ISSN 1725-2482

Jornal Oficial da União Europeia

C 128

Edição em língua portuguesa

Comunicações e Informações

52.º ano

6 de Junho de 2009

Número de informação | Índice | Página

PT

(continua no verso da capa)

IV *Informações*

INFORMAÇÕES ORIUNDAS DAS INSTITUIÇÕES E DOS ÓRGÃOS DA UNIÃO EUROPEIA

Comissão

Rectificações

PT

I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados 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

(2009/C 128/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,

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 — CONTEXTO DO PARECER

1. Em 28 de Maio de 2008, a Presidência do Conselho da União Europeia anunciou ao COREPER, na perspectiva da cimeira da UE de 12 de Junho de 2008, que o Grupo de Contacto de Alto Nível UE-EUA sobre o intercâmbio de informações e a protecção da vida privada e dos dados pessoais tinha concluído o seu relatório, que foi divulgado em 26 de Junho de 2008 [1].

2. O relatório identifica princípios comuns para a protecção da vida privada e dos dados como primeiro passo para o intercâmbio de informações com os Estados Unidos com vista a lutar contra o terrorismo e a criminalidade transnacional.

3. Na sua declaração, a Presidência do Conselho anuncia que acolheria com satisfação quaisquer ideias sobre o seguimento a dar a este relatório, e nomeadamente as eventuais reacções às recomendações sobre as orientações nele preconizadas. A Autoridade Europeia para a Protecção de Dados responde a este convite emitindo o parecer a seguir apresentado, baseado na apreciação da situação tal como foi divulgada e sem prejuízo de qualquer posição que venha a tomar tendo em conta a evolução da questão.

4. A AEPD toma nota de que os trabalhos do Grupo de Contacto de Alto Nível tiveram lugar num contexto em que, em especial desde 11 de Setembro de 2001, se desenvolveu o intercâmbio de dados entre os EUA e a UE, através de acordos internacionais ou outros tipos de instrumentos. Entre estes convém referir os acordos da Europol e do Eurojust com os Estados Unidos, e igualmente os acordos PNR e o caso Swift que levaram a uma troca de cartas entre as autoridades da UE e dos EUA para estabelecer garantias de protecção mínimas dos dados [2].

[1] Documento do Conselho n.º 9831/08, disponível em: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

[2] — Acordo entre os Estados Unidos da América e o Serviço Europeu de Polícia, de 6 de Dezembro de 2001, e Acordo suplementar entre os Estados Unidos da América e o Serviço Europeu de Polícia sobre o intercâmbio de dados pessoais e informações afins, publicado no sítio interne da Europol;
— Acordo entre os Estados Unidos da América e o Eurojust sobre cooperação judicial, de 6 de Novembro de 2006, publicado no sítio interne do Eurojust;
— 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 assinado em Bruxelas em 23 Julho 2007 e em Washington em 26 Julho 2007 (Acordo PNR 2007), JO L 204/2006, de 4.8.2007, p. 18.
— Troca de cartas entre as autoridades dos EUA e da UE sobre o Programa de Detecção do Financiamento do Terrorismo, de 28 de Junho de 2007.

5. Além disso, a UE negoceia e celebra igualmente acordos semelhantes que prevêem o intercâmbio de dados pessoais com outros países terceiros. Um exemplo recente deste tipo de instrumentos é o Acordo entre a União Europeia e a Austrália sobre o tratamento de dados originários da União Europeia contidos nos Registos de Identificação dos Passageiros (PNR) e a transferência desses dados pelas transportadoras aéreas para os serviços aduaneiros da Austrália ([3]).

6. É possível constatar que o pedido de informações pessoais por parte das autoridades de aplicação da lei de países terceiros é cada vez maior, e que abrange desde bases de dados governamentais tradicionais a outros tipos de dossiês, nomeadamente dossiês de dados recolhidos pelo sector privado.

7. Enquanto elemento de referência importante, a AEPD recorda ainda que a questão da transferência de dados pessoais para países terceiros no âmbito da cooperação policial e judicial em matéria penal é tratada na Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal ([4]) que será provavelmente adoptada antes do final de 2008.

8. Esta troca transatlântica de informações só poderá aumentar e abranger outros sectores em que são tratados dados pessoais. Neste contexto, um diálogo sobre a «aplicação transatlântica da lei» é ao mesmo tempo bem vindo e sensível: bem vindo no sentido em que poderá proporcionar um quadro mais claro para os intercâmbios de dados actuais ou futuros; sensível porque esse quadro poderá legitimar transferências maciças de dados num domínio — aplicação da lei — em que o impacto sobre os indivíduos é particularmente grave, e em que são ainda mais necessárias salvaguardar e garantias rigorosas e fiáveis ([5]).

9. O presente parecer tratará no capítulo seguinte da situação actual e dos possíveis rumos a tomar. O Capítulo III incidirá no âmbito e natureza de um instrumento que permita a partilha da informação. No Capítulo IV, o parecer analisará de uma perspectiva jurídica geral as questões ligadas ao conteúdo de um eventual acordo. Tratará de questões como as condições de avaliação do nível de protecção previsto pelos Estados Unidos, e discutirá a questão da utilização do quadro regulador da UE como marco de referência, a fim de avaliar o nível de protecção. Este capítulo conterá igualmente uma lista das exigências de base a incluir neste tipo de acordo. Por último, no Capítulo V, o presente parecer fornecerá uma análise dos princípios de privacidade que se prendem com o conteúdo do relatório.

([3]) JO L 213 de 8.8.2008, p. 49.

([4]) Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, versão de 24 de Junho de 2008 disponível em http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

([5]) Quanto à necessidade de um quadro jurídico claro, ver Capítulos III e IV do presente parecer.

II. SITUAÇÃO ACTUAL E POSSÍVEIS RUMOS A TOMAR

10. A AEPD avalia a situação actual do seguinte modo: foram realizados alguns progressos no que diz respeito à definição de normas comuns relativas ao intercâmbio de informação e à protecção da vida privada e dos dados pessoais.

11. No entanto, os trabalhos preparatórios para qualquer tipo de acordo entre a UE e os EUA não estão ainda concluídos, sendo necessário prosseguir os trabalhos. O relatório do Grupo de Contacto de Alto Nível refere uma série de questões pendentes das quais a questão preponderante é a questão da «reparação». Persiste o desacordo sobre o âmbito necessário da reparação judicial ([6]). Foram identificadas outras cinco questões pendentes no Capítulo 3 do relatório. Além disso, decorre do presente parecer que muitas outras questões ainda não estão resolvidas, como por exemplo as respeitantes ao âmbito e natureza de um instrumento relativo ao intercâmbio da informação.

12. Uma vez que a opção preferida no relatório é um acordo vinculativo — preferência partilhada pela AEPD — é ainda mais necessário usar de prudência. Antes de se poder chegar a um acordo, é necessário um trabalho de preparação cuidadoso e aprofundado.

13. Por último, de acordo com a AEPD, o âmbito mais indicado para a celebração de um acordo seria o Tratado de Lisboa, na condição, obviamente, de que este entre em vigor. Com efeito, ao abrigo do Tratado de Lisboa, não se poria a questão da incerteza jurídica sobre a linha divisória entre os pilares da UE. Além disso, seria garantido o total envolvimento do Parlamento Europeu bem como o controlo judicial do Tribunal de Justiça.

14. Nessas circunstâncias, a melhor maneira de avançar seria elaborar um roteiro com vista a um eventual acordo numa fase posterior. Esse roteiro incluiria os seguintes elementos:

— Orientações para o prosseguimento dos trabalhos do Grupo de Contacto de Alto Nível (ou de qualquer outro grupo) bem como um calendário;

— Numa fase inicial, discussão e possível acordo sobre questões fundamentais como o âmbito e a natureza do acordo;

— Com base num entendimento comum destas questões fundamentais, o aprofundamento dos princípios relativos à protecção dos dados;

— Participação das partes interessadas nas diferentes fases do processo;

— Do lado europeu, tratamento das restrições institucionais.

([6]) Página 5 do relatório, parte C.

III. **ÂMBITO E NATUREZA DE UM INSTRUMENTO RELATIVO À PARTILHA DA INFORMAÇÃO**

15. No entender da AEPD, é essencial que o âmbito e a natureza de um eventual instrumento que inclua princípios de protecção dos dados sejam claramente definidos, enquanto primeiro passo para o desenvolvimento de tal instrumento.

16. Quanto ao âmbito, as questões importantes que exigem resposta são:

— quais são os actores envolvidos, dentro e fora da área de aplicação da lei;

— o que se pretende com o «objectivo de aplicação da lei» e a sua relação com outros objectivos como a segurança nacional, e mais especificamente o controlo das fronteiras e a saúde pública;

— de que maneira este instrumento se pode inserir na perspectiva de uma zona de segurança transatlântica global.

17. A definição da natureza deverá clarificar as seguintes questões:

— se tal for pertinente, ao abrigo de que pilar o instrumento será negociado;

— se o instrumento em questão será vinculativo para a UE e os EUA;

— se o mesmo terá efeitos directos, no sentido em que prevê direitos e obrigações para as pessoas que podem ser aplicados junto de uma autoridade judicial;

— se o instrumento em si permitirá o intercâmbio de informação ou estabelecerá uma norma mínima para o intercâmbio de informação a complementar através de acordos específicos;

— de que modo o instrumento se articulará com os instrumentos existentes: respeitá-los-á, substitui-los-á ou complementá-los-á?

III.1. **Escolha do instrumento**

Actores envolvidos

18. Embora não haja uma indicação clara no relatório do Grupo de Contacto de Alto Nível sobre o âmbito exacto do futuro instrumento, pode ser deduzido dos princípios nele referidos que prevê abranger tanto as transferências entre intervenientes públicos e privados ([7]) como entre as autoridades públicas.

([7]) Ver em especial o Capítulo 3 do relatório, «Questões pendentes pertinentes para as relações transatlânticas», ponto 1: «Coerência das obrigações das entidades privadas durante as transferências de dados».

— Entre os intervenientes públicos e privados:

19. A AEPD reconhece a lógica da aplicabilidade de um futuro instrumento às transferências entre actores públicos e privados. O desenvolvimento de tal instrumento é realizado na sequência dos pedidos apresentados pela parte EUA de informação provenientes de partes privadas nos últimos anos. A AEPD toma nota de que os actores privados estão a tornar-se uma fonte de informação sistemática numa perspectiva de aplicação da lei, seja a nível dos EUA, seja a nível internacional ([8]). O caso SWIFT constituiu um precedente importante, tendo uma empresa privada sido solicitada a transmitir sistematicamente os dados em grande quantidade às autoridades de aplicação da lei de um Estado terceiro ([9]). A recolha de dados PNR das companhias de aviação insere-se na mesma lógica. No seu parecer sobre um projecto de decisão-quadro para um sistema europeu de PNR, a AEPD já questionou a legitimidade desta tendência ([10]).

20. Há mais duas razões para estar relutante quanto à inclusão de transferências entre intervenientes públicos e privados no âmbito de um futuro instrumento.

21. Em primeiro lugar, tal inclusão poderá ter um efeito não desejado no território da própria UE. A AEPD está seriamente preocupada com a possibilidade de empresas privadas (tais como instituições financeiras) serem, em princípio, transferidas para países terceiros, uma vez que tal poderia provocar uma forte pressão no sentido de disponibilizar igualmente na UE o mesmo tipo de dados às autoridades de aplicação da lei. O sistema PNR é um exemplo de um desenvolvimento não desejado desse tipo, que teve início com uma recolha em larga escala de dados relativos aos passageiros nos EUA, que foram seguidamente transpostos para o contexto interno europeu ([11]) sem que a necessidade e a proporcionalidade do sistema tenham sido claramente demonstradas.

22. Em segundo lugar, no seu parecer sobre a proposta da Comissão relativa aos dados PNR da UE a AEPD levantou igualmente a questão do âmbito de protecção dos dados (primeiro ou terceiro pilar) aplicável às condições da

([8]) Ver sobre esta questão o parecer da AEDP de 20 de Dezembro de 2007 sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei, JO C 110 de 1.5.2008, p. 1. «Tradicionalmente, tem havido uma clara separação entre as actividades policiais e as do sector privado, sendo as funções policiais desempenhadas por serviços especificamente dedicados, em particular as forças de polícia, e sendo os intervenientes privados solicitados, caso a caso, a comunicar dados pessoais a esses serviços de aplicação da lei. Há agora uma tendência para impor a cooperação para efeitos de aplicação da lei a intervenientes privados numa base sistemática».

([9]) Ver parecer 10/2006, de 22 de Novembro de 2006, do Grupo do Artigo 29. sobre o tratamento de dados pessoais pela Sociedade Mundial de Telecomunicações Financeiras Interbancárias (SWIFT), WP 128.

([10]) Parecer emitido em 20 de Dezembro de 2007.

([11]) Ver a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (*Passenger Name Record* — PNR) para efeitos de aplicação da lei, referida na nota de pé-de-página 8, tal como actualmente debatida no Conselho.

cooperação entre os intervenientes públicos e privados: deverão as regras ser baseadas na qualidade do controlador de dados (sector privado) ou na finalidade prosseguida (aplicação da lei)? A linha de demarcação entre o primeiro e o terceiro pilar está longe de ser clara em situações em que são impostas obrigações aos intervenientes privados de tratar os dados pessoais para efeitos de aplicação da lei. Neste contexto é digno de nota que o Advogado-Geral Yves Bot, no seu recente parecer no processo relativo à conservação de dados ([12]) proponha uma linha de demarcação para estas situações, mas acrescenta à sua proposta: «Esta linha de demarcação não está com certeza isenta de críticas e pode, sob determinados aspectos, parecer superficial.» A AEPD toma nota igualmente de que o acórdão PNR do Tribunal ([13]) não dá resposta cabal à questão do quadro jurídico aplicável. Por exemplo, o facto de certas actividades não estarem abrangidas pela Directiva 95/46/CE não significa automaticamente que essas actividades podem ser reguladas ao abrigo do terceiro pilar. O referido acórdão resulta possivelmente numa lacuna no que diz respeito à legislação aplicável e em todo o caso gera incerteza jurídica no que se refere às garantias jurídicas disponíveis para as pessoas em causa.

23. Nesta perspectiva, a AEPD salienta que deverá ser garantido que um futuro instrumento que preveja princípios gerais de protecção de dados não pode legitimar as transferências transatlânticas de dados pessoais entre intervenientes públicos e privados. Estas transferências apenas podem ser incluídas num futuro instrumento desde que:

— o futuro instrumento estipule que a transferência só é autorizada se se comprovar que é absolutamente necessária para um fim específico, a decidir caso a caso,

— a própria transferência for rodeada por importantes garantias de protecção dos dados (tal como descrito no presente parecer).

Além disso, a AEPD toma nota da incerteza quanto ao quadro de protecção de dados aplicável e argumenta, portanto, em todo o caso a favor da não inclusão das transferências de dados pessoais entre entidades públicas e privadas no estado actual da legislação da UE.

— Entre autoridades públicas:

24. O âmbito exacto do intercâmbio de informação não é claro. Como primeiro passo no prosseguimento dos trabalhos com vista à criação de um instrumento comum, o âmbito previsto para tal instrumento deverá ser clarificado. Subsistem designadamente algumas questões:

— No que diz respeito às bases de dados situadas na UE, o instrumento em causa visará as bases de dados centralizadas (parcialmente) geridas pela UE como as bases de dados da Europol e do Eurojust, ou as bases de dados descentralizadas geridas pelos Estados-Membros, ou tanto umas como outras?

— O âmbito do instrumento alarga-se às redes interconexas, ou seja, as garantias previstas abrangerão os dados intercambiados entre os Estados-Membros ou as agências, na UE bem como nos EUA?

— O instrumento abrangerá apenas o intercâmbio entre bases de dados no domínio da aplicação da lei (polícia, justiça, eventualmente as alfândegas) ou igualmente outras bases de dados como as bases de dados fiscais?

— O instrumento também abrangerá as bases de dados de agências nacionais de segurança, ou permitirá o acesso por essas agências a bases de dados das autoridades de aplicação da lei no território da outra parte contratante (EUA à UE e vice-versa)?

— O instrumento abrangerá as transferências de informação caso a caso, ou o acesso permanente às bases de dados existentes? Esta última hipótese levantará certamente questões relativas à proporcionalidade, tal como exposto de forma mais aprofundada no ponto 3 do Capítulo V.

Objectivo da aplicação da lei

25. A definição do objectivo de um eventual acordo também suscita incerteza. O objectivo da aplicação da lei é claramente indicado na introdução bem como no primeiro princípio anexo ao relatório, e será analisado em profundidade no Capítulo IV do presente parecer. A AEPD toma nota de que decorre do atrás exposto que o intercâmbio de dados incidirá em questões do terceiro pilar, mas poder-se-á pôr a questão de saber se se trata apenas de um primeiro passo no sentido de uma troca de informação mais ampla. Parece claro que objectivo da «segurança pública» exposto no relatório inclui a luta contra o terrorismo, a criminalidade organizada e outros crimes. No entanto, será que também permite o intercâmbio de dados no caso de outros interesses públicos como eventuais riscos de saúde pública?

26. A AEPD recomenda que o objectivo seja restringido ao tratamento de dados identificados com precisão e à justificação das escolhas de política conducentes a essa definição do objectivo.

([12]) Parecer do Advogado-Geral Yves Bot de 14 de Outubro de 2008, Irlanda c/Parlamento Europeu e Conselho (Processo C-301/06), ponto 108.

([13]) Decisão 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.

Um espaço transatlântico de segurança global

27. O vasto âmbito deste relatório deverá ser colocado na perspectiva da zona de segurança transatlântica global discutida pelo chamado «Grupo do Futuro» ([14]). O relatório deste Grupo, apresentado em Junho de 2008, põe um certo ênfase na dimensão externa da política de assuntos internos e advoga que «*até 2014, a União Europeia deverá ter tomado posição quanto ao objectivo político de realizar com os Estados Unidos um espaço euro-atlântico de cooperação no domínio da liberdade, segurança e justiça*». Tal cooperação iria além da segurança em sentido estrito e incluiria temas tratados no actual Título IV do Tratado CE, como a imigração, os vistos e o asilo e a cooperação no domínio do direito civil. Importa levantar a questão de saber até que ponto um acordo relativo a princípios de protecção de base, como os referidos no relatório do Grupo de Contacto de Alto Nível, poderá e deverá constituir a base para um intercâmbio de informação numa área tão vasta.

28. Normalmente, até 2014 a estrutura de pilares deixará de existir e não haverá uma base jurídica para a protecção de dados dentro da própria UE (ao abrigo do Tratado de Lisboa, artigo 16.º do Tratado relativo ao funcionamento da União Europeia). No entanto, o facto de haver harmonização a nível da UE no que diz respeito à *regulamentação* da protecção de dados não implica que qualquer acordo com um país terceiro possa prever a *transferência* de quaisquer dados pessoais, qualquer que seja o seu objectivo. Consoante o contexto e as condições do tratamento, poderão ser exigidas garantias de protecção de dados adequadas para domínios específicos como a aplicação da lei. A AEPD recomenda que sejam tidas em conta as consequências destas diferentes perspectivas na elaboração de um futuro acordo.

III.2. **Natureza do acordo**

O quadro institucional europeu

29. Numa perspectiva a curto prazo, em todo o caso, é essencial determinar ao abrigo de que pilar o acordo será negociado. Tal é necessário nomeadamente dado que o quadro regulador interno para a protecção de dados será afectado por tal acordo. O quadro será o do primeiro pilar — basicamente a Directiva 95/46/CE com o seu regime específico para a transferência de dados para países terceiros — ou o do terceiro pilar com um regime menos restritivo aplicável às transferências para países terceiros? ([15]).

30. Embora o objectivo da aplicação da lei prevaleça, tal como já referido, o relatório do Grupo de Contacto de Alto Nível refere no entanto a recolha de dados junto de intervenientes privados, e os objectivos podem igualmente ser interpretados em sentido lato susceptível de ir além da segurança, incluindo por exemplo as questões relativas à imigração e ao controlo das fronteiras, mas também possivelmente à saúde pública. Face a estas incertezas, seria francamente preferível esperar pela harmonização dos pilares ao abrigo da legislação da UE, tal como previsto no Tratado de Lisboa, para estabelecer claramente a base jurídica para as negociações e o papel exacto das instituições europeias, especialmente o do Parlamento Europeu e da Comissão.

Carácter vinculativo do instrumento

31. Deverá ficar claro se as conclusões dos debates resultarão num memorando de entendimento ou noutro instrumento não vinculativo, ou num acordo internacional vinculativo.

32. A AEPD apoia a preferência dada no relatório a um acordo vinculativo. Um acordo oficial vinculativo é, no entender da AEPD, uma condição prévia indispensável a qualquer transferência para fora da UE, independentemente do respectivo objectivo. Não é possível efectuar nenhuma transferência de dados para um país terceiro sem que as condições e garantias adequadas estejam previstas num quadro jurídico específico (e vinculativo). Por outras palavras, um memorando de entendimento ou outro instrumento não vinculativo pode ser útil para proporcionar orientação para as negociações de outros instrumentos vinculativos, mas não pode nunca sobrepor-se à necessidade de um acordo vinculativo.

Efeito directo

33. As disposições do instrumento deverão ser igualmente vinculativas para os EUA e para a UE e seus Estados-Membros.

34. Deverá além disso ser garantido que as pessoas têm direito a exercer os seus direitos e nomeadamente a obter reparação, com base nos princípios acordados. De acordo com a AEPD, a melhor maneira de o conseguir é formular as disposições substantivas do instrumento de forma a que estas produzam efeito directo para os residentes da União Europeia e possam ser invocadas em tribunal. O efeito directo das disposições de um acordo internacional, bem como as condições da sua transposição para a legislação europeia e nacional destinadas a garantir a eficácia das medidas têm de ser clarificados no instrumento.

Relações com outros instrumentos

35. Em que medida o acordo é autónomo ou tem de ser completado caso a caso por outros acordos sobre intercâmbios específicos de dados constitui igualmente uma questão fundamental. Põe-se, de facto, a questão de saber se um simples acordo poderá abranger de forma adequada, com um conjunto de normas único, as múltiplas

([14]) Relatório do Grupo Consultivo Informal de Alto Nível sobre o Futuro da Política Europeia de Assuntos Internos, «Liberdade, Segurança, Vida Privada — Política Europeia de Assuntos Internos num mundo aberto», Junho de 2008, disponível em register.consilium.europa.eu

([15]) Ver artigos 11.º a 13.º da Decisão-Quadro relativa à protecção de dados pessoais referida no ponto 7 do presente parecer.

especificidades do tratamento de dados no terceiro pilar. Ainda suscita mais dúvidas que o referido acordo possa *permitir*, sem debate e garantias adicionais, uma aprovação global de qualquer transferência de dados pessoais qualquer que seja o seu objectivo e natureza. Além disso, os acordos com países terceiros não são necessariamente permanentes, uma vez que podem ser ligados a ameaças específicas, ser sujeitos a revisão e a cláusulas de caducidade. Por outro lado, as normas mínimas comuns tal como reconhecidas num instrumento vinculativo poderão facilitar os debates sobre a transferência de dados pessoais em relação com uma base de dados concreta ou operações de tratamento de dados.

36. A AEPD seria, portanto, favorável ao desenvolvimento de um conjunto mínimo de critérios de protecção de dados a complementar caso a caso através de disposições adicionais específicas, tal como referido no relatório do Grupo de Contacto de Alto Nível, em vez da alternativa de um acordo autónomo. Estas disposições específicas adicionais são uma condição prévia para permitir a transferência de dados num caso específico. Tal constituiria um incentivo a uma abordagem harmonizada em termos de protecção de dados.

Aplicação aos instrumentos existentes

37. Deverá igualmente analisar-se de que forma um eventual acordo geral se articularia com os acordos já existentes celebrados entre a UE e os EUA. Convém notar que estes acordos não têm o mesmo carácter vinculativo: merecem referência especial o acordo PNR (o que apresenta o maior grau de certeza jurídica), os acordos Europol e Eurojust, ou a troca de cartas SWIFT ([16]). Será que um novo quadro geral viria complementar estes instrumentos existentes ou estes se manteriam inalterados, uma vez que o novo quadro seria aplicável apenas a outros intercâmbios futuros de dados pessoais? No entender da AEPD, a coerência jurídica exigiria um conjunto de regras harmonizado que seja aplicável tanto aos acordos existentes como aos acordos futuros em matéria de transferências de dados e que os complemente.

38. A aplicação do acordo geral aos instrumentos existentes teria a vantagem de reforçar o carácter vinculativo destes. Tal seria particularmente apreciado no que diz respeito aos instrumentos que não são juridicamente vinculativos, como a troca de cartas SWIFT, uma vez que imporia o cumprimento de um conjunto de princípios gerais relativos à vida privada.

IV. **AVALIAÇÃO JURÍDICA GERAL**

39. Este capítulo analisará a forma de avaliar o nível de protecção de um quadro ou instrumento específico, incluindo a questão dos marcos de referência a utilizar e as exigências de base necessários.

Nível de protecção adequado

40. De acordo com a AEPD, deverá ser claro que um dos principais resultados de um futuro instrumento será que a transferência de dados pessoais para os Estados Unidos só se poderá efectuar desde que as autoridades dos Estados Unidos garantam um nível de protecção adequado (e vice-versa).

41. A AEPD considera que só um verdadeiro teste de adequação dá garantias suficientes no que diz respeito ao nível de protecção dos dados pessoais. Considera que um acordo-quadro geral com um âmbito tão vasto como o preconizado no relatório do Grupo de Contacto de Alto Nível teria dificuldades em passar, enquanto tal, um verdadeiro teste de adequação. A adequação do acordo geral apenas poderá ser reconhecida se for combinada com a adequação dos acordos específicos celebrados caso a caso.

42. A apreciação do nível de protecção oferecido pelos países terceiros não é um exercício inabitual, em especial para a Comissão Europeia: a adequação é, ao abrigo do primeiro pilar, uma exigência para a transferência. Foi avaliada em diversas ocasiões nos termos do artigo 25.º da Directiva 95/46 com base em critérios específicos e confirmada por decisões da Comissão Europeia ([17]). Ao abrigo do terceiro pilar, tal sistema não é explicitamente previsto: a avaliação da adequação da protecção apenas é recomendada na situação específica dos artigos 11.º e 13.º da (ainda não adoptada) decisão-quadro relativa à protecção dos dados ([18]) e é deixada aos Estados-Membros.

43. No caso em apreço, o âmbito do exercício abrange o objectivo da aplicação da lei, sendo os debates conduzidos pela Comissão sob supervisão do Conselho. O contexto é diferente da avaliação dos princípios de «porto seguro» ou a adequação da legislação canadiana, e tem mais ligações com as recentes negociações PNR com os EUA e a Austrália que se desenrolaram num quadro jurídico do terceiro pilar. No entanto, os princípios do Grupo de Contacto de Alto Nível foram igualmente mencionados no contexto do programa de isenção de vistos que diz respeito às fronteiras e à imigração e portanto às questões do primeiro pilar.

44. A AEPD recomenda que qualquer averiguação da adequação ao abrigo de um futuro instrumento deverá basear-se

([16]) Ver nota de pé-de-página 2.

([17]) As decisões da Comissão sobre a adequação da protecção dos dados pessoais nos países terceiros, incluindo a Argentina, o Canadá, a Suíça, os Estados Unidos, Guernsey, a Ilha de Man e Jersey estão disponíveis em http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Restringida à transferência por um Estado-Membro para um país terceiro ou organismo internacional de dados recebidos de uma autoridade competente de outro Estado-Membro.

nas experiências adquiridas nestes diferentes domínios. Recomenda que a noção de «adequação» no contexto de um futuro instrumento seja desenvolvida com base em critérios semelhantes aos utilizados em anteriores avaliações da adequação.

Reconhecimento mútuo — reciprocidade

45. Um segundo elemento do nível de protecção diz respeito ao reconhecimento mútuo pela UE e pelos EUA dos respectivos sistemas. O relatório do Grupo de Contacto de Alto Nível refere a este respeito que o objectivo seria obter o reconhecimento da eficácia dos respectivos sistemas de protecção da vida privada e dos dados nos domínios abrangidos por estes princípios ([19]) e chegar a uma aplicação equivalente e recíproca da legislação relativa à protecção da vida privada e dos dados pessoais.

46. Para a AEPD é óbvio que o reconhecimento mútuo (ou reciprocidade) apenas é possível se for garantido um nível de protecção adequado. Por outras palavras, o futuro instrumento deverá harmonizar um nível mínimo de protecção (através de uma averiguação da adequação, tendo em conta a necessidade de acordos específicos numa base caso a caso). Só com base nesta condição prévia poderá ser reconhecida a reciprocidade.

47. O primeiro elemento a ter em conta é a reciprocidade das disposições substantivas em matéria de protecção de dados. Na opinião da AEPD, um acordo deveria abranger o conceito de reciprocidade das disposições substantivas em matéria de protecção de dados por forma a garantir, por um lado, que o tratamento dos dados no território da UE (e dos EUA) respeite plenamente a legislação nacional relativa à protecção de dados, e, por outro, que o tratamento dos dados fora do respectivo país de origem e abrangido pelo acordo respeite os princípios da protecção de dados tal como constam do acordo.

48. O segundo elemento é a reciprocidade dos mecanismos de reparação. Dever-se-ia garantir que os cidadãos europeus disponham de vias de recurso adequadas quando os dados que lhes dizem respeito sejam tratados nos Estados Unidos (independentemente da legislação aplicável a esse tratamento), mas igualmente que a União Europeia e os seus Estados-Membros concedam direitos equivalentes aos cidadãos dos EUA.

49. O terceiro elemento é a reciprocidade do acesso aos dados pessoais pelas autoridades de aplicação da lei. Se um instrumento permite às autoridades dos Estados Unidos o acesso a dados provenientes da União Europeia, a reciprocidade implica que seja concedido às autoridades da UE igual acesso a dados provenientes dos EUA. A reciprocidade não deve afectar a eficácia da protecção da pessoa em causa. Esta é uma condição prévia para permitir o acesso «transatlântico» pelas autoridades de aplicação da lei. Isto significa, concretamente, que:

— Não deve ser permitido o acesso directo pelas autoridades dos Estados Unidos a dados dentro do território da UE (e vice-versa). O acesso apenas deverá ser concedido numa base indirecta no âmbito de um sistema de «empurro»;

— Esse acesso deverá efectuar-se sob o controlo das autoridades responsáveis pela protecção dos dados e das autoridades judiciais do país em que ocorre o tratamento dos dados;

— O acesso das autoridades dos Estados Unidos às bases de dados na UE deverá respeitar as disposições substantivas em matéria de protecção de dados (ver atrás) e garantir uma reparação total à pessoa em causa.

Precisão do instrumento

50. A especificação das condições de avaliação (adequação, equivalência, reconhecimento mútuo) é essencial uma vez que determina o conteúdo, em termos de precisão, certeza jurídica e eficácia da protecção. O conteúdo de um futuro instrumento tem de ser preciso e exacto.

51. Além disso, deverá ficar claro que qualquer acordo específico celebrado posteriormente terá de incluir garantias de protecção de dados pormenorizadas e completas sobre a pessoa concernida pelo intercâmbio de dados previsto. Só um nível duplo deste tipo de princípios concretos de protecção de dados garantirá a necessária harmonização entre o acordo geral e os acordos específicos, tal como já observado nos pontos 35 e 36 do presente parecer.

Desenvolver um modelo para outros países terceiros

52. Merece especial atenção a questão de saber até que ponto um acordo com os EUA poderá ser um modelo para outros países terceiros. A AEPD toma nota de que, além dos EUA, o referido relatório do Grupo do Futuro também indica a Rússia como parceiro estratégico da UE. Na medida em que os princípios são neutros e respeitam as garantias fundamentais da UE, poderão constituir um precedente útil. No entanto, eventuais especificidades ligadas, por ex, ao quadro jurídico do país destinatário ou ao objectivo da transferência poderão impedir a mera transposição do acordo. Outro factor igualmente decisivo será a situação dos países terceiros em termos de democracia: dever-se-á assegurar que os princípios acordados serão efectivamente garantidos e implementados no país destinatário.

Que marcos de referência para avaliar o nível de protecção?

53. A adequação, implícita ou explícita, deverá respeitar o quadro jurídico internacional e europeu e sobretudo, as garantias de protecção de dados acordadas em comum, as quais estão consagradas nas Orientações das Nações Unidas,

([19]) Capítulo A. Acordo internacional vinculativo, p. 8.

na Convenção 108 do Conselho da Europa e o seu protocolo adicional, nas Orientações da OCDE e no projecto de decisão-quadro relativa à protecção dos dados, bem como, para os aspectos do primeiro pilar, na Directiva 95/46/CE ([20]). Todos estes instrumentos contêm princípios semelhantes que são mais amplamente reconhecidos como sendo a parte essencial da protecção de dados pessoais.

54. É muito importante que os princípios atrás referidos sejam devidamente tidos em conta, se se atender ao impacto de um potencial acordo como o previsto no relatório do Grupo de Contacto de Alto Nível. Um instrumento que abranja todo o sector de *aplicação da lei* de um país terceiro constituiria de facto uma situação sem precedente. As decisões sobre a adequação existentes no primeiro pilar, bem como os acordos celebrados com países terceiros no terceiro pilar da UE (Europol, Eurojust) estiveram sempre ligados a uma transferência de dados específica, enquanto neste caso poderiam ser tornadas possíveis transferências com um âmbito muito mais vasto, tendo em conta o grande objectivo prosseguido (combate às infracções penais, segurança pública e nacional, controlo das fronteiras) e o número desconhecido de bases de dados abrangidas.

Exigências de base

55. As condições a preencher no contexto da transferência de dados pessoais para países terceiros foram elaboradas num documento de trabalho do Grupo do Artigo 29.º ([21]). Qualquer acordo sobre princípios relativos à vida privada deverá ser sujeito a um teste de conformidade que garanta a eficácia das garantias de protecção dos dados.

— Quanto ao fundo: os princípios relativos à protecção dos dados deverão prever um alto nível de protecção, e cumprir normas que estejam em consonância com os princípios da UE. Os 12 princípios incluídos no relatório do Grupo de Contacto de Alto Nível continuarão a ser analisados na perspectiva do Capítulo V do presente parecer;

— Quanto à concretização: dependendo da natureza do acordo, e em especial no caso de se tratar de um acordo oficial internacional, as regras e procedimentos deverão ser definidos em pormenor, por forma a permitir uma execução efectiva;

— Quanto à supervisão: a fim de garantir o cumprimento das regras acordadas, deverão ser instituídos mecanismos de controlo, tanto a nível interno (auditorias) como externo (revisões). Esses mecanismos têm de ser igualmente acessíveis a ambas as partes no acordo. A supervisão inclui mecanismos que garantem o cumprimento das regras a nível macro, tais como mecanismos comuns de revisão, e o cumprimento a nível micro, como a reparação individual.

56. Além destas três exigências de base, deverá ser prestada especial atenção às especificidades ligadas ao processamento de dados pessoais num contexto de aplicação da lei. Trata-se de facto de um domínio em que os direitos fundamentais podem sofrer restrições. Deverão portanto ser adoptadas garantias para compensar a restrição dos direitos individuais, especialmente no que diz respeito aos seguintes aspectos, atendendo ao seu impacto nas pessoas:

— Transparência: a informação e o acesso aos dados pessoais poderão ser limitados num contexto de aplicação da lei, devido por exemplo à discrição exigida por certas investigações. Enquanto na UE são tradicionalmente instituídos mecanismos adicionais para compensar esta limitação dos direitos fundamentais (que envolvem muitas vezes autoridades independentes de protecção de dados), deverá ser garantida a existência de mecanismos de compensação semelhantes uma vez transferida a informação para um país terceiro;

— Reparação: pelas razões atrás referidas, as pessoas deverão beneficiar de possibilidades alternativas de defender os seus direitos, em especial através de uma autoridade de supervisão independente e em tribunal;

— Conservação de dados: a justificação para o período de conservação dos dados poderá não ser transparente. Têm de ser tomadas medidas por forma a que tal não impeça o exercício efectivo dos direitos pelas pessoas em causa ou pelas autoridades de supervisão;

([20]) — Orientações das Nações Unidas sobre os dossiês relativos aos dados pessoais computorizados, adoptado pela Assembleia Geral em 14 de Dezembro de 1990, disponível em www.unhchr.ch/html/menu3/b/71.htm
— Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa, de 28 de Janeiro de 1981, disponível em www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— OCDE: Linhas de orientação sobre a protecção da privacidade e os fluxos transfronteiras de dados pessoais, adoptadas em 23 de Setembro de 1980, disponíveis em www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Decisão-Quadro do Conselho relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal, disponível em http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371
— Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, JO L 281 de 23.11.1995, p. 31.

([21]) Documento de trabalho de 24 de Julho de 1998 relativo às transferências de dados para países terceiros: Aplicação dos artigos 25.º e 26.º da Directiva da UE relativa à protecção dos dados; WP12.

— Responsabilização das autoridades de aplicação da lei: na falta de transparência efectiva, os mecanismos de controlo quer pelas pessoas quer pelas partes interessadas institucionais não podem de forma alguma ser exaustivos. Seria ainda assim essencial que tais controlos sejam firmemente estabelecidos, atendendo ao carácter sensível dos dados e às medidas coercivas que podem ser tomadas contra as pessoas com base no tratamento dos dados. A responsabilização é uma questão decisiva no que diz respeito aos mecanismos de controlo nacionais e igualmente às possibilidades de revisão pelo país ou região de origem dos dados. Tais mecanismos de revisão estão previstos em acordos específicos como o acordo PNR, e a AEPD recomenda vivamente a sua inclusão no instrumento geral.

V. **ANÁLISE DOS PRINCÍPIOS**

Introdução

57. Este capítulo analisa os 12 princípios incluídos no documento do Grupo de Contacto de Alto Nível segundo a seguinte perspectiva:

— Estes princípios mostram que os EUA e a UE têm alguns pontos de vista em comum sobre os princípios, podendo ser detectadas certas similitudes com os princípios da Convenção 108;

— No entanto, um acordo quanto ao nível dos princípios não é suficiente. Um instrumento jurídico deverá ser suficientemente forte para garantir o cumprimento;

— A AEPD lamenta que os princípios não sejam acompanhados de um memorando explicativo;

— Deveria ficar claro, antes de se entrar na descrição dos princípios, que ambas as partes têm o mesmo entendimento sobre a redacção utilizada, por exemplo no que diz respeito à noção de informação pessoal ou de pessoas protegidas. Neste contexto as definições são bem vindas.

1. Especificação do objectivo

58. O primeiro princípio enumerado no anexo do relatório do Grupo de Contacto de Alto Nível refere que a informação pessoal pode ser tratada para fins legítimos de aplicação da lei. Tal como atrás mencionado, isto diz respeito, no caso da União Europeia, à prevenção, detecção, investigação ou perseguição judicial de infracções penais. No entanto, no caso dos EUA, a interpretação da aplicação da lei vai além das infracções penais e inclui o controlo das fronteiras, a segurança pública e objectivos de segurança nacional. As consequências de tais discrepâncias entre os objectivos declarados pela UE e pelos EUA não são claras. Embora o relatório refira que na prática os objectivos podem coincidir em larga medida, continua a ser imperativo saber exactamente em que medida *não* coincidem. No domínio da aplicação da lei, tendo em conta o impacto das medidas tomadas sobre as pessoas, o princípio da limitação do objectivo tem de ser rigorosamente observado e os objectivos declarados têm de ser claros e circunscritos. Tendo em conta a reciprocidade prevista no relatório, a aproximação dos referidos objectivos parece igualmente essencial. Em resumo, é necessária uma clarificação da compreensão deste princípio.

2. Integridade/qualidade dos dados

59. A AEPD acolhe favoravelmente a disposição que prevê que a informação pessoal seja exacta, pertinente, atempada e completa, tal como necessário para um tratamento legal. Tal princípio é uma condição de base para um tratamento eficiente dos dados.

3. Necessidade/proporcionalidade

60. O princípio estabelece uma ligação clara entre a informação recolhida e a necessidade dessa informação para cumprir um objectivo de aplicação da lei juridicamente estabelecido. Esta exigência de uma base legislativa é um elemento positivo para avaliar a legitimidade do tratamento. A AEPD toma nota, no entanto, de que, embora isto reforce a certeza jurídica do tratamento, a base jurídica para esse tratamento consiste numa lei de um país terceiro. Uma lei de um país terceiro não pode, por si só, constituir uma base legítima para uma transferência de dados pessoais ([22]). No contexto do relatório do Grupo de Contacto de Alto Nível, parece assente que a legitimidade da lei de um país terceiro, por exemplo os Estados Unidos, é, em princípio, reconhecida. Deve ter-se presente que, se tal argumentação pode encontrar justificação neste caso atendendo a que os Estados Unidos são um Estado democrático, o mesmo regime não seria válido e não poderia ser transposto para as relações com qualquer outro país terceiro.

61. Qualquer transferência de dados pessoais tem de ser pertinente, necessária e adequada nos termos do anexo ao relatório do Grupo de Contacto de Alto Nível. A AEPD salienta que para ser proporcionado, o tratamento não pode ser indevidamente intrusivo, e as respectivas modalidades têm de ser equilibradas, tendo em conta os direitos e interesses das pessoas em causa.

62. Por esta razão, o acesso à informação deverá ter lugar numa base caso a caso, dependendo das necessidades práticas no contexto de uma investigação específica. O acesso permanente pelas autoridades de aplicação da lei do país terceiro a bases de dados situadas na UE seria considerado

([22]) Ver nomeadamente as alíneas c) e e) do artigo 7.º da Directiva 95/46/CE. No seu parecer 6/2002, de 24 de Outubro de 2002, sobre a transmissão da informação contida no manifesto de passageiros e outros dados pelas companhias aéreas aos Estados Unidos, o Grupo do Artigo 29.º declarou que não lhe parecia aceitável que uma decisão unilateral tomada por um país terceiro por razões do seu interesse público pudesse levar à transferência rotineira e por grosso de dados protegidos ao abrigo da directiva.

desproporcionado e sem justificação suficiente. A AEPD recorda que mesmo no contexto dos acordos existentes em matéria de intercâmbio de dados, por ex. no caso do acordo PNR, o intercâmbio de dados se baseia em circunstâncias específicas e é efectuado por um período limitado ([23]).

63. Segundo a mesma lógica, o período de conservação de dados deverá ser regulamentado: os dados deverão ser conservados tanto tempo quanto necessário, atendendo ao objectivo específico prosseguido. Se deixarem de ser pertinentes em relação ao objectivo identificado, deverão ser suprimidos. A AEPD opõe-se vivamente à constituição de armazéns de dados em que a informação sobre pessoas não suspeitas seja armazenada tendo em vista a sua eventual utilidade no futuro.

4. Segurança da informação

64. São desenvolvidos nos princípios medidas e procedimentos destinados a proteger os dados da utilização abusiva, alteração e outros riscos, havendo também uma disposição que limita o acesso a pessoas autorizadas. A AEPD considera satisfatórios estes aspectos.

65. Além disso, o princípio poderá ser complementado por uma disposição que preveja que deverão ser conservados registos das pessoas que têm acesso aos dados, o que reforçaria a eficácia das garantias no que diz respeito a limitar o acesso e a evitar a utilização abusiva dos dados.

66. Além disso, deverá ser prevista a informação mútua no caso de violação da segurança: caberá aos destinatários nos EUA bem como na UE informar os seus homólogos caso os dados recebidos tiverem sido alvo de divulgação ilícita. Tal contribuirá para aumentar a responsabilidade por um tratamento seguro dos dados.

5. Categorias especiais de informação pessoal

67. O princípio que proíbe o tratamento de dados sensíveis é, no entender da AEPD, consideravelmente enfraquecido pela excepção que permite todo e qualquer tratamento de dados sensíveis para os quais a legislação nacional preveja «garantias adequadas». Devido justamente ao carácter sensível dos dados, qualquer derrogação ao princípio da proibição deve ser justificada de forma adequada e precisa, sendo apresentada uma lista de objectivos e circunstâncias no âmbito dos quais um determinado tipo de dados sensíveis pode ser tratado, bem como uma indicação da qualidade dos controladores habilitados a tratar esse tipo de dados. Entre as garantias a adoptar, a AEPD considera que os dados sensíveis não deveriam constituir um elemento susceptível de desencadear uma investigação. Poderiam estar disponíveis em circunstâncias específicas mas apenas como informação adicional no que diz respeito à pessoa em causa já sob investigação. Estas garantias e condições devem ser enumeradas de forma limitativa no texto do princípio.

6. Responsabilização

68. Tal como desenvolvido nos pontos 55-56, a responsabilização das entidades públicas que tratam os dados pessoais tem de ser eficazmente garantida, e têm de ser dadas garantias no acordo sobre a forma como essa responsabilização se processará. Este aspecto reveste-se de grande importância, atendendo à falta de transparência tradicionalmente associada ao tratamento de dados pessoais num contexto de aplicação da lei. Nesta perspectiva, referir — como é o caso agora no anexo — que as entidades públicas deverão prestar contas sem dar qualquer explicação adicional sobre as modalidades e as consequências dessa prestação de contas não é uma garantia satisfatória. A AEPD recomenda que essa explicação seja dada no texto do instrumento.

7. Supervisão independente e eficaz

69. A AEPD apoia inteiramente a inclusão de uma disposição que preveja a supervisão independente e eficaz realizada por uma ou várias autoridades públicas de supervisão. Considera que se deve esclarecer de que modo se interpreta a independência, nomeadamente em relação a que entidades essas autoridades mantêm essa sua independência e perante que entidades são responsáveis. É necessário estabelecer critérios a este respeito, os quais deverão ter em conta a independência institucional e funcional em relação aos órgãos executivo e legislativo. A AEPD recorda que se trata de um elemento essencial para garantir a efectiva observância dos princípios acordados. As competências de intervenção e aplicação da lei dessas autoridades são igualmente determinantes tendo em conta a questão da responsabilização das entidades públicas que procedem ao tratamento de dados pessoais, tal como já se referiu mais acima. A sua existência e as competências de que estão investidas deverão ser claras para as pessoas a quem os dados dizem respeito, para que estas possam exercer os seus direitos, especialmente quando haja várias autoridades competentes, consoante o contexto do tratamento dos dados.

70. A AEPD recomenda, além disso, que qualquer futuro acordo preveja mecanismos de cooperação entre as autoridades de supervisão.

8. Acesso individual e rectificação

71. É necessário estabelecer garantias específicas no que toca ao acesso e à rectificação dos dados num contexto de aplicação da lei. Nesse sentido, a AEPD saúda o princípio segundo o qual devem ser facultados às pessoas interessadas o acesso e os meios necessários para obter a rectificação e/ou a eliminação das informações de carácter pessoal que lhes digam respeito. Todavia, subsiste alguma incerteza quanto à definição das pessoas em causa (todos devem

([23]) O presente acordo caduca e deixa de produzir efeitos sete anos após a data da sua assinatura, salvo se as partes decidirem de comum acordo substitui-lo.

gozar de protecção e não só os cidadãos do país em questão), bem como relativamente às condições em que as pessoas em causa podem levantar objecções ao tratamento das informações que lhes digam respeito. Importa igualmente precisar quais os «casos adequados» em que são ou não admissíveis objecções. Não deve restar para as pessoas em causa nenhuma dúvida quanto às circunstâncias — consoante, por exemplo, o tipo de autoridade, o tipo de investigação ou outros critérios — em que podem exercer os seus direitos.

72. Além disso, não havendo uma possibilidade directa de levantar objecção ao tratamento dos dados por motivos justificados, deverá estar disponível outra possibilidade indirecta de verificação, através da autoridade independente responsável pela supervisão do tratamento dos dados.

9. Transparência e informação

73. A AEPD salienta uma vez mais a importância de uma efectiva transparência, para que as pessoas em causa possam exercer os seus direitos e para contribuir para a responsabilização geral das autoridades públicas que procedem ao tratamento de dados pessoais. A AEPD apoia os princípios definidos e insiste, em especial, na necessidade de as informações serem fornecidas *tanto* a título geral *como* a título individual, directamente às pessoas em causa, o que se encontra reflectido no princípio definido no ponto 9 do anexo.

74. No entanto, no Capítulo 2, A. B. (Princípios acordados) o relatório refere que, nos EUA, a transparência pode implicar a publicação, individualmente ou em conjunto, no Registo Federal, da informação fornecida a título individual e a sua divulgação em processo judicial. Não deve restar dúvida de que a publicação num jornal oficial não é, por si só, suficiente para assegurar a informação adequada das pessoas em causa. Para além da necessidade de se proceder à informação a título individual, a AEPD recorda que a informação deve ser apresentada de uma forma e numa linguagem facilmente inteligíveis para a pessoa em causa.

10. Reparação

75. A fim de garantir o efectivo exercício dos seus direitos, as pessoas interessadas devem ter a possibilidade de apresentar queixa perante uma autoridade independente de protecção de dados, bem como de recorrerem para um tribunal independente e imparcial. Ambas estas vias de recurso deverão ser igualmente acessíveis.

76. É necessário assegurar o acesso a uma autoridade independente de protecção de dados, uma vez que esta fornece uma assistência flexível e menos onerosa num contexto — da aplicação da lei — que pode ser bastante opaco para o cidadão comum. As autoridades de protecção de dados podem também prestar assistência no exercício de direitos de acesso em nome da pessoa interessada, quando circunstâncias excepcionais vedem a esta última o acesso directo aos dados que lhe dizem respeito.

77. O acesso ao sistema judiciário constitui uma outra garantia indispensável de que as pessoas em causa podem recorrer para uma autoridade que se insere num ramo do sistema democrático distinto do das instituições públicas que procedem efectivamente ao tratamento dos dados que lhes dizem respeito. O Tribunal Europeu de Justiça ([24]) considerou este tipo de recurso efectivo junto de um tribunal como sendo «essencial para garantir ao particular a protecção efectiva do seu direito. […] Constitui um princípio geral do direito comunitário, que decorre das tradições constitucionais comuns dos Estados-Membros e que teve a sua consagração nos artigos 6.º e 13.º da Convenção Europeia dos Direitos do Homem.». A existência de um recurso judicial encontra-se igualmente prevista no artigo 47.º da Carta dos Direitos Fundamentais da União Europeia e no artigo 22.º da Directiva 95/46/CE, sem prejuízo de quaisquer recursos administrativos.

11. Decisões individuais automatizadas

78. A AEPD saúda a disposição que prevê salvaguardas adequadas em caso de tratamento automatizado de dados pessoais. A AEPD regista que as condições de aplicação deste princípio seriam esclarecidas mediante um entendimento comum do que é considerado uma acção adversa significativa contra os interesses relevantes de um particular.

12. Transferências para outros países

79. Nalguns casos, não estão bem esclarecidas as condições a que devem obedecer as transferências de informação para outros países. Em especial, quando a transferência deve obedecer às disposições de acordos e convénios internacionais entre o país emissor e o país receptor, dever-se-ia especificar se se trata de acordos entre os dois países que efectuaram a primeira transferência ou entre os dois países envolvidos na transferência em questão. No entender da AEPD, será sempre necessário um acordo entre os dois países que procedem à primeira transferência.

80. A AEPD regista também uma definição muito ampla dos legítimos interesses públicos que justificam a transferência. Há falta de clareza quanto à segurança pública, parecendo também injustificada e excessiva, num contexto de execução da lei, a extensão das transferências em caso de atentado contra a ética ou as profissões regulamentadas.

VI. **CONCLUSÃO**

81. A AEPD saúda o trabalho conjunto levado a cabo pelas autoridades da UE e dos EUA no domínio da aplicação da lei, em que a protecção de dados é fundamental. No entanto, a AEPD insiste em que se trata de uma questão complexa, em especial no que diz respeito à precisão do respectivo âmbito e natureza, pelo que merece uma análise cuidadosa e aprofundada. Deverá ser cuidadosamente

([24]) Processo 22/84 *Johnston* [1986], Colect., p. 1651; Processo 222/86 *Heylens* [1987], Colect., p. 4097; Processo C-97/91 *Borelli* [1992] Colect., p. I-6313.

apreciado o impacto de um instrumento transatlântico em matéria de protecção de dados tanto para os cidadãos como relativamente ao quadro jurídico actualmente em vigor.

82. A AEPD exige maior clareza e disposições concretas, especialmente no que toca aos seguintes aspectos:

— Clarificação da natureza do instrumento, que deveria ser juridicamente vinculativo para assegurar suficiente certeza jurídica;

— Uma minuciosa averiguação da adequação, com base nos requisitos essenciais em matéria de conteúdo e especificidade do regime e quanto aos seus aspectos que se prendem com a supervisão. A AEPD considera que apenas se poderá reconhecer a adequação do instrumento geral se combinada com acordos específicos numa base caso a caso;

— Um âmbito de aplicação bem delimitado, acompanhado de uma clara definição comum dos objectivos da aplicação da lei;

— Precisão das modalidades da eventual participação de entidades privadas nas transferências de dados;

— Observância do princípio da proporcionalidade, o que implica que o intercâmbio de dados se faça caso a caso, a partir de uma necessidade concreta;

— Existência de mecanismos eficazes de supervisão e de possibilidades de recurso para as pessoas em causa, nomeadamente o recurso judicial e administrativo;

— Medidas eficazes que garantam a todas as pessoas em causa o exercício dos respectivos direitos, independentemente da sua nacionalidade;

— Participação de autoridades independentes em matéria de protecção de dados, especialmente no que diz respeito à supervisão e à assistência às pessoas interessadas.

83. A AEPD insiste na necessidade de evitar qualquer precipitação ao definir os princípios, o que só poderia conduzir a soluções pouco satisfatórias e a um efeito contraproducente em termos de protecção de dados. A melhor maneira de avançar seria pois desenvolver um roteiro com vista a um possível acordo numa fase posterior.

84. A AEPD exige também maior transparência para o processo de definição dos princípios da protecção de dados. Só com a participação de todas as partes interessadas, nomeadamente o Parlamento Europeu, poderá este instrumento granjear, através de um debate democrático, o necessário apoio e reconhecimento.

Feito em Bruxelas, em 11 de Novembro de 2008.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

Parecer da Autoridade Europeia para a Protecção de Dados sobre a comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu — Rumo a uma estratégia europeia em matéria de e-Justice

(2009/C 128/02)

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, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados ([1]),

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados ([2]), nomeadamente o artigo 41.º,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 30 de Maio de 2008, foi aprovada a comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu «Rumo a uma estratégia europeia em matéria de e-Justice» (a seguir designada por «comunicação»). A AEPD apresenta o presente parecer nos termos do artigo 41.º do Regulamento (CE) n.º 45/2001.

2. A comunicação visa propor uma estratégia em matéria de justiça electrónica que pretende aumentar a confiança dos cidadãos no Espaço Europeu de Justiça. A justiça electrónica deverá ter por principal objectivo contribuir para que a justiça seja administrada de forma mais eficaz em toda a Europa, em benefício dos cidadãos. A acção da UE deverá permitir aos cidadãos aceder à informação, sem a oposição das barreiras linguísticas, culturais e jurídicas decorrentes da multiplicidade dos sistemas existentes. Do anexo à comunicação constam um projecto de plano de acção e um calendário para os vários projectos.

3. No presente parecer da AEPD são aduzidas observações à comunicação, na medida em que esta se prende com o tratamento de dados pessoais, a protecção da privacidade no sector das comunicações electrónicas e a livre circulação de dados.

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

II. ANTECEDENTES E CONTEXTO

4. Em Junho de 2007, o Conselho JAI ([3]) identificou uma série de prioridades com o objectivo de desenvolver a justiça electrónica:

   — criação de uma interface europeia, o portal de justiça electrónica;

   — criação de condições para permitir a ligação em rede de vários registos, designadamente registos criminais, registos de insolvências, registos comerciais e de empresas e registos prediais;

   — início dos preparativos para a utilização das TIC no âmbito do procedimento europeu de injunção de pagamento;

   — reforço da utilização da tecnologia da videoconferência em processos transfronteiriços, designadamente em matéria de obtenção de provas;

   — desenvolvimento de ferramentas de apoio à interpretação e à tradução.

5. Desde então, os trabalhos sobre a justiça electrónica registaram sólidos progressos. No entender da Comissão, os trabalhos desenvolvidos neste contexto devem assegurar que seja dada prioridade a projectos operacionais e a estruturas descentralizadas, garantindo ao mesmo tempo a coordenação a nível europeu, devem basear-se nos instrumentos jurídicos em vigor e utilizar ferramentas informáticas para melhorar a sua eficácia. O Parlamento Europeu exprimiu igualmente o seu apoio ao projecto de justiça electrónica ([4]).

6. A Comissão sempre encorajou a utilização das modernas tecnologias da informação tanto no domínio civil como penal, o que deu origem a instrumentos como a ordem de pagamento europeia. Desde 2003, tem vindo a gerir o «portal» da Rede Judiciária Europeia em Matéria Civil e Comercial, acessível aos cidadãos em 22 línguas. A Comissão também criou e estabeleceu o Atlas Judiciário Europeu. Estes instrumentos são elementos precursores de um futuro quadro europeu da justiça electrónica. No domínio penal, a Comissão trabalhou sobre um instrumento destinado a permitir o intercâmbio de informações extraídas do registo criminal entre os Estados-Membros ([5]). Tanto a Comissão como a Eurojust desenvolveram sistemas de comunicação securizados com as autoridades nacionais.

([3]) Doc. 10393/07 JURINFO 21.
([4]) Cf. projecto de relatório da Comissão dos Assuntos Jurídicos do Parlamento Europeu.
([5]) Cf., designadamente, o sistema ECRIS a seguir referido.

7. Nos próximos anos, a justiça electrónica tenciona proporcionar muitas oportunidades para tornar o espaço judiciário europeu uma realidade concreta para os cidadãos. A fim de definir uma estratégia global nesta importante matéria, a Comissão adoptou a presente comunicação sobre justiça electrónica, na qual estabelece critérios objectivos para identificar prioridades, nomeadamente para futuros projectos a nível europeu, a fim de alcançar resultados concretos num prazo razoável.

8. O documento de trabalho dos serviços da Comissão — documento anexo à comunicação — que contém um resumo da avaliação de impacto, inclui também algumas informações de fundo ([6]). O relatório da avaliação de impacto foi preparado tendo em conta os contributos dos Estados-Membros, das autoridades judiciárias, dos profissionais da justiça, dos cidadãos e das empresas. A AEPD não foi consultada. O relatório da avaliação de impacto deu preferência a uma opção política de abordagem dos problemas que alia a dimensão europeia à competência nacional. A comunicação escolheu esta opção política. A estratégia centrar-se-á na utilização da videoconferência, na criação do portal de justiça electrónica, no aperfeiçoamento dos dispositivos de ajuda à tradução, graças ao desenvolvimento de ferramentas de tradução automática em linha, no aperfeiçoamento da comunicação entre autoridades judiciárias e em ferramentas em linha para os procedimentos europeus (por exemplo, o procedimento europeu de injunção de pagamento).

9. A AEPD apoia o enfoque dado às acções acima mencionadas. Em termos gerais, defende uma abordagem global da justiça electrónica. Subscreve a tripla necessidade de se melhorar o acesso à justiça, a cooperação entre as autoridades judiciárias europeias e a eficácia do próprio sistema de justiça. Esta abordagem afecta uma série de instituições e pessoas:

— os Estados-Membros, a quem cabe a responsabilidade principal de garantir sistemas de justiça eficazes e dignos de confiança;

— a Comissão Europeia, enquanto guardiã dos Tratados;

— as autoridades judiciárias dos Estados-Membros, que necessitam de ferramentas de comunicação mais sofisticadas, nomeadamente em casos transfronteiras;

— os profissionais da justiça, os cidadãos e as empresas, que solicitam uma melhor utilização das ferramentas informáticas tendo em vista obter respostas mais satisfatórias às suas necessidades de «justiça».

10. A comunicação está intimamente ligada à proposta de decisão do Conselho relativa à criação do sistema europeu de informação sobre os registos criminais (ECRIS). Em 16 de Setembro de 2008, a AEPD aprovou um parecer sobre esta proposta ([7]) que apoiou, desde que se atendesse a uma série de considerações. A AEPD assinalou, concretamente, que devem ser as garantias adicionais em matéria de protecção de dados a compensar o facto de não existir um quadro jurídico global sobre protecção de dados no domínio da cooperação entre as autoridades policiais e judiciárias. Salientou assim que é necessária uma coordenação eficaz no controlo da protecção de dados do sistema, que envolva as autoridades dos Estados-Membros e a Comissão, na qualidade de fornecedora da infra-estrutura comum de comunicações.

11. Eis algumas recomendações desse parecer que vale a pena evocar:

— Deve fazer-se referência a um elevado nível de protecção de dados como condição prévia das medidas de execução a adoptar;

— Deve ser elucidada a responsabilidade da Comissão pela infra-estrutura comum do sistema, bem como pela aplicabilidade do Regulamento (CE) n.º 45/2001, para melhor garantir a segurança jurídica;

— A responsável pela aplicação informática de ligação também deve ser a Comissão, e não os Estados-Membros, por forma a melhorar a eficácia do intercâmbio e a permitir um melhor controlo do sistema;

— A utilização de traduções automáticas deve ser definida e circunscrita com clareza, para facilitar a compreensão mútua das infracções penais sem afectar a qualidade da informação transmitida.

12. Estas recomendações são ainda esclarecedoras para o contexto em que a actual comunicação vai ser analisada.

III. **O INTERCÂMBIO DE INFORMAÇÃO PREVISTO NA COMUNICAÇÃO**

13. A justiça electrónica tem um âmbito de aplicação muito vasto, que inclui de um modo geral a utilização das TIC na administração da justiça na União Europeia. Abrange várias questões, como projectos que facultam informações aos litigantes de um modo mais eficaz, nas quais se incluem informações em linha sobre os sistemas jurídicos, a legislação e a jurisprudência, sistemas de comunicação electrónica entre os litigantes e os tribunais, bem como a

([6]) Documento de trabalho dos serviços da Comissão — Documento anexo à Comunicação ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu «Rumo a uma estratégia europeia em matéria de e Justice» — Resumo da avaliação de impacto de 30.5.2008, SEC(2008) 1944.

([7]) Cf. o parecer da AEPD sobre a criação do sistema europeu de informação sobre os registos criminais (ECRIS) em aplicação do artigo 11.º da Decisão-Quadro 2008/XX/JAI, disponível no sítio web da AEPD, www.edps.europa.eu, «consultation» e, a seguir, «opinions», «2008».

criação de procedimentos totalmente electrónicos. Abrange ainda projectos europeus, como o recurso aos meios de registo electrónico das audiências, e projectos que envolvem interligações ou o intercâmbio de informação.

14. Apesar de o âmbito de aplicação ser muito vasto, a AEPD apercebeu-se de que haverá informações sobre processos penais e sobre os sistemas judiciários em matéria civil e comercial, mas não sobre os sistemas jurídico-administrativos. Também haverá uma ligação a um Atlas em matéria penal e civil, mas não a um Atlas em matéria administrativa, embora fosse preferível os cidadãos e as empresas poderem ter acesso aos sistemas jurídico-administrativos, isto é a procedimentos de direito administrativo e de recurso administrativo. Também se deveria prever uma ligação à Associação dos Conselhos de Estado. Se existissem mais estas ligações, os cidadãos que tentam orientar-se no emaranhado do direito administrativo e todos os seus tribunais poderiam ficar mais bem informados sobre os sistemas jurídico-administrativos.

15. Por isso, a AEPD recomenda que os procedimentos administrativos sejam incluídos na justiça electrónica. Como parte deste novo elemento, deverão iniciar-se os projectos em matéria de justiça electrónica para aumentar a visibilidade das regras aplicáveis à protecção de dados e das autoridades nacionais responsáveis pela protecção de dados, especialmente no tocante ao tipo de dados tratados no âmbito da justiça electrónica, o que estaria em consonância com a chamada «Iniciativa de Londres», lançada pelas autoridades responsáveis pela protecção de dados, em Novembro de 2006, com o objectivo de «divulgar a protecção de dados e torná-la mais eficaz».

IV. **A NOVA DECISÃO-QUADRO RELATIVA À PROTECÇÃO DOS DADOS PESSOAIS TRATADOS NO ÂMBITO DA COOPERAÇÃO POLICIAL E JUDICIÁRIA EM MATÉRIA PENAL**

16. Com o crescente intercâmbio de dados pessoais entre as autoridades judiciárias previsto na comunicação, o quadro jurídico aplicável em matéria de protecção de dados reveste-se ainda de maior importância. Neste contexto, a AEPD constata que, três anos volvidos sobre a proposta inicial da Comissão, o Conselho da União Europeia aprovou, em 27 de Novembro, a decisão-quadro relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal ([8]). Este novo acto legislativo proporcionará um quadro jurídico geral no que respeita à protecção de dados aplicável às questões do «terceiro pilar», para além das disposições sobre protecção de dados aplicáveis ao «primeiro pilar», previstas na Directiva 95/46/CE.

17. A AEPD acolhe com agrado este instrumento jurídico, que constitui um primeiro avanço significativo para a protecção de dados em matéria de cooperação policial e judiciária. Todavia, o nível de protecção de dados obtido no texto final não é totalmente satisfatório. Concretamente, a decisão-quadro abrange apenas os dados policiais e judiciários trocados entre os Estados-Membros, as autoridades e os sistemas da UE, e não inclui os dados nacionais. Além disso, a decisão-quadro aprovada não estabelece a obrigação de distinguir as diferentes categorias de pessoas a que os dados dizem respeito, como sejam os suspeitos, os criminosos, as testemunhas e as vítimas, de molde a assegurar que os respectivos dados sejam tratados com garantias mais adequadas. Não é totalmente coerente com a Directiva 95/46/CE, nomeadamente no tocante à limitação das finalidades para as quais é possível um tratamento ulterior dos dados. Também não prevê um grupo independente constituído pelas autoridades nacionais e da UE competentes e responsáveis pela protecção de dados, que possa assegurar uma melhor coordenação entre as autoridades responsáveis pela protecção de dados e contribuir significativamente para a aplicação uniforme da decisão-quadro.

18. Isto significaria que, num contexto em que tantos esforços estão a ser envidados para desenvolver sistemas comuns de intercâmbio transfronteiriços de dados pessoais, continua a haver divergências em relação às normas de acordo com as quais esses dados são tratados e os cidadãos podem exercer os seus direitos nos vários países da UE.

19. A AEPD recorda uma vez mais que a garantia de um elevado nível de protecção de dados em matéria de cooperação policial e judiciária, bem como a coerência com a Directiva 95/46/CE, constitui um complemento necessário às demais medidas introduzidas ou previstas para facilitar o intercâmbio transfronteiriço de dados pessoais na aplicação da lei. Isto decorre não só do direito que assiste aos cidadãos de que seja respeitado o direito fundamental à protecção de dados pessoais, mas também da necessidade de as autoridades de aplicação da lei garantirem a qualidade dos dados trocados — tal como é confirmado pelo anexo da comunicação no que respeita à interligação de registos criminais —, de haver confiança entre as autoridades dos diferentes países e, em última análise, da validade jurídica das provas obtidas num contexto transfronteiriço.

20. Por isso, a AEPD incita as instituições da UE a terem concretamente em conta estes elementos, não só quando aplicarem as medidas previstas na comunicação, mas também na perspectiva de iniciarem logo que possível uma reflexão sobre novas melhorias do quadro jurídico para a protecção de dados na aplicação da lei.

V. **PROJECTOS NO DOMÍNIO DA JUSTIÇA ELECTRÓNICA**

Instrumentos de justiça electrónica a nível europeu

21. A AEPD reconhece que os intercâmbios de dados pessoais são elementos essenciais da criação de um espaço de liberdade, segurança e justiça, razão pela qual apoia a proposta de estratégia em matéria de justiça electrónica, ao mesmo tempo que salienta a importância da protecção dos dados neste contexto. Com efeito, o respeito pela protecção dos dados constitui não só uma obrigação jurídica, como um elemento fundamental para o êxito dos sistemas previstos,

([8]) Ainda aguarda a publicação no Jornal Oficial da União Europeia.

por exemplo, para assegurar a qualidade dos intercâmbios de dados. Isto também é válido para as instituições e para os órgãos quando procedem ao tratamento de dados pessoais e quando definem novas políticas. As normas e os princípios devem ser aplicados e seguidos na prática e tidos especialmente em conta nas fases de concepção e construção dos sistemas de informação. A privacidade e a protecção dos dados são essencialmente «factores fundamentais para o êxito» de uma sociedade da informação próspera e equilibrada, pelo que faz todo o sentido investir nelas o mais cedo possível.

22. Neste contexto, a AEPD sublinha que a comunicação não prevê uma base de dados central europeia e saúda a preferência por arquitecturas descentralizadas. A AEPD recorda que deu parecer sobre o ECRIS ([9]) e sobre a Iniciativa de Prüm ([10]) No parecer sobre o ECRIS, a AEPD declarou que uma arquitectura descentralizada evita uma duplicação adicional de dados pessoais na base de dados central. No parecer sobre a Iniciativa de Prüm, advertiu para que fosse tomada na devida conta a dimensão do sistema quando fosse analisada a interligação das bases de dados. Concretamente, há que estabelecer formatos específicos para a comunicação de dados, como pedidos de registos criminais em linha, tendo também em conta as diferenças linguísticas, e controlar permanentemente a exactidão dos intercâmbios de dados. Estes elementos também devem ser tidos em conta no contexto das iniciativas decorrentes da estratégia em matéria de justiça electrónica.

23. A Comissão Europeia tenciona contribuir para o reforço e o desenvolvimento de instrumentos de justiça electrónica a nível europeu, em estreita articulação com os Estados-Membros e outros parceiros. Ao mesmo tempo que apoia os esforços dos Estados-Membros, a Comissão tenciona desenvolver uma série de ferramentas informáticas. Estas permitirão reforçar a interoperabilidade dos sistemas, facilitar o acesso do público à justiça e a comunicação entre as autoridades judiciárias, bem como substanciais economias de escala a nível europeu. Quanto à interoperabilidade das aplicações informáticas utilizadas pelos Estados-Membros, nem todos devem utilizar necessariamente a mesma aplicação informática (software), (embora fosse essa a solução mais prática), mas a aplicação informática deve ser totalmente interoperável.

24. A AEPD recomenda que a interligação e a interoperabilidade dos sistemas tenham devidamente em conta o princípio da limitação da finalidade e se baseiem em normas de protecção de dados («privacidade na concepção»). Qualquer forma de interacção entre sistemas diferentes deverá ser exaustivamente documentada. A interoperabilidade nunca deve conduzir a uma situação em que uma autoridade não habilitada a aceder ou a utilizar determinados dados possa obter esse acesso através de outro sistema de informação. A AEPD deseja salientar uma vez mais que a interoperabilidade não deverá justificar por si só que se contorne o princípio da limitação da finalidade ([11]).

25. Além disso, outro ponto essencial consiste em assegurar que o reforço do intercâmbio transfronteiras de dados pessoais seja acompanhado de um reforço do controlo e da cooperação por parte das autoridades responsáveis pela protecção de dados. No seu parecer, de 29 de Maio de 2006, sobre a decisão-quadro do Conselho relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal ([12]), a AEPD já salientara que a decisão-quadro proposta deveria abordar não só a cooperação entre as autoridades centrais, mas também a cooperação entre as várias autoridades competentes responsáveis pela protecção de dados. Esta necessidade tornou-se ainda mais importante desde que as negociações sobre a decisão-quadro relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal ([13]), recentemente aprovada, levaram à supressão da disposição que estabelecia um grupo de trabalho constituído pelas autoridades responsáveis pela protecção de dados na UE, encarregado de coordenar as actividades das referidas autoridades no que respeita ao tratamento dos dados no âmbito da cooperação policial e judiciária em matéria penal. Por conseguinte, a fim de assegurar um controlo eficaz e a boa qualidade da circulação transfronteiriça dos dados extraídos dos registos criminais, há que estabelecer mecanismos que permitam uma coordenação eficaz entre as autoridades responsáveis pela protecção de dados ([14]). Esses mecanismos também deverão ter em conta a competência de controlo que incumbe à AEPD no que respeita à infra-estrutura da rede S-TESTA ([15]). Os instrumentos de justiça electrónica podem apoiar esses mecanismos, que poderão ser desenvolvidos em estreita cooperação com as autoridades responsáveis pela protecção de dados.

26. No ponto 4.2.1 da comunicação, assinala-se que será importante que os intercâmbios de informações extraídas dos registos criminais se alarguem para além da cooperação judiciária e integrem outros objectivos (por exemplo, o acesso a determinadas profissões). A AEPD salienta que qualquer tratamento de dados pessoais para fins que não sejam aqueles para que foram recolhidos deverá respeitar as condições específicas estabelecidas na legislação aplicável

([9]) Ver nota 4, § 18.
([10]) JO C 89 de 10.4.2008, p. 4.
([11]) JO C 91 de 19.4.2006, p. 53. Cf. também as observações da AEPD sobre a comunicação da Comissão relativa à interoperabilidade das bases de dados europeias, Bruxelas, 10.3.2006.
([12]) JO C 91 de 26.4.2007, p. 9.
([13]) Cf. capítulo IV, *supra*.
([14]) Cf. parecer da AEPD sobre o ECRIS, pontos 8 e 37-38.
([15]) Cf. pontos 27-28 *infra*.

em matéria de protecção de dados. Em particular, o tratamento de dados pessoais para outros fins só deverá ser permitido se for necessário para os interesses previstos na legislação comunitária sobre protecção de dados ([16]), e desde que estabelecidos através de medidas legislativas.

27. No que respeita à interligação dos registos criminais, lê-se na comunicação que, na perspectiva da entrada em vigor da decisão-quadro relativa ao intercâmbio de informações extraídas do registo criminal, a Comissão lançará dois estudos de viabilidade a fim de organizar a evolução do projecto e alargar o intercâmbio de informações aos nacionais de países terceiros objecto de condenações penais. Em 2009, a Comissão porá à disposição dos Estados-Membros uma aplicação informática para que todos os registos criminais participem nos intercâmbios num prazo rápido. Este sistema de referência, em conjugação com o s-TESTA para o intercâmbio de informações, permitirá realizar economias de escala, evitando que cada Estado-Membro tenha de dispor do seu próprio sistema, e simplificará o funcionamento técnico do projecto.

28. Nesta perspectiva, a AEPD saúda a utilização da infra-estrutura s-TESTA, que provou ser um sistema fiável para o intercâmbio de dados, e recomenda que os elementos estatísticos relacionados com os sistemas de intercâmbio de dados previstos sejam definidos pormenorizadamente e tenham devidamente em conta a necessidade de assegurar o controlo da protecção de dados. Por exemplo, os dados estatísticos poderão incluir explicitamente elementos como o número de pedidos de acesso a dados pessoais ou de rectificação dos mesmos, a duração e o completamento do processo de actualização, a qualidade das pessoas que têm acesso a esses dados e os casos de violações da segurança. Além disso, os dados estatísticos e os relatórios neles baseados deverão ser integralmente disponibilizados às autoridades competentes em matéria de protecção de dados.

Tradução automática e base de dados dos tradutores

29. A tradução automática constitui um instrumento útil e pode facilitar a compreensão mútua entre os interlocutores pertinentes dos Estados-Membros. Todavia, o recurso à tradução automática não deve resultar numa menor qualidade das informações trocadas, especialmente quando essas informações forem utilizadas para a tomada de decisões que tenham efeitos jurídicos para os interessados. A AEPD assinala que é importante definir claramente e circunscrever a utilização da tradução automática. O recurso à tradução automática para transmitir informações que não tenham sido rigorosamente pré-traduzidas, tais como comentários ou especificações suplementares aditados em casos particulares, é susceptível de afectar a qualidade das informações transmitidas — e, portanto, das decisões tomadas com base nelas —, pelo que é, em princípio, de excluir ([17]). A AEPD sugere que esta recomendação seja tida em conta nas medidas decorrentes da comunicação.

30. A comunicação pretende criar uma base de dados de tradutores e intérpretes jurídicos para melhorar a qualidade da tradução e interpretação jurídicas. A AEPD subscreve esse objectivo, embora recorde que essa base de dados estará sujeita à aplicação da legislação pertinente em matéria de protecção de dados. Em particular, se a base de dados contiver elementos de avaliação sobre o desempenho dos tradutores, poderá ser objecto de um controlo prévio pelas autoridades competentes em matéria de protecção de dados.

Rumo a um plano de acção europeu de justiça electrónica

31. No ponto 55, a comunicação assinala que é necessário proceder a uma clara repartição das responsabilidades entre a Comissão, os Estados-Membros e os outros intervenientes da cooperação judiciária. A Comissão assumirá o papel geral de coordenação, favorecendo os intercâmbios de boas práticas e trabalhará a nível da concepção e criação do portal e-Justice. Além disso, a Comissão tenciona prosseguir os trabalhos sobre a ligação entre registos criminais e continuará a assumir a responsabilidade directa pela Rede Judiciária em matéria civil e a apoiar a Rede Judiciária em matéria penal. Os Estados-Membros deverão assegurar a actualização das informações relativas aos respectivos sistemas de justiça que constam do sítio da justiça electrónica. Outros intervenientes são as redes judiciárias em matéria civil e penal, bem como a Eurojust. Desenvolverão, em estreito contacto com a Comissão, os instrumentos necessários a uma cooperação judiciária mais eficaz, em especial os instrumentos de tradução automática e um sistema de intercâmbio seguro. Do anexo à comunicação constam um projecto de plano de acção e um calendário para os vários projectos.

32. Neste contexto, a AEPD salienta que no sistema ECRIS, por um lado, não se prevê qualquer base de dados central a nível europeu nem o acesso directo às bases de dados dos registos criminais dos outros Estados-Membros, enquanto que, por outro lado, a nível nacional, a responsabilidade pelas informações correctas se encontra centralizada nas autoridades centrais dos Estados-Membros. No âmbito deste mecanismo, os Estados-Membros são responsáveis pelo funcionamento das bases de dados nacionais dos registos criminais e pela eficácia dos intercâmbios. Não é claro se também são ou não responsáveis pela aplicação informática de ligação. A Comissão porá à disposição dos Estados-Membros uma aplicação informática para que todos os registos criminais participem nos intercâmbios num prazo rápido. Este sistema de referência será conjugado com o s-TESTA para o intercâmbio de informação.

33. A AEPD entende que, também no contexto de iniciativas análogas à justiça electrónica, poderão ser implementados

([16]) Cf. especialmente o artigo 13.º da Directiva 95/46/CE e o artigo 20.º do Regulamento (CE) n.º 45/2001.

([17]) Cf. pontos 39-40 do parecer da AEPD sobre o ECRIS.

sistemas similares, sendo a Comissão responsável pela infra-estrutura comum, embora isto não esteja precisado na comunicação. Por uma questão de segurança jurídica, a AEPD sugere que essa responsabilidade seja clarificada nas medidas decorrentes da comunicação.

Projectos no domínio da justiça electrónica

34. Do anexo consta uma série de projectos a desenvolver nos próximos cinco anos. O primeiro, o desenvolvimento das páginas e-Justice, é sobre o portal de justiça electrónica. A acção carece de um estudo de viabilidade e do desenvolvimento do portal. Além disso, carece da implementação de métodos de gestão e de informações em linha em todas as línguas da UE. Os segundo e terceiro projectos dizem respeito à interligação dos registos criminais. O projecto 2 é sobre a interligação dos registos criminais nacionais. O projecto 3 prevê que, após a apresentação de um estudo de viabilidade e de uma proposta legislativa, seja criado um registo europeu de cidadãos condenados de países terceiros. A AEPD constata que este último projecto deixou de ser referido no programa de trabalho da Comissão e pergunta se isso reflecte uma alteração nas previsões de projectos da Comissão, ou apenas um adiamento deste projecto específico.

35. A comunicação enumera ainda três projectos no domínio dos intercâmbios electrónicos e três projectos no domínio da ajuda à tradução. Dar-se-á início a um projecto-piloto sobre a criação progressiva de um vocabulário jurídico multilingue comparado. Outros projectos pertinentes dizem respeito à criação de formulários dinâmicos que acompanham os textos legislativos europeus e a um maior recurso à videoconferência por parte das autoridades judiciárias. Por último, como parte dos fóruns de justiça electrónica, serão realizadas reuniões anuais sobre a temática da justiça electrónica e desenvolver-se-á a formação de profissionais da justiça em cooperação judiciária. A AEPD sugere que essas reuniões e formações prestem especial atenção à legislação e às práticas no que respeita à protecção de dados.

36. O anexo prevê, assim, um vasto leque de instrumentos europeus com o intuito de facilitar o intercâmbio de informações entre os intervenientes dos vários Estados-Membros. Destes instrumentos, o portal de justiça electrónica, cujo principal responsável será a Comissão, desempenhará um papel importante.

37. Uma característica comum de muitos destes instrumentos será o facto de as informações e os dados pessoais serem intercambiados e geridos por diferentes intervenientes tanto a nível nacional como da UE, sujeitos às obrigações em matéria de protecção de dados e às autoridades de controlo criadas com base na Directiva 95/46/CE ou no Regulamento (CE) n.º 45/2001. A este propósito, como a AEPD já frisou bem no seu parecer sobre o Sistema de Informação do Mercado Interno (IMI) ([18]), é essencial velar por que as responsabilidades no tocante à observância das normas em matéria de protecção de dados sejam asseguradas de forma eficiente e harmoniosa.

38. Para tal, é necessário, por um lado, que seja definida e atribuída claramente a responsabilidade pelo tratamento de dados pessoais no âmbito destes sistemas e, por outro, que sejam estabelecidos os mecanismos de coordenação adequados — especialmente no que respeita ao controlo — sempre que necessário.

39. A utilização das novas tecnologias constitui uma das pedras angulares das iniciativas em matéria de justiça electrónica: interligação dos registos nacionais, desenvolvimento da assinatura electrónica, redes seguras, plataformas virtuais de intercâmbio e uma maior utilização da videoconferência serão elementos essenciais das iniciativas em matéria de justiça electrónica durante os próximos anos.

40. Neste contexto, é essencial que as questões relativas à protecção de dados sejam tidas em conta o mais cedo possível e integradas na arquitectura dos instrumentos previstos. Em particular, tanto a arquitectura do sistema como a aplicação das medidas de segurança adequadas são especialmente importantes. Esta abordagem de «privacidade na concepção» permitiria que as iniciativas em matéria de justiça electrónica pertinentes previssem a gestão eficaz dos dados pessoais ao mesmo tempo que garantissem o respeito pelos princípios de protecção de dados e a segurança dos intercâmbios de dados entre as diferentes autoridades.

41. Além disso, a AEPD salienta que os instrumentos tecnológicos devem ser usados não só para assegurar o intercâmbio de informações, mas também para reforçar os direitos das pessoas em causa. Nesta perspectiva, a AEPD congratula-se com o facto de a comunicação se referir à possibilidade de os cidadãos requererem os seus registos criminais em linha e na língua à sua escolha ([19]). No que respeita a esta questão, a AEPD recorda que, no seu parecer sobre a proposta da Comissão relativa ao intercâmbio de informações extraídas do registo criminal, se congratulou com a possibilidade de a pessoa em causa solicitar informações sobre o seu registo criminal à autoridade central de um Estado-Membro, desde que seja ou tenha sido residente ou nacional do Estado-Membro requerente ou requerido. No domínio da coordenação dos regimes de segurança social, a AEPD também preconizou que se utilizasse como «balcão único» a autoridade que está mais perto da pessoa em causa. Por isso, incentiva a Comissão a prosseguir

([18]) JO C 270 de 25.10.2008, p. 1.
([19]) Cf. página 6 da comunicação.

por este caminho, fomentando os instrumentos tecnológicos, nomeadamente o acesso em linha, e permitindo que os cidadãos controlem melhor os seus dados pessoais mesmo quando se deslocam entre diferentes Estados-Membros.

VI. **CONCLUSÕES**

42. A AEPD apoia a presente proposta de criação da justiça electrónica e recomenda que sejam tidas em conta as observações aduzidas no presente parecer, nomeadamente:

— Ter em conta a recente decisão-quadro relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal — incluindo as suas deficiências — não só aquando da aplicação das medidas previstas na comunicação, mas também na perspectiva de se iniciar logo que possível a reflexão sobre novas melhorias do quadro jurídico para a protecção de dados na aplicação da lei;

— Incluir os processos administrativos na justiça electrónica. Como parte deste novo elemento, deve dar-se início aos projectos em matéria de justiça electrónica para aumentar a visibilidade das regras aplicáveis à protecção de dados e das autoridades nacionais responsáveis pela protecção de dados, especialmente no que respeita ao tipo de dados tratados no âmbito dos projectos em matéria de justiça electrónica;

— Manter a preferência por arquitecturas descentralizadas;

— Assegurar que a interligação e interoperabilidade dos sistemas tenham devidamente em conta o princípio da limitação da finalidade;

— Atribuir responsabilidades claras a todos os que procedam ao tratamento de dados pessoais no âmbito dos sistemas previstos e estabelecer mecanismos que permitam uma coordenação eficaz entre as autoridades responsáveis pela protecção de dados;

— Assegurar que o tratamento de dados pessoais para fins que não sejam aqueles para que foram recolhidos respeite as condições específicas estabelecidas na legislação aplicável no tocante à protecção de dados;

— Definir e circunscrever com clareza a utilização de traduções automáticas, para facilitar a compreensão mútua das infracções penais sem afectar a qualidade da informação transmitida;

— Clarificar a responsabilidade da Comissão pela infra-estrutura comum, como o s-TESTA;

— No que respeita à utilização das novas tecnologias, assegurar que as questões relativas à protecção de dados sejam tidas em conta o mais cedo possível («privacidade na concepção»), bem como fomentar os instrumentos tecnológicos permitindo que os cidadãos controlem melhor os seus dados pessoais mesmo quando se deslocam entre diferentes Estados-Membros.

Feito em Bruxelas, em 19 Dezembro de 2008.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

Projecto de parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.

(2009/C 128/03)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, e nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,

Tendo em conta o 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, e nomeadamente o artigo 41.º,

Tendo em conta o pedido de parecer apresentado pela Comissão nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, enviado à AEPD em 2 de Julho de 2008,

ADOPTOU O SEGUINTE PARECER:

I. **INTRODUÇÃO**

A proposta de directiva relativa à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços

1. Em 2 de Julho de 2008, a Comissão adoptou a proposta de directiva do Parlamento Europeu e do Conselho relativa à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (a seguir: «a proposta») [1]. A proposta foi enviada pela Comissão à AEPD para consulta, nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001.

2. A proposta visa instituir um quadro comunitário para a prestação de cuidados de saúde transfronteiriços na UE, nos casos em que os cuidados de saúde procurados pelos doentes venham a ser prestados num Estado-Membro que não seja o país de residência. Articula-se em torno de três grandes áreas:

   — a definição de princípios comuns a todos os sistemas de saúde da UE, que definam claramente as responsabilidades dos Estados-Membros;

   — o desenvolvimento de um quadro específico para os cuidados de saúde transfronteiriços que elucide os direitos dos doentes a receberem cuidados de saúde noutro Estado-Membro;

   — a promoção da cooperação da UE em matéria de cuidados de saúde, em áreas como o reconhecimento das receitas médicas emitidas noutros países, as redes europeias de referência, a avaliação das tecnologias da saúde, a recolha, qualidade e segurança dos dados.

3. Este quadro possui um duplo objectivo: esclarecer suficientemente os direitos a reembolso por cuidados de saúde recebidos noutros Estados-Membros, e assegurar os requisitos necessários à prestação de cuidados de saúde seguros, eficazes e de elevada qualidade nos cuidados transfronteiriços.

4. A implementação de um sistema de cuidados de saúde transfronteiriços exige o intercâmbio dos dados pessoais pertinentes respeitantes à saúde (a seguir: «dados relativos à saúde») dos doentes entre as organizações autorizadas e os profissionais dos cuidados de saúde dos diferentes Estados-Membros. Estes dados são considerados sensíveis e subordinam-se às regras mais estritas de protecção dos dados consignadas no artigo 8.º da Directiva 95/46/CE sobre categorias especiais de dados.

Consulta da AEPD

5. A AEPD regista com agrado o facto de ser consultado sobre esta questão e o de ser feita referência a essa consulta no preâmbulo da proposta, de harmonia com o artigo 28.º do Regulamento (CE) n.º 45/2001.

6. É a primeira vez que a AEPD é consultada oficialmente sobre uma proposta de directiva no domínio dos cuidados de saúde. No presente parecer, algumas das observações feitas são pois de âmbito mais geral, abordando questões genéricas da protecção dos dados pessoais no sector da saúde, que poderiam também ser aplicáveis a outros instrumentos jurídicos pertinentes (vinculativos ou não vinculativos).

[1] COM(2008) 414 Final. Note-se que uma comunicação complementar sobre um quadro comunitário relativo à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços [COM(2008) 415 final] foi também adoptada na mesma data. Contudo, dado que a comunicação tem uma natureza assaz genérica, a AEPD optou por se concentrar na directiva proposta.

7. Logo à partida, a AEPD gostaria de exprimir o seu apoio às iniciativas de melhoria das condições dos cuidados de saúde transfronteiriços. Esta proposta deveria efectivamente ser vista no contexto do programa comunitário global para melhorar a saúde dos cidadãos na sociedade da informação. Outras iniciativas a este respeito são as previstas directiva e comunicação da Comissão sobre doação e transplantes de órgãos humanos ([1]), a recomendação sobre a interoperabilidade dos registos de saúde electrónicos ([2]), assim como a prevista comunicação sobre tele-medicina. ([3]) Preocupa contudo a AEPD o facto de todas estas iniciativas conexas não se encontrarem estreitamente ligadas e/ou interligadas na área da privacidade e da segurança dos dados, tolhendo assim a adopção de uma abordagem uniforme da protecção dos dados nos cuidados de saúde, especialmente no que respeita à utilização de novas tecnologias no domínio das TIC. A título de exemplo, na presente proposta, embora a tele-medicina seja explicitamente referida no considerando 10 da directiva proposta, não é feita qualquer referência à dimensão de protecção dos dados da comunicação pertinente da CE. Acresce que embora os registos de saúde electrónicos sejam uma via possível para a comunicação transfronteiriça de dados relativos à saúde, não é apresentada qualquer ligação com as questões de privacidade abordadas na recomendação pertinente da Comissão. ([4]) Isto dá a impressão de que ainda não está definida, e nalguns casos nem sequer existe, uma perspectiva global da privacidade dos cuidados de saúde.

8. Isto ressalta também da presente proposta, em que a AEPD lamenta constatar que as implicações para a protecção dos dados não são abordadas em termos concretos. É obviamente possível encontrar referências à protecção dos dados, mas estas são sobretudo de natureza genérica e não reflectem adequadamente as necessidades e exigências específicas relacionadas com a privacidade dos cuidados de saúde transfronteiriços.

9. A AEPD deseja salientar que uma abordagem uniforme e sólida da protecção dos dados em todos os instrumentos em matéria de cuidados de saúde propostos não só garantirá o direito fundamental dos cidadãos à protecção dos seus dados, como contribuirá para a futura evolução dos cuidados de saúde transfronteiriços na UE.

II. **PROTECÇÃO DOS DADOS NOS CUIDADOS DE SAÚDE TRANSFRONTEIRIÇOS**

Contexto geral

10. O objectivo mais destacado da Comunidade Europeia tem sido a realização de um mercado interno, um espaço sem fronteiras internas no qual é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais. Permitir que os cidadãos circulem e residam mais facilmente num Estado-Membro diferente do de origem levou obviamente a questões relacionadas com os cuidados de saúde. Por esse motivo, nos anos 90, o Tribunal de Justiça foi confrontado no contexto do mercado interno com questões respeitantes ao eventual reembolso de despesas médicas efectuadas noutro Estado-Membro. O Tribunal de Justiça reconheceu que a liberdade de prestação de serviços, tal como consignada no artigo 49.º do Tratado CE, compreende a liberdade de as pessoas se mudarem para outro Estado-Membro para receberem tratamento médico. ([5]) Nesta lógica, os doentes que quisessem receber cuidados de saúde transfronteiriços não mais poderiam ser tratados de forma distinta dos nacionais nos seus países de origem que tivessem recebido o mesmo tratamento sem atravessarem a fronteira.

11. Estes acórdãos do Tribunal encontram-se no cerne da presente proposta. Uma vez que a jurisprudência do Tribunal se baseia em processos individuais, a presente proposta pretende melhorar a clareza a fim de assegurar uma aplicação mais geral e eficaz das liberdades de receber e prestar serviços de saúde. Mas, como já se referiu, a proposta faz também parte de um programa mais ambicioso cujo propósito é melhorar a saúde dos cidadãos na sociedade da informação, onde a UE vê grandes possibilidades de reforçar os cuidados de saúde transfronteiriços através da utilização das tecnologias da informação.

12. Por razões óbvias, fixar regras para os cuidados de saúde transfronteiriços é um assunto delicado. Toca uma área sensível, em que os Estados-Membros instituíram sistemas nacionais divergentes, por exemplo no que respeita ao seguro e reembolso das despesas ou à organização das infra-estruturas dos cuidados de saúde, incluindo as redes de informação e as aplicações de cuidados de saúde. Embora na proposta em apreço o legislador comunitário se centre apenas nos cuidados de saúde *transfronteiriços*, as regras influenciarão pelo menos a forma como os sistemas nacionais de cuidados de saúde são organizados.

13. A melhoria das condições dos cuidados de saúde transfronteiriços beneficiará os cidadãos. Porém, acarretará ao mesmo tempo alguns riscos para esses cidadãos. Muitos problemas práticos, inerentes à cooperação transfronteiras entre pessoas de países diferentes que falam línguas diferentes, têm de ser resolvidos. dado que uma boa saúde é da maior importância para todos os cidadãos, qualquer risco de comunicação falseada e subsequente inexactidão deve ser obviado. Escusado será dizer que o reforço dos cuidados de saúde transfronteiriços conjugado com a utilização das evoluções das tecnologias da informação tem

([1]) Anunciadas no programa de trabalho da Comissão.
([2]) Recomendação da Comissão de 2 de Julho de 2008 relativa à interoperabilidade transfronteiriça dos sistemas de registos de saúde electrónicos [notificada sob o número C(2008)3282], JO L 190, 18.7.2008, pág. 37.
([3]) Anunciada no programa de trabalho da Comissão.
([4]) É ilustrativo o facto de não figurar qualquer referência à privacidade na Comunicação referida na nota de rodapé 1, que se destina a instituir um quadro comunitário relativo à aplicação dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços.
([5]) Ver Processo 158/96, *Kohll*, [1998] CJ I-1931, ponto 34. Ver também entre outros Processo C-157/99, *Smits e Peerbooms* [2001] CJ I-5473 e Processo C-385/99, *Müller-Fauré e Van Riet* [2003] CJ I-12403.

grandes implicações para a protecção dos dados pessoais. Um intercâmbio dos dados relativos à saúde mais eficaz, e portanto crescente, o aumento da distância entre as pessoas e as instâncias em causa e as diferentes leis nacionais que dão, execução às regras de protecção dos dados, levam a questões de segurança dos dados e de certeza jurídica.

Protecção dos dados relativos à saúde

14. Cabe salientar que os dados relativos à saúde constituem uma categoria especial de dados que merece uma protecção mais elevada. Como recentemente afirmou o Tribunal Europeu dos Direitos do Homem no contexto do artigo 8.º da Convenção Europeia dos Direitos do Homem: «A protecção dos dados pessoais, em especial os dados clínicos, tem uma importância fundamental para o gozo do direito ao respeito pela vida privada e familiar garantido pelo artigo 8.º da Convenção». ([1]) Antes de se exporem as regras mais restritas aplicáveis ao tratamento dos dados relativos à saúde consignadas na Directiva 95/46/CE, aludir-se-á brevemente à noção de «dados relativos à saúde».

15. A Directiva 95/46/CE não contém uma definição explícita de «dados relativos à saúde». Em regra, é aplicada uma interpretação lata que amiúde define os dados relativos à saúde como «dados pessoais que tenham uma ligação clara e estreita com a descrição do estado de saúde de uma pessoa». ([2]) Neste particular, os dados relativos à saúde incluem em regra os dados clínicos (isto é, requisições e receitas ou prescrições médicas, relatórios de exames médicos, testes de laboratório, radiografias, etc.), bem como dados administrativos e financeiros relacionados com a saúde (e.g. documentos respeitantes a admissões hospitalares, número de beneficiário de segurança social, marcações de consultas médicas, requisições para a prestação de cuidados de saúde, etc.). Cumpre assinalar que o termo «dados clínicos» ([3]) é também utilizado por vezes para referir dados relacionados com a saúde, assim como o termo «dados relativos aos cuidados de saúde». ([4]) No presente parecer será utilizada a noção de «dados relativos à saúde».

16. A norma ISO 27799 fornece uma definição útil de «dados relativos à saúde»: «qualquer informação que se relacione com a saúde física ou mental de uma pessoa, ou com a prestação de serviços de saúde a uma pessoa, e que possa incluir: a) informação acerca da inscrição da pessoa para a prestação de serviços de saúde; b) informação acerca de pagamentos ou da elegibilidade para os cuidados de saúde respeitantes à pessoa; c) um número, símbolo ou sinal particular atribuído a uma pessoa para identificar inequivocamente essa pessoa para fins de saúde; d) qualquer informação sobre a pessoa recolhida no decurso da prestação de serviços de saúde a essa pessoa; e) informação obtida a partir de testes ou exames de uma parte do corpo ou de uma substância corporal; e f) identificação de uma pessoa (profissional de saúde) como prestador de cuidados de saúde à pessoa».

17. A AEPD é muito favorável à adopção de uma definição específica do termo «dados relativos à saúde» no contexto da presente proposta que poderia ser igualmente empregue no futuro noutros textos jurídicos comunitários pertinentes (ver secção III *infra*).

18. O artigo 8.º da Directiva 95/46/CE fixa as regras do tratamento de categorias especiais de dados. Essas regras são mais estritas do que as relativas ao tratamento de outros dados, consignadas no artigo 7.º da Directiva 95/46/CE. É o que logo transparece quando o n.º 2 do artigo 8.º declara explicitamente que os Estados-Membros proibirão o tratamento de, designadamente, os dados relativos à saúde. Nos números seguintes do artigo são formuladas várias derrogações a esta proibição, mas que são mais restritivas do que os fundamentos para o tratamento de dados normais tal como definido no artigo 7.º. Por exemplo, a proibição não se aplica se a pessoa em causa tiver dado o seu consentimento *explícito* (alínea a) do n.º 2 do artigo 8.º), ao invés do consentimento *inequívoco* exigido pela alínea a) do artigo 7.º da Directiva 95/46/CE. Além disso, o direito do Estado-Membro pode determinar que em determinados casos nem o consentimento da pessoa em causa pode suspender a proibição. O n.º 3 do artigo 8.º trata exclusivamente do tratamento dos dados relativos à saúde. Segundo este número, a proibição do n.º 1 não se aplica se o processamento for necessário para fins de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos, ou de gestão dos serviços de cuidados de saúde, e quando o tratamento desses dados for efectuado por um profissional da saúde obrigado ao segredo profissional pelo direito nacional ou por regras estabelecidas pelos organismos nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente.

19. O artigo 8.º da Directiva 95/46/CE confere grande destaque ao facto de os Estados-Membros deverem prestar garantias adequadas. O n.º 4 do artigo 8.º, por exemplo, autoriza os Estados-Membros a estabelecerem excepções suplementares à proibição de tratar dados sensíveis por importantes motivos de interesse público, mas sob reserva de garantias adequadas. Isto sublinha em termos genéricos a responsabilidade de os Estados-Membro atribuírem especial atenção a o tratamento de dados sensíveis, como os dados relativos à saúde.

Protecção dos dados relativos à saúde em situações transfronteiriças

Responsabilidades partilhadas entre os Estados-Membros

20. Os Estados-Membros devem estar particularmente cientes da responsabilidade atrás referida uma vez que está em jogo o intercâmbio transfronteiriço de dados relativos à saúde. Tal como acima definido, o intercâmbio transfronteiriço de dados relativos à saúde agrava o risco de um tratamento de dados inexacto ou ilegítimo.

([1]) Ver TEDH 17 de Julho de 2008, *I c. Finlândia* (appl. n.º 20511/03), ponto 38.

([2]) Ver Grupo do Artigo 29.º, Documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde electrónicos (CJ), Fevereiro de 2007, WP 131, ponto II.2. Ver também sobre o significado lato de «dados pessoais»: Grupo do Artigo 29.º, Parecer 4/2007 sobre o conceito de dados pessoais, WP 136.

([3]) Conselho da Europa, Recomendação n.º R(97)5 sobre a protecção dos dados clínicos.

([4]) ISO 27799:2008 «Informática da saúde — Gestão da segurança da informação na saúde utilizando a norma ISO/IEC 27002».

Isto pode obviamente ter consequências tremendamente negativas para a pessoa em causa. Tanto o Estado-Membro de inscrição (onde o doente está segurado) como o Estado-Membro de tratamento (onde os cuidados de saúde transfronteiriços são realmente prestados) estão implicados neste processo, e como tal partilham esta responsabilidade.

21. A segurança dos dados relativos à saúde é, neste contexto, uma questão importante. No recente processo acima evocado, o Tribunal Europeu dos Direitos do Homem atribuiu particular peso à confidencialidade dos dados relativos à saúde: «O respeito pela confidencialidade dos dados relativos à saúde é um princípio vital nos sistemas jurídicos de todas as partes contratantes na Convenção. É essencial não só que se respeite o sentimento de privacidade do doente, mas também que se preserve a sua confiança na profissão médica e nos serviços de saúde em geral». ([1])

22. As normas sobre protecção de dados consignadas na Directiva 95/46/CE, mais exigem que o Estado-Membro de inscrição forneça ao doente informação suficiente, exacta e actualizada sobre a transferência dos seus dados pessoais para outro Estado-Membro, juntamente com a garantia da transferência securizada dos dados para esse Estado-Membro. O Estado-Membro de tratamento deve igualmente securizar a recepção desses dados e proporcionar o nível de protecção adequado quando os dados são efectivamente tratados, seguindo o seu direito interno de protecção dos dados.

23. A AEPD gostaria de frisar bem as responsabilidades partilhadas dos Estados-Membros no âmbito da proposta, tendo igualmente em conta a comunicação electrónica de dados, especialmente no contexto das novas aplicações das TIC, como a seguir se analisará.

Comunicação electrónica de dados relativos à saúde

24. A melhoria do intercâmbio transfronteiriço de dados relativos à saúde é obtida sobretudo pela utilização de tecnologias da informação. Embora o intercâmbio de dados num regime de cuidados de saúde transfronteiriços ainda possa ser efectuado em suporte papel (isto é, o doente muda-se para outro Estado-Membro levando consigo os seus dados relativos à saúde relevantes, como exames de laboratório, requisições médicas, etc.), propõe-se nitidamente utilizar antes meios electrónicos. A comunicação electrónica de dados relativos à saúde será apoiada por sistemas de informação sobre cuidados de saúde (criados ou criar) nos Estados-Membros (em hospitais, clínicas, etc.), bem como a utilização de novas tecnologias, como as aplicações do registo de saúde electrónico (funcionando eventualmente pela Internet), bem como outras ferramentas, como cartões de saúde de doente e de médico. Claro que é igualmente possível utilizar uma combinação de formulários em papel e electrónicos, consoante os sistemas de saúde dos Estados-Membros.

25. As aplicações de saúde em linha e de telemedicina, que se inscrevem no âmbito da directiva proposta, dependerão exclusivamente de o intercâmbio electrónico de dados relativos à saúde (e.g. sinais vitais, imagens, etc.), habitualmente em conjugação com outros sistemas electrónicos de informação sobre cuidados de saúde residentes nos Estados-Membros de tratamento e de inscrição. Compreende sistemas que funcionam tanto entre o doente e o médico (como o acompanhamento e diagnóstico à distância) como entre médicos (como a tele-consulta entre profissionais de saúde para aconselhamento especializado sobre cuidados de saúde concretos. Outras aplicações de cuidados de saúde mais específicas que sustentam a prestação de cuidados de saúde transfronteiriços poderão também depender exclusivamente do intercâmbio electrónico de dados, como as receitas electrónicas (e-receitas) ou requisições electrónicas (e-requisições), que já são utilizadas ao nível nacional nalguns Estados-Membros. ([2])

Áreas de apreensão no intercâmbio transfronteiriço de dados relativos à saúde

26. Atendendo às considerações acima referidas, juntamente com a diversidade dos sistemas de saúde dos Estados-Membros existentes, assim como o crescente desenvolvimento de aplicações de saúde em linha, sobrevêm as seguintes duas grandes áreas de apreensão relativamente à protecção dos dados pessoais nos cuidados de saúde transfronteiriços: a) os diferentes níveis de segurança que podem ser aplicados pelos Estados-Membros para a protecção dos dados pessoais (em termos de medidas técnicas e organizacionais), e b) integração da privacidade nas aplicações de saúde em linha, especialmente nos novos desenvolvimentos. Acresce que outros aspectos, como a utilização secundária de dados relativos à saúde, especialmente na área da produção estatística, poderão também exigir especial atenção. Estas questões são analisadas aprofundadamente mais adiante na presente secção.

Segurança dos dados nos Estados-Membros

27. Pese o facto de as Directivas 95/46/CE e 2002/58/CE serem uniformemente aplicadas na Europa, a interpretação e transposição de certos elementos pode ser distinta de país para país, especialmente nas áreas em que as disposições legais são genéricas e deixadas ao critério dos Estados-Membros. Neste sentido, a principal área de apreço é a segurança do tratamento, ou seja as medidas (técnicas e organizacionais) que os Estados-Membros tomam para garantir a segurança dos dados relativos à saúde.

([1]) ECtHR 17 de Julho de 2008, *I v. Finland* (pedido n.º 20511/03), para 38.

([2]) eHealth ERA Report, Towards the Establishment of an European eHealth Research Area, Comissão Europeia, Sociedade da informação e meios de comunicação social, Março de 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Embora a protecção estrita dos dados relativos à saúde seja uma responsabilidade de todos os Estados-Membros, não existe actualmente uma definição comummente aceite na União de nível de segurança «adequado» de cuidados de saúde que possa ser aplicada no caso dos cuidados de saúde transfronteiriços. Assim, por exemplo, um hospital situado num Estado-Membro pode ser obrigado pela regulamentação nacional em matéria de protecção de dados a adoptar medidas de segurança específicas (como, por exemplo, a definição da política de segurança ou códigos de conduta, regras específicas em matéria de subcontratação e utilização de contratantes externos, requisitos de auditoria, etc.), ao passo que o mesmo pode não suceder noutros Estados-Membros. Esta incoerência pode ter impacto sobre o intercâmbio de dados transfronteiriço, especialmente em forma electrónica, dado que não é possível garantir que os dados sejam securizados (dos pontos de vista técnico e organizacional) ao mesmo nível nos diferentes Estados-Membros.

29. É pois necessária uma maior harmonização neste domínio, em termos de se definir um conjunto comum de requisitos de segurança para os cuidados de saúde que deve ser adoptado comummente pelos prestadores de serviços de saúde dos Estados-Membros. Esta necessidade coaduna-se em definitivo com a necessidade genérica de definir princípios comuns a todos os sistemas de saúde da UE, como enuncia a proposta.

30. Essa definição deve ser genérica, sem impor aos Estados-Membros soluções técnicas precisas mas fixando ainda assim uma base para o reconhecimento e a aceitação mútuas, por exemplo nos domínios da definição de políticas de segurança, da identificação e autenticação de doentes e profissionais de saúde, etc. As normas europeias e internacionais em vigor (isto é, ISO e CEN) sobre cuidados de saúde e segurança, bem como conceitos técnicos reconhecidos e juridicamente fundados (como as assinaturas electrónicas [1]) poderiam servir de roteiro nessa tentativa.

31. A AEPD apoia a tese de uma harmonização da segurança dos cuidados de saúde ao nível da UE e é de opinião que a Comissão deveria tomar as iniciativas pertinentes, já no quadro da presente proposta (ver secção III *infra*).

Privacidade nas aplicações de saúde em linha

32. A privacidade e a segurança devem fazer parte da concepção e implementação de qualquer sistema de cuidados de saúde, especialmente das aplicações de saúde em linha referidas na presente proposta («privacidade na concepção»). Este requisito indiscutível já foi defendido noutros documentos de orientação política relevantes [2], tanto gerais como específicos aos cuidados de saúde. [3]

33. No quadro da interoperabilidade dos sistemas de saúde em linha analisada na proposta, a noção de «privacidade na concepção» deve ser uma vez mais salientada enquanto base de todos os desenvolvimentos previstos. Esta noção aplica-se em vários planos distintos: organizacional, semântico, técnico.

— No plano organizacional, a privacidade deve ser considerada na definição dos procedimentos necessários para o intercâmbio de dados relativos à saúde entre os organismos responsáveis pelos cuidados de saúde nos Estados-Membros. Isto pode ter um impacto directo sobre o tipo de intercâmbio e a medida em que os dados são transferidos (como a utilização de números de identificação em vez dos nomes reais dos doentes, quando seja possível).

— No plano semântico, os requisitos de privacidade e segurança devem ser incorporados nas novas normas e regimes, isto é na definição do modelo de receita médica electrónica tal como analisado na proposta. Este poderia tirar partido das normas técnicas em vigor neste domínio, e.g. normas em matéria de confidencialidade dos dados e de assinaturas electrónicas, e tratar de necessidades específicas dos cuidados de saúde como a autenticação com base nas funções de profissionais de saúde habilitados.

— No plano técnico, as arquitecturas de sistema e aplicações para o utilizador devem adaptar tecnologias destinadas a reforçar a privacidade que implementem a referida definição semântica.

34. A AEPD pensa que o domínio das receitas electrónicas poderia servir para começar a integração de requisitos de privacidade e segurança na fase mais incipiente do desenvolvimento (ver secção III *infra*).

Outros aspectos

35. Um aspecto suplementar que poderia ser ponderado no quadro do intercâmbio transfronteiriço de dados relativos à saúde é a utilização secundária dos dados relativos à saúde e em especial a utilização dos dados para fins estatísticos, como já definida na presente proposta.

36. Como se referiu no ponto 18, o n.º 4 do artigo 8.º da Directiva 95/46/CE prevê a possibilidade de utilização secundária de dados relativos à saúde. Todavia, este tratamento suplementar só pode ser efectuado por «importantes motivos de interesse público» e tem de ser sujeito a «garantias adequadas» previstas no direito interno ou por decisão da autoridade de supervisão. [4] Além disso, no caso do tratamento de dados estatísticos, como refere também o

[1] Directiva 1999/93/CE do Parlamento Europeu e do Conselho de 13 de Dezembro de 1999 relativa a um quadro legal comunitário para as assinaturas electrónicas, JO L 13, 19.1.2000, págs. 12–20.

[2] A AEPD e a investigação e desenvolvimento tecnológico da UE, Documento de orientação política, AEPD, Abril de 2008 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

[3] Recomendação da Comissão de 2 de Julho de 2008 relativa à interoperabilidade transfronteiriça dos sistemas de registos de saúde electrónicos [notificada sob o número C(2008) 3282], JO L 190, 18.7.2008, pág. 37.

[4] Ver também considerando 34 da Directiva 95/46/CE. Ver também sobre este ponto o parecer do WP 29 sobre o TEDH referido acima na nota de rodapé 8, pág. 16.

parecer da AEPD sobre o regulamento proposto relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho ([1]), sobrevém um risco suplementar do significado distinto que as noções de «confidencialidade» e de «protecção de dados» podem ter na aplicação da legislação relativa à protecção de dados por um lado e da legislação relativa às estatísticas por outro lado.

37. A AEPD deseja salientar os elementos supra no contexto de a presente proposta. Devem ser inseridas referências mais explícitas aos requisitos de protecção de dados respeitantes à utilização ulterior dos dados relativos à saúde (ver secção III *infra*).

III. **ANÁLISE PORMENORIZADA DA PROPOSTA**

As disposições da proposta em matéria de protecção de dados

38. A proposta contém uma série de referências à protecção dos dados e à privacidade em várias partes do documento, mais concretamente:

— o considerando 3 declara — designadamente — que a directiva tem de ser transposta e aplicada respeitando plenamente os direitos à vida privada e à protecção dos dados pessoais;

— o considerando 11 refere-se ao direito fundamental à privacidade no tratamento de dados pessoais e à confidencialidade como dois dos princípios de funcionamento comuns que são partilhados pelos sistemas de saúde de toda a Comunidade;

— o considerando 17 descreve o direito à protecção dos dados pessoais como um direito individual fundamental que deve ser garantido, centrando-se especialmente no direito de acesso da pessoa aos dados relativos à saúde — também no contexto dos cuidados de saúde transfronteiriços — consignado na Directiva 95/46/CE;

— o artigo 3.º, que define a relação entre a directiva e outras disposições comunitárias, refere-se no n.º 1 às Directivas 95/46/CE e 2002/58/CE;

— o artigo 5.º sobre as responsabilidades do Estado-Membro de tratamento, estipula no n.º 1-F que a protecção do direito à privacidade é uma dessas responsabilidades, em conformidade com as medidas nacionais de execução das Directivas 95/46/CE e 2002/58/CE;

— o artigo 6.º sobre os cuidados de saúde prestados noutro Estado-Membro, salienta no n.º 5 o direito de acesso dos doentes aos seus registos médicos quando se deslocam a outro Estado-Membro para aí receberem cuidados de saúde ou procurem receber cuidados de saúde prestados noutro Estado-Membro, novamente em conformidade com as medidas nacionais de execução das Directivas 95/46/CE e 2002/58/CE;

— o artigo 12.º sobre o ponto de contacto nacional para os cuidados de saúde transfronteiriços, afirma na alínea a) do n.º 2 que esses pontos de contacto devem ser responsáveis por — designadamente — facultar e divulgar informação aos doentes sobre as garantias de protecção dos dados pessoais dadas noutro Estado-Membro;

— o artigo 16.º sobre a saúde em linha, declara que as medidas necessárias para garantir a interoperabilidade dos sistemas de tecnologias da informação e da comunicação devem respeitar o direito fundamental à protecção dos dados pessoais em conformidade com o direito aplicável;

— por fim, no n.º 1 do artigo 18.º refere-se — entre outras coisas — que a recolha de dados para fins estatísticos e de controlo deve ser efectuada em conformidade com o direito nacional e comunitário relativo à protecção dos dados pessoais.

39. A AEPD congratula-se com o facto de a protecção dos dados ter sido tida em conta na redacção da proposta e o de se ter tentado mostrar a necessidade global de privacidade no contexto dos cuidados de saúde transfronteiriços. Contudo, as disposições existentes na proposta sobre a protecção dos dados são demasiado genéricas ou então remetem para as responsabilidades dos Estados-Membros de uma forma assaz selectiva ou dispersa:

— Concretamente, os considerandos 3 e 11, juntamente com a alínea a) do n.º 1 do artigo 3.º, o artigo 16.º e o n.º 1 do artigo 18.º abordam com efeito o quadro jurídico geral da protecção dos dados (os dois últimos no contexto da saúde em linha e da recolha estatística), mas não fixam requisitos específicos respeitantes à privacidade.

— No que respeita às responsabilidades dos Estados-Membros, é feita uma referência genérica na alínea f) do n.º 1 do artigo 5.º

— O considerando 17 e o n.º 5 do artigo 6.º fornecem uma referência mais concreta ao direito de acesso dos doentes no Estado-Membro de tratamento.

— Por fim, a alínea a) do n.º 2 do artigo 12.º contém uma disposição sobre o direito dos doentes à informação no Estado-Membro de inscrição (através do funcionamento dos pontos de contacto nacionais).

Além disso, como já se referiu na introdução do presente parecer, não há qualquer ligação e/ou referência aos aspectos de privacidade evocados noutros instrumentos jurídicos comunitários (vinculativos ou não vinculativos) na área dos cuidados de saúde, especialmente no que respeita à utilização de novas aplicações no domínio das TIC (como a tele-medicina e os registos de saúde electrónicos).

([1]) JO C 295, 7.12.2007, pág. 1.

40. Deste modo, embora a privacidade seja geralmente referida como requisito dos cuidados de saúde transfronteiriços, continua a não haver um retrato global, seja em termos das obrigações dos Estados-Membros, seja das especificidades introduzidas pela natureza transfronteiriça da prestação de cuidados de saúde (ao invés da prestação de cuidados de saúde ao nível nacional). Mais concretamente:

— As responsabilidades dos Estados-Membros não são expostas de uma forma integrada, dado que algumas obrigações (direitos de acesso e informação) são salientadas — embora em partes distintas da proposta — ao passo que outras são totalmente omissas, como a segurança do tratamento.

— Não é feita qualquer referência às preocupações suscitadas pelas incoerências dos Estados-Membros em matéria de medidas de segurança e à necessidade de harmonizar a nível europeu a segurança dos dados relativos à saúde, no contexto dos cuidados de saúde transfronteiriços.

— Não é feita qualquer referência à integração da privacidade nas aplicações de saúde em linha. Isto também não se encontra adequadamente reflectido no caso das e-receitas.

41. Além disso, o artigo 18.º, que trata de recolha de dados para fins estatísticos e de controlo, suscita algumas apreensões concretas. O n.º 1 refere «dados estatísticos e *outros dados adicionais*»; refere-se além disso no plural a «efeitos de controlo» e enumera seguidamente as áreas que são sujeitas a esses efeitos de controlo, a saber a prestação de cuidados de saúde transfronteiriços, os cuidados prestados, os seus prestadores e os doentes, os custos e os resultados. Neste contexto, já assaz impreciso, é feita uma referência genérica ao direito da protecção dos dados, mas não são fixados requisitos específicos a respeito da utilização ulterior dos dados relativos à saúde, como prevê o n.º 4 do artigo 8.º da Directiva 95/46/CE. Além disso, o n.º 2 contém a obrigação incondicional de transferir a grande quantidade de dados para a Comissão pelo menos uma vez por ano. Dado que não é feita qualquer referência explícita a um diagnóstico da necessidade dessa transferência, afigura-se que o próprio legislador comunitário já determinou a necessidade dessas transferências para a Comissão.

As recomendações da AEPD

42. Para se abordarem adequadamente os elementos acima referidos, a AEPD fornece algumas recomendações, consignadas nas cinco acções elementares de alteração a seguir descritas.

Acção 1 — Definição de dados relativos à saúde

43. O artigo 4.º define a terminologia básica utilizada na proposta. A AEPD recomenda vivamente que se insira neste artigo uma definição de dados relativos à saúde. Deve ser aplicada uma interpretação lata dos dados relativos à saúde, como a descrita na Secção II do presente parecer (pontos 14 e 15).

Acção 2 — Inserção de um artigo específico sobre a protecção de dados

44. A AEPD recomenda também vivamente a inserção de um artigo específico sobre a protecção de dados na proposta, capaz de enunciar a dimensão global de privacidade de uma forma clara e inteligível. Este artigo deveria a) enunciar as responsabilidades dos Estados-Membros de inscrição e de tratamento incluindo — entre outras — a necessidade de segurança do tratamento, e b) relevar as principais áreas de futuro desenvolvimento, isto é harmonização da segurança e integração da privacidade na saúde em linha. Para estas matérias podem ser previstas disposições específicas (no âmbito do artigo proposto), como se expõe nas acções 3 e 4, *infra*.

Acção 3 — Disposição específica para a harmonização da segurança

45. Na sequência da alteração da acção 2, a AEPD recomenda que a Comissão adopte um mecanismo para definir um nível de segurança comummente aceitável de cuidados de saúde ao nível nacional, que tenha em conta as normas técnicas vigentes neste domínio. Isto dever-se-ia reflectir na proposta. A implementação poderia eventualmente recorrer ao procedimento de comité, já descrito no artigo 19.º e que se aplica a outras partes da proposta. Poder-se-ia ainda utilizar instrumentos adicionais para a produção de orientações pertinentes, incluindo todas as partes interessadas, como o Grupo do Artigo 29.º e a AEPD.

Acção 4 — Integração da privacidade no modelo de receita médica

46. O artigo 14.o sobre o reconhecimento das receitas médicas emitidas noutro Estado-Membro prevê o desenvolvimento de um modelo comunitário de receita médica, apoiando a interoperabilidade das e-receitas. Esta medida será adoptada através do procedimento de comité definido no n.º 2 do artigo 19.º da proposta.

47. A AEPD recomenda que o modelo de receita electrónica proposto incorpore privacidade e segurança, mesmo na sua definição semântica básica. Isso deveria ser referido explicitamente na alínea a) do n.º 2 do artigo 14.º. Também aqui a participação de todos os principais interessados é da maior importância. A este respeito, a AEPD deseja ser informada e participar em futuras medidas tomadas nesta matéria através do proposto procedimento de Comité.

Acção 5 — Utilização ulterior dos dados relativos à saúde para fins estatísticos e de controlo

48. Para evitar mal entendidos, a AEPD incita a que se esclareça a noção «outros dados necessários» no n.º 1 do artigo 18.º. O artigo deveria além disso ser alterado no sentido de remeter mais explicitamente para os requisitos da utilização ulterior dos dados relativos à saúde consignados no n.º 4 do artigo 8.º da Directiva 95/46/CE. Além disso, a obrigação de transmitir todos os dados à Comissão, contida no n.º 2, deve ser sujeita a um diagnóstico da necessidade de tais transferências para finalidades legítimas devidamente precisadas previamente.

IV. **CONCLUSÕES**

49. A AEPD gostaria de exprimir o seu apoio às iniciativas de melhoria das condições dos cuidados de saúde transfronteiriços. Preocupa-o, contudo, o facto de as iniciativas comunitárias relacionadas com os cuidados de saúde nem sempre serem bem coordenadas no que respeita à utilização das TIC, à privacidade e à segurança, tolhendo assim a adopção de uma abordagem universal da protecção dos dados em relação aos cuidados de saúde.

50. A AEPD regista com agrado que se tenha feito referência à privacidade na presente proposta. São contudo necessárias algumas alterações, como se explica na Secção III do presente parecer, a fim de estabelecer requisitos claros para os Estados-Membros de tratamento e para os de inscrição, assim como tratar correctamente a dimensão de protecção dos dados dos cuidados de saúde transfronteiriços:

— Deve ser inserida uma definição de dados relativos à saúde no artigo 4.º, que abranja quaisquer dados pessoais que possam ter uma ligação clara e estreita com a descrição do estado de saúde de uma pessoa. Deve em princípio abranger os dados clínicos, bem como dados administrativos e financeiros relacionados com a saúde.

— A inserção de um artigo específico sobre a protecção de dados é vivamente recomendada. Este artigo deveria definir com clareza o retrato geral, enunciando as responsabilidades dos Estados-Membros de inscrição e de tratamento e relevando as principais áreas de futuro desenvolvimento, ou seja a harmonização da segurança e a integração da privacidade, especialmente nas aplicações da saúde em linha.

— Recomenda-se que a Comissão adopte um mecanismo no quadro desta proposta para definir um nível de segurança comummente aceitável de cuidados de saúde ao nível nacional, que tenha em conta as normas técnicas vigentes neste domínio. Iniciativas suplementares e/ou complementares, que incluam todas as partes interessadas, o Grupo do Artigo 29.º e a AEPD, deve também ser encorajadas.

— Recomenda-se que a noção de «privacidade na concepção» seja incorporada no modelo comunitário de receita electrónica proposto (também ao nível semântico). Isto deveria ser referido explicitamente na alínea a) do n.º 2 do artigo 14.º. a AEPD deseja ser informada e participar em futuras medidas tomadas nesta matéria através do proposto procedimento de Comité.

— Recomenda-se que se precise a redacção do artigo 18.º e que se insira uma referência mais explícita aos requisitos específicos respeitantes à utilização ulterior dos dados relativos à saúde, como prevê o n.º 4 do artigo 8.º da Directiva 95/46/CE.

Feito em Bruxelas, em 2 de Dezembro de 2008.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

Segundo parecer da Autoridade Europeia para a Protecção de Dados sobre a revisão da Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)

(2009/C 128/04)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,

Tendo em conta 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,

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, especialmente o artigo 41.º,

APROVOU O SEGUINTE PARECER:

I. INTRODUÇÃO

Antecedentes

1. Em 13 de Novembro de 2007, a Comissão Europeia adoptou uma proposta (a seguir designada por «proposta» ou «proposta da Comissão») que altera, dentre outras, a Directiva relativa à privacidade no sector das comunicações electrónicas (Directiva «Privacidade e Comunicações Electrónicas») [1]. Em 10 de Abril de 2008, a AEPD emitiu um parecer sobre a proposta da Comissão no qual formulou recomendações destinadas a melhorá-la a fim de garantir que as modificações sugeridas proporcionem a maior protecção possível da privacidade e dos dados pessoais das pessoas singulares («primeiro parecer da AEPD») [2].

2. A AEPD recebeu positivamente a proposta da Comissão de se criar um sistema de notificação obrigatória das violações da segurança que exija que as empresas notifiquem as pessoas sempre que os seus dados pessoais tenham sido colocados em risco. Além disso, elogiou a nova disposição que permite que as pessoas colectivas (por exemplo, associações de consumidores e prestadores de serviços Internet) intentem acções contra os autores de *spam*, em complemento dos instrumentos já existentes de luta contra o *spam*,

3. Durante os debates parlamentares que antecederam a primeira leitura do Parlamento Europeu, a AEPD apresentou um novo contributo ao emitir observações sobre determinadas questões suscitadas nos relatórios elaborados pelas comissões do Parlamento Europeu competentes para rever as Directivas «Serviço Universal» [3] e «Privacidade e Comunicações Electrónicas» («observações») [4]. As observações abordaram essencialmente assuntos relacionados com o tratamento dos dados de tráfego e a protecção dos direitos de propriedade intelectual.

4. Em 24 de Setembro de 2008, o Parlamento Europeu («PE») aprovou uma resolução legislativa sobre a Directiva «Privacidade e Comunicações Electrónicas» («primeira leitura») [5]. A AEPD acolheu favoravelmente várias alterações do PE aprovadas na sequência do parecer e das obser vações da AEPD supramencionados. Entre as importantes modificações introduzidas, contava-se a inclusão dos prestadores de serviços da sociedade da informação (isto é,

[1] A revisão da Directiva «Privacidade e Comunicações Electrónicas» insere-se no âmbito de um processo de revisão mais vasto que tem por objectivo a criação de uma autoridade da UE em matéria de telecomunicações e a revisão das Directivas 2002/21/CE, 2002/19/CE, 2002/20/CE, 2002/22/CE e 2002/58/CE e do Regulamento (CE) n.º 2006/2004 (a seguir designada, no seu conjunto, por «revisão do pacote Telecom»).

[2] Parecer de 10 de Abril de 2008 sobre a proposta de directiva que altera, dentre outras, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva Privacidade e Comunicações Electrónicas), JO C 181 de 18.7.2008, p. 1.

[3] Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Directiva «Serviço Universal»), JO L 108, de 24.4.2002, p. 51.

[4] «*EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy)*» [Observações da AEPD sobre determinadas questões suscitadas no relatório da Comissão do Mercado Interno e da Protecção dos Consumidores sobre a revisão das Directivas 2002/22/CE («Serviço Universal») e 2002/58/CE («Privacidade e Comunicações Electrónicas»)], 2 de Setembro de 2008. Disponível no sítio: www.edps.europa.eu

[5] Resolução legislativa do Parlamento Europeu, de 24 de Setembro de 2008, sobre uma proposta de directiva do Parlamento Europeu e do Conselho que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor [COM(2007) 698 — C6-0420/2007 — 2007/0248(COD)].

empresas que operam na internet) no âmbito de aplicação da obrigação de notificar violações da segurança. A AEPD congratulou-se igualmente com a alteração que permite que as pessoas singulares e colectivas intentem acções por infracção a qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas» (e não apenas por violação das disposições relativas ao *spam*, como inicialmente previa a proposta da Comissão). A primeira leitura do Parlamento foi seguida da adopção, pela Comissão, de uma proposta alterada relativa à Directiva «Privacidade e Comunicações Electrónicas» (a seguir designada por «proposta alterada») ([6]).

5. Em 27 de Novembro de 2008, o Conselho chegou a um acordo político sobre a revisão das regras relativas ao pacote Telecom, incluindo a Directiva «Privacidade e Comunicações Electrónicas», acordo esse que dará lugar à posição comum do Conselho («posição comum») ([7]). A posição comum, que poderá integrar a proposta de alterações do PE, será notificada ao PE nos termos do n.º 2 do artigo 251.º do Tratado que institui a Comunidade Europeia.

Observações gerais sobre a posição comum

6. O Conselho modificou elementos essenciais do texto da proposta e não aceitou muitas das alterações aprovadas pelo PE. Sendo embora certo que a posição comum contém elementos positivos, a AEPD está, na generalidade, preocupada com o seu conteúdo, em especial porque a posição comum não incorpora algumas das alterações positivas apresentadas pelo PE, na proposta alterada ou nos pareceres da AEPD e nos pareceres das autoridades europeias de protecção de dados emitidos no âmbito do Grupo do Artigo 29.º ([8]).

7. Pelo contrário, em não poucos casos, as disposições da proposta alterada e as alterações do PE, que ofereciam salvaguardas aos cidadãos, foram suprimidas ou substancialmente enfraquecidas. Em consequência, o nível de protecção concedido às pessoas singulares na posição comum ficou consideravelmente enfraquecido. É por este motivo que a AEPD emite agora um segundo parecer, na esperança de que, à medida que a Directiva «Privacidade e Comunicações Electrónicas» for percorrendo todas as etapas do processo legislativo, serão aprovadas novas alterações que restabeleçam as salvaguardas em matéria de protecção de dados.

8. Esse segundo parecer centra-se nalgumas preocupações essenciais, mas não retoma todos os aspectos abordados no primeiro parecer da AEPD ou nas observações, que não obstante continuam todos válidos. Em especial, o presente parecer debruça-se sobre os seguintes pontos:

— Disposições em matéria de notificação das violações da segurança;

— O escopo da aplicação da Directiva «Privacidade e Comunicações Electrónicas» às redes privadas e às redes privadas acessíveis ao público;

— Tratamento de dados de tráfego para fins de segurança;

— Capacidades de as pessoas colectivas intentarem acções por infracção à Directiva «Privacidade e Comunicações Electrónicas».

9. No âmbito da análise dos pontos acima enunciados, o presente parecer examina a posição comum do Conselho e compara-a à primeira leitura do PE e à proposta alterada da Comissão. O presente parecer inclui recomendações destinadas a racionalizar as disposições da Directiva «Privacidade e Comunicações Electrónicas» e a garantir que a directiva continue a proteger adequadamente a privacidade e os dados pessoais das pessoas singulares.

II. DISPOSIÇÕES EM MATÉRIA DE NOTIFICAÇÃO DAS VIOLAÇÕES DA SEGURANÇA

10. A AEPD apoia a adoção de um sistema de notificação das violações da segurança nos termos do qual as autoridades e as pessoas singulares sejam notificadas sempre que os seus dados pessoais tenham sido colocados em risco ([9]). A notificação das violações da segurança pode ajudar as pessoas singulares a tomar as medidas necessárias para atenuar os potenciais danos decorrentes de tal situação. Além disso, a obrigação de notificação das violações da segurança incentivará as empresas a melhorar a segurança dos dados e a prestar mais contas no que respeita aos dados pessoais pelos quais são responsáveis.

11. A proposta alterada da Comissão, a primeira leitura do Parlamento Europeu e a posição comum do Conselho constituem três abordagens diferentes da notificação de violações da segurança actualmente em análise. Cada uma destas três abordagens apresenta aspectos positivos. Todavia, a AEPD considera que todas elas podem ser melhoradas e preconiza que sejam tidas em conta as recomendações a seguir formuladas na ponderação das últimas etapas para a adopção de um sistema de notificação das violações da segurança.

([6]) Proposta alterada de directiva do Parlamento Europeu e do Conselho que altera a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação no domínio da defesa do consumidor, Bruxelas, 6.11.2008 COM(2008) 723 final.

([7]) Disponível no sítio web do Conselho.

([8]) Parecer 2/2008 sobre a Directiva 2002/58/CE relativa à privacidade no sector das comunicações electrónicas (Directiva Privacidade Electrónica), disponível no sítio web do Grupo do Artigo 29.º.

([9]) No presente parecer usa-se a expressão «colocados em risco» sempre que tenha ocorrido uma violação de dados pessoais resultante, de modo acidental ou ilegal, da destruição, da perda, da alteração ou da divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados.

12. Na análise dos três sistemas de notificação das violações da segurança, há cinco pontos críticos a levar em consideração: *i)* a definição de violação da segurança; *ii*) as entidades abrangidas pela obrigação de notificação («entidades abrangidas»); *iii*) o critério que determina a obrigação de notificar; *iv*) a determinação da entidade responsável por decidir se uma violação da segurança preenche ou não esse critério; *v)* os destinatários da notificação.

Análise geral das abordagens da Comissão, do Conselho e do PE

13. O Parlamento Europeu, a Comissão e o Conselho adoptaram todos abordagens diferentes para a notificação das violações da segurança. A primeira leitura do PE modificou o sistema de notificação das violações da segurança apresentado na proposta inicial da Comissão ([10]). No âmbito da abordagem do PE, a obrigação de notificar aplica-se não só aos prestadores de serviços de comunicações electrónicas publicamente disponíveis (PPECS), como também aos prestadores de serviços da sociedade da informação (ISSP). Além disso, ao abrigo desta abordagem todas as violações de dados pessoais têm de ser notificadas à autoridade reguladora nacional ou às autoridades competentes (conjuntamente designadas por «autoridades»). Se as autoridades considerarem que a violação é *grave*, exigem aos PPECS e aos ISSP que notifiquem sem demora a pessoa afectada. Em caso de violações que representem um perigo iminente e directo, os PPECS e os ISSP notificam as pessoas em causa antes de notificarem as autoridades, sem aguardar uma decisão regulamentar. O texto prevê uma isenção da obrigação de notificação dos consumidores para as entidades que possam demonstrar às autoridades que «*foram aplicadas*» «*medidas tecnológicas de protecção adequadas*» que tornam os dados indecifráveis a qualquer pessoa que não esteja autorizada a aceder a eles.

14. A abordagem do Conselho também prevê que tanto os assinantes como as autoridades devem ser notificados, mas só nos casos em que a *entidade abrangida* considere que a violação representa um *grave risco* para a privacidade do assinante (por exemplo furto ou usurpação de identidade, danos físicos, humilhação significativa ou prejuízo para a reputação).

15. A proposta alterada da Comissão mantém a obrigação, proposta pelo PE, de notificar às autoridades todas as violações. Todavia, contrariamente à abordagem do PE, a proposta alterada prevê uma isenção da obrigação de notificação das pessoas em causa se o PPECS demonstrar à autoridade competente: *i)* que não existe «*probabilidade*» *razoável* de efeitos lesivos (por exemplo, prejuízos económicos, danos sociais ou furto de identidade) em consequência da violação ou *ii*) que foram aplicadas «*medidas tecnológicas de protecção adequadas*» aos dados a que diz respeito a violação. Assim, a abordagem da Comissão inclui uma análise baseada no efeito lesivo no contexto das notificações às pessoas em causa.

16. Importa registar que, no âmbito das abordagens do PE ([11]) e da Comissão, cabe em última instância *às autoridades* decidir se a violação é ou não grave ou se existe uma probabilidade razoável de que venha a ter efeitos lesivos. Em sentido contrário, na abordagem do Conselho a decisão é deixada às *entidades em causa*.

17. As abordagens do Conselho e da Comissão aplicam-se ambas apenas aos PPECS e não aos ISSP, contrariamente à abordagem do PE.

Definição de violação da segurança

18. A AEPD congratula-se por verificar que as três propostas legislativas contêm a mesma definição de violação da segurança, a saber: «*uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados […]*» ([12]).

19. Como adiante descrito mais detalhadamente, esta definição é de saudar, uma vez que é suficientemente ampla para abarcar a maioria das situações relevantes susceptíveis de justificar a notificação de violações da segurança.

20. Em primeiro lugar, a definição inclui as situações em que houve um *acesso não autorizado* a dados pessoais por terceiros, como o ataque de um servidor que contenha dados pessoais e a extracção dessas informações.

21. Em segundo lugar, a definição permite igualmente incluir as situações em que houve perda ou divulgação de dados pessoais, mesmo que o acesso não autorizado tenha ainda de ser demonstrado, o que inclui situações em que os dados pessoais possam ter sido perdidos (por exemplo, CD-ROM, chaves USB ou outros dispositivos portáteis) ou tornados publicamente disponíveis por utilizadores regulares (ficheiros de dados de empregados tornados inadvertida e temporariamente acessíveis ao público pela internet). Atendendo a que em muitos casos não haverá provas que demonstrem que os dados em causa podem ou não, em determinado momento, ter sido objecto de acesso ou utilização por terceiros não autorizados, afigura-se adequado incluir estas situações no âmbito de aplicação da definição. Por conseguinte, a AEPD recomenda que se mantenha esta definição. A AEPD recomenda também que a definição de violação da segurança seja incluída no artigo 2.º da Directiva «Privacidade e Comunicações Electrónicas», o que é mais coerente com a estrutura global da directiva e permite assegurar maior clareza.

([10]) Em particular, abordam esta questão as alterações do PE n.os 187, 124 a 127 e 27, 21 e 32.

([11]) Excepto nos casos de perigo iminente e directo, em que as entidades abrangidas devem primeiro notificar os consumidores.

([12]) Alínea i) do artigo 2.º da posição comum e da proposta alterada e n.º 3 do artigo 3.º da primeira leitura do PE.

Entidades a serem abrangidas pela obrigação de notificação

22. No âmbito da abordagem do PE, a obrigação de notificar aplica-se tanto aos PPECS como aos ISSP. No entanto, ao abrigo dos sistemas previstos pelo Conselho e pela Comissão, só os PPECS, como as empresas de telecomunicações e os fornecedores de acesso à Internet, serão obrigados a notificar as pessoas objecto de violações da segurança que coloquem em risco os seus dados pessoais. Outros sectores de actividade, por exemplo, os bancos em linha, os retalhistas em linha, os prestadores de serviços de saúde em linha e outros não são vinculados por esta obrigação. Pelas razões acima expostas, a AEPD considera que, numa perspectiva de política pública, é imperativo assegurar que os serviços da sociedade da informação, que incluem as empresas em linha, os bancos em linha, os prestadores de serviços de saúde em linha, etc., sejam também abrangidos pela obrigação de notificar.

23. Em primeiro lugar, a AEPD regista que, se é certo que as empresas de telecomunicações são alvo de violações da segurança que justificam uma obrigação de notificar, o mesmo acontece para outros tipos de empresas/fornecedores. Os retalhistas, bancos e farmácias em linha são tão susceptíveis, senão mais, de sofrer violações da segurança como as empresas de telecomunicações. Por conseguinte, as considerações relativas aos riscos não apoiam a limitação aos PPECS do âmbito de aplicação da obrigação de notificação das violações. A necessidade de uma abordagem mais ampla é ilustrada pela experiência adquirida noutros países. Por exemplo, nos Estados Unidos, quase todos os Estados (mais de 40 até ao momento) promulgaram leis em matéria de notificação de violações da segurança com um âmbito de aplicação mais vasto, que engloba não apenas os PPECS mas também qualquer entidade que detenha os dados pessoais em causa.

24. Em segundo lugar, se a violação dos tipos de dados pessoais tratados de forma regular pelos PPECS pode claramente ter consequências para a privacidade das pessoas, o mesmo se verifica, e talvez até em maior medida, para os tipos de dados pessoais tratados pelos ISSP. Os bancos e outras instituições financeiras podem certamente estar na posse de informações altamente confidenciais (por exemplo, dados das contas bancárias) cuja divulgação pode permitir uma utilização para fins de furto de identidade. Da mesma forma, a divulgação de informações de grande sensibilidade relacionadas com a saúde por serviços de saúde em linha pode ser especialmente lesiva para as pessoas em causa. Assim, os tipos de dados pessoais que podem ser colocados em risco exigem também que a obrigação de notificação das violações da segurança seja aplicada de forma mais ampla e abranja, pelo menos, os ISSP.

25. Foram invocados alguns argumentos jurídicos contra a extensão do âmbito de aplicação deste artigo, ou seja, das entidades abrangidas pela obrigação de notificar. Em especial, o facto de o âmbito de aplicação global da Directiva «Privacidade e Comunicações Electrónicas» apenas dizer respeito aos PPECS foi apresentado como um obstáculo a que a obrigação de notificar se aplique também aos ISSP.

26. Neste contexto, a AEPD gostaria de recordar que: *i)* Não há qualquer tipo de obstáculo jurídico à inclusão de outros actores, para além dos PPECS, no âmbito de aplicação de determinadas disposições da directiva. O legislador comunitário dispõe de plenos poderes discricionários nesta matéria. *ii)* Existem outros precedentes, na Directiva «Privacidade e Comunicações Electrónicas» em vigor, de aplicação a outras entidades que não os PPECS.

27. Por exemplo, o artigo 13.º aplica-se não só aos PPECS mas também a qualquer empresa que envie comunicações não solicitadas, exigindo para tal um consentimento prévio. Por seu lado, o n.º 3 do artigo 5.º da Directiva «Privacidade e Comunicações Electrónicas», que proíbe, nomeadamente, a armazenagem de informações tais como *cookies* no equipamento terminal dos utilizadores, vincula não só os PPECS como também qualquer pessoa que procure armazenar informações ou obter acesso à informação armazenada no equipamento terminal das pessoas em causa. Além disso, no âmbito do processo legislativo em curso, a Comissão até propôs alargar a aplicação do n.º 3 do artigo 5.º aos casos em que as tecnologias deste tipo (*cookies*/*software* espião) são transmitidas não só através de sistemas de comunicações electrónicas mas também por qualquer outro método (distribuição por telecarregamento a partir da internet ou utilização de um suporte externo de armazenamento de dados, nomeadamente CD-ROM, memórias *flash* USB, outros dispositivos de memória *flash*, etc.). Todos estes elementos são de saudar e deverão ser mantidos, constituindo ainda precedentes pertinentes para a presente discussão sobre o âmbito de aplicação.

28. Além disso, no âmbito do processo legislativo em curso, a Comissão e o PE — e pode considerar-se que também o Conselho —, propuseram um novo n.º 6-A para o artigo 6.º, analisado mais adiante, que se aplica a outras entidades que não os PPECS.

29. Por último, tendo em conta os elementos globalmente positivos derivados da obrigação de notificar violações da segurança, é muito provável que os cidadãos esperem beneficiar-se dessas vantagens quando os seus dados pessoais tenham sido colocados em risco não só por PPECS mas também por ISSP. As expectativas dos cidadãos não poderão ser satisfeitas se, por exemplo, não forem notificados quando um banco em linha tiver perdido informações sobre as suas contas bancárias.

30. Em resumo, a AEPD está convicta de que os benefícios da notificação das violações da segurança só se farão plenamente sentir se o âmbito de aplicação das entidades abrangidas incluir tanto os PPECS como os ISSP.

Critério que determina a notificação

31. No que se refere ao critério que determina a notificação, como a seguir explicado mais pormenorizadamente, a AEPD considera que o critério previsto na proposta alterada (existência de uma «*probabilidade razoável de lesar*») é o mais adequado dos três critérios propostos. Contudo, é importante assegurar que o termo «lesar» tenha uma acepção suficientemente ampla para cobrir todas as situações pertinentes de efeitos negativos na privacidade ou noutros interesses legítimos das pessoas singulares. De outra forma, seria preferível criar um novo critério segundo o qual a notificação seja obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*».

32. Tal como referido na secção anterior, as condições em que as pessoas devem ser notificadas (designadas por «factor de determinação» ou «critério») variam nas abordagens do PE, da Comissão e do Conselho. Obviamente, o volume de notificações que as pessoas receberem dependerá, em larga medida, do «factor de determinação» ou «critério» previsto para a notificação.

33. No âmbito dos sistemas propostos pelo Conselho e pela Comissão, a notificação deve ter lugar se a violação representar «*um grave risco para a privacidade do assinante*» (Conselho) e se for razoável «*a probabilidade de os interesses dos consumidores serem lesados em consequência da violação*» (Comissão). Ao abrigo do sistema proposto pelo PE, o factor que determina a notificação das pessoas é a «*gravidade da violação*» (ou seja, a notificação das pessoas é exigida quando a violação é considerada «*grave*»). A notificação não é necessária abaixo deste limiar ([13]).

34. A AEPD entende que, se os dados pessoais tiverem sido colocados em risco, poderá defender-se que as pessoas a quem esses dados pertencem têm o direito de ser do facto informadas, em todas as circunstâncias. Todavia, é perfeitamente legítimo analisar se esta é uma solução adequada tendo em conta outros interesses e considerações.

35. Tem sido sugerido que a obrigação de notificar sempre que os dados pessoais tenham sido colocados em risco ou, por outras palavras, sem qualquer limite, pode conduzir a uma sobrenotificação e a uma certa «fatiga» perante tal excesso de notificações, o que poderá gerar um efeito de «dessensibilização». Como adiante descrito mais detalhadamente, a AEPD é sensível a este argumento; no entanto, deseja ao mesmo tempo salientar o seu receio de que a sobrenotificação possa constituir um sinal de falha generalizada das práticas seguidas em matéria de segurança da informação.

36. Como anteriormente referido, a AEPD está ciente das potenciais consequências negativas da sobrenotificação e gostaria de ajudar a garantir que o quadro jurídico adoptado para a notificação das violações da segurança não tenha esse resultado. Se as pessoas passarem a receber frequentes notificações de violação, mesmo nas situações que não geram efeitos negativos ou lesivos nem qualquer apreensão, poderemos acabar por comprometer um dos principais objectivos da notificação, uma vez que as pessoas poderão, paradoxalmente, ignorar as notificações nos casos em que teriam efectivamente necessidade de tomar medidas para se protegerem. Assim, importa estabelecer o equilíbrio certo e assegurar uma notificação pertinente, dado que, se as pessoas não reagirem às notificações recebidas, a eficácia dos sistemas de notificação ficará altamente reduzida.

37. A fim de adoptar um critério adequado que não leve a sobrenotificações, haverá que ter em conta, para além do factor que determina a notificação, outros factores, especialmente a definição de violação da segurança e as informações abrangidas pela obrigação de notificar. A este respeito, a AEPD observa que, no âmbito das três abordagens propostas, o volume de notificações pode vir a ser elevado, tendo em conta a ampla definição de violação da segurança acima analisada. Este receio de sobrenotificação é ainda realçado pelo facto de a definição de violação da segurança abranger todos os tipos de dados pessoais. Embora a AEPD considere que esta (não limitação dos tipos de dados pessoais sujeitos a notificação) é a abordagem correcta, ao contrário de outras abordagens, como as da legislação dos EUA, em que os critérios se centram na sensibilidade das informações, a questão da sobrenotificação não deixa de ser um factor a ter em conta.

38. À luz do acima exposto, e atendendo às diferentes variáveis tomadas em conjunto, a AEPD considera adequado incluir um limiar ou critério abaixo do qual a notificação não seja obrigatória.

39. Os critérios propostos, ou seja, que a violação representa um «*grave risco para a privacidade*» ou tem «*razoável probabilidade de lesar*» parecem ambos abranger, por exemplo, os danos sociais ou os prejuízos para a reputação e as perdas económicas. Por exemplo, esses critérios permitem contemplar as situações de risco de furto de identidade através da divulgação de elementos de identificação não públicos tais como números de passaporte, bem como a exposição das informações relativas à vida privada das pessoas. A AEPD congratula-se com esta abordagem. A AEPD está convicta de que os benefícios da notificação das violações da segurança não serão plenamente atingidos se o sistema de notificação apenas abranger as violações conducentes a prejuízos económicos.

([13]) Ver nota 11 relativa à excepção a esta regra.

40. Dos dois critérios propostos, a AEPD prefere o da Comissão («*razoável probabilidade de lesar*»), uma vez que este permite proporcionar um nível de protecção das pessoas mais adequado. É bastante mais provável que as violações preencham os critérios de notificação se estes se referirem à sua *razoável probabilidade de lesar* a privacidade das pessoas do que se se referirem ao seu *grave risco* de causar tal efeito. Assim, abranger apenas as violações que apresentam um grave risco para a privacidade das pessoas limitará consideravelmente o número de violações a notificar. Além disso, dará um excessivo poder discricionário aos PPECS e aos ISSP para decidir se a notificação é ou não requerida, na medida em que lhes será muito mais fácil justificar conclusões no sentido de que não há qualquer *risco grave* de efeitos lesivos do que no sentido de que não existe *probabilidade razoável de lesar*. Muito embora haja certamente que evitar a sobrenotificação, em última análise deve privilegiar-se a protecção da privacidade das pessoas, que deverão ser protegidas pelo menos quando a violação tenha razoável probabilidade de as lesar. Por outro lado, a expressão *probabilidade razoável* será mais eficaz na prática, tanto para as entidades abrangidas como para as autoridades competentes, uma vez que exige uma avaliação objectiva da situação e do respectivo contexto.

41. Além disso, as violações de dados pessoais podem ter efeitos lesivos susceptíveis de variar e que podem ser difíceis de quantificar. Com efeito, a divulgação de dados do mesmo tipo pode, consoante as circunstâncias de cada caso, lesar significativamente certas pessoas e ter efeitos menos lesivos para outras. Assim, não serão adequados critérios que exijam que os efeitos lesivos sejam substanciais, significativos ou graves. Por exemplo, a abordagem do Conselho, que requer que a violação afecte *gravemente* a privacidade das pessoas, proporciona uma protecção inadequada, na medida em que esse critério exige que o efeito na privacidade seja «grave». Essa opção dá também lugar a avaliações subjectivas.

42. Embora, como acima descrito, a existência de uma *razoável probabilidade de lesar* pareça constituir um critério adequado para a notificação das violações da segurança, a AEPD continua preocupada pelo facto de esta opção poder não cobrir todas as situações que justificam a notificação das pessoas, isto é, todas as situações em que existe uma probabilidade razoável de ocorrência de efeitos negativos na privacidade ou noutros direitos legítimos das pessoas. Por esta razão, poder-se-á analisar a possibilidade de escolher um critério segundo o qual a notificação será obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*».

43. Este novo critério oferece a vantagem suplementar da coerência com a legislação da UE em matéria de protecção de dados. Com efeito, a Directiva «Protecção de Dados» refere-se frequentemente aos efeitos negativos nos direitos e nas liberdades das pessoas em causa. Por exemplo, o artigo 18.º e o considerando 49, que dizem respeito à obrigação de notificação das operações de tratamento de dados às autoridades de protecção de dados, autorizam os Estados-Membros a conceder isenções desta obrigação nos casos em que «*o tratamento não seja susceptível de prejudicar os direitos e liberdades das pessoas em causa*». O n.º 6 do artigo 16.º da posição comum apresenta uma redacção semelhante, a fim de permitir que as pessoas colectivas intentem acções contra os autores de *spam*.

44. Além disso, atendendo ao acima exposto, será de esperar que as entidades abrangidas, em especial as autoridades competentes para fazer cumprir a legislação em matéria de protecção de dados, estejam mais familiarizadas com o critério supramencionado, o que deverá facilitar a sua avaliação quanto a saber se determinada violação preenche o critério necessário.

Entidade encarregada de decidir se as violações da segurança preenchem ou não o critério

45. No âmbito da abordagem do PE (excepto em casos de perigo iminente) e da proposta alterada da Comissão, caberá às autoridades dos Estados-Membros decidir se as violações da segurança preenchem ou não o critério que determina a obrigação de notificação das pessoas em causa.

46. A AEPD considera que a participação de uma autoridade na decisão relativa ao preenchimento do critério é importante, na medida em que constitui, até certo ponto, uma garantia de correcta aplicação da lei. Este sistema pode impedir as empresas de avaliarem inadequadamente as violações como não tendo efeitos lesivos/graves e de assim evitarem notificações que, na realidade, são necessárias.

47. Por outro lado, a AEPD receia que um regime que exija que a avaliação seja realizada por autoridades possa ser pouco viável e difícil de aplicar ou possa, na prática, revelar-se contraproducente. Tal regime poderá assim até reduzir as salvaguardas em matéria de protecção de dados das pessoas.

48. Com efeito, no âmbito dessa abordagem, as autoridades de protecção de dados são susceptíveis de ser «inundadas» de notificações de violações da segurança e podem ter de enfrentar sérias dificuldades para proceder às necessárias avaliações. Importa recordar que, para avaliar se determinada violação preenche ou não o critério, as autoridades terão de dispor de suficientes informações internas, frequentemente de carácter técnico complexo, que terão de tratar com grande rapidez. Tendo em conta a dificuldade da avaliação e o facto de algumas autoridades disporem de recursos limitados, a AEPD receia que seja muito difícil às autoridades respeitar esta obrigação e que para tal sejam desviados recursos destinados a outras prioridades importantes. Além disso, um sistema deste tipo pode sujeitar as autoridades a uma pressão excessiva; com efeito, se decidirem que a violação não é grave e no entanto as pessoas em causa sofrerem danos, as autoridades poderão eventualmente ser responsabilizadas.

49. A dificuldade acima referida é ainda sublinhada se se tiver em conta que o tempo é um factor essencial na minimização dos riscos decorrentes das violações da segurança. A não ser que as autoridades possam proceder às avaliações em prazos muito curtos, o tempo suplementar necessário para que realizem as avaliações pode aumentar os danos sofridos pelas pessoas em causa. Por conseguinte, este passo adicional, destinado a proporcionar maior protecção às pessoas, pode paradoxalmente resultar numa diminuição da protecção oferecida em relação aos sistemas baseados na notificação directa.

50. Pelos motivos acima expostos, a AEPD considera que será preferível criar um sistema em que caiba às entidades em causa avaliar se as violações preenchem ou não o critério, tal como previsto na abordagem do Conselho.

51. Todavia, a fim de evitar qualquer risco de eventual abuso, por exemplo de as entidades recusarem proceder à notificação em circunstâncias em que esta é claramente exigível, é da maior importância incluir algumas das salvaguardas em matéria de protecção de dados adiante descritas.

52. Em primeiro lugar, a obrigação de as entidades abrangidas decidirem se devem ou não enviar notificações deve, evidentemente, ser acompanhada da obrigação de notificação às autoridades de todas as violações que preenchem o critério exigido. Nesses casos, as entidades abrangidas deverão ser obrigadas a informar as autoridades da violação e dos motivos subjacentes à sua decisão quanto à notificação, bem como do conteúdo de qualquer notificação enviada.

53. Em segundo lugar, deve ser atribuído às autoridades um real papel de supervisão. No desempenho deste papel, as autoridades devem ter a possibilidade, mas não a obrigação, de investigar as circunstâncias da violação e de exigir as medidas correctivas que possam ser adequadas ([14]). Neste contexto, deverão poder não só exigir a notificação das pessoas (quando ainda não tenha sido realizada), como também impor a obrigação de tomar medidas para evitar novas violações. As autoridades deverão dispor de efectivos poderes e recursos nesta matéria, bem como da margem de manobra necessária para decidir se devem ou não reagir a determinada violação da segurança. Em outras palavras, as autoridades poderão assim ser selectivas e lançar investigações, por exemplo, em caso de violações da segurança de grande dimensão e verdadeiramente lesivas, verificando e fazendo cumprir os requisitos da legislação.

54. Para conseguir o acima exposto, para além dos poderes reconhecidos ao abrigo da Directiva «Privacidade e Comunicações Electrónicas», nomeadamente do n.º 3 do artigo 15.º-A, e da Directiva «Protecção de Dados», a AEPD recomenda que se insira o seguinte texto: «*Se o assinante ou pessoa em causa ainda não tiver sido notificado, a autoridade nacional competente, tendo analisado a natureza da violação, pode exigir ao PPECS ou ao ISSP que proceda a essa notificação*».

55. A AEPD recomenda ainda que o PE e Conselho confirmem a proposta do PE (emenda 122, n.º 1-A do artigo 4.º) de que as entidades têm obrigação de avaliar e identificar os riscos associados aos seus sistemas, bem como aos dados pessoais que tencionam tratar. De acordo com essa obrigação, as entidades deverão definir medidas de segurança adaptadas e precisas, que serão aplicadas aos respectivos casos e que deverão ficar à disposição das autoridades. Em caso de violação da segurança, esta obrigação ajudará as entidades abrangidas — e, eventualmente, também as autoridades, no seu papel de supervisão — a determinar se o facto de as informações em causa terem sido colocadas em risco pode ou não ter efeitos negativos ou lesivos para as pessoas.

56. Em terceiro lugar, a obrigação de as entidades abrangidas decidirem se devem ou não notificar as pessoas deve ser acompanhada da obrigação de manter uma plataforma de auditoria interna pormenorizada e exaustiva que descreva todas as violações ocorridas e respectivas notificações, bem como todas as medidas tomadas para evitar futuras violações. Esta plataforma de auditoria interna deve ser colocada à disposição das autoridades para efeitos de análise e eventual investigação, o que lhes permitirá desempenhar o seu papel de supervisão. Para tal, poder-se-á adoptar uma formulação nos seguintes moldes: «*Os PPECS e os ISSP conservarão e manterão actualizados registos exaustivos que descrevam pormenorizadamente todas as violações de segurança ocorridas, as informações técnicas pertinentes conexas e as medidas correctivas tomadas. Esses registos conterão igualmente uma referência a todas as notificações emitidas aos assinantes ou pessoas em causa e às autoridades nacionais competentes, incluindo a respectiva data e conteúdo. Os registos serão apresentados à autoridade nacional competente a pedido desta*».

57. Evidentemente, para garantir uma implementação coerente deste critério, bem como de outros aspectos pertinentes do quadro relativo às violações da segurança, tais como o formato e os procedimentos de notificação, será conveniente que a Comissão adopte medidas de execução técnica, após consulta da AEPD, do Grupo do Artigo 29.º e das partes interessadas relevantes.

([14]) O n.º 3 do artigo 15.º-A reconhece estes poderes de supervisão ao dispor que «*os Estados-Membros assegurarão que as autoridades nacionais competentes e, se for caso disso, outros organismos nacionais, disponham de todos os poderes e recursos de investigação necessários, nomeadamente a possibilidade de obterem quaisquer informações relevantes de que necessitem para acompanhar e fazer cumprir as disposições nacionais aprovadas nos termos da presente directiva.*».

Destinatários da notificação

58. No que respeita aos destinatários das notificações, a AEPD prefere a terminologia do PE e da Comissão à do Conselho. Com efeito, o PE substituiu o termo «assinantes» por «utilizadores». A Comissão utiliza as expressões «assinante» e «outra pessoa afectada». Tanto a formulação do PE como a da Comissão permitem incluir como destinatários das notificações não só os actuais assinantes como os antigos assinantes e partes terceiras, tais como utilizadores que estabelecem relações com algumas entidades abrangidas sem serem assinantes das mesmas. A AEPD aprecia esta abordagem e convida o PE e o Conselho a mantê-la.

59. Todavia, a AEPD regista um certo número de incoerências em matéria de terminologia na primeira leitura do PE, que deverão ser corrigidas. Por exemplo, o termo «assinantes» foi substituído na maioria dos casos, mas não em todos, por «utilizadores», e noutros casos por «consumidores». O texto deverá ser harmonizado.

III. ÂMBITO DE APLICAÇÃO DA DIRECTIVA «PRIVACIDADE E COMUNICAÇÕES ELECTRÓNICAS»: REDES PÚBLICAS E PRIVADAS

60. O n.º 1 do artigo 3.º da Directiva «Privacidade e Comunicações Electrónicas» em vigor define as principais entidades a que a directiva diz respeito, isto é, aquelas que tratam dados «*no contexto da*» prestação de serviços públicos de comunicações electrónicas nas redes públicas (atrás designados por «PPECS») ([15]). Como exemplos de actividades de PPECS, podem citar-se o fornecimento de acesso à Internet, a transmissão de informações através das redes electrónicas, as ligações de telemóveis e de telefones fixos, etc.

61. O PE aprovou uma emenda (n.º 121) que modifica o artigo 3.º da proposta inicial da Comissão, alargando o âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas» por forma a incluir o «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas e privadas e em redes privadas acessíveis ao público na Comunidade, […]*» (n.º 1 do artigo 3.º da Directiva «Privacidade e Comunicações Electrónicas»). Infelizmente, o Conselho e a Comissão não estiveram em condições de aceitar esta emenda, pelo que não incluíram esta abordagem na posição comum nem na proposta alterada.

Aplicação da Directiva «Privacidade e Comunicações Electrónicas» às redes privadas acessíveis ao público

62. Pelas razões a seguir expostas, e para ajudar a promover um consenso, a AEPD exorta a que se mantenha o espírito da emenda 121. A AEPD sugere ainda que se inclua uma alteração que permita clarificar melhor os tipos de serviços abrangidos pelo âmbito de aplicação alargado.

63. As redes privadas são frequentemente utilizadas para fornecer serviços de comunicações electrónicas, tais como o acesso à internet, a um número indefinido de pessoas, que pode ser potencialmente elevado. É o que acontece, por exemplo, no caso do acesso à internet nos cibercafés, bem como nos pontos de acesso sem fios disponíveis nos hotéis, restaurantes, aeroportos, comboios e outros estabelecimentos abertos ao público em que este tipo de serviço é muitas vezes oferecido como complemento de outros serviços (bebidas, alojamento, etc.).

64. Em todos os exemplos acima referidos, o serviço de comunicações em causa, nomeadamente o acesso à internet, é disponibilizado ao público, não através de uma rede pública, mas antes de uma rede que se pode considerar privada, isto é, uma rede operada por entidades privadas. Além disso, embora nos casos supramencionados o serviço de comunicações seja fornecido ao público, o facto de a rede utilizada ser privada e não pública faz com que *se possa defender* que as disposições da Directiva «Privacidade e Comunicações Electrónicas», ou pelo menos algumas delas, não se aplicam à prestação desse serviço ([16]). Consequentemente, os direitos fundamentais das pessoas singulares garantidos pela Directiva «Privacidade e Comunicações Electrónicas» não são protegidos nesses casos e é criada uma situação jurídica desigual entre os utilizadores que acedem aos serviços de acesso internet através de telecomunicações públicas e aqueles que o fazem através de telecomunicações privadas, apesar de o risco para a privacidade e os dados pessoais das pessoas, em todos os casos acima referidos, ser idêntico ao que existe quando o serviço é fornecido através de redes públicas. Em resumo, não parece haver *razões* que justifiquem a diferença de tratamento, ao abrigo da directiva, entre os serviços de comunicações fornecidos através de redes privadas e os fornecidos através de redes públicas.

65. Assim, a AEPD é favorável a uma alteração, como a emenda 121 do PE, que preveja que a Directiva «Privacidade e Comunicações Electrónicas» se aplica também ao tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações *privadas*.

66. Todavia, a AEPD reconhece que esta formulação poderá acarretar consequências imprevisíveis e eventualmente indesejadas. Com efeito, a mera referência às redes privadas

([15]) «A presente directiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas publicamente disponíveis nas redes públicas de comunicações».

([16]) Poderá também argumentar-se, em sentido contrário, que o facto de o serviço de comunicações ser fornecido ao público, mesmo tratando-se de uma rede privada, implica que a prestação desse serviço é abrangida pelo quadro jurídico existente, apesar de a rede ser privada. De facto, por exemplo na França os empregadores que fornecem um acesso Internet aos seus empregados têm sido equiparados aos fornecedores de acesso internet que oferecem esse acesso a título comercial. Esta interpretação não é amplamente aceite.

poderá ser interpretada como abrangendo situações que claramente não se destinam a ser abrangidas pela directiva. Por exemplo, poder-se-á afirmar que uma interpretação literal ou estrita desta formulação pode implicar que os proprietários de casas equipadas com sistemas sem fios ([17]), que permitem a ligação de qualquer pessoa dentro do seu raio de acção (geralmente a própria casa) são abrangidos pelo âmbito de aplicação da directiva, mesmo não sendo esta a intenção da emenda 121. A fim de evitar esta interpretação, a AEPD sugere que a emenda 121 seja reformulada, nomeadamente no que se refere ao âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas», passando a ter a seguinte redacção: «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas ou em redes de comunicações privadas acessíveis ao público na Comunidade, …*».

67. Esta nova formulação ajudará a clarificar que só as redes privadas acessíveis ao público serão abrangidas pela Directiva «Privacidade e Comunicações Electrónicas». Ao prever que as disposições da Directiva «Privacidade e Comunicações Electrónicas» se apliquem *apenas* às *redes privadas acessíveis ao público* (e não a todas as redes privadas), limitar-se-á o âmbito de aplicação da directiva por forma a que abranja apenas os serviços de comunicações fornecidos através de redes privadas que são intencionalmente tornados *acessíveis* ao público. Esta formulação ajudará a sublinhar ainda mais que a *acessibilidade* da rede privada *ao público em geral* é o principal factor para a determinação das entidades abrangidas pela directiva (para além do fornecimento de um serviço de comunicações publicamente disponível). Por outras palavras, independentemente da sua natureza pública ou privada, se a rede for intencionalmente tornada acessível ao público para o fornecimento de um serviço público de comunicações, como o acesso Internet, e mesmo que esse serviço seja complementar de outro serviço (por exemplo, alojamento num hotel), o serviço/rede em causa ficará abrangido pela Directiva «Privacidade e Comunicações Electrónicas».

68. A AEPD observa que a abordagem acima defendida, que prevê que as disposições da Directiva «Privacidade e Comunicações Electrónicas» se apliquem às *redes privadas acessíveis ao público*, é coerente com as abordagens adoptadas em vários Estados-Membros em que as autoridades já consideraram que este tipo de serviços, bem como os serviços fornecidos em redes meramente privadas, são abrangidos pelo âmbito de aplicação das disposições nacionais de execução da directiva ([18]).

69. Para reforçar a segurança jurídica no que se refere às entidades abrangidas pelo novo âmbito de aplicação, poderá ser útil introduzir na Directiva «Privacidade e Comunicações Electrónicas» uma alteração que defina as «redes privadas acessíveis ao público»; essa alteração poderá ter a seguinte redacção: «*rede privada acessível ao público é uma rede operada por entidades privadas a que o público em geral tem normalmente acesso sem quaisquer restrições, a título oneroso ou gratuito, ou no contexto de outros serviços ou ofertas, sujeito à aceitação dos termos e condições aplicáveis*».

70. Na prática, a abordagem acima referida significa que serão abrangidas as redes privadas nos hotéis e outros estabelecimentos que fornecem um acesso internet ao público em geral através de uma rede privada. Inversamente, não será abrangido o fornecimento de serviços de comunicações em redes exclusivamente privadas em que o serviço se restrinja a um grupo limitado de pessoas identificáveis. Por conseguinte, não serão abrangidas, por exemplo, as redes privadas virtuais nem as casas de consumidores equipadas com sistemas sem fios. Também não serão abrangidos os serviços fornecidos através de redes exclusivamente empresariais.

Redes privadas abrangidas pelo âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas»

71. A exclusão das redes privadas enquanto tais, como acima sugerido, deverá ser considerada uma medida temporária sujeita a posterior debate. Com efeito, esta opção poderá ter de ser reconsiderada, atendendo, por um lado, às implicações, em termos de privacidade, da exclusão das redes exclusivamente privadas enquanto tais e, por outro, ao facto de essa exclusão afectar um grande número de pessoas que habitualmente acedem à Internet através de redes empresariais. Por este motivo, e a fim de fomentar o debate sobre esta questão, a AEPD recomenda a inclusão, na Directiva «Privacidade e Comunicações Electrónicas», de um considerando que preveja que a Comissão realizará uma consulta pública sobre a aplicação da directiva a todas as redes privadas, com o contributo da AEPD, das autoridades de protecção de dados e de outras partes interessadas pertinentes. Esse considerando poderá ainda especificar que, na sequência dessa consulta pública, a Comissão deverá elaborar uma proposta adequada para alargar ou limitar os tipos de entidades a abranger pela directiva.

72. Além do acima exposto, os artigos da Directiva «Privacidade e Comunicações Electrónicas» deverão ser alterados em conformidade, de forma que todas as disposições operacionais se refiram explicitamente não só às redes públicas como também às redes privadas acessíveis ao público.

IV. **TRATAMENTO DE DADOS DE TRÁFEGO PARA FINS DE SEGURANÇA**

73. Durante o processo legislativo relacionado com a revisão da Directiva «Privacidade e Comunicações Electrónicas», as empresas que prestam serviços de segurança insistiram em que era necessário introduzir na directiva uma disposição que legitimasse a recolha de dados de tráfego para garantir uma efectiva segurança em linha.

([17]) Tipicamente redes locais sem fios.
([18]) Ver nota 16.

74. Em consequência, o PE introduziu a emenda 181, que criou um novo n.º 6-A do artigo 6.º que autoriza expressamente o tratamento de dados de tráfego para fins de segurança: «*Sem prejuízo do respeito de outras disposições para além das que figuram no artigo 7.º da Directiva 95/46/CE e no artigo 5.º da presente directiva, os dados relativos ao tráfego podem ser tratados no interesse legítimo do controlador dos dados para fins de aplicação de medidas técnicas destinadas a garantir a segurança das redes e da informação, nos termos da alínea c) do artigo 4.º do Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, de um serviço público de comunicações electrónicas, de uma rede pública ou privada de comunicações electrónicas, de um serviço da sociedade da informação ou do respectivo equipamento terminal e de comunicação electrónica, salvo se os direitos fundamentais e as liberdades da pessoa em questão prevalecerem sobre o referido interesse. Esse tratamento deve restringir-se ao estritamente necessário para efeitos de actividades em matéria de segurança.*».

75. Na sua proposta alterada, a Comissão aceitou esta emenda quanto ao seu princípio, mas suprimiu uma cláusula essencial destinada a assegurar que as restantes disposições da directiva devem ser respeitadas, a saber a seguinte: «*sem prejuízo […] da presente directiva*». O Conselho aprovou uma versão reformulada, que enfraquece mais um pouco as importantes protecções e equilíbrios de interesses proporcionados pela emenda 181, tendo adoptado a seguinte redacção: «*Os dados de tráfego podem ser tratados, na medida do estritamente necessário, para garantir […] a segurança das redes e da informação, na acepção da alínea c) do artigo 4.º do Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação*».

76. Conforme adiante explicado mais detalhadamente, o n.º 6-A do artigo 6.º é desnecessário e apresenta riscos de utilização abusiva, em especial se for adoptado sob uma forma que não inclua importantes salvaguardas, cláusulas relativas ao respeito das outras disposições da directiva e equilíbrios de interesses. Por conseguinte, a AEPD recomenda que se rejeite esta disposição ou, pelo menos, se assegure que qualquer disposição sobre esta questão inclua os tipos de salvaguardas previstos na emenda 181 tal como adoptada pelo PE.

Fundamentos jurídicos para o tratamento de dados de tráfego aplicáveis aos serviços de comunicações electrónicas e outros responsáveis pelo tratamento de dados no âmbito da legislação relativa à protecção de dados em vigor

77. As possibilidades de tratamento legal de dados de tráfego por fornecedores de serviços de comunicações electrónicas publicamente disponíveis são reguladas pelo artigo 6.º da Directiva «Privacidade e Comunicações Electrónicas», que restringe o tratamento de dados de tráfego a um número limitado de fins tais como a facturação, a interligação e a comercialização. O tratamento destes dados só pode ser realizado em determinadas condições, como o consentimento das pessoas em causa na hipótese de comercialização. Além disso, outros responsáveis pelo tratamento de dados, tais como os prestadores de serviços da sociedade da informação, podem tratar dados de tráfego ao abrigo do artigo 7.º da Directiva «Protecção de Dados», que dispõe que os responsáveis pelo tratamento de dados podem tratar dados pessoais se cumprirem pelo menos uma das bases jurídicas (também designadas por fundamentos jurídicos) enumeradas.

78. Como exemplo de uma dessas bases jurídicas, pode mencionar-se a alínea a) do artigo 7.º da Directiva «Protecção de Dados», que exige o consentimento da pessoa em causa. Por exemplo, se um retalhista em linha desejar tratar dados de tráfego para efeitos de publicidade ou *marketing*, tem de obter o consentimento da pessoa em causa. Outra base jurídica prevista no artigo 7.º pode permitir, em certos casos, o tratamento de dados de tráfego para fins de segurança por, nomeadamente, empresas de segurança que oferecem serviços de segurança. Esta possibilidade baseia-se na alínea f) do artigo 7.º que dispõe que os responsáveis pelo tratamento de dados podem tratar dados pessoais se «*for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa …*». A Directiva «Protecção de Dados» não especifica as situações em que o tratamento de dados pessoais satisfaz este requisito. Em vez disso, a decisão é tomada pelos responsáveis pelo tratamento de dados, caso a caso, frequentemente com a concordância das autoridades nacionais de protecção de dados e outras autoridades.

79. Há que analisar a articulação entre o artigo 7.º da Directiva «Protecção de Dados» e a proposta de n.º 6-A do artigo 6.º da Directiva «Privacidade e Comunicações Electrónicas». A proposta de n.º 6-A do artigo 6.º especifica as circunstâncias em que são cumpridos os requisitos da alínea f) do artigo 7.º acima descrita. Com efeito, ao autorizar o tratamento de dados de tráfego para ajudar a garantir a segurança das redes e da informação, o n.º 6-A do artigo 6.º permite esse tratamento para prosseguir interesses legítimos do responsável pelo tratamento de dados.

80. Como adiante explicado mais pormenorizadamente, a AEPD considera que a proposta do n.º 6-A do artigo 6.º não é nem necessária nem útil. Com efeito, de um ponto de vista jurídico, em princípio, é desnecessário estabelecer se determinado tipo de actividade de tratamento de dados — aqui o tratamento de dados de tráfego para fins de segurança — cumpre os requisitos da alínea f) do artigo 7.º da Directiva «Protecção de Dados» ou não; neste caso, poderá ser exigível o consentimento da pessoa em causa, por força da alínea a) do artigo 7.º. Como acima referido, esta avaliação é normalmente levada

a cabo pelos responsáveis pelo tratamento de dados, isto é, pelas empresas, a nível de execução, em concertação com as autoridades de protecção de dados e, se necessário, pelos tribunais. Em termos gerais, a AEPD considera que, em casos específicos, o tratamento legítimo de dados de tráfego para fins de segurança, efectuado sem prejudicar os direitos e liberdades fundamentais das pessoas em causa, é susceptível de cumprir os requisitos da alínea f) do artigo 7.º da Directiva «Protecção de Dados», e pode por isso ser realizado. Além disso, não há qualquer outro precedente nas Directivas «Protecção de Dados» e «Privacidade e Comunicações Electrónicas» no sentido de prever isenções ou disposições especiais para certos tipos de actividades de tratamento de dados que satisfazem os requisitos da alínea f) do artigo 7.º, nem tem sido demonstrada a necessidade de tal excepção. Pelo contrário, como acima observado, afigura-se que, em muitas circunstâncias, este tipo de actividade está claramente contemplado no texto actual. Por conseguinte, é em princípio desnecessária uma disposição jurídica que confirme esta avaliação.

Versões do PE, do Conselho e da Comissão do n.º 6-A do artigo 6.º

81. Como acima explicado, importa salientar que, embora desnecessária, a emenda 181, tal como aprovada pelo PE, foi redigida, até certo ponto, tendo em conta princípios de protecção da privacidade e dos dados consagrados na legislação relativa à protecção de dados. A emenda 181 do PE poderá atender ainda mais aos interesses da protecção de dados e da privacidade, por exemplo, através da inserção da expressão «em casos específicos» para garantir a aplicação selectiva deste artigo, ou através da inclusão de um período de conservação específico.

82. A emenda 181 contém alguns elementos positivos. Confirma que o tratamento deverá respeitar qualquer outro princípio em matéria de protecção de dados aplicável ao tratamento de dados pessoais («*sem prejuízo do respeito de outras disposições […] da Directiva 95/46/CE e […] da presente directiva*»). Além disso, embora permita o tratamento de dados de tráfego para fins de segurança, a emenda 181 estabelece um equilíbrio entre os interesses da entidade que trata os dados de tráfego e os das pessoas cujos dados são tratados, de modo a que o tratamento dos dados só possa ser realizado se os direitos e liberdades fundamentais da pessoa em causa não prevalecerem sobre os interesses da entidade que trata os dados («*salvo se os direitos fundamentais e as liberdades da pessoa em questão prevalecerem sobre o referido interesse*»). Este requisito é essencial na medida em que pode permitir o tratamento de dados de tráfego em casos específicos; todavia, não permite que uma entidade trate dados de tráfego em bloco.

83. A versão da emenda reformulada pelo Conselho contém elementos positivos, nomeadamente o facto de manter a expressão «*estritamente necessário*», que realça o carácter limitado do âmbito de aplicação deste artigo. Todavia, a versão do Conselho suprime as salvaguardas em matéria de protecção de dados e de privacidade acima referidas. Embora, em princípio, se apliquem as disposições gerais relativas à protecção de dados, quer sejam ou não feitas referências específicas em cada caso, a versão do Conselho do n.º 6 do artigo 6.º-A pode ser interpretada como conferindo plenos poderes discricionários para o tratamento de dados de tráfego sem qualquer das salvaguardas em matéria de protecção de dados e privacidade aplicáveis sempre que são tratados dados de tráfego. Por conseguinte, poderá defender-se que os dados de tráfego podem ser recolhidos, armazenados e posteriormente utilizados sem que seja necessário respeitar os princípios e as obrigações específicas em matéria de protecção de dados de outro modo aplicáveis aos responsáveis, tais como o princípio da qualidade ou a obrigação de o tratamento ser efectuado de forma lícita e leal e de os dados serem mantidos confidenciais e conservados de forma segura. Além disso, como o artigo não inclui qualquer referência aos princípios de protecção de dados que impõem limites temporais para o armazenamento das informações ou prazos específicos, a versão do Conselho pode ser interpretada no sentido de permitir a recolha e o tratamento de dados de tráfego para fins de segurança por um período indefinido.

84. O Conselho enfraqueceu, ainda, a protecção da privacidade nalgumas partes do texto, ao utilizar uma formulação potencialmente mais abrangente. Por exemplo, a referência ao «*interesse legítimo do controlador dos dados*» foi suprimida, o que levanta dúvidas quanto ao tipo de entidades que poderão prevalecer-se desta excepção. É da maior importância evitar abrir a possibilidade a que qualquer utilizador ou entidade jurídica beneficie desta alteração.

85. As recentes experiências do PE e do Conselho demonstram que é difícil definir por lei o âmbito e as condições em que o tratamento de dados para fins de segurança pode ser legalmente realizado. É improvável que algum artigo, já existente ou novo, permita suprimir os riscos evidentes de aplicação excessivamente ampla da excepção acima referida, por motivos não exclusivamente relacionados com a segurança ou por entidades que não deveriam poder beneficiar dessa excepção. Isto não significa que tal tratamento não deve nunca ter lugar. No entanto, a questão de saber se e em que medida pode ser efectuado poderá ser mais bem avaliada a nível de execução. As entidades que pretendam realizar tal tratamento deverão discutir o respectivo âmbito e condições de aplicação com as autoridades de protecção de dados e, eventualmente, com o Grupo do Artigo 29.º. Em alternativa, a Directiva «Privacidade e Comunicações Electrónicas» poderá incluir um artigo que permita o tratamento de dados de tráfego para fins de segurança sob reserva de autorização expressa das autoridades de protecção de dados.

86. Tendo em conta, por um lado, os riscos que o n.º 6-A do artigo 6.º coloca para o direito fundamental das pessoas singulares à protecção dos dados e à privacidade e, por outro, o facto de, tal como explicado no presente parecer, essa disposição ser desnecessária de um ponto de vista jurídico, a AEPD chegou à conclusão de que a melhor solução consistirá em suprimir inteiramente essa disposição.

87. Se, contra a recomendação da AEPD, for aprovado algum texto nos moldes da actual versão do n.º 6-A do artigo 6.º, tal texto deverá em qualquer caso incorporar as salvaguardas em matéria de protecção de dados acima analisadas. Deverá ainda ser adequadamente integrado na estrutura existente do artigo 6.º, de preferência enquanto novo n.º 2-A.

V. **CAPACIDADE DE AS PESSOAS COLECTIVAS INTENTAREM ACÇÕES POR INFRACÇÃO À DIRECTIVA «PRIVACIDADE E COMUNICAÇÕES ELECTRÓNICAS»**

88. O PE aprovou a emenda 133, que permite que os fornecedores de acesso à internet e outras entidades jurídicas como as associações de consumidores intentem acções junto dos tribunais contra os infractores de qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas» ([19]). Infelizmente, nem a Comissão nem o Conselho aceitaram esta emenda. A AEPD considera esta emenda muito positiva e recomenda que seja mantida.

89. Para entender a importância desta emenda, é necessário ter em mente que, em matéria de privacidade e de protecção de dados, o prejuízo causado à pessoa em causa, considerada individualmente, não é em geral só por si suficiente para que esta intente uma acção judicial. As pessoas geralmente não recorrem aos tribunais por sua própria iniciativa por terem recebido *spams* ou por o seu nome ter sido indevidamente incluído numa lista. Esta emenda permitirá às associações de consumidores e aos sindicatos que representam os interesses dos consumidores, a nível colectivo, intentar acções judiciais em seu nome. O facto de dispor de uma mais ampla diversidade de mecanismos para fazer cumprir a lei é susceptível de estimular um maior respeito da mesma, sendo por isso no interesse da aplicação eficaz das disposições da Directiva «Privacidade e Comunicações Electrónicas».

90. Existem precedentes jurídicos nos quadros jurídicos de alguns Estados-Membros, que já prevêem a possibilidade de recurso colectivo a fim de permitir que os consumidores ou grupos de interesses exijam reparação pela parte responsável pelos prejuízos causados.

91. Além disso, em alguns Estados-Membros ([20]) o direito da concorrência autoriza os consumidores e os grupos de interesses (para além do *concorrente afectado*) a intentarem uma acção judicial contra a entidade infractora. A lógica subjacente a esta abordagem é a de que as empresas que infringem o direito da concorrência são susceptíveis de beneficiar do facto de os consumidores que sofrem apenas prejuízos marginais terem geralmente relutância em intentar acções judiciais. Esta lógica pode ser aplicada, *mutatis mutandis*, no domínio da protecção de dados e da privacidade.

92. Mais importante ainda, como acima referido, permitir que as entidades jurídicas como as associações de consumidores e os PPECS intentem acções judiciais fortalece a posição dos consumidores e promove o cumprimento, em termos globais, da legislação relativa à protecção de dados. Se as empresas infractoras correrem maior risco de ser processadas, é provável que passem a investir mais no respeito da legislação relativa à protecção de dados, o que a longo prazo aumentará o nível de protecção da privacidade e dos consumidores. Por todos estes motivos, a AEPD convida o PE e o Conselho a aprovar uma disposição que autorize as entidades jurídicas a intentar acções judiciais contra os infractores de qualquer disposição da Directiva «Privacidade e Comunicações Electrónicas».

([19]) N.º 6 do artigo 13.º da primeira leitura do PE.

([20]) Ver, por exemplo, o parágrafo 8 da UWG — Lei alemã sobre a concorrência desleal.

VI. **CONCLUSÃO**

93. A posição comum do Conselho, a primeira leitura do Parlamento Europeu e a proposta alterada da Comissão contêm, em graus diversos, elementos positivos que poderão servir para reforçar a protecção da privacidade e dos dados pessoais das pessoas singulares.

94. Todavia, a AEPD considera que é possível introduzir melhorias, em especial no que respeita à posição comum do Conselho que, infelizmente, não manteve algumas das alterações do PE destinadas a ajudar a assegurar uma adequada protecção da privacidade e dos dados pessoais das pessoas singulares. A AEPD insta o PE e o Conselho a restabelecerem as salvaguardas em matéria de privacidade incorporadas na primeira leitura do PE.

95. A AEPD considera, ainda, que é oportuno racionalizar algumas das disposições da directiva. Esta racionalização é especialmente necessária no caso das disposições relativas à violação da segurança, uma vez que a AEPD entende que os benefícios da notificação das violações só se farão plenamente sentir se o respectivo quadro jurídico for fixado desde o início. Por último, a AEPD considera igualmente oportuno melhorar e clarificar a formulação de algumas disposições da directiva.

96. Tendo em conta o acima exposto, a AEPD insta o PE e o Conselho a redobrarem os esforços para melhorar e clarificar algumas disposições da Directiva «Privacidade e Comunicações Electrónicas», restabelecendo simultaneamente as alterações adoptadas pelo PE em primeira leitura destinadas a proporcionar um nível adequado de protecção da privacidade e dos dados. Para este fim, os pontos 97, 98, 99 e 100 *infra* fazem uma síntese das questões em jogo e apresentam algumas recomendações e propostas de redacção. A AEPD apela a todas as partes envolvidas para que as tenham em conta ao longo do processo conducente à aprovação final da Directiva «Privacidade e Comunicações Electrónicas».

Violação da segurança

97. O Parlamento Europeu, a Comissão e o Conselho adoptaram todos abordagens diferentes para a notificação das violações da segurança. As diferenças entre os três modelos dizem respeito, respectivamente, às entidades abrangidas pela obrigação, ao factor ou critério que determina a notificação, às pessoas com direito a serem notificadas, etc. O PE e o Conselho deverão fazer tudo o que estiver ao seu alcance para elaborar um quadro jurídico sólido em matéria de violação da segurança. Para tal, o PE e o Conselho deverão:

— *Manter* a definição de violação da segurança contida nos textos do PE, do Conselho e da Comissão, uma vez que é suficientemente ampla para abarcar a maioria das situações relevantes susceptíveis de justificar a notificação de violações da segurança;

— No que se refere às entidades a abranger pelo requisito de notificação proposto, *incluir* os prestadores de serviços da sociedade da informação. Os retalhistas, bancos e farmácias em linha são tão susceptíveis, senão mais, de sofrer violações de segurança quanto as empresas de telecomunicações. Os cidadãos esperam ser notificados não só quando os fornecedores de acesso à Internet sejam objecto de violações da segurança mas também, muito especialmente, quando sejam os seus bancos e farmácias em linha a ser afectados;

— No que toca ao factor que determina a notificação, o critério enunciado na proposta alterada (existência de uma «*probabilidade» razoável «de lesar*») é adequado e garante um bom funcionamento do sistema. Contudo, importa assegurar que o termo «lesar» tenha uma acepção suficientemente ampla para cobrir todas as situações pertinentes de efeitos negativos na privacidade ou noutros interesses legítimos das pessoas singulares. De outra forma, será preferível criar um novo critério segundo o qual a notificação será obrigatória «*se for razoável a probabilidade de a violação ter efeitos negativos nas pessoas*». A abordagem do Conselho, que requer que a violação afecte *gravemente* a privacidade das pessoas, proporciona uma protecção inadequada, na medida em que esse critério exige que o efeito na privacidade seja «grave». Essa opção dá também lugar a avaliações subjectivas;

— Embora a participação de uma autoridade para determinar se a entidade abrangida deve ou não notificar as pessoas tenha certamente efeitos positivos, poderá ser pouco viável e difícil de aplicar, podendo ainda desviar recursos destinados a outras prioridades importantes. Se as autoridades não puderem reagir com extrema rapidez, a AEPD receia que um sistema deste tipo possa até diminuir a protecção das pessoas singulares e sujeitar as autoridades a uma pressão excessiva. Assim, globalmente, a AEPD preconiza *criar* um sistema em que caiba às entidades em causa avaliar se devem ou não proceder à notificação;

— Para permitir às autoridades supervisionar as avaliações realizadas pelas entidades abrangidas quanto à questão da notificação, *implementar* as seguintes salvaguardas:

  — *garantir* que as entidades abrangidas sejam obrigadas a notificar as autoridades de todas as violações que preenchem o critério exigido,

  — *atribuir* às autoridades um papel de supervisão que lhes permita ser selectivas, a fim de garantir a sua eficácia. Para tal, inserir o seguinte texto: «*Se o assinante ou pessoa em causa ainda não tiver sido notificado, a autoridade nacional competente, tendo analisado a natureza da violação, pode exigir ao PPECS ou ao ISSP que proceda a essa notificação*»,

  — *aprovar* uma nova disposição que exija que as entidades mantenham uma plataforma de auditoria interna pormenorizada e exaustiva. Para tal, poder-se-á adoptar a seguinte formulação: «*Os PPECS e os ISSP deverão conservar e manter actualizados registos exaustivos que descrevam pormenorizadamente todas as violações da segurança ocorridas, as informações técnicas pertinentes conexas e as medidas correctivas tomadas. Esses registos deverão conter igualmente uma referência a todas as notificações emitidas aos assinantes ou pessoas em causa e às autoridades nacionais competentes, incluindo a respectiva data e conteúdo. Os registos deverão ser apresentados à autoridade nacional competente a pedido desta.*»;

— Para garantir uma implementação coerente do quadro jurídico relativo às violações da segurança, *dar* à Comissão a possibilidade de adoptar medidas de execução técnicas, após consulta prévia da AEPD, do Grupo do Artigo 29.º e de outras partes interessadas relevantes;

— No que respeita às pessoas a notificar, *utilizar* a terminologia da Comissão ou do PE (*pessoas em causa* ou *utilizadores afectados*), uma vez que abrange todas as pessoas cujos dados pessoais tenham sido colocados em risco.

Redes privadas acessíveis ao público

98. Os serviços de comunicações são frequentemente disponibilizados ao público não através de redes públicas, mas sim de redes operadas por entidades privadas (por exemplo, pontos de acesso sem fios disponíveis em hotéis ou aeroportos), que se podem considerar não abrangidas pela directiva. O PE aprovou a emenda 121 (artigo 3.º), que alarga o âmbito de aplicação da directiva por forma a incluir as redes de comunicações públicas e privadas e as redes privadas acessíveis ao público. A este respeito, o PE e o Conselho deverão:

— *Manter* o espírito da emenda 121, mas *reformulando*-a de modo a que o âmbito de aplicação da Directiva «Privacidade e Comunicações Electrónicas» inclua apenas o «*tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações electrónicas publicamente disponíveis em redes de comunicações públicas ou em redes de comunicações privadas acessíveis ao público na Comunidade*». As redes exclusivamente privadas (ao contrário das redes privadas acessíveis ao público) não serão assim explicitamente abrangidas;

— *Alterar* todas as disposições operacionais em conformidade, de modo que se refiram explicitamente não só às redes públicas como também às redes privadas acessíveis ao público;

— *Incluir uma alteração com a seguinte definição: «rede privada acessível ao público é uma rede operada por entidades privadas a que o público em geral tem normalmente acesso sem quaisquer restrições, a título oneroso ou gratuito, ou no contexto de outros serviços ou ofertas, sob reserva de aceitação dos termos e condições aplicáveis»*. Desse modo, reforçar-se-á a segurança jurídica no que se refere às entidades abrangidas pelo novo âmbito de aplicação;

— *Adoptar* um novo considerando segundo o qual a Comissão realizará uma consulta pública sobre a aplicação da Directiva «Privacidade e Comunicações Electrónicas» a todas as redes privadas, com o contributo da AEPD, do Grupo do Artigo 29.º e de outras partes interessadas pertinentes. Especificar que, na sequência dessa consulta pública, a Comissão deverá elaborar as propostas adequadas para alargar ou limitar os tipos de entidades a abranger pela Directiva «Privacidade e Comunicações Electrónicas».

Tratamento de dados de tráfego para fins de segurança

99. Em primeira leitura, o PE aprovou a emenda 181 (n.º 6 do artigo 6.º-A), que autoriza o tratamento dos dados de tráfego para fins de segurança. Na sua posição comum, o Conselho aprovou uma nova versão que enfraquece algumas das salvaguardas em matéria de privacidade. A este respeito, a AEPD recomenda que o PE e o Conselho:

— *Rejeitem* esta disposição na sua totalidade, uma vez que é desnecessária e que, em caso de utilização abusiva, poderá ameaçar indevidamente a protecção de dados e a privacidade das pessoas singulares;

— Em alternativa, caso seja aprovada uma variante da versão actual do n.º 6 do artigo 6.º-A, *incorporem* as salvaguardas em matéria de protecção de dados analisadas no presente parecer (semelhantes às constantes da emenda do PE).

Acções intentadas em caso de infracção à Directiva «Privacidade e Comunicações Electrónicas»

100. O Parlamento aprovou a emenda 133 (n.º 6 do artigo 13.º), que dá às entidades jurídicas a possibilidade de intentar acções junto dos tribunais contra os infractores de qualquer disposição da directiva. Infelizmente, o Conselho não manteve esta emenda. O Conselho e o PE deverão:

— *Aprovar* a disposição que confere às entidades jurídicas, tais como as associações de consumidores e associações profissionais, a possibilidade de intentar acções judiciais em caso de infracção a qualquer disposição da directiva (e não apenas em caso de infracção das disposições relativas ao *spam*, como prevêem actualmente a posição comum e a proposta alterada). O facto de dispor de uma mais ampla diversidade de mecanismos para fazer cumprir a lei estimulará um maior respeito da mesma e uma eficaz aplicação das disposições da Directiva «Privacidade e Comunicações Electrónicas» no seu conjunto.

Resposta ao desafio

101. Em todas as questões acima debatidas, o PE e o Conselho devem dar resposta ao desafio que consiste na definição de regras e disposições adequadas que sejam simultaneamente viáveis e funcionais e que respeitem os direitos das pessoas singulares em matéria de privacidade e protecção de dados. A AEPD espera que as partes envolvidas envidem os maiores esforços para responder a este desafio e que o presente parecer permita contribuir para esses esforços.

Feito em Bruxelas, em 9 de Janeiro de 2009.

Autoridade Europeia para a Protecção de Dados

Peter HUSTINX

Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de directiva do Conselho que obriga os Estados-Membros a manterem um nível mínimo de reservas de petróleo bruto e/ou de produtos petrolíferos

(2009/C 128/05)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente o artigo 8.º,

Tendo em conta a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [1],

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, nomeadamente o artigo 41.º [2],

Tendo em conta o pedido de parecer apresentado pela Comissão nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001, enviado à AEPD em 14 de Novembro de 2008,

ADOPTOU O SEGUINTE PARECER:

I. **INTRODUÇÃO**

1. Em 13 de Novembro de 2008, a Comissão adoptou uma proposta de directiva do Conselho que obriga os Estados-Membros a manterem um nível mínimo de reservas de petróleo bruto e/ou de produtos petrolíferos (a seguir designada «proposta») [3].

2. A proposta tem por objectivo garantir um nível elevado de segurança dos aprovisionamentos de petróleo na Comunidade através de mecanismos fiáveis e transparentes assentes na solidariedade entre os Estados-Membros, manter um nível mínimo de reservas de petróleo ou de produtos petrolíferos e criar os meios processuais necessários para lidar com uma eventual escassez grave.

3. Em 14 de Novembro de 2008, a Comissão enviou a proposta à AEPD para consulta, nos termos do n.º 2 do artigo 28.º do Regulamento (CE) n.º 45/2001. A AEPD congratula-se com o facto de ser consultada sobre o assunto e assinala que esta consulta é mencionada no preâmbulo da proposta, em conformidade com o artigo 28.º do Regulamento (CE) n.º 45/2001.

4. Antes da adopção da proposta, a Comissão consultou a AEPD, a título informal, acerca de um artigo específico do projecto de proposta (o actual artigo 19.º). A AEPD regozijou-se com a consulta informal, uma vez que teve assim oportunidade de formular algumas sugestões antes de a proposta ser adoptada pela Comissão.

II. **ANÁLISE DA PROPOSTA**

Análise geral

5. A presente questão constitui uma boa ilustração da necessidade de ter sempre em consideração as regras de protecção de dados. Numa situação em que se trata da obrigação dos Estados-Membros de manterem reservas petrolíferas de segurança, que são sobretudo propriedade de entidades colectivas, o tratamento de dados pessoais não se afigura uma hipótese muito óbvia, mas, mesmo que não seja encarado como tal, pode ainda assim ocorrer. Convém, de qualquer modo, ter em conta essa possibilidade e agir em conformidade.

6. Na presente situação, são basicamente duas as actividades previstas na directiva que poderão implicar o tratamento de dados pessoais. A primeira delas, a cargo dos Estados-Membros, consiste na recolha de informações sobre as reservas de petróleo e subsequente transmissão dessas informações à Comissão. Quanto à segunda actividade, trata-se do poder da Comissão para efectuar controlos nos Estados-Membros. A recolha de informações acerca dos proprietários de reservas de petróleo pode abranger dados pessoais, como os nomes e os contactos dos directores das companhias. Assim, com essa recolha de informações e com a subsequente transmissão à Comissão, está-se perante o tratamento de dados pessoais, o que determina a aplicabilidade da legislação nacional de execução da Directiva 95/46/CE ou do Regulamento (CE) n.º 45/2001, consoante a pessoa que esteja de facto a tratar os dados. Também o poder conferido à Comissão para realizar controlos em relação às reservas de emergência nos Estados-Membros, o que passa pelo poder de recolher informações em geral, é susceptível de envolver a recolha e, assim, o tratamento de dados pessoais.

[1] JO L 281 de 23.11.1995, p. 31.
[2] JO L 8 de 12.1.2001, p. 1.
[3] COM(2008) 775 final.

7. Na consulta informal, que se limitou à disposição sobre o poder de investigação da Comissão, esta foi aconselhada pela AEPD a determinar se o tratamento de dados pessoais no contexto de uma investigação será meramente incidental ou terá carácter regular e se servirá os objectivos visados. Em função das conclusões dessa apreciação, foram sugeridas duas abordagens.

8. No caso de o tratamento de dados pessoais não estar previsto e ser, pois, meramente incidental, a AEPD recomendou que, em primeiro lugar, se reconheça explicitamente que a sua prática não serve os objectivos da investigação da Comissão, e, em segundo lugar, se declare que os dados pessoais com que a Comissão venha a deparar no decurso da investigação não serão recolhidos nem tidos em conta, sendo imediatamente destruídos se acaso forem recolhidos de forma acidental. Como cláusula de salvaguarda geral, a AEPD sugeriu ainda a inclusão de uma disposição em que se declare que a directiva não prejudicará as regras de protecção de dados estabelecidas na Directiva 95/46/CE e no Regulamento (CE) n.º 45/2001.

9. Se, por outro lado, o tratamento de dados estiver previsto a título regular no contexto de uma investigação da Comissão, a AEPD recomendou a inclusão de uma menção que reflicta o resultado de uma avaliação devidamente conduzida a respeito da protecção de dados. Eis os elementos que dela deverão fazer parte: I) o objectivo concreto do tratamento de dados, II) a necessidade de tratar os dados para alcançar esse objectivo, III) a proporcionalidade do tratamento de dados.

10. Embora os conselhos informais da AEPD apenas digam respeito ao poder de investigação da Comissão, as suas observações também se aplicam à outra grande actividade enunciada na directiva proposta, a saber, a recolha e a transmissão de informações à Comissão por parte dos Estados-Membros.

11. Conforme está patente na versão final da proposta de directiva, a Comissão concluiu que, para os objectivos pretendidos, não se prevê o tratamento de dados pessoais. A AEPD regista com satisfação que a primeira abordagem por si sugerida se encontra plenamente reflectida na proposta.

12. A AEPD manifesta, pois, o seu apoio à forma como a Comissão garantiu o cumprimento das regras de protecção de dados na directiva proposta. Na próxima parte do presente parecer, apenas serão formuladas algumas recomendações de pormenor.

Observações sobre elementos de pormenor

13. O artigo 15.º da proposta de directiva trata da obrigação dos Estados-Membros de enviarem à Comissão um resumo estatístico semanal dos níveis das reservas comerciais mantidas no seu território nacional. As informações em causa, que, em princípio, conterão poucos dados pessoais. Todavia, podem vir a conter informações sobre as pessoas singulares a quem pertencem as reservas de petróleo ou que trabalham para a entidade colectiva proprietária das reservas. Para evitar que os Estados-Membros facultem à Comissão informações desse tipo, o n.º 1 do artigo 15.º prevê que, se o fizerem, «(se absterão) de fazer menção dos nomes dos proprietários das reservas em questão». Embora se deva ter presente que a supressão de um nome nem sempre impedirá que, a partir dos dados, se possa identificar uma pessoa singular, parece que, na situação em apreço (resumo estatístico dos níveis das reservas de petróleo), essa frase suplementar será suficiente para garantir que não sejam transmitidos dados pessoais à Comissão.

14. O poder de investigação da Comissão está previsto no artigo 19.º da proposta de directiva, disposição que revela claramente que a Comissão seguiu a primeira abordagem, conforme enunciado no ponto 8. Prevê o referido artigo que as acções de controlo realizadas pela Comissão não podem envolver o tratamento de dados pessoais. E mesmo que a Comissão venha a deparar com dados pessoais, estes não podem ser tidos em conta e devem ser destruídos em caso de recolha acidental. A fim de alinhar o texto pela formulação utilizada nas leis de protecção de dados, e para evitar todo e qualquer mal-entendido, a AEPD recomenda que, na primeira frase do n.º 2, a palavra «recolha» seja substituída por «tratamento».

15. A AEPD regista com satisfação que a proposta também inclui uma cláusula de salvaguarda geral a respeito da legislação pertinente em matéria de protecção de dados. O artigo 20.º lembra com clareza aos Estados-Membros, à Comissão e a outros órgãos comunitários as obrigações que lhes são impostas, respectivamente, pela Directiva 95/46/CE e pelo Regulamento (CE) n.º 45/2001. A cláusula salienta igualmente os direitos conferidos pelas regras em causa às pessoas a quem os dados dizem respeito, especialmente o direito de oposição ao tratamento, o direito de acesso e o direito de rectificação em caso de inexactidão. Haverá talvez uma observação a fazer quanto à parte onde esta disposição foi inserida no texto da proposta. Pelo seu carácter geral, a disposição não se limita unicamente ao poder de investigação da Comissão. A AEPD recomenda, pois, que o artigo passe para a primeira parte da directiva, sendo colocado, por exemplo, a seguir ao artigo 2.º

16. Também o considerando 25 faz referência à Directiva 95/46/CE e ao Regulamento (CE) n.º 45/2001. É, todavia, pouco claro quanto ao objectivo perseguido, uma vez que apenas menciona a legislação sobre protecção de dados enquanto tal, sem maiores detalhes. Deveria ficar claramente indicado no considerando que as disposições da directiva não prejudicam a legislação mencionada. Além disso, a última frase do considerando leva a crer que a legislação sobre protecção de dados exige explicitamente que os responsáveis pelo tratamento destruam de imediato os dados recolhidos de forma acidental. Trata-se de uma obrigação que, embora possa resultar das regras estabelecidas, não se encontra prevista expressamente na legislação

em causa. É princípio geral da protecção de dados que os dados pessoais não serão conservados por mais tempo do que o necessário para as finalidades para que foram recolhidos ou tratados posteriormente. Se a primeira parte do considerando for adaptada no sentido que acaba de ser proposto, a última frase torna-se supérflua. A AEPD propõe assim que seja suprimida a última frase do considerando 25.

III. **CONCLUSÃO**

17. A AEPD manifesta o seu apoio à forma como a Comissão garantiu o cumprimento das regras de protecção de dados na directiva proposta.

18. Em termos mais específicos, a AEPD recomenda o seguinte:

— na primeira frase do n.º 2 do artigo 19.º, substituição da palavra «recolha» por «tratamento»;

— transferência do artigo 20.º, que é a disposição geral sobre protecção de dados, para a primeira parte da directiva, mais concretamente logo a seguir ao artigo 2.º;

— no considerando 25, aditamento de uma indicação segundo a qual as disposições da directiva não prejudicam o disposto na Directiva 95/46/CE e no Regulamento (CE) n.º 45/2001;

— supressão da última frase do considerando 25.

Feito em Bruxelas, em 3 de Fevereiro de 2009.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

IV

(Informações)

INFORMAÇÕES ORIUNDAS DAS INSTITUIÇÕES E DOS ÓRGÃOS DA UNIÃO EUROPEIA

COMISSÃO

Taxas de câmbio do euro [1]

5 de Junho de 2009

(2009/C 128/06)

1 euro =

	Moeda	Taxas de câmbio		Moeda	Taxas de câmbio
USD	dólar americano	1,4177	AUD	dólar australiano	1,7606
JPY	iene	137,48	CAD	dólar canadiano	1,5657
DKK	coroa dinamarquesa	7,4472	HKD	dólar de Hong Kong	10,9887
GBP	libra esterlina	0,87920	NZD	dólar neozelandês	2,2263
SEK	coroa sueca	10,9250	SGD	dólar de Singapura	2,0530
CHF	franco suíço	1,5191	KRW	won sul-coreano	1 768,65
ISK	coroa islandesa		ZAR	rand	11,4189
NOK	coroa norueguesa	8,9700	CNY	yuan-renminbi chinês	9,6871
BGN	lev	1,9558	HRK	kuna croata	7,3550
CZK	coroa checa	27,003	IDR	rupia indonésia	14 078,75
EEK	coroa estoniana	15,6466	MYR	ringgit malaio	4,9556
HUF	forint	289,10	PHP	peso filipino	67,016
LTL	litas	3,4528	RUB	rublo russo	43,5789
LVL	lats	0,7094	THB	baht tailandês	48,464
PLN	zloti	4,5420	BRL	real brasileiro	2,7345
RON	leu	4,2185	MXN	peso mexicano	18,7066
TRY	lira turca	2,1834	INR	rupia indiana	66,7910

[1] *Fonte*: Taxas de câmbio de referência publicadas pelo Banco Central Europeu.

RECTIFICAÇÕES

Rectificação à Taxa de juro aplicada pelo Banco Central Europeu às suas principais operações de refinanciamento

(Jornal Oficial da União Europeia C 124 de 4 Junho de 2009)

(2009/C 128/07)

Na página 1 e na capa:

em vez de: «a partir de 4 de Junho de 2009: 1,00 %»,

deve ler-se: «a partir de 1 de Junho de 2009: 1,00 %».

Preço das assinaturas 2009 (sem IVA, portes para expedição normal incluídos)

Jornal Oficial da União Europeia, séries L + C, só edição impressa	22 línguas oficiais da UE	1 000 EUR por ano (*)
Jornal Oficial da União Europeia, séries L + C, só edição impressa	22 línguas oficiais da UE	100 EUR por mês (*)
Jornal Oficial da União Europeia, séries L + C, edição impressa + CD-ROM anual	22 línguas oficiais da UE	1 200 EUR por ano
Jornal Oficial da União Europeia, série L, só edição impressa	22 línguas oficiais da UE	700 EUR por ano
Jornal Oficial da União Europeia, série L, só edição impressa	22 línguas oficiais da UE	70 EUR por mês
Jornal Oficial da União Europeia, série C, só edição impressa	22 línguas oficiais da UE	400 EUR por ano
Jornal Oficial da União Europeia, série C, só edição impressa	22 línguas oficiais da UE	40 EUR por mês
Jornal Oficial da União Europeia, séries L + C, CD-ROM mensal (cumulativo)	22 línguas oficiais da UE	500 EUR por ano
Suplemento do Jornal Oficial (série S), Adjudicações e Contratos Públicos, CD-ROM, duas edições por semana	Multilingue: 23 línguas oficiais da UE	360 EUR por ano (= 30 EUR por mês)
Jornal Oficial da União Europeia, série C — Concursos	Língua(s) de acordo com o concurso	50 EUR por ano

(*) Venda avulsa: até 32 páginas: 6 EUR
de 33 a 64 páginas: 12 EUR
mais de 64 páginas: preço fixado caso a caso

O *Jornal Oficial da União Europeia*, publicado nas línguas oficiais da União Europeia, pode ser assinado em 22 versões linguísticas. Compreende as séries L (Legislação) e C (Comunicações e Informações).

Cada versão linguística constitui uma assinatura separada.

Por força do Regulamento (CE) n.º 920/2005 do Conselho, publicado no Jornal Oficial L 156 de 18 de Junho de 2005, nos termos do qual as instituições da União Europeia não estão temporariamente vinculadas à obrigação de redigir todos os seus actos em irlandês nem a proceder à sua publicação nessa língua, os Jornais Oficiais publicados em irlandês são comercializados à parte.

A assinatura do Suplemento do Jornal Oficial (série S — Adjudicações e Contratos Públicos) reúne a totalidade das 23 versões linguísticas oficiais num CD-ROM multilingue único.

A pedido, a assinatura do *Jornal Oficial da União Europeia* dá direito à recepção dos diversos anexos do Jornal Oficial. Os assinantes são avisados da publicação dos anexos através de um «Aviso ao leitor» inserido no *Jornal Oficial da União Europeia*.

Vendas e assinaturas

As publicações pagas editadas pelo Serviço das Publicações estão disponíveis através da nossa rede de distribuidores comerciais, cuja lista está disponível na internet no seguinte endereço:

http://publications.europa.eu/others/agents/index_pt.htm

EUR-Lex (http://eur-lex.europa.eu) oferece acesso directo e gratuito ao direito da União Europeia. Este sítio permite consultar o *Jornal Oficial da União Europeia* e inclui igualmente os tratados, a legislação, a jurisprudência e os actos preparatórios da legislação.

Para mais informações sobre a União Europeia, consultar: http://europa.eu

Serviço das Publicações
Publications.europa.eu

SERVIÇO DAS PUBLICAÇÕES OFICIAIS DAS COMUNIDADES EUROPEIAS
L-2985 LUXEMBURGO

PT