I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre as negociações em curso da União Europeia sobre um Acordo Comercial Anticontrafacção (ACTA)

(2010/C 147/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia e, nomeadamente, o seu artigo 16.º,

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia e, nomeadamente, o seu 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 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, [2]

Tendo em conta o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [3] e, nomeadamente, o seu artigo 41.º,

ADOPTOU O PRESENTE PARECER:

I. **INTRODUÇÃO**

1. A União Europeia encontra-se envolvida em negociações tendentes à elaboração de um Acordo Comercial Anticontrafacção (ACTA). Estas negociações foram iniciadas em 2007 por um primeiro grupo de partes interessadas, tendo depois prosseguido com mais participantes, nomeadamente, a Austrália, o Canadá, a Coreia, os Estados Unidos, o Japão, Marrocos, o México, a Nova Zelândia, Singapura, a Suíça e a União Europeia. A Comissão Europeia recebeu um mandato do Conselho para participar nestas negociações em 2008.

2. A AEPD reconhece que o comércio transfronteiriço de bens contrafeitos e pirateados, que muitas vezes envolve redes de crime organizado, é uma preocupação crescente e que exige a adopção de mecanismos de cooperação adequados a nível internacional para a luta contra esta forma de criminalidade.

3. A AEPD salienta que a negociação pela União Europeia de um acordo multilateral, cujo objecto principal é garantir o respeito dos direitos de propriedade intelectual, levanta questões de relevo em relação ao impacto das medidas de combate à contrafacção e à pirataria sobre os direitos fundamentais das pessoas, em particular o seu direito à privacidade e à protecção de dados.

4. Nesse sentido, a AEPD lamenta em particular não ter sido consultada pela Comissão Europeia em relação ao conteúdo de um acordo dessa natureza. Assim, a AEPD adoptou, por sua iniciativa, o presente parecer, com base no artigo 41.º, n.º 2, do Regulamento (CE) n.º 45/2001, no intuito de dar orientações à Comissão sobre os aspectos relacionados com a privacidade e a protecção de dados que devem ser tidos em consideração nas negociações do ACTA.

II. **PONTO DA SITUAÇÃO E CONTEÚDO PREVISTO DO ACTA**

5. A 7.ª ronda negocial realizou-se no México, de 26 a 29 de Janeiro de 2010, tendo por objectivo a conclusão de um acordo durante o ano de 2010. No entanto, até à data não foi ainda divulgado um projecto oficial do acordo.

[1] JO L 281 de 23.11.1995, p. 31.
[2] JO L 201 de 31.7.2002, p. 37.
[3] JO L 8 de 12.1.2001, p. 1.

6. As negociações visam a adopção de um novo acordo multilateral que se destina a reforçar o respeito dos direitos de propriedade intelectual (DPI) e a combater a contrafacção e a pirataria. Se for adoptado, este novo acordo criará normas internacionais aperfeiçoadas em matéria de combate às infracções a grande escala dos DPI. A DG Comércio da Comissão Europeia salientou, em particular, que «o enfoque recai nas actividades de contrafacção e pirataria com um impacto significativo nos interesses comerciais e não tanto nas actividades dos cidadãos comuns». ([4])

7. No que toca ao conteúdo do acordo, a *Síntese dos principais elementos em análise* divulgada pela DG Comércio da Comissão Europeia em Novembro de 2009 indica que a realização do objectivo de luta contra a pirataria e a contrafacção do ACTA terá três componentes principais: i) a cooperação internacional, ii) as práticas de aplicação e iii) a definição de um quadro jurídico para garantir o respeito dos DPI em vários domínios identificados, em particular no ambiente digital. ([5]) As medidas previstas abordarão, designadamente, os procedimentos legais (nomeadamente injunções, providências), o papel e as responsabilidades dos fornecedores de serviços Internet (FSI) na prevenção de infracções dos direitos de autor através da Internet, assim como as medidas de cooperação transfronteiriças para impedir que os bens atravessem as fronteiras. Contudo, a informação tornada pública apenas descreve as linhas gerais do acordo e não apresenta pormenores de medidas específicas e concretas.

8. A AEPD observa que, mesmo que o ACTA vise apenas as infracções a grande escala dos DPI, não se pode excluir que as actividades dos cidadãos comuns sejam capturadas nas malhas do ACTA, em especial porque as medidas de aplicação ocorrem no ambiente digital. A AEPD salienta que isso obrigará à criação das garantias necessárias de protecção dos direitos fundamentais das pessoas. Além disso, a legislação em matéria de protecção de dados abrange todas as pessoas, incluindo aquelas que eventualmente participem em actividades de contrafacção e pirataria; o combate às infracções a grande escala irá certamente implicar o tratamento de dados pessoais.

9. Nesse sentido, a AEPD incita vivamente a Comissão Europeia a estabelecer um diálogo público e transparente sobre o ACTA, porventura por intermédio de uma consulta pública, a qual também contribuiria para assegurar que as medidas a aprovar estivessem em conformidade com os requisitos da legislação comunitária em matéria de privacidade e de protecção de dados.

III. ÂMBITO DAS OBSERVAÇÕES DA AEPD

10. A AEPD apela à UE, em particular à Comissão Europeia que recebeu o mandato para concluir o acordo, que procure alcançar um equilíbrio adequado entre as exigências em matéria de protecção dos direitos da propriedade intelectual e os direitos à privacidade e à protecção dos dados das pessoas singulares.

11. A AEPD realça que a privacidade e a protecção de dados são valores fundamentais da União Europeia, reconhecidos no artigo 8.º da CEDH e nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia ([6]), que devem ser respeitados em todas as políticas e regras adoptadas pela UE, conforme estabelece o artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

12. Além disso, a AEPD salienta que qualquer acordo alcançado pela União Europeia em relação ao ACTA deve estar em conformidade com as obrigações legais impostas à UE em matéria de privacidade e protecção de dados, conforme está estabelecido, nomeadamente, na Directiva 95/46/CE, na Directiva 2002/58/CE ([7]) e na jurisprudência do Tribunal Europeu dos Direitos do Homem ([8]) e do Tribunal de Justiça ([9]).

13. A privacidade e a protecção de dados devem ser tidas em conta logo desde o início das negociações e não após a definição e a decisão sobre os regimes e os procedimentos, quando, portanto, é demasiado tarde para encontrar soluções alternativas e compatíveis com a privacidade.

14. Face à escassa informação tornada pública, a AEPD observa que não está em condições de apresentar uma análise das disposições específicas do ACTA. Neste seu parecer, a AEPD irá, por conseguinte, centrar-se na descrição das eventuais ameaças à privacidade e à protecção de dados de possíveis medidas concretas que o acordo, tal como foi divulgado, poderá suscitar em dois domínios diferentes: respeito dos direitos de propriedade intelectual no ambiente digital (capítulo IV) e mecanismos de cooperação internacional (capítulo V).

([4]) Ver http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, p. 2.

([5]) Ver nota de rodapé n.º 2, atrás.

([6]) Carta dos Direitos Fundamentais da União Europeia, JO C 303 de 14.12.2007, p. 1.

([7]) Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), JO L 201 de 31.7.2002, p. 37.

([8]) Interpretação dos principais elementos e condições estabelecidos no artigo 8.º da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (CEDH) aprovada em Roma, em 4 de Novembro de 1950, conforme a sua aplicação às diferentes áreas. Ver, em particular, a jurisprudência mencionada noutra secção do presente parecer.

([9]) Ver, em particular o processo C-275/06, *Productores de Música de España* (Promusicae), Colectânea [2008], p. I-271 e o processo C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, ainda não publicado.

IV. RESPEITO DOS DIREITOS DE PROPRIEDADE INTELECTUAL NO AMBIENTE DIGITAL

IV.1. Necessidade de analisar as implicações em termos de privacidade/protecção de dados das «políticas de corte de acesso à Internet em três etapas»

15. Segundo a Comissão Europeia, o ACTA irá criar um quadro jurídico para combater a pirataria no ambiente digital. ([10]) Este quadro jurídico criará as condições nas quais os FSI e outros intermediários em linha ([11]) poderão ser responsabilizados em resultado da utilização das suas instalações para a transmissão de material que viole direitos de autor. O quadro jurídico pode ainda estipular as medidas e os remédios a aplicar aos utilizadores da Internet que carreguem ou descarreguem material que viole direitos de autor. Embora não tenham sido oficialmente divulgados pormenores desse enquadramento, tendo em conta a informação disponível nos diferentes canais, é previsível que nele se inclua a obrigação de os FSI adoptarem «políticas de corte de acesso à Internet em três etapas», que também são designados por regimes de «resposta gradual». Este tipo de regimes permitiria aos titulares dos direitos de autor vigiarem os utilizadores da Internet e identificarem os alegados infractores dos direitos de autor. Após os titulares dos direitos de autor contactarem o FSI do alegado infractor, o FSI avisaria o utilizador identificado como infractor de que o seu acesso à Internet seria desligado após três advertências.

16. Em simultâneo com as negociações sobre o ACTA, começam a ser aplicadas políticas de corte de acesso à Internet em três etapas em alguns Estados-Membros, como a França. Estas políticas também têm sido debatidas em vários fóruns da União Europeia, como o diálogo com as partes interessadas sobre carregamentos e descarregamentos ilegais actualmente em curso, sob a égide da DG MARKT, no âmbito da aprovação da comunicação da Comissão sobre o reforço do controlo do respeito dos direitos de propriedade intelectual no mercado interno. ([12]) Este tema também é debatido no Parlamento Europeu no contexto do debate em curso sobre um projecto de resolução do Parlamento Europeu sobre o reforço do controlo do respeito dos direitos de propriedade intelectual no mercado interno (designado por «relatório Gallo»).

17. Tais práticas são altamente invasivas da esfera privada das pessoas, pois implicam a vigilância generalizada das actividades dos utilizadores da Internet, incluindo as actividades legítimas. Afectam milhões de utilizadores da Internet que cumprem a lei, nomeadamente um grande número de crianças e adolescentes. São realizadas por entidades privadas e não pelas autoridades responsáveis pela aplicação da lei. Além disso, actualmente, a Internet desempenha um papel fundamental em quase todos os aspectos da vida moderna, pelo que os efeitos do corte de acesso à Internet podem ser enormes, impedindo o acesso das pessoas ao trabalho, à cultura, às aplicações de governo electrónico, etc.

18. Face ao exposto, torna-se relevante avaliar em que medida estas políticas estão em conformidade com a legislação da União Europeia em matéria de protecção de dados e privacidade, mais concretamente, se as políticas de corte de acesso à Internet em três etapas constituem uma medida necessária ao respeito dos direitos de propriedade intelectual. Nesse âmbito, deve ainda ser analisada a existência de outros métodos menos invasivos.

19. Ainda não é certo que as políticas de corte de acesso à Internet em três etapas venham a integrar o ACTA. No entanto, estas políticas poderão vir a ser aplicadas noutras áreas onde teriam um potencial enorme impacto na protecção dos dados pessoais e da privacidade. Por estes motivos, a AEPD considera necessário abordá-las no presente parecer. Antes de proceder à análise atrás mencionada, a AEPD irá descrever brevemente o quadro jurídico aplicável à protecção de dados e à privacidade.

20. Importa salientar que, além da protecção de dados e da privacidade, as políticas de corte de acesso à Internet em três etapas suscitam dúvidas em relação a outros valores, como o processo equitativo e a liberdade de expressão. No entanto, o presente parecer visará apenas as questões relacionadas com a protecção dos dados pessoais e a privacidade das pessoas singulares.

IV.2. As políticas de corte de acesso à Internet em três etapas e a aplicação do quadro jurídico comunitário em matéria de protecção de dados/privacidade

Configuração das políticas de corte de acesso à Internet em três etapas

21. Muito resumidamente, ao abrigo das políticas de corte de acesso à Internet em três etapas, os titulares de direitos de autor utilizam meios técnicos automatizados, eventualmente fornecidos por terceiros, para identificar alegadas violações dos direitos de autor mediante a vigilância das actividades dos utilizadores da Internet, por exemplo, através da supervisão de fóruns, de blogues ou fazendo-se passar por utilizadores que partilham ficheiros em redes

([10]) Ver nota de rodapé n.º 2, atrás.

([11]) Os diferentes intermediários em linha podem ser definidos com base nas suas funções. Contudo, no mundo real, os intermediários normalmente acumulam várias funções. Entre os intermediários em linha incluem-se: a) *fornecedores de acesso:* os utilizadores ligam-se à rede através de uma ligação estabelecida com o servidor do *fornecedor de acesso*; b) *fornecedores de rede*: fornecem os encaminhadores, ou seja, as instalações técnicas necessárias para a transmissão de dados; c) *fornecedores de alojamento*: alugam espaço nos seus servidores para o qual os utilizadores ou os fornecedores de conteúdo podem carregar conteúdo. Os utilizadores podem carregar ou descarregar materiais de um serviço em linha, como um sistema de boletim informativo ou redes posto-a-posto (P2P).

([12]) Comunicação da Comissão ao Conselho, ao Parlamento Europeu e ao Comité Económico e Social Europeu — Reforçar o controlo do respeito dos direitos de propriedade intelectual no mercado interno, Bruxelas, 11 de Setembro de 2009, COM(2009) 467 final.

posto-a-posto (P2P) para identificar outros utilizadores que, alegadamente, trocam materiais protegidos por direitos de autor. ([13])

22. Após identificarem os alegados utilizadores da Internet envolvidos em práticas que violam direitos de autor, nomeadamente mediante a recolha dos endereços de Protocolo Internet (endereços IP) desses utilizadores, os titulares dos direitos de autor enviam os endereços IP dos referidos utilizadores para o(s) fornecedor(es) de serviços Internet pertinentes, que avisam o utilizador a quem pertence o endereço IP da sua potencial violação de direitos de autor. Após um determinado número de advertências pelo FSI, este cessa ou suspende automaticamente a ligação à Internet do assinante do serviço. ([14])

Quadro jurídico comunitário em matéria de protecção de dados/ /privacidade

23. As políticas de corte de acesso à Internet em três etapas têm de cumprir os requisitos que emanam do direito à privacidade, conforme estipula o artigo 8.º da CEDH e o artigo 7.º da Carta dos Direitos Fundamentais, e do direito à protecção de dados, conforme estipula o artigo 8.º da Carta dos Direitos Fundamentais e o artigo 16.º do TFUE, e nos termos da Directiva 95/46/CE e na Directiva 2002/58/CE.

24. Na opinião da AEPD, a vigilância do comportamento de um utilizador na Internet e a recolha dos seus endereços IP equivalem a uma ingerência nos seus direitos de respeito da vida privada e da inviolabilidade de correspondência; por outras palavras, existe uma ingerência no direito à vida privada. Esta opinião está em consonância com a jurisprudência do Tribunal Europeu dos Direitos do Homem. ([15])

25. A Directiva 95/46/CE é aplicável ([16]) visto que as políticas de corte de acesso à Internet em três etapas implicam o processamento de endereços IP que, em determinadas circunstâncias, sem dúvida devem ser considerados dados pessoais. Os endereços IP são identificadores que se assemelham a uma sequência de números separados por pontos, como 122.41.123.45. Um contrato com um fornecedor de serviços Internet permite ao assinante ter acesso à Internet. Sempre que o assinante tiver acesso à Internet, é-lhe atribuído um endereço IP através do dispositivo usado para o acesso à Internet (um computador, por exemplo). ([17])

26. Se um utilizador realizar uma determinada actividade, por exemplo, carregar material para a Internet, o utilizador poderá ser identificado por terceiros através do endereço IP que utilizar. Por exemplo, o utilizador com o endereço IP 122.41.123.45 carrega material que alegadamente viola direitos de autor para um serviço P2P às 15h00 do dia 1 de Janeiro de 2010. O FSI poderá associar esse endereço IP ao nome do assinante a quem o endereço foi atribuído e, assim, determinar a sua identidade.

27. Considerando a definição de dados pessoais constante do artigo 2.º da Directiva 95/46/CE, «qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação» ([18]), a única conclusão possível é que os endereços IP e as informações sobre as actividades associadas aos referidos endereços constituem dados pessoais em todos os casos pertinentes para o presente parecer. Na verdade, um endereço IP funciona como um número de identificação que permite determinar o nome do assinante ao qual o endereço IP foi atribuído. Além disso, as informações recolhidas sobre o assinante com esse endereço IP («carregou determinado material para o sítio Web ZS às 15h00 de 1 de Janeiro de 2010») *é relativa a*, ou seja, diz directamente respeito às actividades de uma pessoa identificável (o detentor do endereço IP) e, por conseguinte, devem ser consideradas dados pessoais.

([13]) A tecnologia P2P é uma arquitectura de *software* de computação distribuída que permite a computadores individuais ligarem-se e comunicarem directamente com outros computadores.

([14]) Exemplos de sanções alternativas são a limitação da funcionalidade da ligação à Internet, como, por exemplo, a velocidade de ligação, o volume de dados, etc.

([15]) Ver, nomeadamente, TEDH 26 de Junho de 2006, *Weber e Saravia contra Alemanha* (dec.), n.º 54934/00, ponto 77, e TEDH 1 de Julho de 2008, *Liberty e outros contra o Reino Unido*, n.º 58243/00.

([16]) O Tribunal de Justiça adopta uma abordagem genérica quanto à aplicabilidade da Directiva 95/46/CE, cujas disposições devem ser interpretadas à luz do artigo 8.º da CEDH. O Tribunal de Justiça declarou no seu acórdão de 20 de Maio de 2003, *Rundfunk*, processos apensos C-465/00, C-138/01 e C-139/01, Colectânea [2003], p. I-4989, ponto 68, que «as disposições da Directiva 95/46/CE, na medida em que regulam o tratamento de dados pessoais susceptíveis de pôr em causa as liberdades fundamentais e, em especial, o direito à vida privada, devem necessariamente ser interpretadas à luz dos direitos fundamentais que, segundo jurisprudência constante, são parte integrante dos princípios gerais de direito cujo respeito é assegurado pelo Tribunal de Justiça».

([17]) O endereço IP que o FSI atribui ao utilizador pode ser o mesmo sempre que o utilizador navegar na Internet (neste caso designado por endereço IP estático). Os outros endereços IP são dinâmicos, o que significa que o fornecedor de acesso à Internet atribui um endereço IP diferente aos seus clientes sempre que estes têm acesso à Internet. Como é óbvio, o FSI pode associar o endereço IP à conta do assinante a que o endereço IP (estático ou dinâmico) foi atribuído.

([18]) O considerando 26 complementa esta definição: «Considerando que os princípios da protecção devem aplicar-se a qualquer informação relativa a uma pessoa identificada ou identificável; que, para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa; que os princípios da protecção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável; … ».

28. Estas opiniões são integralmente partilhadas pelo Grupo de Trabalho de Protecção de Dados do Artigo 29.º que, num documento sobre as questões de protecção de dados ligadas aos direitos de propriedade intelectual, afirmou que os endereços IP recolhidos para garantir o respeito dos direitos de propriedade intelectual, ou seja, para identificar os utilizadores da Internet que alegadamente violaram direitos de propriedade intelectual, são dados pessoais na medida em que são utilizados para a aplicação dos referidos direitos contra uma determinada pessoa. ([19])

29. A Directiva 2002/58/CE também é aplicável, pois as políticas de corte de acesso à Internet em três etapas implicam a recolha de dados sobre o tráfego e as comunicações. A Directiva 2002/58/CE regula a utilização desses dados e estabelece o princípio da confidencialidade das comunicações efectuadas através de redes de comunicações públicas e dos dados inerentes a essas comunicações.

IV.3. **Necessidade das políticas de corte de acesso à Internet em três etapas**

30. O artigo 8.º da CEDH estabelece o princípio da necessidade, segundo o qual qualquer medida que viole o direito à vida privada só é permitida se constituir uma medida que, numa sociedade democrática, seja necessária para o fim legítimo a que se destina. ([20]) O princípio da necessidade também está patente nos artigos 7.º e 13.º da Directiva 95/46/CE e no artigo 15.º da Directiva 2002/58/CE. ([21]) Este princípio exige uma análise da proporcionalidade da medida, que deve ser avaliada com base no equilíbrio dos interesses envolvidos perante o contexto da sociedade democrática no seu conjunto. ([22]) Além disso, implica a avaliação da eventual existência de medidas menos intrusivas.

31. Embora a AEPD reconheça a importância do respeito dos direitos de propriedade intelectual, considera que a política de corte de acesso à Internet em três etapas na sua versão actual — nomeadamente com determinados elementos de aplicação geral — constitui uma medida desproporcionada e, por conseguinte, não pode ser considerada uma medida necessária. A AEPD está ainda convicta de que existem soluções alternativas, menos intrusivas, ou que as políticas pretendidas podem ser executadas de uma forma menos intrusiva ou com um âmbito mais limitado. Além disso, a um nível jurídico mais aprofundado, a abordagem das três etapas também não é isenta de problemas. Estas conclusões serão explicadas adiante.

Desproporcionalidade das políticas com a abordagem das três etapas

32. A AEPD pretende salientar as vastas implicações das medidas propostas. A este respeito, importa mencionar os seguintes elementos:

i) A vigilância (não anunciada) afectaria milhões de pessoas e *todos* os utilizadores, independentemente de estarem sob suspeita.

ii) A vigilância implicaria a gravação sistemática de dados, alguns dos quais passíveis de originar processos civis ou penais; além disso, parte da informação recolhida seria, por isso, considerada dados sensíveis na acepção do artigo 8.º da Directiva 95/46/CE, obrigando a salvaguardas mais rigorosas.

iii) A vigilância é susceptível de detectar numerosos casos de «falsos positivos». A violação dos direitos de autor não é uma questão a que se possa responder com um simples «sim» ou «não». Muitas vezes, os tribunais são obrigados a analisar uma grande quantidade de pormenores técnicos e jurídicos ao longo de dezenas de páginas, a fim de determinarem se existe um ilícito ([23]).

([19]) Grupo de Trabalho de Protecção de Dados do Artigo 29.º, Documento de trabalho sobre as questões de protecção de dados ligadas aos direitos de propriedade intelectual (WP 104), adoptado em 18 de Janeiro de 2005. Este grupo de trabalho foi criado ao abrigo do artigo 29.º da Directiva 95/46/CE. É um órgão consultivo independente europeu sobre a protecção de dados e a privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Directiva 95/46/CE e no artigo 15.º da Directiva 2002/58/CE. Ver também o parecer do grupo de trabalho 4/2007 sobre o conceito de dados pessoais (WP 136), adoptado em 20 de Junho de 2007, nomeadamente na página 16.

([20]) O artigo 8.º da CEDH refere expressamente o requisito de que qualquer ingerência ou restrição seja «necessária numa sociedade democrática».

([21]) O artigo 13.º da Directiva 95/46/CE apenas permite uma restrição quando «constitua uma medida necessária à protecção: a) Da segurança do Estado; b) Da defesa; c) Da segurança pública; d) Da prevenção, investigação, detecção e repressão de infracções penais e de violações da deontologia das profissões regulamentadas; e) De um interesse económico ou financeiro importante de um Estado-Membro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal; f) De missões de controlo, de inspecção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d) e e); g) De pessoa em causa ou dos direitos e liberdades de outrem». O artigo 15.º da Directiva 2002/58/CE dispõe que «essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.º 1 do artigo 13.º da Directiva 95/46/CE».

([22]) Ver também TEDH, 2 de Agosto de 1984, *Malone contra o Reino Unido*, Série A n.º 82, p. 32, pontos 81 e seguintes e TEDH 4 de Dezembro de 2008, *Marper contra o Reino Unido* [GS], n.º 30562/04 e n.º 30566/04, pontos 101 e seguintes.

([23]) Os tribunais poderão ter de avaliar se o material está efectivamente protegido por direitos de autor, que direitos foram violados, se a utilização se enquadra no âmbito da utilização justa («fair use»), a lei aplicável, os danos, etc.

iv) Os *efeitos* potenciais da vigilância, que podem levar ao corte de acesso à Internet. Esta situação contenderia com o direito à liberdade de expressão, a liberdade de informação e o acesso à cultura, a aplicações de governo electrónico, a mercados, ao correio electrónico e, nalguns casos, com actividades de âmbito profissional. Neste contexto, é particularmente importante ter a noção de que os efeitos não se cingiriam ao alegado infractor, afectando todos os membros da família que utilizassem a mesma ligação à Internet, incluindo crianças que utilizam a Internet para as suas actividades escolares.

v) A entidade responsável pela avaliação e pelas decisões é geralmente uma entidade privada (ou seja, os titulares dos direitos ou o FSI). A AEPD já manifestou num parecer anterior as suas dúvidas quanto à vigilância de pessoas por entidades privadas (por exemplo, os FSI ou os titulares dos direitos), em domínios que, em princípio, se inserem na esfera de competências das autoridades responsáveis pela aplicação da lei ([24]).

33. A AEPD não está convencida de que os benefícios das medidas compensem o impacto nos direitos fundamentais das pessoas. A protecção dos direitos de autor é um interesse dos titulares dos direitos e da sociedade. No entanto, as limitações aplicadas aos direitos fundamentais não parecem justificadas quando se compara a gravidade da ingerência, ou seja, a escala da devassa da vida privada patente nos elementos atrás expostos, com os benefícios esperados, nomeadamente a prevenção da violação dos direitos de propriedade intelectual, que se caracteriza por um grande número de pequenas infracções de direitos de propriedade intelectual. Conforme se pode ler nas conclusões da advogada-geral Kokott no caso *Promusicae*: «não é seguro que o filesharing privado, especialmente quando é feito sem fins lucrativos, represente uma ameaça suficientemente grave para justificar a invocação dessa excepção. Na verdade, discute-se em que medida o filesharing privado provoca um dano real» ([25]).

34. Neste âmbito, vale a pena recordar também a reacção do Parlamento Europeu aos «regimes de três etapas» no contexto da revisão do pacote legislativo relativo às telecomunicações, em particular da alteração n.º 138 à directiva-quadro. ([26]) Esta alteração estabelecia que qualquer restrição aos direitos ou às liberdades fundamentais apenas pudesse ser aplicada se fosse adequada, proporcional e necessária no contexto de uma sociedade democrática, devendo a sua execução ser sujeita a garantias processuais adequadas nos termos da CEDH e dos princípios gerais do direito comunitário, incluindo o da protecção jurisdicional efectiva e o do processo equitativo. ([27])

35. Nesta perspectiva, a AEPD salienta ainda que qualquer limitação dos direitos fundamentais estará sujeita a um controlo apertado a nível da UE e nacional. A este respeito, é possível estabelecer um paralelo com a directiva relativa à conservação de dados, Directiva 2006/24/CE ([28]), a qual derroga do princípio geral da protecção de dados que dita a eliminação dos dados quando deixam de ser necessários para a finalidade para a qual foram recolhidos. Esta directiva estipula a conservação de dados relativos ao tráfego para efeitos de combate aos crimes graves. Importa salientar que a conservação só é permitida para «crimes graves», que a conservação está limitada a «dados de tráfego» (o que, em princípio, exclui a informação sobre o conteúdo das comunicações) e que são aduzidas garantias rigorosas. Contudo, foram suscitadas dúvidas quanto à sua compatibilidade com as normas relativas aos direitos fundamentais; o Tribunal Constitucional da Roménia decidiu que a conservação global é incompatível com os direitos fundamentais ([29]) e existe actualmente um processo pendente no Tribunal Constitucional da Alemanha. ([30])

Existência de outros meios menos intrusivos

36. As conclusões *supra* são reforçadas pelo facto de existirem meios menos intrusivos para o mesmo fim. A AEPD insiste que se analisem e experimentem esses modelos menos intrusivos.

([24]) Parecer da AEPD sobre a proposta de decisão do Parlamento Europeu e do Conselho que estabelece um programa comunitário plurianual para a protecção das crianças na utilização da Internet e de outras tecnologias das comunicações, JO C 2 de 7.1.2009, p. 2.

([25]) Ver o processo mencionado na nota de rodapé n.º 8, ponto 106.

([26]) Ver Directiva 2009/140/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, JO L 337 de 18.12.2009, p. 37.

([27]) Redacção final da «alteração n.º 138»: «Artigo 1.3-A. As medidas tomadas pelos Estados-Membros relativamente ao acesso ou à utilização de serviços e aplicações através de redes de comunicações electrónicas pelos utilizadores finais devem respeitar os direitos e as liberdades fundamentais das pessoas singulares, conforme garantidas pela Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e pelos princípios gerais do direito comunitário. Qualquer dessas medidas relativas ao acesso ou à utilização de serviços e aplicações através de redes de comunicações electrónicas pelos utilizadores finais, susceptível de restringir esses direitos ou liberdades fundamentais, só pode ser aplicada se for adequada, proporcional e necessária no contexto de uma sociedade democrática, devendo a sua execução ser sujeita a garantias processuais adequadas nos termos da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e dos princípios gerais do direito comunitário, incluindo o da protecção jurisdicional efectiva e o do processo equitativo. Nestas circunstâncias, essas medidas só podem ser tomadas no devido respeito pelo princípio da presunção de inocência e pelo direito à privacidade. É garantido um procedimento prévio, justo e imparcial, incluindo o direito de audiência do(s) interessado(s), sem prejuízo da necessidade de prever condições e mecanismos processuais apropriados em casos de urgência devidamente justificados em conformidade com a Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais. É garantido o direito a uma fiscalização jurisdicional efectiva e atempada.»

([28]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, JO L 105 de 13.4.2006, p. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. Neste contexto, a AEPD recorda que a Directiva 2002/22/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (directiva serviço universal), com a última redacção que lhe foi dada, que integra o pacote legislativo para as telecomunicações recém-reformado, contém regras e procedimentos para limitar as pequenas violações de direitos de autor entre consumidores. ([31]) Entre esses procedimentos conta-se a obrigação de os Estados-Membros produzirem informação de interesse público normalizada sobre vários temas, com menção específica das violações dos direitos de autor e de direitos conexos, bem como as respectivas consequências jurídicas ([32]). Os Estados-Membros podem depois solicitar aos FSI a distribuição dessa informação a todos os seus clientes e a sua inclusão nos respectivos contratos.

38. O sistema destina-se a informar e a dissuadir da divulgação de informação sujeita a direitos de autor e da prática de actividades ilícitas, ao mesmo tempo que evita a vigilância da utilização da Internet e outras dúvidas relacionadas com a privacidade e a protecção de dados. A directiva relativa aos direitos dos cidadãos deve ser aplicada até Maio de 2001, mas esses procedimentos ainda não estão em vigor. Por conseguinte, ainda não houve oportunidades para colocar à prova as suas vantagens. Assim, parece prematuro desvalorizar os potenciais resultados positivos destes novos procedimentos e adoptar as «políticas de corte de acesso à Internet em três etapas», que são muito mais limitadoras dos direitos fundamentais.

39. Além do atrás exposto, importa recordar que a Directiva 2004/48/CE, de 28 de Abril de 2004, relativa ao respeito dos direitos de propriedade intelectual prevê vários instrumentos para garantir o respeito dos direitos de propriedade intelectual em tribunal (analisados adiante, nos pontos 43 e seguintes). ([33])

([31]) Ver Directiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, JO L 337 de 18.12.2009, p. 11.

([32]) Em particular, o artigo 21.º, n.º 4, da Directiva 2009/136/CE estabelece que «Os Estados-Membros podem exigir que as empresas referidas no n.º 3 forneçam, quando adequado, informações gratuitas de interesse público aos actuais e aos novos assinantes, utilizando meios idênticos aos que são vulgarmente utilizados por essas empresas na sua comunicação com os assinantes. Nesse caso, essas informações devem ser prestadas pelas autoridades públicas competentes, num formato normalizado, e incluir, nomeadamente, os seguintes pontos: a) As utilizações mais comuns dos serviços de comunicações electrónicas para a prática de actividades ilícitas ou divulgação de conteúdos nocivos, em particular nos casos em que possa haver desrespeito dos direitos e liberdades fundamentais de outrem, incluindo violações dos direitos de autor e direitos conexos, e as respectivas consequências jurídicas (…).» Além disso, nos termos do artigo 20.º, n.º 2, «Os Estados-Membros podem também exigir que o contrato inclua informações, fornecidas pelas autoridades competentes, sobre a utilização das redes e os serviços de comunicações electrónicas para actividades ilícitas ou divulgação de conteúdos nocivos, bem como sobre os meios de protecção contra riscos para a segurança pessoal, para a privacidade e para os dados pessoais referidos na alínea a) do n.º 4 do artigo 21.º e relevantes para o serviço prestado».

([33]) JO L 157 de 30.4.2004, p. 45 (a seguir: Directiva RDPI).

40. A Directiva RDPI só recentemente começou a ser transposta para as ordens jurídicas dos Estados-Membros. Ainda não houve tempo suficiente para avaliar se as suas disposições são adequadas para garantir o respeito dos direitos de propriedade intelectual. Por conseguinte, a eventual necessidade de substituir o sistema actual, baseado em processos judiciais e que ainda não foi testado, afigura-se, no mínimo, duvidosa. Face ao atrás exposto, coloca-se a inevitável questão dos motivos pelos quais as sanções civis e penais vigentes em matéria de direitos de autor não são adequadas para as infracções actuais. Assim, antes de propor medidas políticas do tipo em causa, a Comissão deve produzir informação fiável que demonstre por que razão o quadro jurídico actual não produziu os efeitos esperados.

41. Além disso, não há elementos que permitam aferir se foram analisados a fundo modelos económicos alternativos que não impliquem a vigilância sistemática das pessoas. Por exemplo, se os titulares dos direitos de autor demonstrassem os prejuízos em que incorrem devido à utilização de P2P, os titulares dos direitos e os FSI poderiam, por exemplo, experimentar assinaturas de acesso à Internet diferenciadas em que parte do preço de uma assinatura com acesso ilimitado fosse atribuída aos titulares dos direitos de autor.

Possibilidade de vigilância com objectivos específicos e menos intrusiva

42. Além da utilização de modelos totalmente diferentes, que devem ser investigados e testados, a vigilância com objectivos específicos poderia ser sempre utilizada de uma forma menos intrusiva.

43. O respeito dos direitos de propriedade intelectual também pode ser garantido mediante a vigilância de um número reduzido de pessoas suspeitas de violação de direitos de autor em larga escala. A Directiva RDPI fornece algumas orientações nesse sentido, estabelecendo as condições em que as autoridades podem ordenar a divulgação dos dados na posse dos fornecedores de acesso à Internet para efeitos de aplicação dos direitos de propriedade intelectual. O artigo 8.º estipula que as autoridades judiciais competentes possam ordenar que os FSI forneçam informações pessoais na sua posse sobre os alegados infractores (por exemplo, informações sobre a origem e as redes de distribuição dos bens ou serviços que violam um direito de propriedade intelectual) em resposta a um pedido justificado e razoável em casos de infracções *à escala comercial*. ([34])

44. Assim, o critério «escala comercial» é decisivo. De acordo com este critério, a vigilância poderá ser proporcional no quadro de situações limitadas, específicas e *ad hoc*, onde

([34]) Esta faculdade é confirmada no considerando 14 da Directiva RDPI.

existam suspeitas bem fundamentadas de violação dos direitos de autor à escala comercial. Este critério poderia abranger situações de violação flagrante dos direitos de autor por pessoas singulares com o objectivo de obter benefícios económicos, directos ou indirectos, de natureza comercial.

45. Na prática, para aplicarem o critério atrás descrito, os titulares de direitos de autor poderiam proceder à vigilância com objectivos específicos de determinados endereços IP, a fim de aferirem a escala da violação dos direitos de autor. Consequentemente, os titulares dos direitos de autor seriam autorizados a manter relatórios de alegadas infracções para os mesmos fins. Essas informações só devem ser utilizadas após a verificação da escala da infracção. Por exemplo, casos manifestos de infracções de grande escala ou infracções menores mas com carácter de continuidade, ao longo de um determinado período, tendo em vista a obtenção de vantagens comerciais ou ganhos financeiros. Realça-se a necessidade de continuidade ao longo de determinados períodos, a qual será explicada adiante na análise sobre o princípio da conservação.

46. Assim, nesses casos, a recolha de informações para demonstrar a alegada utilização abusiva da Internet poderia ser considerada proporcional e necessária para efeitos de preparação de acções judiciais, incluindo processos.

47. A AEPD considera, a título de garantia adicional, que as operações de tratamento de dados com vista à recolha desse tipo de provas devem estar sujeitas à verificação e autorização prévias por parte das autoridades nacionais de protecção de dados. Estas opiniões baseiam-se no facto de as operações de tratamento de dados representarem riscos específicos para os direitos e liberdades das pessoas face aos fins das operações, designadamente a execução de acções que podem eventualmente constituir um crime, e em virtude da natureza sensível dos dados recolhidos. O facto de o tratamento implicar a vigilância de comunicações electrónicas é um factor adicional que exige uma supervisão reforçada.

48. A AEPD considera que a «escala comercial» incorporada na Directiva RDPI é um elemento muito adequado para fixar os limites à vigilância, a fim de ser respeitado o princípio da proporcionalidade. Além disso, não parecem existir provas concludentes de que os critérios propostos na Directiva RDPI impossibilitem ou inviabilizem acções judiciais eficazes contra a violação dos direitos de autor. Por exemplo, a informação de que na Alemanha, desde 2008, na sequência da transposição da Directiva RDPI, já houve cerca de 3 000 decisões judiciais para obrigar os FSI a facultar aos tribunais informações de 300 000 assinantes parece sugerir precisamente o contrário.

49. Em suma, dado que a Directiva RDPI só está em vigor há dois anos, é difícil compreender o que leva os legisladores a quererem afastar-se dos critérios incorporados nesta directiva a favor de métodos mais intrusivos, quando a UE está agora a começar a testar os métodos recentemente adoptados. Pela mesma razão, é também difícil compreender a necessidade de substituir o sistema actual, baseado em processos judiciais, por outro tipo de medidas (além das questões que suscita em matéria de processo equitativo e que não são aqui abordadas).

IV.4. **Conformidade das políticas de corte de acesso à Internet em três etapas com as disposições de protecção de dados mais específicas**

50. Há outras razões mais específicas, no plano jurídico, que tornam problemática a abordagem das três etapas do ponto de vista da protecção de dados. A AEPD pretende chamar a atenção para a fundamentação jurídica dúbia para o tratamento de dados que é exigida pela Directiva 95/46/CE e para a obrigação de eliminação dos ficheiros de registo contida na Directiva 2002/58/CE.

Base jurídica para o tratamento de dados

51. A abordagem das três etapas implica o tratamento de dados pessoais, alguns dos quais serão utilizados para procedimentos legais ou administrativos tendentes à interrupção do fornecimento de acesso à Internet a infractores reincidentes. Deste ponto de vista, os referidos dados são considerados dados sensíveis na acepção do artigo 8.º da Directiva 95/46/CE. O artigo 8.º, n.º 5, estipula que «O tratamento de dados relativos a infracções, condenações penais ou medidas de segurança só poderá ser efectuado sob o controlo das autoridades públicas ou se o direito nacional estabelecer garantias adequadas e específicas …»

52. Neste contexto, é pertinente recordar o documento do Grupo de Trabalho de Protecção de Dados do Artigo 29.º atrás mencionado, que aborda a questão do tratamento de dados judiciais. ([35]) Segundo o grupo de trabalho: «Se qualquer indivíduo tem obviamente o direito de tratar dados judiciais no âmbito do seu próprio processo, o princípio não vai ao ponto de permitir a investigação aprofundada, a recolha e a centralização de dados pessoais por terceiros, incluindo, em especial, uma pesquisa sistemática em grande escala, como a exploração da Internet(…). Esse tipo de investigação é da competência das autoridades judiciárias». ([36]) Embora a recolha de provas concretas e específicas, em particular nos casos de infracções graves, possa ser necessária para estabelecer e exercer direitos num processo judicial, a AEPD partilha integralmente das opiniões do Grupo de Trabalho de Protecção de Dados do Artigo 29.º sobre a falta de legitimidade de investigações de larga escala que impliquem o tratamento de quantidades enormes de dados de utilizadores da Internet.

53. A discussão em torno do princípio da proporcionalidade atrás descrito e o critério da «escala comercial» são pertinentes para determinar em que condições a recolha de endereços IP e de informação conexa será legítima.

([35]) Ver o ponto 28 do presente parecer.
([36]) Nosso realce.

54. Os FSI poderão tentar legitimar o tratamento efectuado pelos titulares dos direitos de autor mediante a inserção de cláusulas nos contratos dos clientes, que permitam a vigilância dos seus dados e o corte das respectivas assinaturas. Se celebrassem contratos com cláusulas desse tipo, considerar-se-ia que os clientes aceitaram a vigilância. No entanto, esta prática suscita desde logo a questão básica da capacidade de uma pessoa singular para autorizar um FSI a efectuar um tratamento de dados que não será realizado pelo FSI, mas sim por terceiros que não se encontram subordinados à autoridade do FSI.

55. Em segundo lugar, existe a questão da validade do consentimento. No artigo 2.º, alínea h), da Directiva 95/46/CE, consentimento é definido como «qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objecto de tratamento». Importa aqui realçar que, para ser válido, o consentimento deve configurar manifestação de vontade, livre, específica e informada da pessoa em causa, conforme estabelece o artigo 2.º, alínea h), da Directiva. A AEPD tem sérias dúvidas de que as pessoas tenham a oportunidade de tomar uma decisão genuína quando lhes é pedido o consentimento para vigiar as suas actividades na Internet, em especial porque a alternativa seria não ter acesso à Internet e isso poderia pôr em causa muitos outros aspectos da sua vida.

56. Em terceiro lugar, é altamente questionável se esse tipo de vigilância fosse sequer considerado *necessário* para a execução de um contrato de que a pessoa em causa é parte, conforme estabelece o artigo 7.º, alínea b), da Directiva 95/46/CE, dado que a vigilância não é, obviamente, um objecto do contrato celebrado pelo sujeito em causa, mas tão-só um meio para o FSI servir outros interesses.

Eliminação dos ficheiros de registo

57. Nos termos da Directiva 2002/58/CE, mais concretamente do seu artigo 6.º, os dados de tráfego, como os endereços IP, apenas podem ser recolhidos e armazenados por motivos directamente relacionados com as comunicações, entre os quais a facturação, a gestão do tráfego e a prevenção de fraudes. Posteriormente, esses dados devem ser eliminados, sem prejuízo das obrigações previstas na directiva relativa à conservação de dados que, conforme foi referido, apenas determina a conservação de dados de tráfego e a sua divulgação às autoridades policiais e judiciais no âmbito da investigação de **crimes graves**. ([37])

58. Em conformidade com o atrás exposto, os fornecedores de serviços Internet devem eliminar todos os ficheiros de registo que revelem as actividades dos utilizadores da Internet assim que esses ficheiros deixem de ser necessários para os fins supramencionados. Tendo em conta que os ficheiros de registo não são necessários para fins de facturação, três a quatro semanas deverá ser um período suficiente para conservação dos ficheiros pelo FSI para efeitos de gestão do tráfego. ([38])

59. Assim, quando são contactados pelos titulares dos direitos de autor, salvo nos casos em que esse contacto ocorra no período limitado atrás indicado, os FSI não deverão ter ficheiros de registo que associem os endereços IP aos assinantes pertinentes. Os ficheiros de registo só deverão ser conservados além do período mencionado quando para tal existam razões justificadas no âmbito das finalidades previstas na lei.

60. Na prática, isto significa que, salvo nos casos em que os titulares dos direitos de autor formulem os seus pedidos aos FSI com grande celeridade, estes fornecedores não poderão atender a esses pedidos pela simples razão de já não disporem da informação. Esta circunstância, só por si, já estabelece os limites do que se entende por práticas de vigilância aceitáveis, tal como foram descritas mais atrás no presente parecer.

Riscos dos efeitos de contaminação

61. Além do impacto das políticas de corte de acesso à Internet em três etapas na privacidade e nos dados pessoais, a AEPD está ainda preocupada com os seus efeitos de contaminação. Caso as políticas de corte de acesso à Internet em três etapas fossem autorizadas, poderiam ser apenas o início da legitimação de formas ainda mais sistemáticas de vigilância das actividades dos utilizadores da Internet, em diferentes domínios e para diferentes fins.

62. A AEPD insta a Comissão a velar por que o ACTA não ultrapasse nem colida com o actual regime da UE em matéria de aplicação dos DPI, que respeita os direitos e as liberdades fundamentais e as liberdades cívicas, como a protecção de dados pessoais.

V. **PREOCUPAÇÕES EM MATÉRIA DE PROTECÇÃO DE DADOS RESPEITANTES AOS MECANISMOS DE COOPERAÇÃO INTERNACIONAL**

63. Um dos meios propostos pelos participantes no ACTA para tratar a questão do respeito dos DPI consiste no reforço da cooperação internacional, com uma série de medidas que

([37]) Ver o ponto 35 do presente parecer.

([38]) Gestão do tráfego compreende a análise do tráfego na rede informática para optimizar ou assegurar o desempenho, tempos de espera mais reduzidos e/ou o aumento da largura de banda utilizável.

permitiriam assegurar o respeito dos direitos de propriedade intelectual nas jurisdições dos signatários do ACTA.

64. Em face da informação disponível, é previsível que várias das medidas planeadas para garantir o respeito dos direitos de propriedade intelectual envolvam a partilha de informações sobre alegadas violações dos DPI entre as autoridades públicas (como as autoridades aduaneiras, a polícia e a justiça) e também entre agentes públicos e privados (como os FSI e as organizações de titulares de direitos de propriedade intelectual). Essas transferências de dados suscitam várias questões do ponto de vista da protecção de dados.

V.1. **São as trocas de dados previstas no contexto do ACTA legítimas, necessárias e proporcionais?**

65. No estado actual do processo negocial, em que uma série de elementos concretos relativos ao tratamento de dados continuam por definir ou são desconhecidos, é impossível verificar se o quadro de medidas proposto está em conformidade com os princípios fundamentais de protecção de dados e com a legislação comunitária em matéria de protecção de dados.

66. Em primeiro lugar, pode-se questionar se as transferências de dados para países terceiros no âmbito do ACTA são legítimas. A relevância da adopção de medidas a nível internacional nesse domínio está sujeita a ser questionada enquanto não houver acordo entre os Estados-Membros da UE em relação à harmonização das medidas de execução no ambiente digital e aos tipos de sanções penais a aplicar. ([39])

67. Face ao atrás exposto, os princípios da necessidade e da proporcionalidade das transferências de dados ao abrigo do ACTA seriam mais fáceis de cumprir se o acordo se limitasse expressamente ao combate às violações mais graves dos DPI, em vez de permitir transferências de dados em massa relacionados com suspeitas de violação de DPI. Será necessário definir com rigor o que constituem as «violações mais graves dos DPI» no âmbito das quais podem ocorrer transferências de dados.

68. Além disso, deve ser dedicada especial atenção às pessoas que intervêm nas trocas de dados e, também, se os dados serão partilhados apenas entre autoridades públicas ou se existirão trocas entre agentes privados e autoridades públicas. Conforme já foi referido no presente parecer, o envolvimento de agentes privados num domínio que, em princípio, está sob a alçada das autoridades responsáveis pela aplicação da lei suscita uma série de questões. ([40]) As condições nas quais os agentes privados intervêm na recolha de dados pessoais e na troca desses dados com as autoridades públicas em relação com a violação de DPI devem estar muito limitadas a circunstâncias específicas, com garantias adequadas.

V.2. **Legislação aplicável em matéria de protecção de dados que rege as transferências de dados no contexto do ACTA**

Regime geral das transferências de dados

69. O quadro geral de protecção de dados aplicável na UE encontra-se definido na Directiva 95/46/CE. Os artigos 25.º e 26.º da Directiva 95/46/CE definem o regime aplicável às transferências de dados para países terceiros. O artigo 25.º determina que apenas se realizem transferências para países que assegurem um nível de protecção adequado, caso contrário as transferências são, em princípio, proibidas.

70. O nível de adequação dos países terceiros é avaliado caso a caso pela Comissão Europeia, que promulgou uma série de decisões em reconhecimento da adequação de uma série de países após uma análise rigorosa pelo Grupo de Trabalho de Protecção de Dados do Artigo 29.º ([41])

71. A AEPD observa que a maioria dos participantes no ACTA não integra a lista de países que proporcionam protecção de dados adequada, elaborada pela Comissão: com a excepção da Suíça e, em circunstâncias específicas, do Canadá e dos EUA, a nenhum outro participante no ACTA é reconhecida a capacidade de proporcionar um nível adequado de protecção. Assim, os dados a transferir da UE para estes países estão sujeitos ao cumprimento de uma das condições do artigo 26.º, n.º 1, da Directiva 95/46/CE ou as partes deverão aduzir salvaguardas adequadas para a transferência de dados em conformidade com o artigo 26.º, n.º 2, da Directiva.

Regime específico para transferências de dados no domínio da aplicação do direito penal

72. Embora a Directiva 95/46/CE constitua o principal instrumento de protecção de dados na UE, o seu âmbito encontra-se limitado, pois exclui expressamente, *inter alia*, as actividades do Estado no domínio do direito penal (artigo 3.º). As trocas de dados para fins da aplicação do direito penal estão, por conseguinte, fora do âmbito da

([39]) Existe actualmente uma proposta relativa às sanções penais em análise no Conselho, COM(2006) 168 de 26 de Abril de 2006.

([40]) Ver os pontos 32 e 52 do presente parecer. Ver também o parecer da AEPD, de 11 de Novembro de 2008, sobre o relatório final do Grupo de Contacto de Alto Nível UE-EUA sobre o intercâmbio de informações e a protecção da vida privada e dos dados pessoais, JO C 128 de 6.6.2009, p. 1.

([41]) Ver as decisões da Comissão Europeia relativas à adequação da Argentina, Canadá, Suíça, «porto seguro» dos EUA e autoridades norte-americanas no contexto de PNR, Guernesey, Ilha de Man e Jersey; disponíveis em http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

Directiva 95/46/CE e estarão sujeitas aos princípios gerais de protecção de dados da Convenção 108 do Conselho da Europa e respectivo protocolo adicional, de que todos os Estados-Membros da UE são signatários. ([42]) Além disso, serão aplicáveis as regras adoptadas pela UE em matéria de cooperação policial e judicial no domínio penal estabelecidas na Decisão-Quadro do Conselho 2008/877/JAI. ([43])

73. Estes instrumentos também têm como princípio a existência de um nível adequado de protecção de dados no país terceiro para o qual os dados serão transferidos. Estão previstas várias derrogações, em especial quando o país terceiro fornece salvaguardas adequadas. À semelhança das trocas de dados ao abrigo da Directiva 95/46/CE, as trocas de dados no domínio da aplicação do direito penal irão, por conseguinte, obrigar à adução de salvaguardas adequadas entre as partes da transferência de dados, para que a transferência se possa realizar.

Rumo a um novo regime de transferências de dados

74. No futuro mais próximo, é previsível a aprovação pela UE de novas regras comuns de protecção de dados aplicáveis a todos os domínios de actividades da UE com base no artigo 16.º do TFUE. Assim, dentro de alguns anos poderá existir um quadro completo de protecção de dados a nível da UE, que estabeleça regras coerentes para a protecção de dados em todos os domínios de actividades da UE e que aplique o mesmo nível de salvaguardas e garantias a todas as actividades de tratamento de dados. Conforme referiu Viviane Reding ([44]), Comissária para a Justiça, os Direitos Fundamentais e a Cidadania, este novo quadro deve funcionar como um «único instrumento jurídico moderno e abrangente» para toda a protecção de dados na UE. Este quadro é particularmente bem-vindo, pois traria mais clareza e coerência às regras aplicáveis na UE respeitantes à protecção de dados.

75. No plano internacional, a AEPD salienta também a Resolução relativa a normas internacionais para a protecção dos dados pessoais e da privacidade recentemente adoptada pelas autoridades de protecção de dados e que é um primeiro passo para a criação de normas mundiais de protecção de dados. ([45]) As normas internacionais contemplam uma série de salvaguardas de dados semelhantes às mencionadas na Directiva 95/46/CE e na Convenção 108. Embora as normas internacionais ainda não tenham força vinculativa, constituem orientações úteis para os princípios de protecção de dados que podem ser aplicados voluntariamente por países terceiros, para que o seu quadro jurídico seja compatível com as normas da União Europeia. A AEPD considera que os signatários do ACTA devem também ter em conta os princípios enunciados nas normas internacionais ao tratarem dados pessoais provenientes da UE.

V.3. **Necessidade de aplicar salvaguardas adequadas para a protecção das transferências de dados da UE para países terceiros**

Que forma devem revestir as salvaguardas para serem eficazes na protecção das transferências de dados para países terceiros?

76. Caso seja demonstrada a necessidade de transferência de dados pessoais para países terceiros, a AEPD salienta que a União Europeia deve negociar com os países terceiros destinatários, além do acordo sobre o ACTA, instrumentos específicos que contenham garantias de protecção de dados adequadas para reger a troca de dados pessoais.

77. Regra geral, as salvaguardas de protecção de dados adequadas devem ser vertidas num acordo vinculativo entre a UE e o país terceiro destinatário, por meio do qual a parte receptora se compromete a respeitar a legislação comunitária em matéria de protecção de dados e a conceder às pessoas singulares os mesmos direitos e recursos que estão previstos no direito comunitário. A necessidade de um acordo vinculativo emana do artigo 26.º, n.º 2, da Directiva 95/46/CE e do artigo 13.º, n.º 3, alínea b), da decisão-quadro, sendo ainda suportada pela prática vigente na UE de conclusão de acordos específicos para possibilitar transferências de dados específicas para países terceiros. ([46])

78. De igual modo, ao abrigo das normas internacionais, o destinatário poderá ser obrigado a garantir que conseguirá prestar o nível de protecção necessário para a transferência se realizar. Estas garantias também podem tomar a forma de um compromisso contratual.

Conteúdo das salvaguardas a aduzir pelos signatários do ACTA a respeito das transferências de dados pessoais

79. A AEPD sublinha especificamente que as trocas de dados internacionais para efeitos de aplicação da lei são uma matéria muito sensível do ponto de vista da protecção de dados, pois esse quadro poderia legitimar transferências de

([42]) Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, adoptada em Estrasburgo em 28 de Janeiro de 1981, e Conselho da Europa, Protocolo Adicional à Convenção para a protecção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal no que respeita às autoridades de controlo e aos fluxos de dados transfronteiriços, Estrasburgo, 8 de Novembro de 2001.

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

([44]) Ver Respostas da Comissária indigitada Viviane Reding ao questionário do Parlamento Europeu, p. 5, http://www.europarl.europa.eu/hearings/static/commissiners/answers/reding_replies_pt.pdf

([45]) Resolução aprovada em Madrid em Novembro de 2009.

([46]) Por exemplo, os acordos da Europol e do Eurojust com os EUA, o acordo relativo aos registos de identificação dos passageiros (PNR), o acordo Swift, o acordo entre a UE e a Austrália sobre o tratamento e transferência de dados de registos de identificação dos passageiros (PNR) obtidos da União Europeia pelo serviço aduaneiro australiano.

dados em massa num domínio em que o impacto nas pessoas se afigura especialmente grave e onde são tanto mais necessárias salvaguardas rigorosas e fiáveis.

80. A AEPD refere que as condições específicas e as salvaguardas apenas podem ser definidas caso a caso, à luz de todos os parâmetros dos intercâmbios de dados. No entanto, para fins de orientação, a AEPD destaca a seguir alguns dos princípios e salvaguardas que devem ser aduzidas pelos destinatários externos para as transferências de dados se realizarem:

— Importa verificar qual é a justificação jurídica para a realização das actividades de tratamento de dados (ou seja, as operações de tratamento baseiam-se numa obrigação jurídica, no consentimento das pessoas em causa ou noutra justificação válida?) e se as transferências de dados respeitam a finalidade inicial da recolha de dados. Não devem ser efectuadas transferências fora do âmbito da finalidade especificada,

— A quantidade e os tipos de dados pessoais a trocar devem ser especificados com clareza e reduzidos ao mínimo estritamente necessário para permitir o cumprimento da finalidade da transferência. Dos dados pessoais recolhidos e transferidos poderão constar, nomeadamente, o endereço IP dos utilizadores da Internet, a data e a hora da alegada infracção e o tipo de infracção. A AEPD recomenda que os dados não sejam associados a uma pessoa específica durante a fase de investigação e recorda que a identificação de um suspeito apenas pode ocorrer no cumprimento da lei e sob o controlo e um juiz. Assim, a AEPD refere que os dados relacionados com violações ou suspeitas de violações de DPI são uma categoria especial de dados, cujo tratamento está geralmente restrito a autoridades responsáveis pela aplicação da lei e obriga à aplicação de salvaguardas adicionais. Por conseguinte, as pessoas autorizadas a tratar os dados relativos a violações e suspeitas de violações de DPI, bem como as condições para o tratamento desses dados, devem ser definidas especificamente em conformidade com a legislação existente em matéria de protecção de dados,

— É necessário definir claramente quem são as pessoas entre as quais os dados poderão ser partilhados, sendo em princípio proibidas transferências subsequentes para outros destinatários, salvo se essas transferências subsequentes forem necessárias para uma investigação específica. Esta limitação reveste-se de uma importância fundamental, visto que os destinatários designados não devem partilhar informações indevidamente com destinatários não autorizados,

— A AEPD parte do princípio de que o ACTA irá, por um lado, prever a cooperação entre as autoridades públicas e, por outro lado, delegar tarefas de execução em organizações privadas (como os FSI, as organizações de titulares de direitos de autor, etc.). Neste último caso, é necessário avaliar cuidadosamente as condições e o nível de envolvimento das organizações privadas na aplicação dos direitos de propriedade industrial, porquanto as medidas do ACTA não devem conferir um direito *de facto* aos FSI e às organizações de titulares de direitos de propriedade industrial para vigiarem o comportamento dos utilizadores em linha. Além disso, o tratamento de dados pessoais por organizações privadas no contexto da aplicação da lei apenas deve ser efectuado se existir uma base jurídica adequada. É também importante esclarecer se as organizações privadas serão obrigadas a colaborar com a polícia e o âmbito dessa colaboração, a qual deve estar limitada apenas aos «crimes graves», cuja definição também deve ser elaborada com rigor, visto que nem todas as violações de DPI devem ser consideradas crimes sérios,

— O método utilizado para a troca de dados pessoais deve ser escolhido sem margem para dúvidas e, em particular, deve ser especificado se será efectuado através de um sistema de empurro («push»), em que, por exemplo, os FSI e as organizações de titulares de direitos de propriedade intelectual transferem, sob o seu controlo, determinados dados para terceiros, como a polícia e as autoridades responsáveis pela aplicação da lei no estrangeiro. Ou se, em alternativa, deve ser utilizado um sistema de puxo («pull»), em que, por exemplo, a polícia e as autoridades responsáveis pela aplicação da lei teriam acesso directo às bases de dados de entidades privadas ou a bases de dados onde a informação está centralizada. Como já foi referido no contexto dos registos de identificação dos passageiros (PNR), um sistema de empurro («push») é a única opção compatível com os princípios comunitários de protecção de dados, pois permite ao remetente na UE, que provavelmente é o controlador dos dados, exercer o controlo sobre a transferência de dados ([47]),

— Deve ser especificado o período de conservação de dados pessoais pelos destinatários, bem como a razão pela qual a conservação é necessária. O período de conservação deve ser proporcional ao fim em vista, o que implica a remoção ou a eliminação dos dados quando deixem de ser necessários para cumprir esse fim,

— As obrigações aplicáveis aos controladores de dados nos países terceiros devem ser estabelecidas com clareza. Devem ser garantidos mecanismos de fiscalização e/ou mecanismos de responsabilização aplicáveis, de forma a existirem recursos e sanções eficazes contra os controladores de dados em caso de tratamento indevido ou outros incidentes significativos. Além disso, devem ser

([47]) Ver o parecer 4/2003 do Grupo de Trabalho de Protecção de Dados do Artigo 29.º sobre o nível de protecção conferido pelos EUA à transferência de dados dos passageiros, WP78, 13 de Junho de 2003.

adoptados mecanismos de recurso que permitam às pessoas singulares apresentar uma queixa a uma autoridade independente de protecção de dados, a fim de disporem de um direito de recurso efectivo perante um tribunal independente e imparcial, ([48])

— O instrumento acordado entre as partes deve especificar claramente os direitos das pessoas em causa no que respeita aos seus dados pessoais quando esses dados sejam tratados por destinatários externos, a fim de que as pessoas em causa disponham de meios eficazes para assegurarem os seus direitos em relação a um tratamento de dados efectuado num país estrangeiro,

— A transparência é, portanto, fundamental, e as partes do instrumento de protecção de dados devem alcançar um acordo quando ao método de informação das pessoas em causa sobre o tratamento de dados em curso, assim como sobre os seus direitos e as modalidades para os exercerem.

VI. **CONCLUSÕES**

81. A AEPD aconselha vivamente a Comissão Europeia a estabelecer um diálogo público e transparente sobre o ACTA, porventura por intermédio de uma consulta pública, a qual também contribuiria para garantir que as medidas a aprovar estivessem em conformidade com os requisitos da legislação comunitária em matéria de privacidade e protecção de dados.

82. No âmbito das negociações em curso sobre o ACTA, a AEPD exorta a Comissão Europeia a que procure alcançar um equilíbrio adequado entre as exigências em matéria de protecção dos direitos da propriedade intelectual e os direitos à privacidade e à protecção dos dados. A AEPD salienta a especial importância de a privacidade e a protecção de dados serem tidas em conta desde o início das negociações, antes de qualquer acordo sobre medidas, evitando-se desse modo a necessidade de encontrar, *a posteriori*, soluções alternativas e compatíveis com a privacidade.

83. Embora a propriedade intelectual seja importante para a sociedade e mereça protecção, não deve ser colocada acima dos direitos fundamentais das pessoas à vida privada, à protecção dos dados e a outros direitos como a presunção da inocência, a protecção judicial eficaz e a liberdade de expressão.

84. Conquanto o actual projecto do ACTA contemple ou, pelo menos, proponha políticas de corte de acesso à Internet em três etapas, o ACTA traduzir-se-ia em profundas restrições dos direitos e liberdades fundamentais dos cidadãos europeus, nomeadamente a protecção dos dados pessoais e da privacidade.

85. A AEPD considera que as políticas de corte de acesso à Internet em três etapas não são necessárias para atingir o objectivo do respeito dos direitos de propriedade intelectual. A AEPD está convicta de que existem soluções alternativas, menos intrusivas, ou que, pelo menos, as políticas pretendidas podem ser executadas de uma forma menos intrusiva ou com um âmbito mais limitado, nomeadamente sob a forma de vigilância *ad hoc* com objectivos específicos.

86. As políticas de corte de acesso à Internet em três etapas afiguram-se ainda problemáticas a um nível jurídico mais aprofundado, em especial porque o tratamento de dados judiciais, nomeadamente por organizações privadas, deve assentar sobre uma base jurídica adequada. Os regimes de três fases podem ainda implicar a conservação de ficheiros de registo por prazos mais longos, o que contraria a legislação vigente.

87. Além disso, na medida em que o ACTA implique a troca de dados pessoais entre autoridades e/ou organizações privadas localizadas nos países signatários, a AEPD insta a União Europeia a aplicar as salvaguardas adequadas. Essas salvaguardas devem ser aplicáveis a todas as transferências de dados efectuadas no âmbito do ACTA — no domínio da aplicação do direito civil, penal ou digital — e devem estar em conformidade com os princípios de protecção de dados da Convenção 108 e da Directiva 95/46/CE. A AEPD recomenda que as referidas salvaguardas revistam a forma de acordos vinculativos entre os remetentes na UE e os destinatários em países terceiros.

88. A AEPD pretende ainda ser consultada em relação às medidas a aplicar a respeito das transferências de dados que ocorrerão no âmbito do ACTA, a fim de verificar a sua proporcionalidade e se garantem um nível adequado de protecção de dados.

Feito em Bruxelas, em 22 de Fevereiro de 2010.

Peter HUSTINX

Autoridade Europeia para a Protecção de Dados

([48]) Ver o 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, 11 de Novembro de 2008.