem como sobre pedidos de acesso de outros Estados-Membros. A exposição de motivos dá uma justificação para esta restrição do âmbito da proposta. Declara que o acesso às informações e respectivo intercâmbio entre os órgãos repressivos competentes é matéria que exorbita do âmbito do Tratado CE.

40. A AEPD não se rende a esta declaração na exposição de motivos. Uma intervenção da Comunidade fundada no artigo 95.º CE (mercado interno) tem de ter por objecto principal remover os obstáculos ao comércio. Segundo a jurisprudência do Tribunal de Justiça, essa intervenção tem de ser autenticamente adequada para contribuir para a remoção desse obstáculo. Porém, na sua intervenção, o legislador comunitário tem de assegurar o respeito pelos direitos fundamentais (n.º 2 do artigo 6.º do TUE; ver secção II do presente parecer). Por todas estas razões, a instauração de regras em matéria de conservação de dados a nível comunitário no interesse do mercado interno pode exigir que também o respeito pelos direitos fundamentais seja tratado a nível da Comunidade Europeia. Se o legislador comunitário não pudesse definir regras em matéria de acesso e utilização dos dados, não poderia cumprir a sua obrigação por força do artigo 6.º do TUE, dado que tais regras são indispensáveis para assegurar que os dados sejam conservados no devido respeito pelos direitos fundamentais. Por outras palavras, para a AEPD as regras em matéria de acesso, utilização e intercâmbio dos dados são indissociáveis da própria obrigação de conservar os dados.

41. Quanto à determinação das autoridades competentes, a AEPD admite que é da responsabilidade dos Estados-Membros. Assim o é também a organização dos órgãos repressivos e da protecção judicial. Todavia, um acto comunitário pode impor aos Estados-Membros condições quanto à designação de autoridades competentes, o controlo judicial ou o acesso dos cidadãos à justiça. Estas disposições asseguram a existência a nível nacional de mecanismos apropriados para garantir a plena eficácia do acto, que compreende o cumprimento integral da legislação em matéria de protecção de dados.

42. A AEPD evoca outro ponto, relacionado com a base jurídica. Cabe ao legislador comunitário escolher a base jurídica adequada e, nessa conformidade, o processo legislativo adequado. Essa escolha transcende a missão da AEPD. Porém, à luz das importantes questões fundamentais em jogo, a AEPD exprime na situação em apreço forte preferência pelo processo de co-decisão. Só esse procedimento constitui um processo de tomada de decisão transparente com a plena participação das três instituições em causa e no respeito integral dos princípios em que se funda a União.

IV A necessidade de harmonização

43. A proposta de directiva harmoniza os tipos de dados a conservar, os prazos durante os quais os dados devem ser conservados, bem como as finalidades para as quais os dados podem ser fornecidos às autoridades competentes. A proposta preconiza a harmonização integral desses elementos. Possui, neste particular, uma natureza fundamentalmente diferente do projecto de decisão-quadro, que prevê normas mínimas.

44. A AEPD salienta a necessidade de harmonizar plenamente estes elementos, na perspectiva do funcionamento do mercado interno, das necessidades da acção repressiva e — em último mas não menos importante lugar — da CEDH e dos princípios da protecção dos dados.

45. Quanto ao funcionamento do mercado interno, a harmonização das obrigações de conservar os dados justifica a escolha da base jurídica da proposta (artigo 95.º TCE). Permitir diferenças essenciais entre as leis dos Estados-Membros não removeria as actuais perturbações no mercado interno das comunicações electrónicas, que se devem designadamente à adopção (iminente) de medidas legislativas nos Estados-Membros nos termos do artigo 15.º da Directiva 2002/58/CE (ver ponto 19 do presente parecer).

46. Isto é tanto mais importante quanto para uma quantidade assinalável de comunicações electrónicas, tem relevância a jurisdição de mais de um Estado-Membro. Entre outros exemplos: chamadas telefónicas transfronteiriças, itinerância das comunicações, travessia de fronteiras *durante* as comunicações móveis e utilização de um prestador de um Estado-Membro que não é o país de residência do indivíduo.

47. Acresce que neste contexto a falta de harmonização prejudicaria as necessidades da acção repressiva, na medida em que as autoridades competentes têm de cumprir diferentes requisitos legais. Este facto pode dificultar o intercâmbio de informações entre as autoridades dos Estados-Membros.

48. Por último, a AEPD frisa — fazendo referência à sua responsabilidade nos termos do artigo 41.º do Regulamento (CE) n.º 45/2001 — que a harmonização plena dos principais elementos contidos na proposta é indispensável ao cumprimento da CEDH e dos princípios da protecção dos dados. Qualquer medida legislativa que obrigue a conservar os dados de tráfego ou de localização tem que restringir claramente o número de dados a conservar, os prazos de conservação e (os fins de) o acesso aos dados e sua ulterior utilização, para ser aceitável sob o ângulo da protecção dos dados e para cumprir os requisitos de necessidade e de proporcionalidade.

V **Comentários ao articulado da proposta**

Artigo 3.º: Obrigação de conservar os dados

49. O artigo 3.º é a disposição-chave da proposta. O n.º 1 do artigo 3.º introduz a obrigação de conservar os dados relativos ao tráfego e os dados relativos à localização, ao passo que o n.º 2 do artigo 3.º consubstancia o princípio da restrição à finalidade. O n.º 2 do artigo 3.º fixa três importantes restrições. Os dados conservados só serão fornecidos:

— às entidades nacionais competentes;

— em casos específicos;

— para efeitos de prevenção, investigação, detecção e instauração de acções penais contra infracções penais graves, tais como o terrorismo e a criminalidade organizada.

O n.º 2 do artigo 3.º remete para a legislação interna dos Estados-Membros no qual se refere à especificação de outras restrições.

50. A AEPD reconhece com agrado no n.º 2 do artigo 3.º uma disposição importante, mas considera que as restrições não são suficientemente precisas, que o acesso e a utilização ulterior deveriam ser regulados explicitamente na directiva e que são necessárias salvaguardas suplementares. Como se afirmou na secção III do presente parecer, a AEPD não está convencida de que a omissão da inclusão de disposições (exactas) sobre o acesso aos dados relativos ao tráfego ou à localização e a sua utilização ulterior seja uma consequência inevitável da base jurídica da proposta (artigo 95.º TCE). Isto leva aos seguintes comentários.

51. Em primeiro lugar: não se precisa que outras partes interessadas, como o próprio prestador, não têm acesso aos dados. Nos termos do artigo 6.º da Directiva 2002/58/CE, os prestadores só podem tratar os dados relativos ao tráfego até ao termo do prazo de conservação dos dados para efeitos de facturação. Segundo a AEPD, não há qualquer justificação para um acesso por parte dos prestadores ou de outras partes interessadas que não seja o acesso previsto ao abrigo da Directiva 2002/58/CE, e sujeito às condições dessa directiva.

52. A AEPD recomenda que se adite uma disposição no texto que garanta que os indivíduos que não sejam autoridades competentes não têm acesso aos dados. Esta disposição poderia ser formulada nos seguintes termos: «os dados só podem ser acedidos e/ou tratados para os fins referidos no n.º 2 do artigo 3.º» ou «os prestadores garantirão efectivamente que o acesso só seja concedido às autoridades competentes».

53. Em segundo lugar: a restrição a casos específicos parece proibir o acesso de rotina para «operações de pesca» ou para actividades de prospecção de dados. Todavia, o texto da proposta deveria precisar que os dados só podem ser fornecidos se isso for necessário relativamente a uma infracção penal concreta.

54. Em terceiro lugar: a AEPD regista com agrado o facto de a finalidade do acesso se restringir a infracções penais graves, tais como o terrorismo e a criminalidade organizada. Noutros casos menos graves, o acesso aos dados de tráfego ou de localização não será facilmente proporcionado. Todavia, a AEPD não tem a certeza de que esta restrição seja suficientemente rigorosa, especialmente quando for pedido acesso relacionado com crimes graves que não sejam o terrorismo e a criminalidade organizada. A prática nos Estados-Membros será variável. A AEPD salientou na secção IV do presente parecer a necessidade de harmonização integral dos principais elementos contidos na proposta. A AEPD recomenda pois que se restrinja a disposição a *certas* infracções penais graves.

55. Em quarto lugar: ao contrário do projecto de decisão-quadro, a proposta não contém uma disposição relativa ao acesso. Do ponto de vista da AEPD, o acesso aos dados e a sua ulterior utilização não deveriam ser ignorados na directiva. São indissociáveis do objecto (ver secção III do presente parecer).

56. A AEPD recomenda que se adite à proposta um ou mais artigos sobre o acesso aos dados relativos ao tráfego e à localização pelas autoridades competentes e sobre a ulterior utilização dos dados. O objectivo destes artigos deveria ser o de assegurar que os dados apenas são utilizados para os fins referidos no n.º 2 do artigo 3.º, que as autoridades velam pela qualidade, confidencialidade e segurança dos dados que tenham obtido e que os dados serão apagados quando já não forem necessários para a prevenção, investigação,

detecção e instauração de acções penais contra a infracção penal concreta. Acresce que dever-se-ia estipular que o acesso em casos concretos deveria estar sujeito a controlo judicial nos Estados-Membros.

57. Em quinto lugar: a proposta não contém salvaguardas suplementares para efeitos de protecção de dados. Os considerandos remetem simplesmente para as salvaguardas da legislação vigente, mais concretamente a Directiva 95/46/CE e a Directiva 2002/58/CE. A AEPD discorda desta abordagem restrita da protecção dos dados, apesar da especial importância das salvaguardas (suplementares) (ver secção II do presente parecer).

58. Como tal, a AEPD recomenda que se insira um número em matéria de protecção de dados. Nesse número poderiam ser inseridas as anteriores recomendações a respeito do n.º 2 do artigo 3.º, bem como outras disposições em matéria de protecção de dados, tais como disposições respeitantes ao exercício dos seus direitos pela pessoa a quem os dados dizem respeito (ver secção II do presente parecer), à qualidade e segurança dos dados, e aos dados de tráfego ou de localização de pessoas não suspeitas de actividade criminosa.

Artigo 4.º: Categorias de dados a conservar

59. De um modo geral, a AEPD acolhe com agrado o artigo e o anexo, devido:

— À técnica legislativa escolhida, com descrições funcionais no corpo da directiva e pormenores técnicos num anexo. É suficientemente flexível para reagir adequadamente à evolução tecnológica e proporciona certeza jurídica ao cidadão;

— À destrinça entre dados respeitantes a telecomunicações e dados da Internet, apesar de a destrinça se tornar tecnologicamente menos importante. Sob o ângulo da protecção dos dados, todavia, a distinção é importante, uma vez que na Internet não é clara a linha divisória entre dados, de conteúdo e dados de tráfego (ver, por exemplo, o reconhecimento no n.º 2 do artigo 1.º da Directiva de que as informações consultadas na Internet são dados de conteúdo);

— Ao grau de harmonização: a proposta preconiza um grau elevado de harmonização com uma lista exaustiva das categorias de dados a conservar (por oposição ao projecto de decisão-quadro, que contém uma lista mínima com ampla margem para os Estados-Membros acrescentarem dados). Sob o ângulo da protecção dos dados, a harmonização plena é essencial (ver secção IV).

60. A AEPD recomenda as seguintes alterações:

— O n.º 2 do artigo 4.º deve conter critérios mais substanciais para assegurar a não inclusão dos dados de conteúdo. Deve ser aditada a seguinte frase: «O anexo não pode conter dados que revelem o conteúdo de uma comunicação.»

— O artigo 5.º abre a possibilidade de revisão do anexo por via de uma directiva da Comissão («comitologia»). A AEPD aconselha que as revisões do anexo com impacto significativo sobre a protecção de dados sejam de preferência feitas por via de uma directiva, nos termos do processo de co-decisão. ([1])

Artigo 7.º: Prazos de conservação

61. A AEPD regista com agrado o facto de os prazos de conservação da proposta serem significativamente mais curtos que os previstos no projecto de decisão-quadro:

— Recordando as dúvidas exprimidas no presente parecer sobre a prova da necessidade de conservar os dados relativos ao tráfego até um ano, o prazo de um ano reflecte as práticas dos órgãos repressivos, *tais como as indicam* os números que foram fornecidos pela Comissão e a Presidência do Conselho.

— Esses números revelam também que, salvo em casos excepcionais, a conservação de dados por períodos mais longos não espelha as práticas dos órgãos repressivos.

— Um prazo mais curto de 6 meses para os dados relacionados com comunicações electrónicas efectuadas única ou principalmente através do protocolo Internet é importante sob o ângulo da protecção dos dados, dado que a conservação das comunicações pela Internet gera vastas bases de dados (esses dados não são habitualmente conservados para efeitos de facturação), a linha divisória com os dados de conteúdo é vaga e a conservação durante mais de 6 meses não espelha as práticas dos órgãos repressivos.

62. Dever-se-ia elucidar no texto que:

— os prazos de conservação de 6 meses e de um ano são prazos máximos de conservação;

([1]) Ver, no mesmo sentido, o parecer da AEPD 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 (Par. 3.12).

— os dados são apagados no termo do prazo de conservação. O texto deveria também elucidar de que modo os dados devem ser apagados. Segundo a AEPD, o prestador tem de apagar os dados por meios automatizados, pelo menos diariamente.

Artigo 8.º: Requisitos de armazenamento para os dados conservados

63. Este artigo relaciona-se estreitamente com o n.º 2 do artigo 3.º e contém uma importante disposição capaz de assegurar que o acesso em casos específicos possa ser restringido aos dados especificamente necessários. Pressupõe-se no artigo 8.º e no n.º 2 do artigo 3.º que os dados necessários são transmitidos pelos prestadores às autoridades e que estas não têm acesso directo às bases de dados. A AEPD recomenda que se enuncie essa presunção explicitamente no texto.

64. A disposição deve ser precisada, prevendo que:

— os dados necessários são transmitidos pelos prestadores às autoridades (ver ponto 63);

— os prestadores devem instalar a arquitectura técnica necessária, incluindo motores de busca, para facilitar o acesso direccionado aos dados especificados;

— os prestadores devem velar por que só os membros do seu pessoal com responsabilidades técnicas especificadas tenham acesso às bases de dados por razões técnicas e que esses membros do pessoal estejam alertados para o carácter sensível dos dados e trabalhem subordinados a rigorosas regras de confidencialidade;

— a transmissão dos dados deve efectuar-se não só sem demora, como sem revelar outros dados relativos ao tráfego e à localização para além dos dados necessários para os fins do pedido.

Artigo 9.º: Estatísticas

65. A obrigação de os prestadores fornecerem estatísticas anualmente ajuda as instituições comunitárias a acompanhar a eficácia da execução e aplicação da presente proposta. É necessária informação adequada.

66. Segundo a AEPD, essa obrigação consubstancia o princípio da transparência. O cidadão europeu tem direito a saber qual é a eficácia da conservação dos dados. Por esse motivo, o prestador devia ser além disso obrigado a manter listas de ligações e efectuar (auto) auditorias sistemáticas, a fim de permitir que as autoridades nacionais de protecção de dados controlem a aplicação na prática das normas em matéria de protecção de dados [1]. A proposta deveria ser alterada nesse sentido.

Artigo 10.º: Custos

67. Como se afirmou na secção II, existe uma relação directa entre a adequação das medidas de segurança e os custos destas medidas ou, por outras palavras, entre segurança e custos. A AEPD encara pois o artigo 10.º — que prevê o reembolso dos encargos adicionais comprovados — como uma disposição importante, que poderá funcionar como incentivo a que os prestadores invistam nas infra-estruturas técnicas.

68. Segundo as estimativas do estudo de impacto transmitido pela Comissão à AEPD, os custos da conservação dos dados são consideráveis. Para uma rede e um prestador de serviços de grandes dimensões, os custos seriam mais de 150 milhões de euros, para um prazo de conservação de 12 meses, com custos operacionais anuais de cerca de 50 milhões de euros [2]. Não há todavia números sobre os custos das medidas de protecção complementares, tais como motores de busca dispendiosos (ver o comentário sobre o artigo 6.º), nem sobre as consequências financeiras (estimadas) do reembolso integral dos encargos suplementares dos prestadores.

69. Segundo a AEPD, são necessários números mais exactos para se poder julgar a proposta em toda a sua plenitude. Sugere que se esclareça as consequências financeiras da proposta na exposição de motivos.

70. Quanto ao disposto no próprio artigo 10.º, a relação entre a adequação das medidas de segurança e os custos deve ser precisada no texto da disposição. Acresce que a proposta deve prever normas mínimas para as medidas de segurança a tomar pelos prestadores para terem direito a ser reembolsados por um Estado-Membro. Segundo a AEPD, a determinação dessas normas não poderá ser deixada inteiramente aos

[1] Ver, no mesmo sentido, o parecer da AEPD 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 (Par. 3.9).

[2] A Comissão refere-se a números da ETNO (Associação dos operadores de redes de telecomunicações da UE) e a um relatório do Deputado Alvaro do PE sobre o projecto de decisão-quadro.

Estados-Membros. Isto poderá prejudicar o grau de harmonização preconizado pela Directiva. Deve ter-se ainda em conta que os Estados-Membros suportam as consequências financeiras do reembolso.

Artigo 11.º: Alteração da Directiva 2002/58/CE

71. A relação com o n.º 1 do artigo 15.º da Directiva 2002/58/CE deve ser elucidada, já que a presente proposta destitui essa disposição de muito do seu conteúdo. As referências no n.º 1 do artigo 15.º da Directiva 2002/58/CE aos artigos 6.º e 9.º (da mesma directiva) devem ser suprimidas ou pelo menos alteradas no sentido de precisarem que os Estados-Membros já não têm competência para adoptar legislação respeitante a infracções penais complementar à presente proposta. Tem de ser removida qualquer ambiguidade a respeito das suas demais competências — por exemplo, no tocante à conservação de dados para fins de infracções penais «não graves».

Artigo 12.º: Avaliação

72. A AEPD regista com agrado que a proposta contém um artigo sobre a avaliação da directiva, no prazo de três anos a contar da sua entrada em vigor. A avaliação assume particular relevância face às dúvidas acerca da necessidade da proposta e da sua proporcionalidade.

73. Nesta óptica, a AEPD aconselha que se preveja uma obrigação ainda mais estrita, que contenha os seguintes elementos:

— A avaliação deveria compreender um diagnóstico da eficácia da aplicação da directiva na óptica da acção repressiva, bem como um diagnóstico do impacto sobre os direitos fundamentais da pessoa a quem os dados dizem respeito. A Comissão deve incluir quaisquer provas que possam afectar a avaliação;

— A avaliação deveria ter lugar periodicamente (pelo menos de dois em dois anos);

— A Comissão deveria ser obrigada a apresentar alterações à proposta, sempre que oportuno (como no artigo 18.º da Directiva 2002/58/CE).

VI **Conclusões**

Condições prévias

74. É essencial para a AEPD que a proposta respeite os direitos fundamentais. Uma medida legislativa susceptível de lesar a protecção garantida pelo direito comunitário e mais concretamente pela jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem não só é inaceitável, como ilegal.

75. A necessidade e a proporcionalidade da obrigação de conservar dados — na sua acepção plena — têm de ser provadas.

76. Quanto à necessidade: a AEPD reconhece as alterações das circunstâncias, mas ainda não está convencida da necessidade de conservar dados relativos ao tráfego e à localização para fins repressivos, como definida na proposta.

77. Não obstante, a AEPD expõe no presente parecer a sua opinião sobre a proporcionalidade da proposta. Em primeiro lugar, a mera conservação dos dados relativos ao tráfego e à localização não constitui por si só uma resposta adequada ou eficaz. São necessárias medidas suplementares, por forma a assegurar às autoridades um acesso direccionado e rápido aos dados necessários num caso concreto. Em segundo lugar, a proposta deve:

— Limitar os prazos de conservação. Os prazos têm de reflectir as necessidades da acção repressiva;

— Limitar o número de dados a armazenar. Esse número tem de reflectir as necessidades da acção repressiva e assegurar que o acesso aos dados de conteúdo não seja possível;

— Conter medidas de segurança adequadas.

Apreciação geral

78. A AEPD sublinha a importância do facto de o texto actual da proposta prever uma harmonização plena dos principais elementos da proposta, em particular os tipos de dados a conservar, os prazos durante os quais os dados devem ser conservados, bem como (os fins de) o acesso aos dados e sua ulterior utilização.

79. Nalguns pontos é necessária uma maior clarificação, por exemplo para garantir o apagamento adequado dos dados no termo do seu prazo de conservação e para impedir eficazmente o acesso e utilização por diversos grupos de partes interessadas.

80. A AEPD considera essenciais os seguintes pontos para que a proposta seja aceitável sob o ângulo da protecção dos dados:

— O aditamento à proposta de disposições específicas sobre o acesso aos dados relativos ao tráfego e à localização pelas autoridades competentes e sobre a ulterior utilização dos dados, enquanto elemento essencial e indissociável do objecto;

— O aditamento à proposta de mais salvaguardas suplementares para efeitos de protecção de dados (ao contrário de uma mera referência às salvaguardas da legislação existente, mais exactamente na Directiva 95/46/CE e na Directiva 2002/58/CE), designadamente para assegurar o exercício dos direitos das pessoas a quem os dados dizem respeito;

— O aditamento à proposta de mais incentivos a que os prestadores invistam em infra-estruturas técnicas adequadas, incluindo incentivos financeiros. Estas infra-estruturas só podem ser adequada caso existam motores de busca eficazes.

Recomendações de alterações à proposta

81. Quanto ao n.º 2 do artigo 3.º:

— Aditar uma disposição que assegure que os indivíduos que não sejam as autoridades competentes não têm acesso aos dados. Esta disposição poderia ser formulada nos seguintes termos: «os dados só podem ser acedidos e/ou tratados para os fins referidos no n.º 2 do artigo 3.º» ou «os prestadores garantirão efectivamente que o acesso só seja concedido às autoridades competentes»;

— Precisar que os dados só podem ser fornecidos se isso for necessário relativamente a uma infracção penal concreta;

— Limitar a disposição a *certas* infracções penais graves;

— Aditar à proposta um ou mais artigos sobre o acesso aos dados relativos ao tráfego e à localização pelas autoridades competentes e sobre a ulterior utilização dos dados, bem como uma disposição no sentido de o acesso em casos concretos dever estar sujeito a controlo judicial nos Estados-Membros;

— Inserir um número em matéria de protecção de dados.

82. Quanto aos artigos 4.º e 5.º:

— Aditar no n.º 2 do artigo 4.º a seguinte frase: «O anexo não pode conter dados que revelem o conteúdo de uma comunicação»;

— Precisar que as revisões do anexo com impacto significativo sobre a protecção de dados devem de preferência ser feitas por via de uma directiva, nos termos do processo de co-decisão.

83. Quanto ao artigo 7.º, precisar no texto que:

— Os prazos de conservação de 6 meses e de um ano são prazos máximos de conservação;

— Os dados são apagados no termo do prazo de conservação. O texto deveria também elucidar de que forma devem ser apagados os dados, a saber pelo prestador por meios automatizados, pelo menos diariamente.

84. Quanto ao artigo 8.º, precisar no texto que:

— Os dados necessários são transmitidos pelos prestadores às autoridades;

— Os prestadores devem instalar a arquitectura técnica necessária, incluindo os motores de busca para facilitar o acesso direccionado aos dados especificados;

— Os prestadores devem velar por que só os membros do seu pessoal com responsabilidades técnicas especificadas tenham acesso às bases de dados por razões técnicas e por que esses membros do pessoal estejam alertados para o carácter sensível dos dados e trabalhem subordinados a rigorosas regras de confidencialidade;

— A transmissão dos dados deveria efectuar-se não só sem demora, como sem revelar outros dados relativos ao tráfego e à localização para além dos dados necessários para os fins do pedido.

85. Quanto ao artigo 9.º:

— Aditar uma disposição que obrigue o prestador a manter listas de ligações e efectuar (auto) auditorias sistemáticas, a fim de permitir que as autoridades nacionais de protecção de dados controlem a aplicação na prática das normas em matéria de protecção de dados.

86. Quanto ao artigo 10.º:

— A relação entre a adequação das medidas de segurança e os encargos deveria ser precisada no texto da disposição;

— Aditar normas mínimas para as medidas de segurança a tomar pelos prestadores para terem direito a ser reembolsados por um Estado-Membro;

— Elucidar as consequências financeiras da proposta na exposição de motivos.

87. Quanto ao artigo 11.º:

— Alteração do n.º 1 do artigo 15.º da Directiva 2002/58/CE para suprimir as remissões para o artigo 6.º e o artigo 9.º (da mesma directiva), ou pelo menos alterá-las para precisar que os Estados-Membros já não têm competência para adoptar legislação respeitante a infracções penais complementares à presente proposta.

88. Quanto ao artigo 12.º, alteração da disposição sobre a avaliação:

— Deveria compreender um diagnóstico da eficácia da aplicação da directiva;

— Deveria ter lugar periodicamente (pelo menos de dois em dois anos);

— A Comissão deveria ser obrigada a apresentar alterações à proposta, sempre que oportuno (como no artigo 18.º da Directiva 2002/58/CE).

Feito em Bruxelas, em 26 de Setembro de 2005.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados