

Jornal Oficial

da União Europeia

C 279



Edição em língua
portuguesa

Comunicações e Informações

54.º ano
23 de Setembro de 2011

<u>Número de informação</u>	<u>Índice</u>	<u>Página</u>
I <i>Resoluções, recomendações e pareceres</i>		
PARECERES		
Autoridade Europeia para a Protecção de Dados		
2011/C 279/01	Parecer da Autoridade Europeia para a Protecção de Dados sobre o relatório de avaliação da Comissão ao Conselho e ao Parlamento Europeu sobre a Directiva relativa à conservação de dados (Directiva 2006/24/CE)	1
2011/C 279/02	Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF) e que revoga o Regulamento (Euratom) n.º 1074/1999	11
2011/C 279/03	Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à integridade e à transparência nos mercados da energia	20
II <i>Comunicações</i>		
COMUNICAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA		
Comissão Europeia		
2011/C 279/04	Não oposição a uma concentração notificada (Processo COMP/M.6349 — Motherson/Cross Industries/ Peguform/Wethje) ⁽¹⁾	28

PT

Preço:
3 EUR

⁽¹⁾ Texto relevante para efeitos do EEE

(continua no verso da capa)

<u>Número de informação</u>	Índice (<i>continuação</i>)	Página
2011/C 279/05	Não oposição a uma concentração notificada (Processo COMP/M.6218 — Ineos/Tessenderlo Group S-PVC Assets) ⁽¹⁾	28

IV *Informações*

INFORMAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

Comissão Europeia

2011/C 279/06	Taxas de câmbio do euro	29
---------------	-------------------------------	----

V *Avisos*

PROCEDIMENTOS ADMINISTRATIVOS

Comissão Europeia

2011/C 279/07	MEDIA 2007 — Desenvolvimento, distribuição, promoção e formação — Convite à apresentação de propostas — EACEA/21/11 — Apoio ao desenvolvimento de projectos de produção — Obras de ficção, documentários de criação e de filmes de animação — Projectos individuais, <i>slate funding</i> e <i>slate funding</i> 2.º estado	30
2011/C 279/08	MEDIA 2007 — Desenvolvimento, distribuição, promoção e formação — Convite à apresentação de propostas — EACEA/22/11 — Apoio ao desenvolvimento de obras interactivas <i>online</i> e <i>offline</i>	33

PROCEDIMENTOS RELATIVOS À EXECUÇÃO DA POLÍTICA DE CONCORRÊNCIA

Comissão Europeia

2011/C 279/09	Notificação prévia de uma concentração (Processo COMP/M.6348 — Arla Foods/Allgäuland) ⁽¹⁾	36
2011/C 279/10	Notificação prévia de uma concentração (Processo COMP/M.6392 — Gores/Mexx) — Processo susceptível de beneficiar do procedimento simplificado ⁽¹⁾	37



⁽¹⁾ Texto relevante para efeitos do EEE

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 de avaliação da Comissão ao Conselho e ao Parlamento Europeu sobre a Directiva relativa à conservação de dados (Directiva 2006/24/CE)

(2011/C 279/01)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia e, nomeadamente, os artigos 7.º e 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 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

I.1. Publicação do relatório

1. Em 18 de Abril de 2011, a Comissão apresentou o seu relatório de avaliação sobre a Directiva relativa à conservação de dados (a seguir designado «o relatório de avaliação») ⁽⁴⁾. O relatório de avaliação foi enviado, a título informativo, à AEPD no próprio dia. Pelas razões expostas na

parte I.2, *infra*, a AEPD emite o presente parecer por sua iniciativa, em conformidade com o artigo 41.º do Regulamento (CE) n.º 45/2001.

2. Antes da adopção da comunicação, a AEPD teve a oportunidade de apresentar observações informais. A AEPD congratula-se pelo facto de diversas observações terem sido tidas em conta pela Comissão na elaboração da versão final do documento.
3. A Comissão elaborou o relatório de avaliação para dar cumprimento à obrigação prevista no artigo 14.º da Directiva relativa à conservação de dados de avaliar a aplicação da directiva e os seus efeitos nos operadores económicos e nos consumidores, a fim de apurar se é necessário alterar as suas disposições ⁽⁵⁾. A AEPD congratula-se com o facto de, apesar de não ser uma exigência formal do artigo 14.º, a Comissão também ter tido em conta no relatório «implicações da Directiva em matéria de direitos fundamentais, tendo em conta as críticas que, em termos gerais, têm sido formuladas relativamente à conservação de dados» ⁽⁶⁾.

I.2. Motivação e objectivo do presente parecer da AEPD

4. A Directiva relativa à conservação de dados constituiu uma resposta da UE a desafios prementes em matéria de segurança, na sequência dos graves ataques terroristas ocorridos em Madrid, em 2004, e em Londres, em 2005. Apesar do objectivo legítimo de criação de um regime de conservação de dados, ouviram-se críticas em relação ao forte impacto que a medida teve na privacidade dos cidadãos.
5. A obrigação de conservação de dados em conformidade com a Directiva relativa à conservação de dados permite que as autoridades competentes nacionais reconstituam a utilização que qualquer pessoa faça da Internet ou do telefone na UE num período que pode ir até dois anos.

⁽¹⁾ JO L 281 de 23.11.1995, p. 31.

⁽²⁾ JO L 201 de 31.7.2002, p. 37, com a redacção que lhe foi dada pela 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).

⁽³⁾ JO L 8 de 12.1.2001, p. 1.

⁽⁴⁾ COM(2011) 225 final.

⁽⁵⁾ A Directiva relativa à conservação de dados Directiva 2006/24/CE foi adoptada em 15 de Março de 2006 e publicada no JO L 105 de 13.4.2006, p. 54. O prazo para a emissão do relatório foi fixado em 15 de Setembro de 2010; ver o artigo 14.º, n.º 1, da Directiva relativa à conservação de dados.

⁽⁶⁾ Ver p. 1 do relatório de avaliação.

6. A conservação de dados de telecomunicações constitui, sem sombra de dúvida, uma ingerência no direito à vida privada das pessoas visadas, consagrado no artigo 8.º da Convenção Europeia dos Direitos do Homem (a seguir designada «CEDH») e no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia.
7. O Tribunal Europeu dos Direitos do Homem (a seguir designado «TEDH») tem reafirmado sistematicamente que o «mero armazenamento de dados relacionados com a vida privada de uma pessoa equivale a uma ingerência na aceção do artigo 8.º [CEDH]»⁽⁷⁾. No que se refere aos dados telefónicos em particular, o TEDH declarou que a «divulgação dessa informação às autoridades policiais sem a autorização do assinante também equivale [...] a uma ingerência num direito consagrado no artigo 8.º [CEDH]»⁽⁸⁾.
8. Decorre do artigo 8.º, n.º 2, da CEDH e do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia que uma ingerência pode ser justificada, se estiver prevista na lei, servir uma finalidade legítima e for necessária numa sociedade democrática para atingir essa finalidade legítima.
9. A AEPD já reconheceu que a disponibilidade de determinados dados de tráfego e localização podem ser essenciais para as autoridades responsáveis pela aplicação da lei no combate ao terrorismo e a outras formas de criminalidade grave. No entanto, a AEPD tem reiteradamente manifestado dúvidas quanto à justificação para a conservação de dados à escala prevista tendo em conta os direitos à vida privada e à protecção de dados⁽⁹⁾. Estas dúvidas têm sido partilhadas por muitas organizações da sociedade civil⁽¹⁰⁾.
10. A AEPD tem acompanhado de perto a criação, aplicação e avaliação da directiva desde 2005, de diferentes formas. A AEPD emitiu um parecer crítico em 2005, na sequência da publicação da proposta de directiva da Comissão⁽¹¹⁾. Após a adopção da directiva, a AEPD tornou-se membro do grupo de peritos «Plataforma relativa à conservação de dados» mencionado no considerando 14 da Directiva relativa à conservação de dados⁽¹²⁾. Além disso, a AEPD participa nos trabalhos do Grupo de Trabalho de Protecção de Dados do Artigo 29.º, que publicou vários documentos sobre a matéria, sendo o mais recente um relatório datado de Julho de 2010 sobre a aplicação prática da directiva⁽¹³⁾. Por último, a AEPD interveio num processo do Tribunal de Justiça da União Europeia em que era contestada a validade da directiva⁽¹⁴⁾.
11. É inegável a importância do relatório de avaliação e do processo de avaliação⁽¹⁵⁾. A Directiva relativa à conservação de dados constitui um exemplo claro de uma medida da UE que visa assegurar a disponibilidade de dados gerados e tratados no quadro de comunicações electrónicas para actividades de aplicação da lei. Agora que a medida já está em vigor há vários anos, uma avaliação da sua aplicação prática deve demonstrar a necessidade e a proporcionalidade reais da medida face aos direitos à vida privada e à protecção de dados. A este respeito, a AEPD referiu-se à avaliação como o «momento da verdade» para a Directiva relativa à conservação de dados⁽¹⁶⁾.
12. O processo de avaliação actual também tem implicações para outros instrumentos que regulam a gestão da informação, nomeadamente o tratamento de grandes volumes de dados pessoais, no domínio da liberdade, da segurança e da justiça. Numa comunicação de 2010, a Comissão concluiu que os mecanismos de avaliação dos diferentes instrumentos apresentam uma grande variação⁽¹⁷⁾. A AEPD considera que o procedimento de avaliação actual deveria ser utilizado como modelo para estabelecer um padrão para a avaliação de outros instrumentos da UE e para garantir que apenas permanecem em vigor as medidas que realmente se justificam.
13. Perante este quadro, a AEPD pretende partilhar as suas reflexões sobre as conclusões do relatório de avaliação num parecer público. Esta iniciativa surge no início do processo, com o objectivo de dar um contributo eficaz e construtivo para os debates que se avizinham, eventualmente no contexto de uma nova proposta legislativa, como refere a Comissão no relatório de avaliação⁽¹⁸⁾.

I.3. Estrutura do parecer

14. O presente parecer analisa e debate o conteúdo do relatório de avaliação do ponto de vista da privacidade e da protecção de dados. Pretende-se analisar se a actual Directiva relativa à conservação de dados cumpre os requisitos destes dois direitos fundamentais, designadamente se a necessidade de conservação de dados regulada na directiva tem sido demonstrada de uma forma suficiente.

15. O presente parecer está estruturado da seguinte forma: a parte II apresenta o conteúdo principal da Directiva relativa

⁽⁷⁾ Ver, por exemplo, o acórdão do TEDH de 4 de Dezembro de 2008, *S. e Marper contra Reino Unido*, 30562/04 e 30566/04, ponto 67.

⁽⁸⁾ Ver o acórdão do TEDH de 2 de Agosto de 1984, *Malone contra Reino Unido*, A-82, ponto 84.

⁽⁹⁾ Ver o parecer da AEPD de 26 de Setembro de 2005 (JO C 298 de 29.11.2005, p. 1). Durante uma conferência organizada pela Comissão, em Dezembro de 2010, a AEPD referiu-se ao instrumento como «o mais invasivo da vida privada alguma vez adoptado pela UE em termos de escala e do número de pessoas que afecta»; ver o discurso de 3 de Dezembro de 2010, que está disponível no sítio Internet da AEPD (<http://www.edps.europa.eu>) em Publicações >> Discursos e Artigos >> 2010.

⁽¹⁰⁾ Ver, a este respeito, a carta de 22 de Junho de 2010 de um grupo alargado de organizações da sociedade civil às comissárias Cecilia Malmström, Viviane Reding e Neelie Kroes (http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf).

⁽¹¹⁾ Ver o parecer da AEPD mencionado na nota de rodapé 9.

⁽¹²⁾ Ver igualmente a Decisão da Comissão de 25 de Março de 2008 (JO L 111 de 23.4.2008, p. 11).

⁽¹³⁾ Ver o WP 172 de 13 de Julho de 2010, Relatório 1/2010 sobre a segunda acção de aplicação conjunta.

⁽¹⁴⁾ Ver o acórdão do TJUE de 10 de Fevereiro de 2009, *Irlanda contra Parlamento Europeu e Conselho*, C-301/06. Ver também ponto 29, adiante, em relação ao processo.

⁽¹⁵⁾ No seu parecer de 2005, a AEPD já tinha salientado a importância da obrigação de avaliar o instrumento (ver nota de rodapé 9, pontos 72-73).

⁽¹⁶⁾ Ver o discurso de 3 de Dezembro de 2010 mencionado na nota de rodapé 9.

⁽¹⁷⁾ COM(2010) 385 de 20 de Julho de 2010, *Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça*, p. 24. Ver, a respeito desta comunicação, o Parecer da AEPD de 30 de Setembro de 2010, que se encontra disponível no sítio Internet da AEPD (<http://www.edps.europa.eu>) em Consultas >> Pareceres >> 2010.

⁽¹⁸⁾ Ver p. 32 do relatório de avaliação.

à conservação de dados e a sua relação com a Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (a seguir designada «Directiva relativa à privacidade e às comunicações electrónicas») (19). A parte III descreve brevemente as alterações introduzidas pelo Tratado de Lisboa, pois são especialmente pertinentes para a matéria em apreço e têm um impacto directo na percepção, avaliação e eventual revisão das regras da UE relativas à conservação de dados. A secção mais extensa do parecer, a parte IV, contém a análise da validade da Directiva relativa à conservação de dados face aos direitos à vida privada e à protecção de dados e tendo em conta as conclusões do relatório de avaliação. Na parte V são analisados eventuais caminhos a seguir. O parecer termina, na parte VI, com uma conclusão.

II. AS REGRAS DA UE EM MATÉRIA DE CONSERVAÇÃO DE DADOS

16. No contexto do presente parecer, conservação de dados designa a obrigação imposta aos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações de conservarem dados de tráfego e localização, bem como os dados conexos necessários para identificar o assinante ou utilizador durante um determinado período. Esta obrigação está estabelecida na Directiva relativa à conservação de dados, que especifica no artigo 5.º, n.º 1, as categorias de dados a conservar. Segundo o artigo 6.º da directiva, os Estados-Membros asseguram que os dados referidos sejam conservados por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação.
17. Só devem ser conservados os dados gerados ou tratados pelos fornecedores no âmbito da prestação dos serviços de comunicações em questão (artigo 3.º), incluindo as chamadas telefónicas falhadas. Nos termos da directiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações (artigo 5.º, n.º 1).
18. Os dados são conservados tendo em vista garantir a disponibilidade desses dados para efeitos «de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro» (artigo 1.º, n.º 1).
19. A Directiva relativa à conservação de dados não estipula mais regras respeitantes às condições nas quais as autoridades competentes nacionais podem ter acesso aos dados conservados. Essas condições devem ser definidas pelos Estados-Membros e não são abrangidas pela directiva. O artigo 4.º da directiva sublinha que as regras nacionais devem cumprir os requisitos da necessidade e da proporcionalidade, sob reserva, nomeadamente, da CEDH.
20. A Directiva relativa à conservação de dados está directamente relacionada com a Directiva relativa à privacidade e às comunicações electrónicas. Esta directiva, que especifica e complementa a Directiva 95/46/CE relativa à conservação de dados, de carácter mais geral, determina que os Estados-Membros devem garantir a confidencialidade das comunicações e respectivos dados de tráfego (20). A Directiva relativa à privacidade e às comunicações electrónicas estipula que os dados de tráfego e localização gerados pela utilização de serviços de comunicações electrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, excepto nos casos e na extensão em que sejam necessários para efeitos de facturação (21). Sujeito ao consentimento do utilizador, determinados dados poderão ser guardados pelo tempo necessário para o fornecimento de um serviço de valor acrescentado.
21. Com base no artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas, os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito das obrigações atrás referidas, sempre que «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 [...]». No artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas, é feita referência explícita à questão da conservação de dados. Os Estados-Membros podem «adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado».
22. A Directiva relativa à conservação de dados destinava-se a harmonizar as iniciativas dos Estados-Membros no âmbito do artigo 15.º, n.º 1, no que se refere à conservação de dados para a investigação, detecção e repressão de crimes graves. Importa salientar que a Directiva relativa à conservação de dados constitui *uma* excepção à obrigação geral consagrada na Directiva relativa à privacidade e às comunicações electrónicas de eliminar os dados quando estes deixam de ser necessários (22).
23. Com a adopção da Directiva relativa à conservação de dados, foi inserida uma alínea suplementar (1-A) no artigo 15.º da Directiva relativa à privacidade e às comunicações electrónicas, segundo a qual o artigo 15.º, n.º 1, não se aplica a dados cuja conservação seja exigida pela Directiva relativa à conservação de dados para os fins mencionados no artigo 1.º, n.º 1, dessa directiva.
24. É referido no relatório de avaliação, como se verá adiante na parte IV.3, que os artigos 15.º, n.º 1, e 15.º, n.º 1-B têm sido utilizados por vários Estados-Membros para justificar a utilização de dados conservados ao abrigo da Directiva relativa à conservação de dados também para outros fins (23). A AEPD tem-se referido a esta situação como um «vazio jurídico» no quadro regulamentar, que prejudica a finalidade da Directiva relativa à conservação de dados, nomeadamente a criação de condições de concorrência equitativas para o sector (24).

(20) Ver artigo 5.º da Directiva relativa à privacidade e às comunicações electrónicas.

(21) Ver artigos 6.º e 9.º da Directiva relativa à privacidade e às comunicações electrónicas.

(22) Ver também o WP29 no Relatório de 13 de Julho de 2010 mencionado na nota de rodapé 13, p. 1.

(23) Ver p. 4 do relatório de avaliação. Ver também, a este respeito, o considerando 12 da Directiva relativa à conservação de dados.

(24) Ver o discurso de 3 de Dezembro de 2010 mencionado na nota de rodapé 9, p. 4.

(19) Ver nota de pé-de-página 2.

III. ALTERAÇÃO DO CONTEXTO JURÍDICO GERAL APÓS LISBOA

25. O contexto jurídico geral da UE pertinente para a Directiva relativa à conservação de dados mudou bastante com a entrada em vigor do Tratado de Lisboa. Uma alteração importante foi a abolição da estrutura de pilares, que estabelecia diferentes procedimentos legislativos e mecanismos de recurso para os diferentes domínios da competência da UE.
26. Com a anterior estrutura de pilares, eram recorrentes os debates sobre a base jurídica correcta de um instrumento da UE, caso o objecto remetesse para competências da UE nos diferentes pilares. A escolha da base jurídica tinha importância, pois determinava diferentes procedimentos legislativos respeitantes, por exemplo, aos requisitos de voto no Conselho (maioria qualificada ou unanimidade) ou à participação do Parlamento Europeu.
27. Estes debates eram muito pertinentes para a conservação de dados. Uma vez que a Directiva relativa à conservação de dados visava a harmonização da obrigação dos operadores e, por conseguinte, a eliminação de obstáculos ao mercado interno, a base jurídica seria o artigo 95.º do anterior Tratado CE (o antigo primeiro pilar). No entanto, a questão poderia ser abordada do ponto de vista da aplicação da lei, argumentando que a finalidade da conservação dos dados era o combate aos crimes graves, no âmbito da cooperação policial e judiciária em matéria penal do anterior Tratado CE (o antigo terceiro pilar) ⁽²⁵⁾.
28. Nessa ocasião, a Directiva relativa à conservação de dados foi adoptada com base no artigo 95.º do anterior Tratado CE, regendo apenas as obrigações dos operadores. A directiva não continha regras relativas ao acesso aos dados conservados e à sua utilização pelas autoridades responsáveis pela aplicação da lei.
29. Após a sua adopção, a validade da directiva foi contestada junto do Tribunal de Justiça. Argumentava-se que a directiva deveria ter sido baseada no terceiro pilar em vez do primeiro, pois os dados eram conservados para uma finalidade (a investigação, detecção e repressão de crimes graves) sob a competência da UE no terceiro pilar ⁽²⁶⁾. No entanto, dado que a conduta das autoridades competentes tinha sido explicitamente excluída do âmbito da directiva, o Tribunal de Justiça concluiu que o Tratado CE fora correctamente utilizado como base para a directiva ⁽²⁷⁾.
30. Desde o início, a AEPD defendeu que, se a UE adoptasse um instrumento relativo à conservação de dados, esse instrumento deveria regular não só a obrigação dos operadores, como também o acesso e a utilização ulterior pelas autoridades responsáveis pela aplicação da lei. No seu parecer de 2005 sobre a proposta da Comissão, a AEPD sublinhou que o acesso e a utilização ulterior pelas autoridades competentes nacionais eram elementos essenciais e indissociáveis do objecto ⁽²⁸⁾.
31. Como se verá pormenorizadamente mais adiante, os efeitos negativos de a regulação da UE incidir apenas sobre metade do objecto são confirmados no relatório de avaliação em apreço. A Comissão conclui que as divergências a nível das legislações nacionais em matéria de acesso e utilização ulterior pelas autoridades competentes suscitaram «dificuldades consideráveis» aos operadores ⁽²⁹⁾.
32. Com a abolição da estrutura de pilares após a entrada em vigor do Tratado de Lisboa, as duas áreas de competência da UE pertinentes foram reunidas no TFUE, que permite a adopção de legislação da UE sujeita ao mesmo procedimento legislativo. Este novo contexto permitiria a adopção de um novo instrumento único relativo à conservação de dados, que regulasse não só as obrigações dos operadores, como também o acesso e a utilização ulterior pelas autoridades responsáveis pela aplicação da lei. Conforme se explica na parte IV.3, adiante, os direitos à vida privada e à protecção de dados exigem que, se for considerada uma medida da UE revista relativa à conservação de dados, essa medida deve pelo menos regular o objecto na sua totalidade.
33. Além de abolir a estrutura de pilares, o Tratado de Lisboa também conferiu à Carta dos Direitos Fundamentais da União Europeia, que anteriormente não era vinculativa e inclui os direitos à vida privada e à protecção de dados nos seus artigos 7.º e 8.º, o mesmo valor jurídico dos tratados ⁽³⁰⁾. Foi, ainda, incluído no artigo 16.º do TFUE um direito subjectivo à protecção de dados, criando uma base jurídica distinta para os instrumentos da UE de protecção dos dados pessoais.
34. A protecção dos direitos fundamentais é, há muito, uma pedra basilar da política da UE, e o Tratado de Lisboa veio reforçar o compromisso com estes direitos no quadro da UE. As alterações introduzidas pelo Tratado de Lisboa motivaram a Comissão a anunciar, em Outubro de 2010, a promoção de uma «cultura de direitos fundamentais» em todas as etapas do processo legislativo e a declarar que a Carta dos Direitos Fundamentais da União Europeia «deve constituir um guia para as políticas da União» ⁽³¹⁾. A AEPD considera que o actual processo de avaliação é uma boa oportunidade para a Comissão dar provas deste compromisso.

⁽²⁵⁾ A primeira proposta de regras da UE relativas à conservação de dados (uma decisão-quadro) baseou-se no anterior Tratado da União Europeia e foi apresentada pela França, Irlanda, Suécia e Reino Unido. Ver o documento do Conselho n.º 8958/04 de 28 de Abril de 2004. A esta proposta seguiu-se uma outra da Comissão baseada no Tratado CE. Ver COM(2005) 438 de 21 de Setembro de 2005.

⁽²⁶⁾ Este argumento baseou-se no acórdão do Tribunal de Justiça nos «processos PNR»; ver acórdão do TJUE de 30 de Maio de 2006, *Parlamento contra Conselho e Comissão*, C-317/04 e C-318/04.

⁽²⁷⁾ Ver acórdão do TJUE de 10 de Fevereiro de 2009, *Irlanda contra Parlamento Europeu e Conselho*, C-301/06, pontos 82 e 83.

⁽²⁸⁾ Ver o parecer de 2005, ponto 80. Ver também, a este respeito, a parte IV.3 do presente parecer.

⁽²⁹⁾ Ver a p. 31 do relatório de avaliação.

⁽³⁰⁾ Ver o artigo 6.º, n.º 1, TUE.

⁽³¹⁾ COM(2010) 573 de 19 de Outubro de 2010, *Estratégia para a aplicação efectiva da Carta dos Direitos Fundamentais pela União Europeia*, p. 4.

IV. A DIRECTIVA RELATIVA À CONSERVAÇÃO DE DADOS CUMPRE OS REQUISITOS EM MATÉRIA DE PRIVACIDADE E PROTECÇÃO DE DADOS?

35. O relatório de avaliação expõe diversas limitações da actual Directiva relativa à conservação de dados. A informação fornecida no relatório mostra que a directiva não conseguiu cumprir a sua principal finalidade, a saber, harmonizar as legislações nacionais em matéria de conservação de dados. A Comissão observa que existem diferenças «consideráveis» entre as legislações de transposição no que respeita à limitação das finalidades, ao acesso aos dados, aos períodos de conservação, à protecção e segurança dos dados e às estatísticas⁽³²⁾. Segundo a Comissão, as diferenças devem-se, em parte, à variação expressamente prevista na directiva. A Comissão refere, contudo, que para além desta variação, «as divergências nacionais na aplicação da conservação de dados suscitaram dificuldades consideráveis aos operadores» e que «continua a haver falta de segurança jurídica para as empresas»⁽³³⁾. Como é natural, essa falta de harmonização é prejudicial para todas as partes envolvidas: cidadãos, empresas, operadores comerciais e autoridades responsáveis pela aplicação da lei.
36. De um ponto de vista do respeito pela vida privada e da protecção de dados, o relatório também justifica a conclusão de que a Directiva relativa à conservação de dados não cumpre os requisitos decorrentes do direito à vida privada e do direito à protecção de dados. Foram identificadas várias deficiências: não foi suficientemente demonstrada a necessidade de conservação de dados prevista na Directiva relativa à conservação de dados, teria sempre sido possível regulamentar a conservação de dados de uma forma menos invasiva da privacidade, e a Directiva relativa à conservação de dados tem falta de «previsibilidade». Estes três aspectos serão explicados em pormenor adiante.

IV.1. Não foi suficientemente demonstrada a necessidade de conservação de dados prevista na Directiva relativa à conservação de dados

37. Uma ingerência no direito à vida privada e à protecção dos dados pessoais só é permitida se constituir uma medida necessária para atingir um fim legítimo. A necessidade da conservação de dados a título de medida de aplicação da lei tem suscitado constantemente um forte debate⁽³⁴⁾. Na proposta de directiva, referia-se que as restrições aos direitos à vida privada e à protecção de dados eram «necessárias para atingir os objectivos, em geral reconhecidos, de prevenção e combate à criminalidade e ao terrorismo»⁽³⁵⁾. No entanto, no parecer de 2005, a AEPD indicou não estar ainda convicta desta afirmação, pois carecia de mais provas⁽³⁶⁾. Mesmo sem provas suplementares, o considerando 9 da Directiva relativa à conservação de dados refere que «a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros».

38. Devido à insuficiência de provas, a AEPD argumentou que a Directiva relativa à conservação de dados se baseava meramente no pressuposto de que a conservação de dados, nos termos em que era desenvolvida na Directiva relativa à conservação de dados, constituía uma medida necessária⁽³⁷⁾. Assim, a AEPD solicitou à Comissão e aos Estados-Membros que utilizassem o relatório de avaliação para fornecerem provas suplementares que confirmassem a validade do pressuposto da necessidade da medida de conservação de dados e da forma como era regulada na Directiva relativa à conservação de dados.
39. Em relação a este aspecto, a Comissão declara no relatório de avaliação que «[a] maioria dos Estados-Membros considera que as normas da UE em matéria de conservação de dados continuam a ser um instrumento necessário para a aplicação da lei, a protecção das vítimas e os sistemas de justiça criminal». É ainda referido que a conservação de dados desempenha um «papel fundamental» na investigação criminal, que é «no mínimo, importante e, em alguns casos, indispensável» e que, sem a conservação de dados, certas condenações por infracções penais «nunca poderiam ter sido alcançadas»⁽³⁸⁾. A Comissão conclui, portanto, que a UE deve «apoiar e regulamentar a conservação de dados enquanto medida de segurança»⁽³⁹⁾.
40. É, no entanto, duvidoso que a Comissão esteja de facto em condições de concluir que a maioria dos Estados-Membros considera a conservação de dados um instrumento necessário. Não são indicados os Estados-Membros que constituem essa maioria, que numa União de 27 Estados-Membros deveriam ser pelo menos 14 para se poder falar na maioria dos Estados-Membros. Os Estados-Membros referidos em concreto no capítulo 5, no qual se baseiam as conclusões, são, no máximo, 9⁽⁴⁰⁾.
41. Além disso, a Comissão parece basear-se sobretudo em declarações dos Estados-Membros, nomeadamente se consideram a conservação de dados um instrumento necessário para efeitos de aplicação da lei. Porém, estas declarações indicam apenas que os Estados-Membros em questão gostariam que existissem regras da UE em matéria de conservação de dados e não permitem concluir, por si só, da necessidade da conservação de dados como medida de aplicação da lei, apoiada e regulamentada pela UE. As declarações relativas à necessidade devem estar sustentadas em provas suficientes.
42. Demonstrar a necessidade de uma medida invasiva da privacidade não é uma tarefa fácil, em especial para a Comissão, que depende em grande medida da informação fornecida pelos Estados-Membros.
43. No entanto, se já existir uma medida, como a Directiva relativa à conservação de dados, e já tiver sido adquirida experiência prática, deverá estar disponível informação

⁽³²⁾ Ver p. 31 do relatório de avaliação.

⁽³³⁾ Ver p. 31 do relatório de avaliação.

⁽³⁴⁾ Ver o parecer da AEPD de 2005. Ver também a carta de 22 de Junho de 2010 de um grupo alargado de organizações da sociedade civil, referida na nota de rodapé 10.

⁽³⁵⁾ COM(2005) 438 de 21 de Setembro de 2005, p. 3.

⁽³⁶⁾ Ver pontos 17 a 22 do parecer de 2005.

⁽³⁷⁾ Ver o discurso de 3 de Dezembro de 2010 mencionado na nota de rodapé 9.

⁽³⁸⁾ Todas as citações foram retiradas da p. 23 ou da p. 31 do relatório de avaliação.

⁽³⁹⁾ Ver p. 31 do relatório de avaliação.

⁽⁴⁰⁾ República Checa, Eslovénia, Reino Unido, Alemanha, Polónia, Finlândia, Países Baixos, Irlanda e Hungria.

qualitativa e quantitativa suficiente que permita avaliar se a medida funciona na prática e se poderiam ter sido alcançados resultados comparáveis sem o instrumento ou com recurso a meios alternativos, menos invasivos da vida privada. Tal informação constituiria uma prova genuína e demonstraria a relação entre utilização e resultado ⁽⁴¹⁾. No que se refere a uma directiva da UE, a informação deve representar a prática, no mínimo, de uma maioria dos Estados-Membros da UE.

44. Após uma análise cuidadosa, a AEPD considera que, embora a Comissão tenha feito um grande esforço de recolha de informação junto dos governos dos Estados-Membros, a informação quantitativa e qualitativa fornecida pelos Estados-Membros não é suficiente para confirmar a necessidade da conservação de dados nos termos em que é desenvolvida na Directiva relativa à conservação de dados. Embora tenham sido apresentados exemplos interessantes da sua utilização, a informação apresentada no relatório tem demasiadas lacunas para permitir conclusões gerais relativas à necessidade do instrumento. Além disso, deveria ser aprofundada a investigação de eventuais meios alternativos. Estes dois aspectos serão agora desenvolvidos.

A informação quantitativa e qualitativa fornecida no relatório de avaliação

45. No que diz respeito à informação quantitativa (estatística) apresentada sobretudo no capítulo 5 e no anexo do relatório de avaliação, faltam elementos essenciais. Por exemplo, as estatísticas não indicam as finalidades de obtenção dos dados. Além disso, os números não revelam se todos os dados a que foi solicitado acesso eram dados armazenados em consequência da obrigação jurídica de conservação de dados ou para fins comerciais. Além disso, não é fornecida informação sobre os resultados da utilização dos dados. Para tirar conclusões, afigura-se ainda problemático o facto de a informação fornecida pelos diferentes Estados-Membros nem sempre ser totalmente comparável e, em muitos casos, os gráficos representam apenas nove Estados-Membros.
46. Os exemplos qualitativos fornecidos no relatório servem para ilustrar melhor a importância dos dados conservados em algumas situações específicas, assim como as eventuais vantagens de um sistema de conservação de dados. No entanto, não é claro em todos os casos se a utilização de dados conservados era a única forma de resolver o crime em questão.
47. Alguns exemplos ilustram a indispensabilidade da medida de conservação de dados para o combate à cibercriminalidade. A este respeito, importa observar que o principal instrumento internacional neste domínio, a Convenção sobre a Cibercriminalidade do Conselho da Europa, não prevê a conservação de dados como medida de combate à cibercriminalidade, mencionando apenas a preservação de dados como um instrumento de investigação ⁽⁴²⁾.
48. A Comissão parece atribuir um grande peso aos exemplos fornecidos pelos Estados-Membros em que dados conserva-

dos foram utilizados para excluir suspeitos da prática de um crime ou confirmar álibis ⁽⁴³⁾. Embora sejam exemplos interessantes da utilização dos dados pelas autoridades responsáveis pela aplicação da lei, não podem ser considerados demonstrativos da necessidade de conservação de dados. Este argumento deve ser utilizado com cautela, pois está sujeito a interpretações incorrectas de que a conservação de dados é necessária para provar a inocência dos cidadãos, o que seria difícil de conciliar com o princípio da presunção de inocência.

49. O relatório de avaliação faz uma breve análise do valor da conservação de dados em relação à evolução tecnológica, mais concretamente em relação à utilização de cartões SIM pré-pagos ⁽⁴⁴⁾. A AEPD sublinha que teria sido útil dispor de mais informação quantitativa e qualitativa sobre a utilização de novas tecnologias não abrangidas pela directiva (como VoIP e as redes sociais) para avaliar a eficácia da directiva.
50. O relatório de avaliação é limitado, pois baseia-se essencialmente na informação quantitativa e qualitativa fornecida pelos Estados-Membros que aplicaram a Directiva relativa à conservação de dados. Teria, no entanto, sido interessante verificar se ocorreram diferenças assinaláveis entre esses Estados-Membros e os Estados-Membros que não aplicaram a directiva. Em especial nos Estados-Membros em que a legislação de aplicação foi anulada (Alemanha, Roménia e República Checa), teria sido interessante ver se existem provas do aumento ou diminuição do êxito das investigações criminais, antes e depois das anulações.
51. A Comissão reconhece que os dados estatísticos e os exemplos são «limitados quanto a alguns aspectos», mas conclui, ainda assim, que as provas atestam o «papel fundamental que a conservação de dados desempenha no âmbito da investigação criminal» ⁽⁴⁵⁾.
52. A AEPD considera que a Comissão deveria ter sido mais crítica com os Estados-Membros. Tal como já foi explicado, as declarações políticas de alguns Estados-Membros em relação à necessidade da medida não justificam, por si, medidas da UE. A Comissão deveria ter insistido para que os Estados-Membros fornecessem provas suficientes para demonstrar a necessidade da medida. Segundo a AEPD, a Comissão deveria, no mínimo, ter sujeitado o seu apoio à conservação de dados como medida de segurança (ver p. 31 do relatório de avaliação) à condição de que os Estados-Membros fornecessem provas suplementares durante a avaliação do impacto.

Meios alternativos

53. A necessidade de conservação de dados prevista na Directiva relativa à conservação de dados também depende da existência de meios alternativos menos invasivos da vida privada que permitam alcançar resultados comparáveis. Isto mesmo foi confirmado pelo Tribunal de Justiça na decisão proferida no processo *Schecke* em Novembro de 2010, que anulou a legislação da UE relativa à publicação de informação sobre os beneficiários de fundos

⁽⁴¹⁾ Ver também, a respeito do princípio da necessidade e da proporcionalidade, o parecer da AEPD de 25 de Março de 2011 sobre a proposta da UE relativa aos dados dos passageiros (PNR), que se encontra disponível no sítio Internet da AEPD (<http://www.edps.europa.eu>) em Consulta >> Pareceres >> 2011.

⁽⁴²⁾ Ver também p. 5 do relatório de avaliação.

⁽⁴³⁾ Ver p. 24 do relatório de avaliação.

⁽⁴⁴⁾ Ver p. 25 do relatório de avaliação.

⁽⁴⁵⁾ Ver p. 31 do relatório de avaliação.

- agrícolas⁽⁴⁶⁾. Um dos motivos para a anulação foi o facto de o Conselho e a Comissão não terem tomado em consideração medidas alternativas conformes com o objectivo dessa publicação e que fossem, ao mesmo tempo, menos lesivas do direito desses beneficiários ao respeito da sua vida privada e à protecção dos seus dados pessoais⁽⁴⁷⁾.
54. A principal alternativa apresentada nos debates relacionados com a Directiva relativa à conservação de dados é o método de preservação dos dados («quick freeze» e «quick freeze plus»)⁽⁴⁸⁾. Consiste na conservação temporária, ou «congelamento», de certos dados de tráfego de telecomunicações e localização relativos exclusivamente a determinados indivíduos suspeitos de actividades criminosas, que podem mais tarde ser disponibilizados às autoridades responsáveis pela aplicação da lei mediante uma autorização judicial.
55. A preservação de dados é mencionada no relatório de avaliação no quadro da Convenção sobre a Cibercriminalidade atrás referida, mas é considerada inadequada porque «não garante a possibilidade de estabelecer pistas de investigação antes de ser dada a ordem de preservação, não permite investigações cujo alvo seja desconhecido nem permite recolher provas relativas, por exemplo, a movimentações das vítimas ou testemunhas de um crime»⁽⁴⁹⁾.
56. A AEPD reconhece que está disponível menos informação quando é utilizado um sistema de preservação de dados em vez de um amplo sistema de conservação de dados. No entanto, é precisamente devido à sua natureza mais específica que constitui um instrumento menos invasivo em termos de escala e do número de pessoas afectadas. A avaliação não se deve centrar apenas nos dados disponíveis, devendo abranger igualmente os diferentes resultados alcançados com ambos os sistemas. A AEPD considera justificada e indispensável uma investigação mais aprofundada sobre esta medida, que pode ser realizada durante a avaliação de impacto nos próximos meses.
57. A este respeito, é deveras infeliz que a Comissão se comprometa, nas conclusões do relatório, a analisar a questão de saber se — e de que modo — uma abordagem da UE em matéria de preservação de dados pode complementar (ou seja, não substituir) a conservação de dados⁽⁵⁰⁾. A possibilidade de conjugar qualquer tipo de regime de conservação com as salvaguardas processuais associadas a várias formas de conservação de dados merece realmente uma análise mais aprofundada. No entanto, a AEPD recomenda que a Comissão analise também, durante a avaliação de impacto, se um sistema de preservação de dados ou outros meios alternativos poderiam substituir, total ou parcialmente, o actual regime de conservação de dados.
- IV.2. A conservação de dados, da forma como é regulada na Directiva relativa à conservação de dados, ultrapassa sempre o necessário
58. Segundo a AEPD, a informação contida no relatório de avaliação não é suficiente para demonstrar a necessidade da medida de conservação de dados nos termos em que é descrita na Directiva relativa à conservação de dados. No entanto, o relatório de avaliação permite concluir que a Directiva relativa à conservação de dados regula esta medida de uma forma que ultrapassa o necessário, ou, pelo menos, não garante que a conservação de dados não seja aplicada dessa forma. Em relação a este aspecto, importa realçar quatro elementos.
59. Em primeiro lugar, a finalidade pouco clara da medida e a noção lata de «entidades nacionais competentes» permitiu que os dados conservados fossem utilizados para demasiadas finalidades e por um número excessivo de entidades. Além disso, não existe coerência nas salvaguardas e nas condições de acesso aos dados. Por exemplo, o acesso não está sujeito à autorização prévia de uma autoridade judicial ou independente em todos os Estados-Membros.
60. Em segundo lugar, o período máximo de conservação de dois anos parece excessivo. A informação estatística de uma série de Estados-Membros no relatório de avaliação mostra que a grande maioria dos pedidos de acesso (86 %) diz respeito a dados até seis meses⁽⁵¹⁾. Além disso, dezasseis Estados-Membros optaram por um período de conservação igual ou inferior a um ano na respectiva legislação⁽⁵²⁾. É um forte indicador de que um período máximo de dois anos ultrapassa largamente o que é considerado necessário pela maioria dos Estados-Membros.
61. Além disso, a inexistência de um período de conservação fixo e comum a todos os Estados-Membros deu origem a uma série de legislações nacionais divergentes, que poderão vir a criar situações complicadas, pois nem sempre é evidente qual a legislação nacional (relativa à conservação de dados e à protecção de dados) que é aplicável quando os operadores armazenam dados num Estado-Membro diferente daquele onde são recolhidos.
62. Em terceiro lugar, o nível de segurança não está suficientemente harmonizado. Uma das principais conclusões do Grupo de Trabalho de Protecção de Dados do Artigo 29.º no seu relatório de Julho de 2010 está relacionada com a existência de uma multiplicidade de medidas de segurança em vigor nos diferentes Estados-Membros. A Comissão parece considerar suficientes as medidas de segurança previstas na actual directiva, pois «não [existem] exemplos concretos de violações graves da vida privada»⁽⁵³⁾. No entanto, ao que tudo indica, a Comissão apenas solicitou informações sobre esta matéria aos governos dos Estados-Membros. Tendo em vista a avaliação da adequação das medidas e regras de segurança actuais, é necessária uma consulta mais alargada e uma análise mais concreta de situações de abuso. Mesmo que não sejam mencionados casos específicos de violações de segurança
-
- (46) Acórdão do TJUE de 9 de Novembro de 2010, *Volker und Markus Schecke*, C-92/09 e C-93/09.
- (47) Acórdão do TJUE, *Schecke*, ponto 81.
- (48) O método «quick freeze» (congelamento rápido) refere-se ao «congelamento» de dados de tráfego e localização relativos a um suspeito específico a partir da data da autorização judicial. O método «quick freeze plus» (congelamento rápido alargado) abrange ainda o «congelamento» de dados já na posse dos operadores para fins de facturação e transmissão.
- (49) Ver p. 5 do relatório de avaliação.
- (50) Ver p. 32 do relatório de avaliação.
-
- (51) Ver p. 22 do relatório de avaliação. 12 % referem-se a dados entre seis e doze meses, e 2 % a dados com mais de um ano.
- (52) Ver p. 14 do relatório de avaliação.
- (53) Ver p. 30 do relatório de avaliação.

no âmbito do relatório, as violações de segurança dos dados e os escândalos no domínio dos dados de tráfego e comunicações electrónicas em alguns Estados-Membros também servem de aviso ilustrativo. Não se pode ignorar este problema, pois a segurança dos dados conservados é crucial para um sistema de conservação de dados, dado que assegura o respeito por todas as outras salvaguardas ⁽⁵⁴⁾.

63. Em quarto lugar, o relatório não esclarece se todas as categorias de dados conservados se revelaram necessárias. Apenas são feitas algumas distinções genéricas entre dados telefónicos e dados da Internet. Alguns Estados-Membros optaram por aplicar um período de conservação mais breve para os dados da Internet ⁽⁵⁵⁾. No entanto, não se podem daí tirar conclusões de carácter geral.

IV.3. A Directiva relativa à conservação de dados tem falta de previsibilidade

64. Outra insuficiência da Directiva relativa à conservação de dados prende-se com a sua falta de previsibilidade. O requisito de previsibilidade emana do requisito genérico, consagrado no artigo 8.º, n.º 2, da CEDH e no artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, de que toda a ingerência deve estar prevista na lei. Segundo o TEDH, isso significa que a medida deve ter uma base jurídica na lei e ser compatível com o Estado de Direito, o que implica que a lei seja adequadamente acessível e previsível ⁽⁵⁶⁾. O Tribunal de Justiça também salientou no acórdão do processo *Österreichischer Rundfunk* que a lei deve ser redigida em termos suficientemente precisos para permitir aos cidadãos ajustarem a sua conduta ⁽⁵⁷⁾. A lei deve indicar com clareza suficiente a margem de manobra das autoridades competentes e a forma de exercício ⁽⁵⁸⁾.

65. Também na lista de controlo da comunicação da Comissão sobre a Carta dos Direitos Fundamentais da União Europeia, uma das questões a responder é se as eventuais limitações dos direitos fundamentais estão formuladas «de modo preciso e previsível» ⁽⁵⁹⁾. Na sua comunicação dedicada à apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça, a Comissão também afirma que os cidadãos «têm o direito de saber quais os dados pessoais tratados e objecto de intercâmbio, por quem e para que efeitos» ⁽⁶⁰⁾.

66. No caso de uma directiva da UE, a responsabilidade pelo respeito dos direitos fundamentais, incluindo o requisito de previsibilidade, cabe sobretudo aos Estados-Membros que transpõem a directiva para a sua ordem jurídica nacional.

⁽⁵⁴⁾ Ver também, a este respeito, o parecer da AEPD de 2005, pontos 29-37. Ver também o discurso da Autoridade Adjunta de 4 de Maio de 2011, que se encontra disponível no sítio Internet da AEPD (<http://www.edps.europa.eu>) em Publicações >> Discursos e Artigos >> 2011.

⁽⁵⁵⁾ Ver p. 14 do relatório de avaliação.

⁽⁵⁶⁾ Ver acórdão do TEDH, *S. e Marper*, mencionado na nota de rodapé n.º 7, ponto 151.

⁽⁵⁷⁾ Acórdão do TJUE de 20 de Maio de 2003, *Österreichischer Rundfunk*, C-465/00, ponto 77, e acórdão do TEDH, *S. e Marper*, mencionado na nota de rodapé n.º 7, ponto 95.

⁽⁵⁸⁾ Ver acórdão do TEDH, *Malone*, mencionado na nota de rodapé n.º 8, pontos 66-68.

⁽⁵⁹⁾ COM(2010) 573, mencionada na nota de rodapé 31, p. 5.

⁽⁶⁰⁾ COM(2010) 385, mencionada na nota de rodapé 17, p. 3.

O respeito dos direitos fundamentais é um requisito bem conhecido para essa transposição ⁽⁶¹⁾.

67. No relatório de avaliação, a Comissão também sublinha que a directiva «não garante, por si só, que os dados conservados são armazenados, extraídos e utilizados no pleno respeito do direito à vida privada e à protecção dos dados pessoais». A Comissão recorda que a «responsabilidade por assegurar o respeito desses direitos incumbe aos Estados-Membros» ⁽⁶²⁾.

68. No entanto, a AEPD considera que a directiva da UE também deveria, até certo ponto, cumprir o requisito da previsibilidade. Ou, reformulando o texto do acórdão do Tribunal de Justiça no processo *Lindqvist*, o regime previsto numa directiva não deve «carece[r] de previsibilidade» ⁽⁶³⁾, em especial quando se trate de uma medida da UE que obriga os Estados-Membros a organizar uma ingerência em grande escala nos direitos à vida privada e protecção de dados dos cidadãos. A AEPD considera que a UE tem a responsabilidade de assegurar, pelo menos, uma finalidade bem definida e uma indicação clara de quem pode ter acesso aos dados e em que condições.

69. Esta posição encontra respaldo no novo contexto jurídico criado pelo Tratado de Lisboa, que, como já foi explicado, reforçou a competência da UE no domínio da cooperação policial e judiciária em matéria penal e o compromisso da UE com o respeito dos direitos fundamentais.

70. A AEPD recorda que o requisito de uma finalidade específica e a subsequente proibição de tratamento de dados de um modo incompatível com essa finalidade («princípio de limitação da finalidade») são fundamentais para a protecção dos dados pessoais, o que é confirmado pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia ⁽⁶⁴⁾.

71. O relatório de avaliação demonstra que a opção de deixar a definição precisa do que constitui um «crime grave» e, posteriormente, do que devem ser consideradas «autoridades competentes» a cargo dos Estados-Membros deu origem a uma grande variedade de finalidades para a utilização dos dados ⁽⁶⁵⁾.

72. A Comissão afirma que a «maior parte dos Estados-Membros que já efectuou a transposição da Directiva para a respectiva legislação autoriza o acesso e a utilização dos dados conservados para fins que vão mais além dos previstos na Directiva, incluindo a prevenção e o combate à criminalidade em geral e a prevenção de riscos para a vida e a integridade física das pessoas» ⁽⁶⁶⁾. Os Estados-Membros exploram o «vazio jurídico» previsto no artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas ⁽⁶⁷⁾. A Comissão considera que

⁽⁶¹⁾ Ver, por exemplo, o acórdão do TJUE de 6 de Novembro de 2003, *Lindqvist*, ponto 87.

⁽⁶²⁾ Ver p. 31 do relatório de avaliação.

⁽⁶³⁾ Acórdão do TJUE, *Lindqvist*, ponto 84.

⁽⁶⁴⁾ Ver também o artigo 6.º da Directiva 95/46/CE.

⁽⁶⁵⁾ Ver p. 8 do relatório de avaliação.

⁽⁶⁶⁾ Ver p. 8 do relatório de avaliação.

⁽⁶⁷⁾ Ver p. 9 e p. 15 do relatório de avaliação.

esta situação pode não garantir uma «previsibilidade suficiente, que constitui uma das exigências de qualquer medida legislativa que restrinja o direito à vida privada»⁽⁶⁸⁾.

73. Nestas circunstâncias, não se pode dizer que a Directiva relativa à conservação de dados, em particular se for lida em conjunto com a Directiva relativa à privacidade e às comunicações electrónicas, proporciona a clareza necessária para cumprir o princípio da previsibilidade a nível da UE.

V. O CAMINHO A SEGUIR: CONSIDERAR TODAS AS OPÇÕES

74. A análise realizada na parte anterior justifica a conclusão de que a Directiva relativa à conservação de dados não cumpre os requisitos decorrentes do direito à vida privada e do direito à protecção de dados. É, portanto, claro que a Directiva relativa à conservação de dados não pode continuar a existir na sua forma actual. Nesse sentido, a Comissão está correcta em apresentar uma proposta de revisão do actual quadro jurídico da UE em matéria de conservação de dados⁽⁶⁹⁾.

75. No entanto, antes de apresentar uma proposta de versão revista da directiva:

- a) A Comissão deve, durante a avaliação de impacto, investir na obtenção de mais provas concretas junto dos Estados-Membros que demonstrem a necessidade da conservação de dados como medida de direito da UE;
- b) Se uma maioria de Estados-Membros considerar a conservação de dados necessária, todos esses Estados-Membros devem fornecer à Comissão provas quantitativas e qualitativas que o demonstrem;
- c) Os Estados-Membros que se oponham a uma medida de conservação de dados com essas características devem facultar informação à Comissão que permita uma avaliação mais vasta da matéria.

76. Além disso, na avaliação de impacto deve ainda ser analisado se outros meios alternativos e menos invasivos da vida privada poderiam ter conduzido ou podem ainda conduzir a resultados comparáveis. A Comissão deve tomar a iniciativa em relação a esta matéria, recorrendo, se necessário, a peritos externos.

77. A AEPD congratula-se pelo anúncio da Comissão de que iria consultar todas as partes interessadas durante a avaliação de impacto⁽⁷⁰⁾. A este respeito, a AEPD incentiva a Comissão a encontrar formas de participação directa dos cidadãos nesse exercício.

78. Importa salientar que uma avaliação da necessidade e a análise de meios alternativos e menos invasivos da vida privada só podem ser realizadas de uma forma justa, se todas as opções para o futuro da directiva estiverem em aberto. A este respeito, a Comissão parece excluir a possibilidade de revogação da directiva, por si só ou conjugada com uma proposta de uma medida alternativa da UE de âmbito mais específico. A AEPD apela, portanto, à Comissão para que tome seriamente em consideração também estas opções na avaliação de impacto.

79. Só se deve considerar uma futura Directiva relativa à conservação de dados se existir acordo em relação à necessidade de regras da UE da perspectiva do mercado interno e da cooperação policial e judiciária em matéria penal e se, durante a avaliação de impacto, for suficientemente demonstrada a necessidade de conservação de dados, apoiada e regulamentada pela UE, o que inclui uma apreciação cuidadosa de medidas alternativas.

80. A AEPD não nega a importância da conservação de dados para fins de aplicação da lei e o importante papel que pode ter em determinados casos. À semelhança do Tribunal Constitucional alemão (*Bundesverfassungsgericht*), a AEPD não exclui que uma obrigação de conservação de dados de telecomunicações bem definida se justifique em determinadas condições muito específicas⁽⁷¹⁾.

81. Assim, qualquer futuro instrumento da UE relativo à conservação de dados deve cumprir os seguintes requisitos básicos:

- Deve ser completo e harmonizar efectivamente as regras relativas à obrigação de conservação de dados, bem como ao acesso aos dados e sua utilização ulterior pelas autoridades competentes;
- Deve ser exaustivo, o que implica ter uma finalidade clara e precisa e colmatar o vazio jurídico existente no artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas;
- Deve ser proporcional e não ir além do necessário (ver, a este respeito, as observações feitas na parte IV.2, *supra*).

82. Como é óbvio, a AEPD analisará cuidadosamente qualquer futura proposta em matéria de conservação de dados à luz destas condições básicas.

VI. CONCLUSÃO

83. A AEPD congratula-se por a Comissão também ter tido em conta no relatório de avaliação as implicações da directiva a nível dos direitos fundamentais, embora tal não fosse exigido no artigo 14.º da Directiva relativa à conservação de dados.

84. O relatório de avaliação mostra que a directiva não conseguiu cumprir a sua principal finalidade, a saber, harmonizar as legislações nacionais em matéria de conservação de dados. Essa falta de harmonização é prejudicial para todas as partes envolvidas: cidadãos, empresas, operadores comerciais e autoridades responsáveis pela aplicação da lei.

85. Com base no relatório de avaliação, pode concluir-se que a Directiva relativa à conservação de dados não cumpre os requisitos decorrentes do direito à vida privada e do direito à protecção de dados, pelos seguintes motivos:

- Não foi suficientemente demonstrada a necessidade de conservação de dados prevista na Directiva relativa à conservação de dados;
- A conservação de dados poderia ter sido regulamentada de uma forma menos invasiva da privacidade;

⁽⁶⁸⁾ Conforme analisado no ponto 24, *supra*.

⁽⁶⁹⁾ Ver p. 32-33 do relatório de avaliação.

⁽⁷⁰⁾ Ver p. 32-33 do relatório de avaliação.

⁽⁷¹⁾ Ver *Bundesverfassungsgericht*, 1 BvR 256/08.

- A Directiva relativa à conservação de dados tem falta de previsibilidade.
86. A AEPD solicita à Comissão que analise seriamente todas as opções na avaliação de impacto, incluindo a possibilidade de revogação da directiva, por si só ou conjugada com uma proposta de uma medida alternativa da UE de âmbito mais específico.
87. Só se deve considerar uma futura Directiva relativa à conservação de dados se existir acordo em relação à necessidade de regras da UE da perspectiva do mercado interno e da cooperação policial e judiciária em matéria penal e se, durante a avaliação de impacto, for suficientemente demonstrada a necessidade de conservação de dados, apoiada e regulamentada pela UE, o que inclui uma apreciação cuidadosa de medidas alternativas. Qualquer instrumento dessa natureza deve cumprir os seguintes requisitos básicos:
- Deve ser completo e harmonizar efectivamente as regras relativas à obrigação de conservação de dados, bem como ao acesso aos dados e sua utilização ulterior pelas autoridades competentes;
 - Deve ser exaustivo, o que implica ter uma finalidade clara e precisa, e colmatar o vazio jurídico existente no artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas;
 - Deve ser proporcional e não ir além do necessário.
- Feito em Bruxelas, em 31 de Maio de 2011.
- Peter HUSTINX
Supervisor Europeu para a Protecção de Dados
-

Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF) e que revoga o Regulamento (Euratom) n.º 1074/1999

(2011/C 279/02)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os artigos 7.º e 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 28.º, n.º 2,

ADOPTOU O SEGUINTE PARECER:

1. INTRODUÇÃO

1. Em 17 de Março de 2011, a Comissão adoptou uma proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF) e que revoga o Regulamento (Euratom) n.º 1074/1999 (a seguir designada «proposta»).

1.1. Consulta da AEPD

2. A proposta foi enviada pelo Conselho à AEPD em 8 de Abril de 2011. A AEPD considera esta comunicação como um pedido para aconselhar as instituições e os órgãos comunitários, como prevê o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001, 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 [a seguir designado por «Regulamento (CE) n.º 45/2001»]. A AEPD congratula-se com o facto de esta consulta ser explicitamente referida no preâmbulo da proposta.

3. A proposta visa alterar os artigos 1.º a 14.º e eliminar o artigo 15.º do Regulamento (CE) n.º 1073/1999. O Regulamento (Euratom) n.º 1074/1999 do Conselho, de 25 de Maio de 1999, relativo aos inquéritos efectuados pela Organização Europeia de Luta Antifraude (OLAF) deverá ser revogado.

4. Anteriormente ⁽³⁾, antes da adopção da proposta, a Comissão concedeu à AEPD a possibilidade de apresentar observações informais. A AEPD congratula-se com a abertura do processo, que ajudou a melhorar o texto do ponto de vista da protecção de dados numa fase precoce. Na verdade, algumas dessas observações foram tidas em conta na proposta.

5. O novo texto é o resultado de um longo processo de revisão. Em 2006, a Comissão apresentou uma proposta de alteração do Regulamento (CE) n.º 1073/1999. Esta proposta legislativa tinha como objectivo «conseguir uma maior eficiência operacional e uma melhor governação do Organismo».

6. Essa proposta anterior foi debatida no Conselho e no Parlamento Europeu no âmbito do processo de co-decisão. A AEPD emitiu o seu parecer em Abril de 2007, o qual continha muitas observações destinadas a tornar o texto da proposta mais coerente com as regras em matéria de protecção de dados consagradas no Regulamento (CE) n.º 45/2001 ⁽⁴⁾. Em 20 de Novembro de 2008, o Parlamento aprovou uma resolução, em primeira leitura ⁽⁵⁾, incluindo aproximadamente cem alterações à proposta.

7. A pedido da Presidência Checa do Conselho (Janeiro-Junho de 2009), a Comissão apresentou em Julho de 2010 um documento de reflexão actualizado sobre a reforma do Organismo dirigido ao Parlamento Europeu e ao Conselho. Em Outubro de 2010, o Parlamento regozijou-se com o documento de reflexão e solicitou à Comissão que retomassem o processo legislativo. Em 6 de Dezembro de 2010, o Conselho adoptou as suas conclusões sobre o documento

⁽³⁾ Em Janeiro de 2011.

⁽⁴⁾ Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF), JO C 91, 26.4.2007, p. 1.

⁽⁵⁾ Resolução legislativa do Parlamento Europeu, de 20 de Novembro de 2008, sobre uma proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF), P6_TA-PROV(2008) 553.

⁽¹⁾ JO L 281 de 23.11.1995, p. 31.

⁽²⁾ JO L 8 de 12.1.2001, p. 1.

de reflexão apresentado pela Comissão. O Comité de Fiscalização do OLAF contribuiu para o debate com os seus pareceres sobre o documento de reflexão e sobre o respeito dos direitos fundamentais e das garantias processuais nos inquéritos efectuados pelo OLAF. A Comissão apresentou a nova proposta subsequentemente.

1.2. A importância da proposta e o parecer da AEPD

8. A proposta contém disposições que têm um forte impacto nos direitos dos indivíduos. O OLAF continuará a recolher e a tratar dados sensíveis sobre suspeitas de infracção, infracções e condenações penais, bem como informação susceptível de ser aproveitada para excluir determinadas pessoas do usufruto de um direito, de uma prestação ou de um contrato, na medida em que tal informação representa um risco particular para os direitos e as liberdades das pessoas em causa. O direito fundamental à protecção de dados pessoais é relevante não apenas em si mesmo, mas também pelas suas fortes ligações a outros direitos fundamentais, como o direito à não discriminação e o direito a um processo justo, incluindo o direito de defesa nos inquéritos do OLAF. O respeito pelo direito a um processo justo afecta a validade das provas e deve ser considerado prioritário pelo OLAF, a fim de reforçar a sua responsabilidade. É, por conseguinte, essencial assegurar que, na execução dos seus inquéritos, direitos fundamentais como os direitos à protecção de dados e à privacidade das pessoas em causa são adequadamente garantidos.

1.3. Principais elementos da proposta

9. O objectivo declarado da proposta é aumentar a eficiência, a eficácia e a responsabilidade do OLAF, salvaguardando, simultaneamente, a independência dos seus inquéritos. Esse objectivo seria alcançado, sobretudo, pelos seguintes meios: i) o aumento da cooperação e do intercâmbio de informações com as outras instituições, serviços, organismos e agências da UE, bem como com os Estados-Membros; ii) o aperfeiçoamento da abordagem *de minimis* ⁽⁶⁾ aos inquéritos; iii) o reforço das garantias processuais das pessoas objecto de inquérito do OLAF; iv) a inclusão da possibilidade de o OLAF celebrar acordos administrativos para favorecer o intercâmbio de informações com a Europol, a Eurojust, as autoridades competentes de países terceiros e as organizações internacionais e v) a clarificação da função de controlo do Comité de Fiscalização.
10. A AEPD apoia os objectivos das alterações propostas e, a este respeito, congratula-se com a proposta. A AEPD aprecia particularmente a introdução do novo artigo 7.º-A, alínea a), consagrado às garantias processuais proporcionadas às pessoas. Relativamente aos direitos à protecção dos dados pessoais e da privacidade, a AEPD considera que, no seu todo, a proposta vem introduzir melhoramentos em relação à situação actual. Em especial, a AEPD regista

com satisfação o reconhecimento expresso da importância dos direitos das pessoas em causa nos termos dos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001 ⁽⁷⁾.

11. No entanto, apesar da impressão globalmente positiva, a AEPD considera que, do ponto de vista da protecção dos dados pessoais, a proposta ainda pode ser melhorada, sem com isso comprometer os objectivos que persegue. A AEPD está preocupada, em particular, com o facto de, por falta de coerência em determinados aspectos, a proposta poder vir a ser interpretada como *lex specialis* para o tratamento dos dados pessoais recolhidos no âmbito de inquéritos do OLAF, prevalecendo sobre a aplicação do quadro geral estabelecido para a protecção de dados no Regulamento (CE) n.º 45/2001. Existe, assim, um risco de as normas de protecção de dados contidas na proposta poderem ser interpretadas *ex contrario* como menos exigentes do que as previstas no regulamento, e isto sem qualquer justificação aparente na própria proposta nem na exposição de motivos.
12. Para evitar que se chegue a tal resultado, apresenta-se nas secções seguintes uma análise da proposta na qual, por um lado, são descritas as suas deficiências e, por outro lado, são sugeridas medidas para as melhorar. A análise cinge-se às disposições que têm impacto directo na protecção dos dados pessoais, com especial relevo para os n.ºs 8, 9, 10, 11 e 12 do artigo 1.º, que aditam ou alteram os artigos 7.º-A, 7.º-B, 8.º, 9.º, 10.º e 10.º-A.

2. ANÁLISE DA PROPOSTA

2.1. Contexto geral

13. O OLAF foi criado em 1999 ⁽⁸⁾ para proteger os interesses financeiros da UE e o dinheiro dos contribuintes contra a fraude, a corrupção e quaisquer outras actividades ilegais. O Organismo está ligado à Comissão, mas é independente desta. O OLAF efectua inquéritos, que podem ser externos ⁽⁹⁾ (em especial, eventuais inquéritos nos Estados-Membros ou em países terceiros) e internos ⁽¹⁰⁾ (inquéritos no interior das instituições, órgãos e organismos), com a finalidade de combater a fraude e as actividades ilegais que possam lesar os interesses financeiros da União Europeia.
14. Além disso, o OLAF pode i) transmitir às autoridades nacionais competentes informações obtidas durante os seus

⁽⁷⁾ Ver proposta, novos artigos 7.º-A e 8.º, n.º 4.

⁽⁸⁾ Decisão 1999/352/CE da Comissão, de 28 de Abril de 1999, que institui o Organismo Europeu de Luta Antifraude (OLAF), JO L 136 de 31.5.1999, p. 20. Ver também Regulamento (CE) n.º 1073/1999 do Parlamento Europeu e do Conselho, de 25 de Maio de 1999, relativo aos inquéritos efectuados pela Organização Europeia de Luta Antifraude (OLAF), JO L 136 de 31.5.1999, p. 1.

⁽⁹⁾ Ver artigo 3.º do Regulamento (CE) n.º 1073/1999.

⁽¹⁰⁾ Ver artigos 1.º e 4.º do Regulamento (CE) n.º 1073/1999.

⁽⁶⁾ Isto é, o OLAF deve definir e concentrar-se nas suas prioridades de inquérito para utilizar os seus recursos de forma eficiente.

inquéritos externos; ii) transmitir às entidades judiciárias as informações colhidas, aquando de inquéritos internos, sobre factos susceptíveis de processo penal e iii) transmitir à instituição, órgão ou organismo em causa informações obtidas durante inquéritos internos ⁽¹¹⁾.

15. O OLAF também pode cooperar estreitamente com a Eurojust ⁽¹²⁾ e a Europol ⁽¹³⁾ no exercício da sua obrigação legal de lutar contra a fraude, a corrupção e quaisquer outras actividades que possam lesar os interesses financeiros da União. Neste contexto, a Europol ⁽¹⁴⁾ e a Eurojust ⁽¹⁵⁾ podem proceder ao intercâmbio de informações operacionais, estratégicas ou técnicas com o OLAF, incluindo dados pessoais.
16. Com base no Regulamento (CE) n.º 1073/1999, o OLAF também pode realizar inquéritos em países terceiros, em conformidade com os vários acordos de cooperação vigentes entre a União Europeia e os países terceiros em causa. As actividades fraudulentas lesivas do orçamento da União também podem ter lugar fora do território da União Europeia, por exemplo, em relação à ajuda externa por esta concedida aos países em desenvolvimento, aos países can-

didatos ou a outros países beneficiários, ou no tocante a violações da legislação aduaneira. Para detectar e combater eficazmente essas infracções, o OLAF também necessita, assim, de realizar inspecções e verificações no local em países terceiros. A importância da cooperação internacional e, conseqüentemente, do intercâmbio de dados, é ilustrada pelos mais de 50 acordos de assistência administrativa mútua em matéria aduaneira que a União Europeia tem actualmente, incluindo com parceiros comerciais de grande dimensão, como a China, os Estados Unidos da América, o Japão, a Turquia, a Federação Russa e a Índia.

17. A aplicação do Regulamento (CE) n.º 45/2001 nas actividades do OLAF tem sido objecto de várias intervenções da AEPD nos últimos anos. Em relação à questão central da proposta (os inquéritos do OLAF), vale a pena mencionar o Parecer de 23 de Junho de 2006 sobre uma notificação de controlo prévio relativa aos inquéritos internos do OLAF ⁽¹⁶⁾; o Parecer de 4 de Outubro de 2007 sobre cinco notificações de controlo prévio relativas aos inquéritos externos ⁽¹⁷⁾ e o Parecer de 19 de Julho de 2007 sobre uma notificação de controlo prévio relativa ao controlo regular da execução da função de inquérito ⁽¹⁸⁾, referente às actividades do Comité de Fiscalização.

⁽¹¹⁾ Ver artigo 10.º do Regulamento (CE) n.º 1073/1999.

⁽¹²⁾ A Eurojust foi criada pela Decisão 2002/187/JAI do Conselho (posteriormente alterada pela Decisão 2003/659/JAI e a Decisão 2009/426/JAI do Conselho, de 16 de Dezembro de 2008, relativa ao reforço da Eurojust como um órgão da União Europeia com personalidade jurídica para incentivar e melhorar a coordenação e a cooperação entre as autoridades judiciais competentes dos Estados-Membros. Em particular, o artigo 26.º, n.º 4, da dita decisão dispôs que «O OLAF pode contribuir para os trabalhos da Eurojust em matéria de coordenação de investigações e procedimentos penais relativos à protecção dos interesses financeiros das Comunidades Europeias, quer por iniciativa da Eurojust, quer a pedido do OLAF, desde que as autoridades nacionais competentes envolvidas não se oponham a essa participação». Em 2008, a Eurojust e o OLAF celebraram um acordo administrativo (Acordo prático sobre as modalidades de cooperação entre a Eurojust e o OLAF, de 24 de Setembro de 2008) destinado a reforçar a cooperação entre as duas entidades e que inclui uma disposição específica sobre a transferência de dados pessoais.

⁽¹³⁾ A Europol é o Serviço Europeu de Polícia, que visa melhorar a eficácia e a cooperação das autoridades competentes dos Estados-Membros na prevenção e no combate ao terrorismo, ao tráfico de estupefacientes e outras formas graves de criminalidade organizada. O artigo 22.º da Decisão do Conselho, de 6 de Abril de 2009, que cria o Serviço Europeu de Polícia (Europol) (2009/371/JAI) dispõe que «Na medida em que seja relevante para o exercício das suas funções, a Europol pode estabelecer e manter relações de cooperação com [...] o OLAF». O mesmo artigo prevê que, até à entrada em vigor dos acordos ou convénios de ordem prática com as diversas entidades da UE com as quais a Europol deve cooperar, a Europol pode «receber directamente e utilizar informações, incluindo dados pessoais, das entidades [...], na medida em que tal seja necessário ao exercício legítimo das suas funções, e pode [...] transmitir directamente informações, incluindo informações pessoais, a essas entidades, na medida em que tal seja necessário ao exercício legítimo das funções do destinatário».

⁽¹⁴⁾ Ver artigo 22.º da Decisão do Conselho, de 6 de Abril de 2009, que cria o Serviço Europeu de Polícia (Europol) (2009/371/JAI), JO L 121 de 15.5.2009, p. 37.

⁽¹⁵⁾ Ver artigo 1.º, n.º 26, da Decisão 2009/426/JAI do Conselho, de 16 de Dezembro de 2008, relativa ao reforço da Eurojust e que altera a Decisão 2002/187/JAI.

2.2. Privacidade e avaliação de impacto

18. Nem na proposta nem na exposição de motivos a esta apensa, se faz qualquer referência ao seu impacto nas regras de protecção de dados ou a uma avaliação do impacto na privacidade e na protecção de dados. Uma explicação da abordagem adoptada em relação ao impacto na protecção de dados tornaria, certamente, a avaliação global da proposta mais transparente. A AEPD manifesta surpresa por a exposição de motivos não conter nenhum capítulo intitulado «Resultados das consultas das partes interessadas e das avaliações de impacto».

2.3. Aplicação do Regulamento (CE) n.º 45/2001

19. Tal como é dito no parecer anterior sobre a proposta apresentada em 2006 ⁽¹⁹⁾, a AEPD congratula-se com o facto de a proposta reconhecer que o Regulamento (CE) n.º 45/2001 é aplicável a todas as actividades de tratamento de dados empreendidas pelo OLAF. Em particular,

⁽¹⁶⁾ Processo 2005-418, disponível no endereço <http://www.edps.europa.eu>

⁽¹⁷⁾ Processos 2007-47, 2007-48, 2007-49, 2007-50, 2007-72, disponíveis no endereço <http://www.edps.europa.eu>

⁽¹⁸⁾ Processo 2007-73, disponível no endereço <http://www.edps.europa.eu>

⁽¹⁹⁾ Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF), JO C 91 de 26.4.2007, p. 1.

a nova formulação do artigo 8.º, n.º 4⁽²⁰⁾, refere claramente o papel do regulamento no contexto das várias actividades do OLAF, o que corresponde a uma actualização do texto do Regulamento (CE) n.º 1073/1999, que apenas mencionava a Directiva 95/46/CE como referência para as obrigações em matéria de protecção de dados.

20. O último período do artigo 8.º, n.º 4, introduz a aplicação do requisito de nomeação de um responsável pela protecção de dados: «O Organismo nomeia um responsável pela protecção dos dados, em conformidade com o disposto no artigo 24.º do Regulamento (CE) n.º 45/2001». Esta inserção, que formaliza a nomeação efectiva do RPD do OLAF, também é saudada pela AEPD.
21. Contudo, a AEPD constata com preocupação que a aplicação das normas de protecção de dados no texto proposto não está totalmente conforme com os requisitos do regulamento e que esse facto poderá suscitar preocupações quanto à sua coerência. Este aspecto será a seguir analisado em pormenor.

3. OBSERVAÇÕES ESPECÍFICAS

3.1. O OLAF e o respeito pelos direitos fundamentais, incluindo os princípios de protecção de dados

22. Os inquéritos do OLAF podem afectar seriamente os direitos fundamentais das pessoas. Tal como afirma o Tribunal de Justiça no acórdão *Kadi* ⁽²¹⁾, estes direitos são protegidos pelo ordenamento jurídico comunitário. De forma mais precisa, no acórdão *Schecke* ⁽²²⁾, o Tribunal, por referência à Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta») ⁽²³⁾, e nomeadamente aos seus artigos 8.º e 52.º, salienta que qualquer restrição ao direito de protecção dos dados pessoais apenas pode ser justificada se for prevista por lei, respeitar o conteúdo essencial do direito, observar o princípio da proporcionalidade e corres-

ponder aos objectivos de interesse geral da União Europeia. A AEPD atribui grande importância ao respeito dos direitos fundamentais nos domínios de actividade do OLAF.

23. O considerando 13 da proposta esclarece que o respeito pelos direitos fundamentais das pessoas sob inquérito deve ser sempre garantido e, nomeadamente, quando são prestadas informações sobre inqueritos em curso. O considerando realça, seguidamente, a necessidade de respeitar a confidencialidade dos inqueritos, os direitos legítimos das pessoas em causa, as disposições nacionais aplicáveis aos processos judiciais e, em última análise, as disposições da União em matéria de protecção de dados. É ainda especificado que o intercâmbio de informações será regido pelos princípios da proporcionalidade e da necessidade de tomar conhecimento.
24. Este considerando parece introduzir uma restrição à aplicabilidade dos direitos fundamentais tanto *ratione personae* (limitação às pessoas sob inquerito) como *ratione materiae* (limitação ao intercâmbio de informações). Esse facto poderia levar a uma interpretação incorrecta do texto, segundo a qual os direitos fundamentais seriam aplicados de «forma restritiva» ⁽²⁴⁾ nos domínios de actividade do OLAF.
25. A AEPD sugere, por conseguinte, que se altere o texto do considerando, a fim de evitar interpretações erradas: o considerando afirma que o respeito pelos direitos fundamentais das «pessoas sob inquerito» deve ser sempre garantido. Como o OLAF não se ocupa apenas de pessoas sob inquerito («suspeitos») mas também de informadores (pessoas que fornecem informações sobre os factos de um caso possível ou concreto), denunciante ⁽²⁵⁾ (pessoas das instituições da UE que comunicam ao OLAF factos relacionados com um caso possível ou concreto) e testemunhas, a disposição deve definir mais amplamente as categorias de «pessoas» que gozam dos direitos fundamentais.

26. Além disso, o considerando 13 refere-se ao respeito pelos direitos fundamentais, especialmente no contexto do «intercâmbio de informações». O considerando menciona que, para além dos direitos fundamentais e da confidencialidade, «[a]s informações transmitidas ou obtidas durante os inqueritos serão tratadas de acordo com as disposições da União em matéria de protecção de dados». A localização desta frase pode suscitar confusão, devendo ser colocada num considerando distinto para esclarecer que o respeito pelas disposições em matéria de protecção de dados é um princípio separado e autónomo, não estando unicamente relacionado com o intercâmbio de informações.

⁽²⁰⁾ «O Organismo trata apenas os dados pessoais necessários para o cumprimento das suas funções por força do presente regulamento. Esse tratamento de dados pessoais deve ser efectuado em conformidade com o Regulamento (CE) n.º 45/2001, nomeadamente a prestação de informações relevantes à pessoa envolvida prevista nos artigos 11.º e 12.º do referido regulamento. Essas informações não podem ser comunicadas a outras pessoas além daquelas que, nas instituições da União ou nos Estados-Membros, devam conhecê-las em razão das suas funções, nem ser utilizadas para outros fins que não seja assegurar a luta contra a fraude, a corrupção e qualquer outra actividade ilegal. (...)».

⁽²¹⁾ Acórdão de 3 de Setembro de 2008 nos processos apensos C-402/05 P e C-415/05 P, *Kadi* contra Conselho da União Europeia e a Comissão das Comunidades Europeias, ponto 283: «[...] os direitos fundamentais fazem parte integrante dos princípios gerais de direito cujo respeito é assegurado pelo Tribunal de Justiça. Para este efeito, o Tribunal inspira-se nas tradições constitucionais comuns aos Estados-Membros e nas indicações fornecidas pelos instrumentos internacionais relativos à protecção dos Direitos do Homem, em que os Estados-Membros colaboraram ou a que aderiram. A CEDH reveste, neste contexto, um significado particular». Ver também ponto 304.

⁽²²⁾ Acórdão de 9 de Novembro de 2010 nos processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke*, ponto 44 e seguintes.

⁽²³⁾ Após a entrada em vigor do Tratado de Lisboa, a CEDH é aplicável a todos os domínios de actividade da União Europeia.

⁽²⁴⁾ Ver também ponto 36, *infra*.

⁽²⁵⁾ Ver parecer sobre uma notificação de controlo prévio recebida do responsável pela protecção de dados do Organismo Europeu de Luta Antifraude (OLAF) sobre os inqueritos internos do OLAF, 23 de Junho de 2006, Processo 2005/0418, disponível no endereço <http://www.edps.europa.eu>

27. A AEPD congratula-se com o facto de o artigo 7.º-A ser especificamente dedicado às garantias processuais durante os inquéritos. Esta nova disposição está conforme com o objectivo declarado da proposta de reforçar a responsabilidade do OLAF. O artigo também refere a Carta, que inclui disposições pertinentes para os inquéritos do OLAF, nomeadamente o artigo 8.º («Protecção de dados pessoais») e o Capítulo VI («Justiça») na sua totalidade.
28. O artigo 7.º-A, n.º 1, da proposta requer que o Organismo procure provas de acusação e de defesa da pessoa envolvida e recorda o dever de conduzir os inquéritos de forma objectiva e imparcial. Estes princípios têm um impacto positivo no princípio de «qualidade dos dados»⁽²⁶⁾ estabelecido no artigo 4.º do Regulamento (CE) n.º 45/2001, na medida em que o critério exige que os dados sejam exactos, conformes com a realidade objectiva, completos e actualizados. A AEPD congratula-se, por conseguinte, com a inserção deste número.

Direito de informação, acesso e rectificação

29. Os números seguintes do artigo 7.º-A referem-se às diversas fases dos inquéritos do OLAF. Essas fases podem resumir-se da seguinte forma: i) entrevistas de testemunhas ou pessoas envolvidas (artigo 7.º-A, n.º 2); ii) constatação de que a pessoa está implicada no inquérito (artigo 7.º-A, n.º 3); iii) conclusões do inquérito fazem referência a uma pessoa (artigo 7.º-A, n.º 4).
30. A AEPD observa que a obrigação de fornecer informações nos termos dos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001 (apenas) é mencionada em relação à fase iii). A AEPD verifica com satisfação que a proposta integrou as recomendações formuladas no seu parecer legislativo de 2006⁽²⁷⁾.
31. Contudo, essa menção selectiva dos direitos da pessoa em causa em relação a uma única fase processual pode ser interpretada no sentido de que as mesmas informações não devem ser prestadas à pessoa em causa (testemunha ou pessoa envolvida) quando esta é convocada para uma entrevista ou quando o membro do pessoal é informado de que pode estar implicado no inquérito. Por motivos de segurança jurídica, a AEPD sugere, assim, que a referência aos artigos pertinentes seja inserida em relação às três situações mencionadas nas alíneas i), ii) e iii). No entanto, uma vez que as informações relacionadas com os artigos 11.º ou 12.º do Regulamento (CE) n.º 45/2001 tenham sido fornecidas à pessoa em causa, não será necessário fornecer as mesmas informações nas fases subsequentes.

⁽²⁶⁾ Ver nota de pé-de-página 25.

⁽²⁷⁾ Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 1073/1999 relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF), JO C 91 de 26.4.2007, p. 1, n.º 14 e seguintes.

32. Além disso, o texto não introduz qualquer especificação sobre os direitos de acesso e rectificação dos dados das pessoas em causa previstos nos artigos 13.º e 14.º do Regulamento (CE) n.º 45/2001. Esses direitos são protegidos pelo artigo 8.º, n.º 2, da Carta e, por isso, merecem um relevo especial entre os direitos da pessoa em causa. A AEPD já solicitou⁽²⁸⁾ que fosse inserida uma especificação mais clara dos direitos de acesso e rectificação da pessoa em causa para evitar o risco de se interpretar que o texto introduz um regime especial «de nível inferior» para as pessoas abrangidas pelos inquéritos do OLAF. A AEPD lamenta que estes aspectos não sejam abordados na proposta.
33. A AEPD também gostaria de assinalar a possibilidade de limitar os direitos de informação, acesso e rectificação em casos específicos, prevista no artigo 20.º do Regulamento (CE) n.º 45/2001. O cumprimento das regras de protecção de dados pelo OLAF pode coexistir, assim, com a necessidade de preservar a confidencialidade dos seus inquéritos. Este aspecto será desenvolvido nos pontos seguintes.

Confidencialidade dos inquéritos e direitos da pessoa em causa

34. Em termos gerais, a AEPD reconhece que a função de inquérito do OLAF requer que este tenha a capacidade de proteger a confidencialidade dos seus inquéritos, a fim de lutar eficazmente contra a fraude e as actividades ilegais que lhe compete combater. A AEPD salienta, todavia, que essa capacidade afecta alguns direitos das pessoas em causa e que o Regulamento (CE) n.º 45/2001 estabelece condições específicas para que tais direitos possam ser restringidos neste contexto (artigo 20.º).
35. Nos termos do artigo 20.º do Regulamento (CE) n.º 45/2001, os direitos previstos pelos artigos 4.º (qualidade dos dados) e 11.º a 17.º (informação, direito de acesso, rectificação, bloqueio, apagamento, direito de obter a notificação a terceiros) podem ser restringidos na medida em que seja necessário para salvaguardar, nomeadamente: «a) a prevenção, investigação, detecção e repressão de infracções penais» ou «b) um interesse económico ou financeiro importante de um Estado-Membro ou das Comunidades Europeias» e «d) funções de controlo, de inspecção [...] associadas ao exercício da autoridade pública, nos casos referidos nas alíneas a) e b)». O mesmo artigo prevê que os principais motivos para a imposição de uma das restrições serão comunicados à pessoa em causa e que esta será informada da possibilidade de recorrer à Autoridade Europeia para a Protecção de Dados (artigo 20.º, n.º 3). Além disso, o artigo 20.º, n.º 5, dispõe que essa comunicação pode ser adiada enquanto o fornecimento da informação à pessoa em causa impedir o efeito da limitação imposta.

⁽²⁸⁾ No seu parecer de 2006, ver nota de rodapé 19, *supra*.

36. O texto da proposta introduz, essencialmente, excepções aos direitos das pessoas em causa por motivos de confidencialidade dos inquéritos. O artigo 7.º-A, n.º 4, prevê que «Sem prejuízo do disposto no artigo 4.º, n.º 6, e no artigo 6.º, n.º 5»⁽²⁹⁾, não devem ser elaboradas conclusões que façam referência a uma pessoa envolvida «no final do inquérito [...], sem que essa pessoa tenha tido a oportunidade de apresentar observações sobre os factos que lhe digam respeito, por escrito ou durante uma entrevista [...], e lhe tenha sido transmitida a informação exigida pelos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001». Afigura-se, por conseguinte, que o texto sugere que, nos casos previstos pelos artigos 4.º, n.º 6, e 6.º, n.º 5, o direito de audiência e o direito de informação da pessoa em causa poderiam ser restringidos.
37. A proposta dispõe ainda que, nos casos em que é necessário preservar a confidencialidade dos inquéritos e que impliquem o recurso a inquéritos da competência de uma autoridade judiciária nacional, o Director-Geral do OLAF pode decidir adiar a possibilidade de a pessoa envolvida apresentar as suas observações. O texto não especifica se, neste contexto, a informação requerida pelos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001 também deve ser adiada.
38. A formulação do texto não é clara. Em primeiro lugar, a ligação entre as eventuais restrições dos direitos da pessoa sob inquérito em relação às conclusões que lhe façam referência e o tipo de informação que o OLAF deve comunicar à entidade da UE competente no inquérito em questão está longe de ser clara. Em segundo lugar, não é claro que categorias de direitos da pessoa em causa são objecto de uma eventual restrição. Em terceiro lugar, o artigo não inclui a garantia necessária do artigo 20.º, n.º 3, do Regulamento (CE) n.º 45/2001.
39. Em consequência, as pessoas poderiam, em alguns casos, ser confrontadas com as conclusões relativas ao inquérito sem terem tido conhecimento de que eram objecto do
- mesmo e sem receberem qualquer informação sobre os motivos que levaram à restrição dos seus direitos de audiência e de informação consagrados nos artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001.
40. Se o artigo 20.º, n.ºs 3 e 5, do Regulamento (CE) n.º 45/2001 for respeitado, esse cenário não entraria, só por si, em conflito com o regulamento. Todavia, o facto de não se fazer no texto uma referência clara aos artigos do regulamento não se afigura coerente com o objectivo da proposta de reforçar as garantias processuais das pessoas envolvidas nos inquéritos do OLAF e de aumentar a responsabilidade deste último.
41. A AEPD sugere, por conseguinte, que uma eventual restrição aos direitos da pessoa em causa na aceção do artigo 20.º do Regulamento (CE) n.º 45/2001 deve ser explicitamente introduzida. Além disso, as garantias processuais do artigo 20.º, n.º 3, devem ser mencionadas no texto, bem como a eventual excepção do artigo 20.º, n.º 5. Essa disposição clara aumentaria a segurança jurídica da pessoa em causa e a responsabilidade do OLAF.
42. Em conclusão, para estabelecer um conjunto claro de direitos para a pessoa em causa e introduzir eventuais excepções devido à confidencialidade dos inquéritos, em conformidade com o artigo 20.º do Regulamento (CE) n.º 45/2001, a AEPD sugere que o texto indique claramente:
- as informações a fornecer à pessoa em causa para dar cumprimento às disposições em matéria de protecção de dados [artigos 11.º e 12.º do Regulamento (CE) n.º 45/2001], no contexto das várias fases dos inquéritos do OLAF⁽³⁰⁾: i) entrevistas (artigo 7.º-A, n.º 2); ii) informação quando uma pessoa puder estar implicada no inquérito (artigo 7.º-A, n.º 3) e iii) no final do inquérito (artigo 7.º-A, n.º 4);
 - o tipo de informações que podem ser adiadas pelo OLAF por motivos de confidencialidade do inquérito, estabelecendo claramente as condições e as categorias de pessoas em causa abrangidas pelo adiamento;
 - as informações que devem ser transmitidas à pessoa em causa para dar cumprimento às disposições em matéria de protecção de dados, caso a comunicação prevista nos artigos 11.º ou 12.º seja adiada ou os direitos de acesso e de rectificação sejam restringidos [nomeadamente, as informações previstas no artigo 20.º, n.º 3, do Regulamento (CE) n.º 45/2001], incluindo a excepção relacionada com a possibilidade de adiar mais ainda a informação ao abrigo do artigo 20.º, n.º 5, do Regulamento (CE) n.º 45/2001.

⁽²⁹⁾ O artigo 4.º, n.º 6 — «Inquéritos internos» — tem o seguinte teor: «Sempre que os inquéritos revelem que um membro ou um membro do pessoal pode estar envolvido num inquérito interno, a instituição, organismo, serviço ou agência a que pertença será informado. Nos casos excepcionais em que a confidencialidade do inquérito não pode ser assegurada, o Organismo utiliza canais alternativos de informação adequados». O artigo 6.º, n.º 5 — «Realização dos inquéritos» — tem o seguinte teor: «Sempre que um inquérito revele que pode ser oportuno tomar medidas administrativas cautelares destinadas a proteger os interesses financeiros da União, o Organismo informa a instituição, organismo, serviço ou agência em causa, o mais rapidamente possível, do inquérito em curso. As informações transmitidas incluem os seguintes elementos: a) A identidade do membro ou dos membros do pessoal envolvidos e um resumo dos factos em questão; b) Qualquer informação susceptível de ajudar a instituição, organismo, serviço ou agência a decidir da oportunidade de adoptar medidas administrativas cautelares destinadas a proteger os interesses financeiros da União; c) Eventuais medidas de confidencialidade recomendadas, em especial nos casos que impliquem o recurso a procedimentos de investigação da competência de uma autoridade judiciária nacional ou, no caso de um inquérito externo, da competência de uma autoridade nacional, em conformidade com o direito nacional aplicável aos inquéritos. [...]», sublinhado acrescentado.

⁽³⁰⁾ Como já foi dito, uma vez que as informações tenham sido comunicadas à pessoa em causa, não será necessário repetir as mesmas informações nas fases seguintes.

3.2. Política de informação

43. A AEPD salienta que quaisquer informações relativas aos inquéritos eventualmente divulgadas pelo OLAF podem envolver dados pessoais sensíveis e que é necessário avaliar essa publicação cuidadosamente. O Tribunal de Primeira Instância (actual Tribunal Geral), no seu acórdão sobre o Processo *Nikolaou*, em 2007 ⁽³¹⁾, deliberou que o OLAF tinha infringido o artigo 8.º, n.º 3, do Regulamento (CE) n.º 1073/1999 ⁽³²⁾ e o Regulamento (CE) n.º 45/2001, ao não cumprir adequadamente a sua obrigação de garantir a protecção dos dados pessoais no contexto de uma «fuga de informações» ⁽³³⁾ e da publicação de um comunicado de imprensa ⁽³⁴⁾.
44. Por conseguinte, a AEPD congratula-se com a introdução do artigo 8.º, n.º 5, que dispõe explicitamente que o Director-Geral assegura que as informações fornecidas ao público são prestadas «de forma neutra, imparcial» e no respeito dos princípios estabelecidos no artigo 8.º e no artigo 7.º-A. À luz das observações acima formuladas sobre o artigo 7.º-A, no que respeita à sua abordagem restritiva das regras do Regulamento (CE) n.º 45/2001, a AEPD congratula-se, em especial, com a referência, no artigo 8.º, n.º 5, à disposição mais geral do artigo 8.º, a qual implica que qualquer tratamento de dados pessoais no contexto da prestação de informações ao público será realizado em conformidade com todos os princípios do Regulamento (CE) n.º 45/2001.

3.3. Confidencialidade da identidade dos denunciante e informadores

45. No contexto da actual revisão, a AEPD gostaria de insistir na necessidade de introduzir uma disposição específica para garantir a confidencialidade da identidade dos denunciante e informadores. A AEPD salienta que os denunciante e informadores se encontram numa posição sensível. Deve garantir-se às pessoas que fornecem esse tipo de informações que a sua identidade é mantida confidencial, sobretudo em relação à pessoa visada pela comunicação da alegada infracção ⁽³⁵⁾. As actuais garantias (Comunicação da Comissão SEC/2004/151/2) não parecem ser suficientes do ponto de vista

⁽³¹⁾ Processo T-259/03, *Nikolaou contra Comissão das Comunidades Europeias*, 12 de Julho de 2007, JO C 247 de 20.10.2007, p. 23.

⁽³²⁾ O artigo refere especificamente às disposições matéria de protecção de dados.

⁽³³⁾ *Nikolaou*, ponto 213.

⁽³⁴⁾ *Nikolaou*, ponto 232.

⁽³⁵⁾ A importância de se manter a identidade do denunciante confidencial já foi salientada pela AEPD numa carta ao Provedor de Justiça Europeu, de 30 de Julho de 2010, no processo 2010-0458, que pode ser consultada no sítio Web da AEPD (<http://www.edps.europa.eu>). Ver também os pareceres de controlo prévio da AEPD, de 23 de Junho de 2006, sobre os inquéritos internos do OLAF (Processo 2005-0418), e de 4 de Outubro de 2007, sobre os inquéritos externos do OLAF (Processos 2007-47, 2007-48, 2007-49, 2007-50, 2007-72).

jurídico. A AEPD observa que a dita disposição seria consentânea com o Parecer do Grupo de Trabalho do Artigo 29.º sobre os regimes internos de denúncia ⁽³⁶⁾.

46. A AEPD recomenda que a actual proposta seja alterada e que se garanta que a identidade dos denunciante e informadores é mantida confidencial durante os inquéritos, desde que com isso não se infrinjam as regras nacionais aplicáveis aos processos judiciais. Designadamente, a pessoa visada pelas alegações pode ter direito a conhecer a identidade do denunciante e/ou informador para agir judicialmente contra os mesmos, caso se prove terem prestado declarações intencionalmente falsas a seu respeito ⁽³⁷⁾.

3.4. Transferências de dados pessoais pelo OLAF

Cooperação com a Eurojust e a Europol

47. A AEPD congratula-se com as especificações feitas no considerando 6 e no artigo 10.º-A e, em particular, com a introdução da exigência de uma base jurídica clara para a cooperação com a Eurojust e a Europol, a qual que está em perfeita sintonia com o Regulamento (CE) n.º 45/2001. Contudo, a proposta deveria ser mais pormenorizada, de modo a reflectir os diferentes regimes de protecção de dados da Eurojust e da Europol.
48. Até agora, o OLAF tem um Acordo prático com a Eurojust ⁽³⁸⁾ que especifica as condições em que a transferência de dados pessoais pode ter lugar. A cooperação entre o OLAF e a Eurojust inclui, designadamente, o intercâmbio de resumos dos processos e de informações estratégicas e operacionais relacionadas com processos, a participação em reuniões e a assistência mútua que possa ser útil para o exercício eficiente e eficaz das respectivas funções. O Acordo prático ⁽³⁹⁾ define, sobretudo, o *modus operandi* para o intercâmbio de informações, incluindo dados pessoais, e em alguns casos também realça ou especifica alguns elementos do quadro jurídico existente.

⁽³⁶⁾ Ver Parecer 1/2006 do Grupo de Trabalho do Artigo 29.º, de 1 de Fevereiro de 2006, sobre a aplicação das regras da UE em matéria de protecção de dados aos regimes internos de denúncia de irregularidades nos seguintes domínios: contabilidade, controlos contabilísticos internos, questões de auditoria, luta contra a corrupção, criminalidade nos sectores bancário e financeiro, disponível no endereço: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

⁽³⁷⁾ Ver Parecer sobre as disposições financeiras aplicáveis ao orçamento anual da União, de 15 de Abril de 2011, disponível no endereço <http://www.edps.europa.eu>

⁽³⁸⁾ Acordo prático sobre as modalidades de cooperação entre a Eurojust e o OLAF, de 24 de Setembro de 2008: ver nota de rodapé 12 *supra*.

⁽³⁹⁾ Acordo prático Eurojust-OLAF, ponto 4.1.

49. Quanto à Europol, não existe um acordo desse tipo com o OLAF⁽⁴⁰⁾, mas a Decisão Europol permite que esta última receba, utilize e transmita directamente informações, incluindo dados pessoais, do OLAF — *inter alia*-, ainda antes da celebração de um acordo de intercâmbio formal, na medida em que tal seja necessário ao exercício legítimo das funções da Europol e do OLAF⁽⁴¹⁾. O intercâmbio também está sujeito à existência de um acordo de confidencialidade entre as duas entidades. O artigo 24.º da Decisão Europol especifica algumas garantias que a Europol deve observar em relação a qualquer transferência de dados que tenha lugar antes da celebração de um acordo de intercâmbio formal: «A Europol é responsável pela legalidade da transmissão de dados. A Europol deve manter um registo de todas as transmissões de dados ao abrigo do presente artigo e dos motivos das mesmas. Os dados apenas são transmitidos se o destinatário garantir que os mesmos serão utilizados exclusivamente para a finalidade para que foram transmitidos». O artigo 29.º da mesma decisão também especifica quando a responsabilidade pelos dados transferidos por terceiros cabe à Europol.

50. A AEPD apoia fortemente a celebração de um acordo específico com a Europol sobre as transferências de dados, e o facto de não ter sido celebrado até à data reforça a necessidade de se introduzirem garantias específicas no texto da proposta. Tendo em conta os diferentes regimes de protecção de dados aplicáveis à transferência de dados pessoais do OLAF para a Eurojust e a Europol e reciprocamente, a AEPD considera que a proposta deve abordar mais claramente as garantias e normas necessárias para reger a cooperação entre o OLAF e esses organismos e a ter em conta nos acordos práticos presentes e futuros celebrados entre eles.

51. A fim de reforçar a necessidade de celebrar um acordo administrativo, a disposição do artigo 10.º-A, n.º 2, deve ser alterada para «O Organismo deve celebrar acordos administrativos [...]». Reflectiria, assim, a disposição similar da Decisão Europol⁽⁴²⁾, que dispõe que a Europol celebra acordos ou convénios de ordem prática com outras instituições, organismos e agências da União. Além disso, a proposta poderia clarificar, no artigo 10.º-A que, como princípio geral, o intercâmbio de dados pessoais com a Eurojust e a Europol se limitará e não excederá o que for *necessário* para o exercício legítimo das funções confiadas ao OLAF, à Europol e à Eurojust. A proposta também deveria impor ao OLAF a obrigação de conservar um registo de todos os dados transmitidos e dos motivos da sua transmissão, para reforçar a sua responsabilidade relativamente à

execução das obrigações impostas pelo Regulamento (CE) n.º 45/2001 no que se refere à transferência de dados pessoais.

Cooperação com países terceiros e organizações internacionais

52. O n.º 3 do artigo 10.º-A menciona que «O Organismo pode [igualmente] celebrar, se adequado, acordos administrativos com os serviços competentes de países terceiros e organizações internacionais. O Organismo coordena a sua actividade com os serviços da Comissão em causa e o Serviço Europeu para a Acção Externa».

53. A AEPD congratula-se com o facto de a cooperação do OLAF com países terceiros e organizações internacionais estar ligada à celebração de acordos administrativos. No entanto, as implicações em matéria de protecção de dados resultantes do possível intercâmbio de dados com países terceiros e organizações internacionais deveriam ser abordadas de forma mais específica na proposta.

54. A proposta deveria ser mais precisa a respeito dos requisitos e condições específicos para as eventuais transferências de dados de e para países terceiros e organizações internacionais. A AEPD recomenda que o texto do artigo 10.º-A, n.º 3, inclua também o seguinte: «Na medida em que a cooperação com organizações internacionais e países terceiros implique a transferência de dados pessoais do OLAF para outras entidades, essa transferência deve ter lugar de acordo com os critérios do artigo 9.º do Regulamento (CE) n.º 45/2001».

Acesso do Comité de Fiscalização a dados pessoais

55. A AEPD regista com satisfação a redacção do artigo 11.º da proposta, nos termos do qual «O Comité de Fiscalização pode solicitar ao Organismo informações adicionais sobre inquéritos em situações devidamente justificadas, sem todavia interferir com o desenrolar dos inquéritos», uma vez que essa redacção exprime o princípio da necessidade em relação a uma eventual transferência de dados pessoais do OLAF para o Comité de Fiscalização.

56. A questão do acesso do Comité de Fiscalização aos dados pessoais das pessoas implicadas, ou possivelmente implicadas, nos inquéritos também deve ser clarificada no contexto do regulamento interno a adoptar pelo Comité com base no novo artigo 11.º, n.º 6. A AEPD gostaria de ser envolvida no processo conducente à adopção do regulamento interno do Comité de Fiscalização. A consulta à AEPD também poderia ser inserida no texto da proposta como um requisito para a adopção do regulamento interno.

⁽⁴⁰⁾ O Acordo Administrativo de 8 de Abril de 2004 está restringido ao intercâmbio de informações estratégicas e exclui expressamente o intercâmbio de dados pessoais, deixando essa questão para um posterior acordo entre a Europol e o OLAF.

⁽⁴¹⁾ Decisão Europol, artigo 22.º, n.º 3, nota de rodapé 14, *supra*.

⁽⁴²⁾ Decisão Europol, artigo 22.º, n.º 2, ver nota de rodapé 14, *supra*: «A Europol celebra acordos ou convénios de ordem prática com as entidades referidas no n.º 1» (nomeadamente, a Eurojust, o OLAF, a Frontex, a CEPOL, o BCE e o OEDT).

4. PLANEAMENTO ESTRATÉGICO

57. Para além de todos os aspectos específicos acima mencionados, a AEPD gostaria de encorajar a Comissão a propor uma abordagem mais aberta ao regime de protecção de dados da UE por parte do OLAF. Seria o momento certo para este último desenvolver planos estratégicos para dar cumprimento a esse regime através de uma clarificação voluntária da abordagem prática a adoptar no tratamento dos seus numerosos ficheiros com dados pessoais. O OLAF poderia explicar de forma proactiva e pública o modo como trata os dados pessoais nas suas diversas actividades. A AEPD está persuadida de que essa abordagem global e explícita aumentaria a transparência do tratamento de dados pessoais realizado pelo OLAF e facilitaria a utilização dos seus processos de inquérito.

58. Por conseguinte, a AEPD sugere que as disposições da proposta atribuam ao Director-Geral a tarefa de assegurar a elaboração e actualização de uma panorâmica global das diversas operações de tratamento do OLAF, ou pelo menos que essa tarefa seja explicitada num considerando. Uma tal panorâmica — cujos resultados seriam divulgados de forma transparente, através, por exemplo, de um relatório anual ou de outras formas — não só aumentaria a eficácia das diversas actividades do OLAF e a sua interacção, mas também incentivaria o Organismo a adoptar uma abordagem mais global em relação à necessidade e proporcionalidade das operações de tratamento. Seria igualmente útil para o OLAF demonstrar de forma mais clara que aplica adequadamente os princípios de privacidade desde a concepção e de responsabilização.

5. CONCLUSÃO

59. Em conclusão, a AEPD congratula-se com as alterações introduzidas no texto e que tornam a proposta mais conforme com o regime da UE em matéria de protecção de dados.

60. Contudo, a AEPD também gostaria de salientar várias deficiências, que devem ser resolvidas através de uma alteração do texto, nomeadamente:

— a proposta deve mencionar claramente o direito à informação das diversas categorias de pessoas em causa,

bem como o direito de acesso e de rectificação relativamente a todas as fases dos inquéritos realizados pelo OLAF;

— a proposta deve clarificar a relação entre a necessidade de confidencialidade dos inquéritos e o regime de protecção de dados aplicável durante os mesmos: a AEPD sugere que os direitos das pessoas em causa sejam claramente definidos e separados, bem como as eventuais excepções resultantes dos requisitos de confidencialidade, e que as garantias previstas pelo artigo 20.º do Regulamento (CE) n.º 45/2001 sejam explicitamente introduzidas;

— a proposta deve clarificar a política do OLAF em matéria de informação do público no que diz respeito à protecção de dados;

— a proposta deve introduzir disposições específicas relativas à confidencialidade dos denunciantes e informadores;

— a proposta deve clarificar os princípios gerais de protecção de dados com base nos quais o OLAF pode transmitir e receber informações, incluindo dados pessoais, de e para outros organismos e agências da UE, países terceiros e organizações internacionais;

— as disposições da proposta devem atribuir ao Director-Geral a tarefa de garantir a elaboração, a actualização e a transparência de uma panorâmica estratégica global das diversas operações de tratamento efectuadas pelo OLAF, ou pelo menos a necessidade de a realizar deve ser explicitada num considerando.

Feito em Bruxelas, em 1 de Junho de 2011.

Giovanni BUTTARELLI

Autoridade Adjunta Europeia para a Protecção de Dados

Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à integridade e à transparência nos mercados da energia

(2011/C 279/03)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia e, nomeadamente, os artigos 7.º e 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⁾ e, nomeadamente, o artigo 41.º,

ADOPTOU O PRESENTE PARECER:

I. INTRODUÇÃO

1. Em 8 de Dezembro de 2010, a Comissão Europeia adoptou uma proposta de regulamento do Parlamento Europeu e do Conselho relativa à integridade e à transparência nos mercados da energia ⁽³⁾ («Proposta»).
2. A Comissão não consultou a AEPD, embora o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 o exigisse. Por iniciativa própria, a AEPD adopta o presente parecer com base no artigo 41.º, n.º 2, desse regulamento. A AEPD está ciente de que as presentes recomendações surgem numa fase tardia do processo legislativo. No entanto, considera adequado e útil emitir o presente parecer tendo em conta o eventual impacto significativo da Proposta no direito à vida privada e à protecção dos dados pessoais. O preâmbulo da Proposta deverá fazer referência ao presente parecer.
3. O principal objectivo da Proposta é impedir a manipulação de mercado e o abuso de informação privilegiada nos mercados grossistas de energia (gás e electricidade). A integridade e a transparência nos mercados grossistas de energia, em que o gás e a electricidade são negociados entre empresas produtoras de energia e comerciantes, são essenciais para os preços que os consumidores acabam por pagar.

4. Com este fim em vista, a Proposta visa estabelecer regras exaustivas a nível da UE para impedir que os comerciantes utilizem informação privilegiada em seu benefício e manipulem o mercado, causando uma subida artificial dos preços que não encontra justificação na disponibilidade, custo de produção, capacidade de armazenamento ou capacidade de transporte de energia. As regras propostas proíbem, especificamente, as seguintes actividades:

- Utilização de informação privilegiada na compra ou venda de energia nos mercados grossistas; informações exclusivas e com impacto na formação de preços devem ser divulgadas antes de a negociação se poder realizar;
- Transacções que originem indicações falsas ou enganosas no que respeita à oferta, à procura ou ao preço dos produtos energéticos grossistas; e
- Divulgação de notícias falsas ou rumores que originem indicações enganosas sobre estes produtos.

5. A responsabilidade pela monitorização do mercado a nível europeu para detectar eventuais infracções caberá à Agência de Cooperação dos Reguladores da Energia («ACER») ⁽⁴⁾.
6. Nos termos da Proposta, a ACER terá acesso em tempo útil a informação sobre as transacções que se realizam nos mercados grossistas de energia, nomeadamente informação sobre preços, quantidades vendidas e as partes envolvidas. Estes dados em massa serão também partilhados com os reguladores nacionais, que serão responsáveis pela investigação das suspeitas de abuso. Nos casos com impacto transfronteiras, a ACER terá poderes de coordenação das investigações. As entidades reguladoras nacionais nos Estados-Membros aplicam as sanções.
7. A Proposta surge na sequência de uma série de outras propostas legislativas recentes com vista a reforçar os regimes de supervisão financeira existentes e a reforçar a coordenação e a cooperação a nível da UE, nomeadamente a Directiva 2003/6/CE do Parlamento Europeu e do Conselho, de 28 de Janeiro de 2003, relativa ao abuso de informação privilegiada e à manipulação de mercado («MAD») ⁽⁵⁾, e a Directiva 2004/39/CE do Parlamento

⁽¹⁾ JO L 281 de 23.11.1995, p. 31 (a seguir designada «Directiva 95/46/CE»).

⁽²⁾ JO L 8 de 12.1.2001, p. 1 [a seguir designado «Regulamento (CE) n.º 45/2001»].

⁽³⁾ COM(2010) 726 final.

⁽⁴⁾ A ACER é um organismo da União Europeia, criado em 2010, que tem por missão assistir as entidades reguladoras da energia nacionais no exercício, a nível da UE, das funções de regulação que desempenham nos Estados-Membros e, se necessário, coordenar a sua actuação.

⁽⁵⁾ Directiva 2003/6/CE do Parlamento Europeu e do Conselho, de 28 de Janeiro de 2003, relativa ao abuso de informação privilegiada e à manipulação de mercado (abuso de mercado) (JO L 96 de 12.4.2003, p. 16).

Europeu e do Conselho, de 21 de Abril de 2004, relativa aos mercados de instrumentos financeiros («MiFID») (1). A AEPD emitiu recentemente um parecer sobre outra destas propostas recentes (2).

II. OBSERVAÇÕES E RECOMENDAÇÕES DA AEPD

8. A Proposta contém várias disposições pertinentes para a protecção dos dados pessoais:

- Artigos 6.º a 8.º relativos à monitorização do mercado e comunicação de dados;
- Artigo 9.º relativo à «protecção dos dados e fiabilidade operacional»;
- Artigos 10.º e 11.º relativos à investigação e aplicação da lei; e
- Artigo 14.º relativo às «relações com países terceiros».

II.1. Monitorização do mercado e comunicação de dados (artigos 6.º a 8.º)

Disposições pertinentes

9. A Proposta parte do princípio de que, para detectar os abusos de mercado: i) é necessário um sistema de monitorização dos mercados que funcione eficazmente e possa aceder em tempo útil a dados completos sobre as transacções, e ii) que contemple o controlo dos mercados a nível da UE. Por conseguinte, a proposta de regulamento estabelece que a ACER recolhe, analisa e partilha (com as autoridades pertinentes a nível nacional e da UE) uma grande quantidade de dados em massa relativos aos mercados grossistas de energia.
10. Em particular, a proposta de regulamento exige que os participantes no mercado forneçam à ACER «registos das suas transacções» de produtos energéticos grossistas. Além dos registos das transacções, os participantes no mercado devem ainda facultar à ACER informação relativa à «capacidade das instalações de produção, armazenamento, consumo ou transporte de electricidade ou de gás natural».
11. A forma e o conteúdo dessa informação, bem como os prazos para o seu fornecimento, serão estabelecidos em actos delegados da Comissão.

Observações e recomendações da AEPD

12. Considerando que a Proposta remete integralmente para os actos delegados a definição do conteúdo da informação a

(1) Directiva 2004/39/CE do Parlamento Europeu e do Conselho, de 21 de Abril de 2004, relativa aos mercados de instrumentos financeiros, que altera as Directivas 85/611/CEE e 93/6/CEE do Conselho e a Directiva 2000/12/CE do Parlamento Europeu e do Conselho e que revoga a Directiva 93/22/CEE do Conselho (JO L 145 de 30.4.2004, p. 1).

(2) Para obter mais informações sobre o contexto alargado das propostas legislativas conexas, ver o parecer da AEPD sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo aos derivados OTC, às contrapartes centrais e aos repositórios de transacções, de 19 de Abril de 2011; em particular, os pontos 4, 5, e 17 a 20.

recolher no quadro deste exercício de monitorização e comunicação, não se pode excluir que sejam abrangidos dados pessoais — ou seja, qualquer informação relativa a uma pessoa singular identificada ou identificável (3). Nos termos do direito da UE em vigor, a recolha destes dados só é permitida se for necessária e proporcional para a finalidade específica a que se destina (4). A proposta de regulamento deve, portanto, especificar claramente se os registos das transacções e as informações sobre as capacidades a recolher para fins de monitorização incluirão dados pessoais e o âmbito desses dados (5).

13. Se estiver previsto o tratamento de dados pessoais, poderão ser necessárias salvaguardas específicas, como disposições relativas à limitação da finalidade, período de conservação e eventuais destinatários da informação. Tendo em conta a sua natureza essencial, estas salvaguardas relativas à protecção de dados devem ser estabelecidas directamente no texto da proposta de regulamento e não em actos delegados.
14. Se, pelo contrário, não estiver previsto o tratamento de dados pessoais (ou esse tratamento assumir um carácter excepcional e estiver limitado a casos pontuais, em que um negociante de produtos energéticos grossistas possa ser uma pessoa singular e não uma entidade jurídica), esse facto deve estar explícito na Proposta, no mínimo, num considerando.

II.2. Protecção dos dados e fiabilidade operacional (artigo 9.º)

Disposições pertinentes

15. O artigo 9.º, n.º 1, estabelece que a ACER «assegura a confidencialidade, a integridade e a protecção» das informações recebidas ao abrigo do artigo 7.º (ou seja, os registos das transacções e as informações sobre as capacidades que forem recolhidos no quadro do exercício de monitorização do mercado). O artigo 9.º estipula ainda que, «se for caso disso», a ACER «dará cumprimento» ao Regulamento (CE) n.º 45/2001 no tratamento de dados pessoais ao abrigo do artigo 7.º
16. Além disso, o artigo 9, n.º 1, também estabelece que a ACER «identifica as fontes de risco operacional e limita esse risco através do desenvolvimento de sistemas, controlos e procedimentos adequados».
17. Por último, o artigo 9.º, n.º 2, permite que a ACER divulgue publicamente partes das informações que detém, «sob condição de não serem divulgadas informações comercialmente sensíveis sobre participantes no mercado ou transacções em concreto».

(3) Ver artigo 2.º, alínea a), da Directiva 95/46/CE e o artigo 2.º, alínea a), do Regulamento (CE) n.º 45/2001.

(4) Ver artigos 6.º, n.º 1, alínea c), e 7.º, alínea c), da Directiva 95/46/CE e artigos 4.º, n.º 1, alínea c), e 5.º, alínea b), do Regulamento (CE) n.º 45/2001.

(5) O artigo 9.º, n.º 1, da Proposta, por referência ao Regulamento (CE) n.º 45/2001, indicia que será esse o caso, mas não acrescenta pormenores. Ver também a este respeito a secção II.2 do presente parecer.

Observações e recomendações da AEPD

18. A AEPD congratula-se com o facto de o artigo 9.º ser dedicado, em parte, à protecção de dados e também por a proposta de regulamento exigir especificamente que a ACER cumpra o Regulamento (CE) n.º 45/2001.

a) Aplicabilidade do Regulamento (CE) n.º 45/2001 e da Directiva 95/46/CE

19. No entanto, a AEPD salienta que o Regulamento (CE) n.º 45/2001 se aplica integralmente à ACER, nos termos do próprio regulamento, em todas as situações em que a ACER trate dados pessoais. Por conseguinte, a Proposta deve recordar que o Regulamento (CE) n.º 45/2001 se aplica à ACER quando esta trata dados ao abrigo do artigo 7.º e também em todas as outras situações, designadamente quando a ACER trata dados pessoais no âmbito de suspeitas de abuso de mercado/infracções ao abrigo do artigo 11.º. Além disso, a fim de ser mais preciso, a AEPD recomenda que em vez de ser utilizada a expressão «se for caso disso» para descrever as situações em que a ACER tem de cumprir o Regulamento (CE) n.º 45/2001, seja utilizada a expressão «sempre que haja lugar ao tratamento de dados pessoais».

20. Deve igualmente ser feita referência à Directiva 95/46/CE, tendo em conta que esta directiva se aplica ao tratamento de dados pessoais pelas entidades reguladoras nacionais envolvidas. De facto, por uma questão de clareza, a AEPD recomenda que a proposta de regulamento mencione, de uma forma geral (pelo menos num considerando), que embora a ACER esteja sujeita ao Regulamento (CE) n.º 45/2001, a Directiva 95/46/CE será aplicável a todas as entidades reguladoras nacionais envolvidas.

b) Responsabilização

21. A AEPD congratula-se com a exigência de que a ACER identifique e limite os riscos operacionais através do desenvolvimento de sistemas, controlos e procedimentos adequados. Com vista ao reforço do princípio da responsabilização⁽¹⁾, caso o tratamento de dados pessoais desempenhasse uma função estrutural, a proposta de regulamento deveria exigir especificamente que a ACER criasse um quadro claro de responsabilização, que assegurasse a conformidade com as normas de protecção de dados e demonstrasse o seu cumprimento. Este quadro claro criado pela ACER deve conter vários elementos, nomeadamente:

- Adopção e actualização, sempre que necessário, de uma política de protecção de dados com base numa avaliação do impacto (deve incluir também uma avaliação dos riscos de segurança); um plano de segurança, que deve estar incluído nesta política de protecção de dados;

⁽¹⁾ Ver secção 7 do parecer da AEPD sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — «Uma abordagem global da protecção de dados pessoais na União Europeia», emitido em 14 de Janeiro de 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

- Realização de auditorias periódicas para avaliar a adequação permanente e a conformidade com a política de protecção de dados (incluindo auditorias ao plano de segurança);

- Divulgação (pelo menos parcial) dos resultados das auditorias, a fim de dar garantias aos intervenientes no que se refere ao cumprimento das regras em matéria de protecção de dados; e

- Notificação de violações de dados e outros incidentes de segurança ao responsável pela protecção de dados da Comissão, às pessoas afectadas e a outros intervenientes e autoridades pertinentes⁽²⁾.

22. Devem também ser aplicáveis requisitos equivalentes às entidades reguladoras nacionais e a outras autoridades da UE pertinentes.

c) Publicação da informação pela ACER

23. No que se refere ao requisito previsto no artigo 9.º, n.º 2, de que a ACER divulgue publicamente partes das informações que detém, a AEPD considera que esta disposição não tem como finalidade autorizar a ACER a publicar os dados para efeitos de «publicitação e denúncia» ou divulgação de actos ilícitos de empresas ou pessoas singulares.

24. No entanto, a Proposta é omissa em relação à intenção de divulgação pública de dados pessoais. Por conseguinte, para evitar qualquer tipo de dúvida, a proposta de regulamento deve estipular especificamente que a informação publicada não deve conter dados pessoais, ou esclarecer que dados pessoais podem eventualmente ser divulgados.

25. Na eventualidade de serem divulgados dados pessoais, a necessidade de divulgação (por exemplo, por razões de transparência) deve ser cuidadosamente ponderada e avaliada face a outras preocupações que também se ponham, como a necessidade de proteger o direito à vida privada e à protecção dos dados pessoais das pessoas em causa.

26. Por conseguinte, antes de qualquer divulgação, deve ser efectuada uma avaliação da proporcionalidade tendo em conta os critérios estabelecidos pelo Tribunal de Justiça da União Europeia no acórdão do processo *Schecke*⁽³⁾. Naquele processo, o TJUE sublinhou que as derrogações à protecção dos dados pessoais e as suas limitações só devem ocorrer na estrita medida do necessário. O TJUE considerou ainda que as instituições europeias devem analisar diferentes métodos de publicação, a fim de encontrarem

⁽²⁾ Ver secção 6.3 do Parecer da AEPD de 14 de Janeiro de 2011 supramencionada.

⁽³⁾ Acórdão do TJUE de 9 de Novembro de 2010, processos apensos C-92/09 e C-93/09 (*Schecke e Eifert*); ver, em particular, os pontos 81, 65 e 86.

um que seja conforme com o objectivo dessa publicação e, ao mesmo tempo, menos lesivo do direito das pessoas ao respeito da sua vida privada e à protecção dos seus dados pessoais.

II.3. Poderes de investigação (artigo 10.º)

Disposições pertinentes

27. A Proposta estabelece que a monitorização dos mercados será seguida de uma investigação nos casos em que haja suspeita de abuso de mercado, a qual poderá conduzir à adopção de sanções apropriadas. O artigo 10.º, n.º 1, em particular, exige que os Estados-Membros invistam as entidades reguladoras nacionais dos poderes de investigação necessários para assegurar a aplicação das disposições do regulamento relativas ao abuso de informação privilegiada e à manipulação de mercado ⁽¹⁾.

Observações e recomendações da AEPD

28. A AEPD congratula-se com a especificação, no artigo 10.º, n.º 1, que: i) os poderes de investigação (apenas) devem ser exercidos a fim de assegurar a aplicação das disposições relativas ao abuso de informação e à manipulação de mercado (artigos 3.º e 4.º), e que ii) esses poderes devem ser exercidos de modo proporcionado.

29. No entanto, a Proposta deve ser ainda mais ambiciosa, a fim de assegurar a certeza jurídica e um nível adequado de protecção para os dados pessoais. Como se demonstrará mais adiante, existem dois problemas no texto do artigo 10.º proposto. Em primeiro lugar, o artigo 10.º não designa com clareza suficiente o âmbito dos poderes de investigação; por exemplo, não é suficientemente claro em relação à eventual necessidade de registos telefónicos privados ou se poderá ser realizada uma inspecção *in loco* numa residência particular. Em segundo lugar, o artigo 10.º também não contempla as necessárias salvaguardas processuais contra o risco de invasão injustificada da vida privada ou utilização ilícita dos dados pessoais; por exemplo, não exige um mandado de uma autoridade judicial.

30. A definição do âmbito dos poderes de investigação e das salvaguardas necessárias é, presumivelmente, deixada a cargo da legislação nacional. De facto, o artigo 10.º, n.º 1, deixa muitas opções em aberto para os Estados-Membros ao estipular que os poderes de investigação «podem ser exercidos: a) directamente, b) em colaboração com outras autoridades ou com as empresas de mercado, ou c) mediante requerimento apresentado às autoridades judiciais competentes». Esta redacção parece permitir divergências nas práticas nacionais, por exemplo, em relação às circunstâncias em que seria necessário um mandado de uma autoridade judicial ou se seria necessário de todo.

⁽¹⁾ Importa salientar que a proposta de regulamento não concede poderes de investigação equivalentes à ACER. Tais poderes também não estão previstos para a ACER no Regulamento (CE) n.º 713/2009 do Parlamento Europeu e do Conselho, de 13 de Julho de 2009, que institui a Agência de Cooperação dos Reguladores da Energia (JO L 211 de 14.8.2009, p. 1).

31. Embora algumas legislações nacionais possam já prever salvaguardas processuais e de protecção de dados adequadas, tendo em vista garantir a certeza jurídica às pessoas, importa fazer determinadas clarificações e estabelecer certos requisitos mínimos no que se refere às salvaguardas processuais e de protecção de dados a nível da UE, na proposta de regulamento, conforme se descreve adiante.

32. Por princípio, a AEPD sublinha que quando a legislação da UE obriga os Estados-Membros a tomar medidas a nível nacional que afectam os direitos fundamentais (como o direito à vida privada e à protecção dos dados pessoais), a legislação deve ainda exigir que sejam tomadas medidas eficazes ao mesmo tempo que as referidas medidas restritivas, para garantir a protecção dos direitos fundamentais em questão. Por outras palavras, a harmonização de medidas eventualmente invasivas da vida privada, como os poderes de investigação, deve ser acompanhada da harmonização das salvaguardas processuais e de protecção de dados, tendo por base as melhores práticas.

33. Uma abordagem desta natureza pode ajudar a evitar divergências demasiado grandes a nível nacional e contribuir para um grau mais elevado e uniforme de protecção dos dados pessoais em toda a União Europeia.

34. Caso não seja exequível, neste momento, a harmonização das salvaguardas mínimas, a AEPD recomenda, pelo menos, que a proposta de regulamento obrigue especificamente os Estados-Membros a adoptarem medidas de aplicação nacionais, com vista a assegurar as salvaguardas processuais e de protecção de dados necessárias. Esta harmonização torna-se ainda mais importante pelo facto de o instrumento jurídico escolhido ser um regulamento, que é directamente aplicável e, em regra, não exige outras medidas de aplicação nos Estados-Membros.

II.4. Inspeções *in loco* [artigo 10.º, n.º 2, alínea c)]

Disposições pertinentes

35. A Proposta estipula que os poderes de investigação a conferir às entidades reguladoras nacionais contemplem especificamente o poder de realizar inspecções *in loco* [artigo 10.º, n.º 2, alínea c)].

Observações e recomendações da AEPD

36. Não é claro se as referidas inspecções se limitariam a propriedades comerciais (instalações, terrenos e veículos) de um participante no mercado ou se também seriam extensíveis à propriedade privada (instalações, terrenos e veículos) de pessoas singulares. É, ainda, pouco claro se as inspecções podem ser realizadas sem aviso prévio («rusgas»).

37. Caso a Comissão tenha em vista exigir que os Estados-Membros autorizem as entidades reguladoras a realizar inspecções *in loco* em propriedades privadas de pessoas singulares ou a realizar rusgas, tal intenção carece, antes de mais, de uma especificação clara.

38. Em segundo lugar, a AEPD salienta que a proporcionalidade das inspecções *in loco* em propriedades privadas (como as residências particulares de pessoas singulares) está longe de ser óbvia e, caso estejam previstas inspecções desta natureza, devem ser especificamente justificadas.
39. Em terceiro lugar, para este caso, seriam necessárias salvaguardas adicionais, em particular no que se refere às condições em que se podem realizar estas inspecções. Por exemplo, e sem limitação, a Proposta deve especificar que as inspecções *in loco* apenas podem ser realizadas numa residência particular, se existir uma suspeita razoável e específica de que estejam guardadas provas nessa residência concreta, que sejam pertinentes para provar uma violação grave dos artigos 3.º ou 4.º do regulamento (ou seja, as disposições relativas à proibição de abuso de informação e à manipulação de mercado). É ainda importante que a Proposta estabeleça a necessidade de um mandado judicial em todos os Estados-Membros⁽¹⁾.
40. Em quarto lugar, para assegurar a proporcionalidade e evitar a ingerência excessiva na vida privada, as inspecções a residências particulares sem aviso prévio devem estar sujeitas à condição suplementar de que o aviso possa levar à destruição ou adulteração de provas. Esta condição deve estar claramente prevista na proposta de regulamento.

II.5. Poderes para ordenar «a comunicação dos registos telefónicos e de transmissão de dados existentes» [artigo 10.º, n.º 2, alínea d)]

Disposições pertinentes

41. O artigo 10.º, n.º 2, alínea d), estipula que os poderes conferidos às entidades reguladoras nacionais incluem especificamente o poder de «ordenar a comunicação dos registos telefónicos e de transmissão de dados existentes».

Observações e recomendações da AEPD

42. A AEPD reconhece a importância dos registos telefónicos e de transmissão de dados nos casos de abuso de informação, especialmente para estabelecer as ligações entre os informadores e os comerciantes. No entanto, o âmbito deste poder não é suficientemente claro, nem estão previstas salvaguardas processuais e de protecção de dados adequadas. Por conseguinte, a AEPD recomenda que a Proposta seja clarificada como se descreve adiante. Devem, em particular, ser considerados os seguintes aspectos:
- a) Que tipo de registos telefónicos e de transmissão de dados podem ser exigidos?
43. Para efeitos de certeza jurídica, a Proposta deve, em primeiro lugar, clarificar que tipos de registos podem ser exigidos pelas autoridades nos casos em que isso se revele necessário.
44. A Proposta deve limitar especificamente o âmbito dos poderes de investigação: i) ao conteúdo dos registos telefóni-

cos, de correio electrónico e de transmissão de dados que tenham sido obtidos regularmente e de forma legítima pelos comerciantes para efeitos da sua actividade, designadamente comprovar operações, e b) a dados de tráfego (por exemplo, quem efectuou a chamada ou enviou a informação, o destinatário e a data/hora) que já estejam disponíveis directamente junto dos participantes no mercado (comerciantes) em questão.

45. Além disso, a Proposta deve também especificar que os registos deverão ter sido recolhidos para uma finalidade legítima e em conformidade com a legislação de protecção de dados aplicável, nomeadamente, a informação adequada das pessoas nos termos dos artigos 10.º e 11.º da Directiva 95/46/CE.

b) A que se refere a qualificação «existentes»?

46. A AEPD congratula-se com o facto de a Proposta limitar o seu poder a registos «existentes» e, por isso, não exigir que os poderes das entidades reguladoras obriguem um comerciante ou terceiros a interceptar, monitorizar ou gravar transmissões telefónicas ou de dados especificamente para efeitos da investigação.

47. No entanto, para evitar qualquer tipo de dúvida, esta intenção deve ser tornada mais clara, pelo menos num considerando. Deve evitar-se dar azo a interpretações da proposta de regulamento no sentido de proporcionar uma base jurídica para as entidades reguladoras nacionais interceptarem, monitorizarem ou gravarem transmissões telefónicas ou de dados, de forma dissimulada ou aberta, com ou sem mandado.

c) Pode também ser ordenada a comunicação do conteúdo de conversas telefónicas e transmissões de dados ou apenas os dados de tráfego?

48. O texto da Proposta faz referência a «registos telefónicos e de transmissão de dados existentes». Não é suficientemente claro se pode ser exigida a comunicação tanto do conteúdo dos dados existentes e das comunicações telefónicas como dos dados de tráfego (por exemplo quem efectuou a chamada ou enviou a informação, o destinatário e a data/hora).

49. Este aspecto deve ser clarificado nas disposições da proposta de regulamento. Conforme foi referido nos pontos 43 a 45, deve ser claramente especificado que tipo de registos podem ser exigidos, sendo necessário garantir em primeiro lugar que a recolha dos dados se processe em conformidade com a legislação aplicável em matéria de protecção de dados.

d) Podem ser exigidos registos aos fornecedores de serviços Internet e operadores de telecomunicações?

50. A Proposta deve especificar de uma forma clara a quem as entidades reguladoras nacionais podem exigir registos. Em relação a este aspecto, a AEPD entende que o artigo 10.º, n.º 2, alínea d), não se destina a permitir que as entidades

⁽¹⁾ Ver, por exemplo, o acórdão do Tribunal Europeu dos Direitos do Homem no processo *Funke contra França* (processo n.º 82/1991/334/407) de 25 de Fevereiro de 1993, pontos 55 a 57.

reguladoras nacionais ordenem a «fornecedores de serviços de comunicações electrónicas acessíveis ao público»⁽¹⁾ (como companhias telefónicas ou fornecedores de serviços Internet) a comunicação de dados de tráfego.

51. Na verdade, a Proposta não faz qualquer referência a esses fornecedores de serviços e também não utiliza a expressão «dados de tráfego». É também significativo que não refira, de forma implícita ou explícita, que a derrogação teria como base os requisitos estabelecidos pela Directiva relativa à privacidade e às comunicações electrónicas⁽²⁾, que estabelece o princípio geral de que os dados de tráfego só podem ser tratados para efeitos de facturação dos assinantes e de pagamento de interligações.

52. Para evitar qualquer tipo de dúvida, a AEPD recomenda que a inexistência na Proposta de uma base jurídica para ordenar a fornecedores de serviços de comunicações electrónicas acessíveis ao público a comunicação de dados seja explicitamente mencionada no texto da proposta de regulamento, pelo menos num considerando.

e) Podem ser exigidos a terceiros?

53. Além disso, a Proposta deve clarificar se as entidades reguladoras nacionais só podem ordenar a comunicação de registos ao participante no mercado sob investigação ou se também têm poderes para ordenar a terceiros a comunicação dos seus registos (como um interveniente numa transacção com o participante no mercado sob investigação ou um hotel onde a pessoa suspeita de abuso de informação tenha ficado alojada).

f) Podem ser exigidos registos privados?

54. Por último, a Proposta deve também clarificar se as entidades reguladoras podem ordenar a comunicação de registos privados de pessoas, como os funcionários ou executivos do participante no mercado sob investigação (por exemplo, mensagens de texto enviadas de dispositivos móveis pessoais ou o histórico de navegação na Internet guardado num computador de casa).

55. A proporcionalidade de ordenar a comunicação de registos privados é discutível e, se estiver prevista, deve esta ter uma justificação específica.

56. À semelhança das inspecções *in loco* (ver pontos 35 a 40 *supra*), a Proposta deve estabelecer a necessidade de um mandado de uma autoridade judicial, assim como outras salvaguardas específicas, caso as autoridades ordenem a comunicação de registos privados.

⁽¹⁾ Ver o artigo 2.º, alínea c), da Directiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva-quadro) (JO L 108 de 24.4.2002, p. 33).

⁽²⁾ Ver o artigo 6.º, n.º 1, da 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).

II.6. Comunicação de suspeitas de abuso de mercado (artigo 11.º): limitação da finalidade e conservação de dados

Disposições pertinentes

57. No que se refere à cooperação transfronteiras, é conferida uma função importante à ACER, designadamente alertar as entidades reguladoras nacionais de eventuais casos de abuso de mercado e facilitar a troca de informação. A fim de facilitar a cooperação, o artigo 11.º, n.º 2, também exige especificamente que as entidades reguladoras nacionais informem a ACER «de forma tão pormenorizada quanto possível» quando tenham motivos justificados para suspeitar de qualquer acto contrário ao disposto na proposta de regulamento. A fim de assegurar uma abordagem coordenada, o artigo 11.º, n.º 3, também obriga à partilha de informação entre as entidades reguladoras nacionais, as autoridades financeiras competentes, a ACER e a Autoridade Europeia dos Valores Mobiliários e dos Mercados (AEVMM)⁽³⁾.

Observações e recomendações da AEPD

58. Em conformidade com o princípio de limitação da finalidade⁽⁴⁾, a Proposta deve estipular explicitamente que quaisquer dados pessoais transmitidos ao abrigo do artigo 11.º da proposta de regulamento (comunicação de suspeitas de abuso de mercado) devem ser utilizados apenas para efeitos da investigação da suspeita de abuso de mercado comunicada. Em nenhum caso a informação deve ser utilizada para outros fins incompatíveis com essa finalidade.

59. Além disso, os dados não devem ser conservados durante longos períodos. Esta limitação é ainda mais importante nos casos em que se demonstre que a suspeita inicial não tinha fundamento. Nesses casos, é necessária uma justificação específica para prolongar a conservação dos dados⁽⁵⁾.

60. A este respeito, a Proposta deve, em primeiro lugar, fixar um período máximo de conservação durante o qual a ACER e outros destinatários da informação podem manter os dados, tendo em conta a finalidade para a qual são armazenados. Salvo no caso de a suspeita de abuso de mercado conduzir a uma investigação específica e a investigação estar ainda em curso, todos os dados pessoais relacionados com a suspeita de abuso de mercado comunicada devem ser eliminados dos registos de todos os

⁽³⁾ A AEVMM é uma autoridade independente da UE que contribui para salvaguardar a estabilidade do sistema financeiro da União Europeia através da garantia da integridade, da transparência, da eficiência e do bom funcionamento dos mercados de valores mobiliários, assim como do reforço da protecção dos investidores.

⁽⁴⁾ Ver artigo 6.º, n.º 1, alínea b), da Directiva 95/46/CE e artigo 4.º, n.º 1, alínea b), do Regulamento (CE) n.º 45/2001.

⁽⁵⁾ A título ilustrativo, a AEPD menciona neste contexto a decisão do Tribunal Europeu dos Direitos do Homem no processo *S. e Marper contra Reino Unido* (2008) (4 de Dezembro de 2008) (requerimentos n.º 30562/04 e n.º 30566/04), segundo a qual a conservação de dados de pessoas não condenadas por uma infracção penal por longos períodos constitui uma violação do direito à vida privada nos termos do artigo 8.º da Convenção Europeia dos Direitos do Homem.

destinatários findo um determinado período. A não ser que se justifique inequivocamente um período de conservação mais alargado, a AEPD considera que a eliminação deve ocorrer, no máximo, dois anos após a data de comunicação da suspeita ⁽¹⁾.

61. Caso a suspeita se revele infundada e/ou um inquérito seja encerrado sem conduzir a mais acções, a Proposta deve obrigar a entidade reguladora que efectuou a comunicação, a ACER e quaisquer terceiros com acesso à informação relativa à suspeita de abuso de mercado a informarem rapidamente esses intervenientes, para que possam actualizar os respectivos registos em conformidade (e/ou eliminar a informação relativa à suspeita comunicada com efeitos imediatos ou findo um prazo de conservação proporcional, conforme for adequado) ⁽²⁾.
62. Estas disposições deverão contribuir para assegurar que, nos casos em que a suspeita não se confirme (ou não seja sequer alvo de um inquérito) ou se conclua pela sua falta de fundamentação, as pessoas inocentes não permaneçam numa «lista negra» e «sob suspeita» por um período excessivamente prolongado [ver o artigo 6.º, alínea e), da Directiva 95/46/CE e o correspondente artigo 4.º, alínea e), do Regulamento (CE) n.º 45/2001].

II.7. Transmissões de dados para países terceiros (artigo 14.º)

Disposições pertinentes

63. Os artigos 7.º, 8.º e 11.º da proposta de regulamento prevêem o intercâmbio de dados e informações entre a ACER, a AEVMM e as autoridades dos Estados-Membros. O artigo 14.º («Relações com países terceiros») estabelece que a ACER «pode ainda celebrar acordos de carácter administrativo com organizações internacionais e com as administrações de países terceiros». Destes acordos pode resultar a transmissão de dados pessoais da ACER e, eventualmente, da ESMA e/ou das autoridades dos Estados-Membros para organizações internacionais e autoridades de países terceiros.

Observações e recomendações da AEPD

64. A AEPD recomenda que o artigo 14.º da Proposta clarifique que as transmissões de dados pessoais apenas podem ser efectuadas em conformidade com o artigo 9.º do Regulamento (CE) n.º 45/2001 e com os artigos 25.º e 26.º da Directiva 95/46/CE. Em particular, as transmissões internacionais apenas deverão realizar-se se o país terceiro em causa assegurar um nível adequado de protecção. Caso tenham como destinatários entidades ou pessoas num país terceiro que não proporcione protecção adequada, as transmissões internacionais apenas deverão realizar-se se o controlador aduzir salvaguardas adequadas no que respeita à

protecção da vida privada e dos direitos fundamentais e liberdades das pessoas, assim como ao exercício dos correspondentes direitos.

65. A AEPD salienta que as derrogações [como as que são mencionadas no artigo 9.º, n.º 6, do Regulamento (CE) n.º 45/2001 e no artigo 26.º, n.º 1, da directiva] não devem, em princípio, ser utilizadas para justificar transmissões de dados em massa, sistemáticas e/ou estruturais para países terceiros.

II.8. Controlo prévio das actividades de coordenação da ACER no que se refere às investigações

66. É provável que alguns dados partilhados entre a ACER, a AEVMM e várias autoridades nos Estados-Membros relativas a suspeitas de infracção contenham dados pessoais, como a identidade dos suspeitos ou de outras pessoas envolvidas (por exemplo, testemunhas, autores de denúncias, funcionários e outras pessoas que agiram em nome das empresas envolvidas na negociação).
67. O artigo 27.º, n.º 1, do Regulamento (CE) n.º 45/2001 estabelece que «as operações de tratamento que possam apresentar riscos específicos para os direitos e liberdades das pessoas em causa, devido à sua natureza, âmbito ou finalidade, são sujeitas a controlo prévio pela Autoridade Europeia para a protecção de dados». O artigo 27.º, n.º 2, confirma especificamente que o tratamento de dados relativos a suspeitas e infracções está sujeito a controlo prévio. Tendo em consideração a função prevista para a ACER a nível da coordenação das investigações, é provável que venha a tratar dados relacionados com «suspeitas» e, por conseguinte, as suas actividades estarão sujeitas a controlo prévio ⁽³⁾.
68. No quadro de um procedimento de controlo prévio, a AEPD pode facultar à ACER mais orientações e recomendações específicas no que se refere ao cumprimento das regras de protecção de dados. As actividades de controlo prévio da ACER poderão ter outras vantagens, tendo em conta que o Regulamento (CE) n.º 713/2009, que institui a ACER, não inclui referências à protecção de dados pessoais e não esteve sujeito a um parecer legislativo da AEPD.

III. CONCLUSÕES

69. A Proposta deve clarificar se podem ser tratados dados pessoais no contexto da monitorização do mercado e da comunicação, bem como as salvaguardas eventualmente aplicáveis. Se, pelo contrário, não estiver previsto o tratamento de dados pessoais (ou esse tratamento assumir um carácter excepcional e estiver limitado a casos pontuais, em que um negociante de produtos energéticos grossistas possa ser uma pessoa singular e não uma entidade jurídica), esse facto deve estar explícito na Proposta, no mínimo, num considerando.

⁽¹⁾ Se a suspeita se revelar fundamentada e der origem a uma investigação, a Proposta deve estabelecer um período de conservação específico — não excessivo — após o encerramento do inquérito.

⁽²⁾ Esta informação também deve ser facultada à pessoa em causa.

⁽³⁾ Importa salientar que o tratamento de dados realizado pelas autoridades nacionais pode também estar sujeito a controlo prévio pelas respectivas autoridades nacionais ou regionais de protecção de dados, ao abrigo das legislações nacionais de protecção de dados adoptadas nos termos do artigo 20.º da Directiva 95/46/CE.

70. As disposições relativas à protecção de dados, segurança dos dados e responsabilização devem ser clarificadas e reforçadas, em especial se o tratamento de dados pessoais desempenhar uma função mais estrutural. A Comissão deve assegurar a existência dos controlos adequados, para assegurar a conformidade com as normas de protecção de dados e demonstrar o seu cumprimento («responsabilização»).
71. A Comissão deve clarificar se as inspecções *in loco* se limitariam a propriedades comerciais (instalações, terrenos e veículos) de um participante no mercado ou se também seriam extensíveis à propriedade privada (instalações, terrenos e veículos) de pessoas singulares. Neste último caso, a necessidade e a proporcionalidade deste poder devem ser justificadas de uma forma inequívoca, devendo ser exigido um mandado judicial e salvaguardas adicionais. Estas condições devem estar claramente previstas na proposta de regulamento.
72. Deve ser clarificado o âmbito dos poderes para exigir a comunicação de «registos telefónicos e de transmissão de dados existentes». A Proposta deve especificar de uma forma clara os registos que podem ser exigidos e a quem podem ser exigidos. O facto de não poder ser ordenada a fornecedores de serviços de comunicações electrónicas acessíveis ao público a comunicação de dados deve ser explicitamente mencionada no texto da proposta de regulamento, pelo menos num considerando. A Proposta deve também clarificar se as entidades reguladoras podem ordenar a comunicação de registos privados de pessoas, como os funcionários ou executivos do participante no mercado sob investigação (por exemplo, mensagens de texto enviadas de dispositivos móveis pessoais ou o histórico de navegação na Internet em casa). Neste último caso, a necessidade e a proporcionalidade deste poder devem ser justificadas de uma forma inequívoca, devendo a Proposta exigir também um mandado judicial.
73. No que se refere à comunicação de suspeitas de abuso de mercado, a Proposta deve estipular explicitamente que quaisquer dados pessoais contidos nessas comunicações devem ser utilizados apenas para efeitos da investigação da suspeita de abuso de mercado comunicada. Salvo no caso de a suspeita de abuso de mercado conduzir a uma investigação específica e a investigação estar ainda em curso (ou se a suspeita se revelar fundamentada e der origem a uma investigação), todos os dados pessoais relacionados com a suspeita de abuso de mercado comunicada devem ser eliminados dos registos de todos os destinatários findo um determinado período (salvo casos devidamente justificados, no máximo, dois anos após a data de comunicação da suspeita). Além disso, as partes envolvidas numa troca de informações devem também informar-se mutuamente, caso a suspeita se revele infundada e/ou um inquérito seja encerrado sem conduzir a mais acções.
74. No que se refere a transmissões de dados para países terceiros, a Proposta deve clarificar que, em princípio, apenas deverão ser transmitidos dados a entidades ou pessoas num país terceiro que não proporcione protecção adequada se o controlador aduzir salvaguardas adequadas no que respeita à protecção da vida privada e dos direitos fundamentais e liberdades das pessoas, assim como ao exercício dos correspondentes direitos.
75. A ACER deve apresentar à AEPD, para controlo prévio, as suas actividades de tratamento de dados pessoais no âmbito da coordenação de investigações ao abrigo do artigo 11.º da proposta de regulamento.

Feito em Bruxelas, em 21 de Junho de 2011.

Giovanni BUTTARELLI

Autoridade Adjunta Europeia para a Protecção de Dados

II

(Comunicações)

COMUNICAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

COMISSÃO EUROPEIA

Não oposição a uma concentração notificada**(Processo COMP/M.6349 — Motherson/Cross Industries/Peguform/Wethje)****(Texto relevante para efeitos do EEE)**

(2011/C 279/04)

Em 16 de Setembro de 2011, a Comissão decidiu não se opor à concentração notificada e declarou-a compatível com o mercado comum. Esta decisão baseia-se no n.º 1, alínea b), do artigo 6.º do Regulamento (CE) n.º 139/2004 do Conselho. O texto integral da decisão apenas está disponível na língua inglês e será tornado público após terem sido suprimidos quaisquer segredos comerciais que possa conter. Poderá ser consultado:

- no sítio *web* Concorrência da Comissão, na secção consagrada à política da concorrência, (<http://ec.europa.eu/competition/mergers/cases/>). Este sítio permite aceder às decisões respeitantes às operações de concentração a partir da denominação da empresa, do número do processo, da data e do sector de actividade,
- em formato electrónico, no sítio EUR-Lex (<http://eur-lex.europa.eu/en/index.htm>), que proporciona o acesso em linha ao direito comunitário, através do número do documento 32011M6349.

Não oposição a uma concentração notificada**(Processo COMP/M.6218 — Ineos/Tessenderlo Group S-PVC Assets)****(Texto relevante para efeitos do EEE)**

(2011/C 279/05)

Em 26 de Julho de 2011, a Comissão decidiu não se opor à concentração notificada e declarou-a compatível com o mercado comum. Esta decisão baseia-se no n.º 1, alínea b), do artigo 6.º do Regulamento (CE) n.º 139/2004 do Conselho. O texto integral da decisão apenas está disponível na língua inglês e será tornado público após terem sido suprimidos quaisquer segredos comerciais que possa conter. Poderá ser consultado:

- no sítio *web* Concorrência da Comissão, na secção consagrada à política da concorrência, (<http://ec.europa.eu/competition/mergers/cases/>). Este sítio permite aceder às decisões respeitantes às operações de concentração a partir da denominação da empresa, do número do processo, da data e do sector de actividade,
- em formato electrónico, no sítio EUR-Lex (<http://eur-lex.europa.eu/en/index.htm>), que proporciona o acesso em linha ao direito comunitário, através do número do documento 32011M6218.

IV

(Informações)

INFORMAÇÕES DAS INSTITUIÇÕES, ÓRGÃOS E ORGANISMOS DA UNIÃO EUROPEIA

COMISSÃO EUROPEIA

Taxas de câmbio do euro ⁽¹⁾

22 de Setembro de 2011

(2011/C 279/06)

1 euro =

Moeda	Taxas de câmbio	Moeda	Taxas de câmbio		
USD	dólar americano	1,3448	AUD	dólar australiano	1,3691
JPY	iene	102,59	CAD	dólar canadiano	1,3894
DKK	coroa dinamarquesa	7,4458	HKD	dólar de Hong Kong	10,4904
GBP	libra esterlina	0,87325	NZD	dólar neozelandês	1,7185
SEK	coroa sueca	9,2762	SGD	dólar de Singapura	1,7547
CHF	franco suíço	1,2275	KRW	won sul-coreano	1 605,66
ISK	coroa islandesa		ZAR	rand	11,0754
NOK	coroa norueguesa	7,8270	CNY	yuan-renminbi chinês	8,6040
BGN	lev	1,9558	HRK	kuna croata	7,4845
CZK	coroa checa	24,878	IDR	rupia indonésia	12 246,50
HUF	forint	293,06	MYR	ringgit malaio	4,2744
LTL	litas	3,4528	PHP	peso filipino	58,919
LVL	lats	0,7093	RUB	rublo russo	43,2059
PLN	zloti	4,4863	THB	baht tailandês	41,379
RON	leu	4,3055	BRL	real brasileiro	2,4887
TRY	lira turca	2,4636	MXN	peso mexicano	18,6738
			INR	rupia indiana	66,6720

⁽¹⁾ Fonte: Taxas de câmbio de referência publicadas pelo Banco Central Europeu.

V

(Avisos)

PROCEDIMENTOS ADMINISTRATIVOS

COMISSÃO EUROPEIA

MEDIA 2007 — DESENVOLVIMENTO, DISTRIBUIÇÃO, PROMOÇÃO E FORMAÇÃO

Convite à apresentação de propostas — EACEA/21/11

Apoio ao desenvolvimento de projectos de produção — Obras de ficção, documentários de criação e de filmes de animação — Projectos individuais, *slate funding* e *slate funding* 2.º estado

(2011/C 279/07)

1. Objectivos e descrição

O presente convite à apresentação de propostas tem por base a Decisão n.º 1718/2006/CE do Parlamento Europeu e do Conselho, de 15 de Novembro de 2006, que institui um programa de apoio ao sector audiovisual europeu (MEDIA 2007).

Um dos objectivos do programa consiste em promover, através da concessão de apoio financeiro, o desenvolvimento de projectos de produção destinados aos mercados europeu e internacional apresentados por companhias de produção europeias independentes nas seguintes categorias: obras de ficção, documentários de criação e filmes de animação.

2. Candidatos elegíveis

O presente convite à apresentação de propostas destina-se às empresas europeias cujas actividades contribuem para a prossecução dos objectivos supramencionados, sobretudo às companhias de produção europeias independentes.

As empresas candidatas devem estar estabelecidas num dos seguintes países:

- Os 27 países da União Europeia;
- Os países da EEE, a Suíça e a Croácia.

3. Acções elegíveis

São elegíveis as actividades de desenvolvimento das seguintes obras audiovisuais (obras isoladas ou séries):

- Obras de ficção destinadas a exploração comercial com a duração mínima de 50 minutos;
- Documentários de criação destinados a exploração comercial com a duração mínima de 25 minutos (duração de cada episódio no caso de uma série);
- Filmes de animação destinados a exploração comercial com a duração mínima de 24 minutos.

Não são elegíveis as actividades de desenvolvimento e produção das seguintes categorias de obras:

- Programas gravados ao vivo, jogos televisivos, *talk shows*, *reality shows*, programas escolares, didácticos e de aprendizagem;
- Documentários de promoção do turismo, *making-of*, reportagens, programas sobre animais, programas noticiosos e *docu-soaps*;
- Projectos que promovem directa ou indirectamente mensagens que contrariam as políticas da União Europeia. Por exemplo, projectos contrários aos interesses de saúde pública (álcool, tabaco, drogas), respeito pelos direitos humanos, segurança das pessoas, liberdade de expressão, etc.;
- Projectos que fazem a apologia da violência e/ou do racismo e/ou com conteúdo pornográfico;
- Obras de natureza publicitária;
- Produções institucionais destinadas a promover uma determinada organização ou as suas actividades.

O convite à apresentação de propostas 21/11 tem dois prazos-limite. Para ser incluída no 1.º prazo-limite, a candidatura deve ser enviada à Agência entre a data da publicação do convite à apresentação de propostas e 25 de Novembro de 2011. Para ser incluída no 2.º prazo-limite, a candidatura deve ser enviada à Agência entre 26 de Novembro de 2011 e 13 de Abril de 2012, a data de encerramento do convite à apresentação de propostas.

O projecto deverá estar concluído, no máximo, até 30 de Junho de 2014 relativamente às candidaturas apresentadas dentro do 1.º prazo-limite e até 30 de Novembro de 2014 relativamente às candidaturas apresentadas dentro do 2.º prazo-limite ou, se anterior, até à data em que o projecto entrar em produção.

4. Critérios de atribuição

A ponderação dos critérios de atribuição (total de 100 pontos) é a seguinte:

Para projectos individuais

- Critérios relativos à empresa candidata (40 pontos):
 - qualidade da estratégia de desenvolvimento (10),
 - coerência do orçamento de desenvolvimento (10),
 - qualidade da estratégia de financiamento (10),
 - qualidade da estratégia de distribuição (10);
- Critérios relativos ao projecto apresentado (60 pontos):
 - qualidade do projecto (40),
 - potencial de produção e viabilidade do projecto (10),
 - potencial de distribuição europeia e internacional (10).

Para slate funding e slate funding 2.º estado

- Critérios relativos à empresa candidata (60 pontos):
 - capacidade de desenvolvimento e produção da empresa a nível europeu (15 pontos para *slate funding*; 30 pontos para *slate funding* 2.º estado),
 - qualidade da estratégia de desenvolvimento e coerência do orçamento de desenvolvimento (15 pontos para *slate funding*; 10 pontos para *slate funding* 2.º estado),

- qualidade da estratégia de financiamento (15 pontos para *slate funding*; 10 pontos para *slate funding* 2.º estado),
- qualidade da estratégia de distribuição (15 pontos para *slate funding*; 10 pontos para *slate funding* 2.º estado),
- Critérios relativos aos projectos apresentados (40 pontos):
 - qualidade dos projectos (10),
 - potencial da equipa criativa (10),
 - potencial de produção e viabilidade do projecto (10),
 - potencial de distribuição europeia e internacional (10).

5. Orçamento

O orçamento total disponível ascende a 17 milhões de EUR. O apoio financeiro é concedido sob a forma de uma subvenção.

O apoio financeiro máximo para projectos individuais varia entre 10 000 EUR e 60 000 EUR, salvo no que respeita a longas-metragens de animação destinadas a exibição em salas de cinema, para as quais o limite máximo é de 80 000 EUR. O apoio financeiro concedido não poderá ultrapassar, em caso algum, 50 % das despesas elegíveis apresentadas pelo produtor (60 % para projectos susceptíveis de contribuírem para a valorização da diversidade cultural europeia).

O apoio financeiro máximo para *slate funding* e *slate funding* 2.º estado varia entre 70 000 EUR e 190 000 EUR. O apoio financeiro concedido não poderá ultrapassar, em caso algum, 50 % das despesas elegíveis apresentadas pelo produtor.

A Agência reserva-se o direito de não conceder a totalidade dos fundos disponíveis

6. Prazo-limite para a apresentação de candidaturas

As candidaturas deverão ser submetidas à EACEA usando os formulários de candidatura em linha e, em simultâneo, enviando o dossiê de candidatura em papel antes de **25 de Novembro de 2011 e 13 de Abril de 2012** (ver ponto 3) para o seguinte endereço:

Agência de Execução relativa à Educação, ao Audiovisual e à Cultura (EACEA) — MEDIA
Constantin DASKALAKIS
BOUR 3/30
Avenue du Bourget/Bourgetlaan 1
1140 Bruxelles/Brussel
BELGIQUE/BELGIË

Apenas serão aceites as candidaturas apresentadas nos formulários oficiais, devidamente assinadas pela pessoa autorizada a assumir compromissos juridicamente vinculativos em nome do organismo candidato.

As candidaturas enviadas por fax ou correio electrónico não serão aceites.

7. Informações complementares

O texto integral das directrizes, bem como os formulários de candidatura, encontram-se na seguinte página Internet: <http://www.ec.europa.eu/media>

As candidaturas devem cumprir todas as disposições das directrizes e a sua apresentação deve ser efectuada através dos formulários previstos para o efeito.

MEDIA 2007 — DESENVOLVIMENTO, DISTRIBUIÇÃO, PROMOÇÃO E FORMAÇÃO**Convite à apresentação de propostas — EACEA/22/11****Apoio ao desenvolvimento de obras interactivas *online* e *offline***

(2011/C 279/08)

1. Objectivos e descrição

O presente convite à apresentação de propostas tem por base a Decisão n.º 1718/2006/CE do Parlamento Europeu e do Conselho, de 15 de Novembro de 2006, que institui um programa de apoio ao sector audiovisual europeu (MEDIA 2007).

Um dos objectivos do programa consiste em promover, através do fornecimento de apoio financeiro, o desenvolvimento de projectos de produção destinados aos mercados europeu e internacional apresentados por empresas de produção independente.

2. Candidatos elegíveis

O presente aviso dirige-se às companhias europeias cujas actividades contribuem para a realização dos objectivos referidos *supra*, nomeadamente as companhias independentes de produção.

Os candidatos deverão estar estabelecidos num dos países seguintes:

- Os 27 Estados-Membros da União Europeia;
- Os países da EEE, a Suíça e a Croácia.

3. Acções elegíveis

São elegíveis as actividades das seguintes obras interactivas:

Desenvolvimento do conceito (até à primeira aplicação executável) do conteúdo digital interactivo complementar de um projecto audiovisual (obra de ficção, documentário de criação ou filme de animação), especificamente desenvolvido para, pelo menos, uma das plataformas seguintes:

- Internet;
- PC;
- Consola;
- Dispositivo portátil;
- Televisão interactiva.

Este conteúdo digital deverá possuir as seguintes características:

- Um nível substancial de interactividade com uma componente narrativa;
- Originalidade, criatividade e inovação, por comparação com trabalhos já existentes;
- Potencial comercial à escala europeia.

O trabalho interactivo apresentado poderá apenas complementar os seguintes tipos de projectos audiovisuais destinados a exploração comercial:

- Obra de ficção com, pelo menos, 50 minutos (no caso de uma série, duração total da série);

- Documentário de criação com, pelo menos, 25 minutos (no caso de uma série, duração por episódio);
- Filme de animação com, pelo menos, 24 minutos (no caso de uma série, duração total da série).

Não são elegíveis as seguintes actividades:

Não são elegíveis as actividades de desenvolvimento e produção das seguintes categorias:

- Obras de referência (enciclopédias, atlas, catálogos, bases de dados ...);
- Obras explicativas (programas educativos, manuais ...);
- Ferramentas e serviços relativos ao *software*;
- Serviços de informação ou meramente transaccionais;
- Programas e revistas de informação;
- Projectos de promoção do turismo;
- Projectos artísticos multimédia;
- Sítios Internet que sejam ou estejam especificamente dedicados a plataformas sociais, *networking* social, fóruns na Internet, blogs ou actividades similares;
- Projectos que promovem directa ou indirectamente mensagens que contrariam as políticas da União Europeia. Por exemplo, todos os projectos contrários aos interesses de saúde pública (álcool, tabaco, drogas), respeito pelos direitos humanos, segurança das pessoas, liberdade de expressão, etc., são interditos;
- Projectos que fazem apologia da violência e/ou do racismo e/ou com conteúdo pornográfico;
- Obras de natureza publicitária (em particular quando o conteúdo é dedicado a uma marca);
- Produções institucionais destinadas a promover uma determinada organização ou as suas actividades.

O convite à apresentação de propostas 22/11 tem dois prazos-limite. Para ser incluída no 1.º prazo-limite, a candidatura deve ser enviada à Agência entre a data da publicação do convite à apresentação de propostas e 25 de Novembro de 2011. Para ser incluída no 2.º prazo-limite, a candidatura deve ser enviada à Agência entre 26 de Novembro 2011 e 13 de Abril de 2012, a data de encerramento do convite à apresentação de propostas.

O projecto deverá estar concluído, no máximo, até 30 de Junho de 2014 relativamente às candidaturas apresentadas dentro do 1.º prazo-limite e até 30 de Novembro de 2014 relativamente às candidaturas apresentadas dentro do 2.º prazo-limite ou, se anterior, até à data em que o projecto entrar em produção.

4. Critérios de adjudicação

Serão atribuídos pontos, num máximo de 100, com base na seguinte ponderação:

- Critérios relativos à empresa candidata (40 pontos):
 - qualidade da estratégia de desenvolvimento (10),

- coerência do orçamento de desenvolvimento (10),
- capacidade da empresa para realizar o projecto (10),
- qualidade da estratégia de financiamento (10);
- Critérios relativos ao projecto apresentado (60 pontos):
 - qualidade do conteúdo e originalidade do conceito em relação a obras existentes (20),
 - inovação, relevância das técnicas utilizadas no trabalho e qualidade da interactividade (20),
 - potencial para exploração à escala europeia e adequação ao público-alvo (20).

5. Orçamento

O orçamento total disponível ascende a 2,5 milhões de EUR. A contribuição financeira é atribuída na forma de um subsídio.

O apoio financeiro máximo varia entre 10 000 EUR e 150 000 EUR.

O apoio financeiro concedido não poderá ultrapassar, em caso algum, 50 % das despesas elegíveis apresentadas pelo produtor (60 % para projectos susceptíveis de contribuir para a valorização da diversidade cultural europeia).

A Agência reserva-se o direito de não conceder a totalidade dos fundos disponíveis

6. Prazo-limite para apresentação de candidaturas

As candidaturas deverão ser submetidas à EACEA usando os formulários de candidatura em linha e, em simultâneo, enviando o dossiê de candidatura em papel antes de **25 de Novembro de 2011 e 13 de Abril de 2012** (ver ponto 3) para o seguinte endereço:

Agência de Execução relativa à Educação, ao Audiovisual e à Cultura (EACEA) — MEDIA
Constantin DASKALAKIS
BOUR 3/30
Avenue du Bourget/Bourgetlaan 1
1140 Bruxelles/Brussel
BELGIQUE/BELGIË

Apenas serão aceites as candidaturas apresentadas nos formulários oficiais, devidamente assinadas pela pessoa autorizada a assumir compromissos juridicamente vinculativos em nome do organismo candidato.

As candidaturas enviadas por fax ou correio electrónico não serão aceites.

7. Informações complementares

O texto integral das directrizes, bem como os formulários de candidatura, encontram-se na seguinte página Internet:

<http://ec.europa.eu/media>

As candidaturas devem cumprir todas as disposições das directrizes e a sua apresentação deve ser efectuada através dos formulários previstos para o efeito.

PROCEDIMENTOS RELATIVOS À EXECUÇÃO DA POLÍTICA DE CONCORRÊNCIA

COMISSÃO EUROPEIA

Notificação prévia de uma concentração **(Processo COMP/M.6348 — Arla Foods/Allgäuland)**

(Texto relevante para efeitos do EEE)

(2011/C 279/09)

1. A Comissão recebeu, em 15 de Setembro de 2011, uma notificação de um projecto de concentração, nos termos do artigo 4.º do Regulamento (CE) n.º 139/2004 do Conselho ⁽¹⁾, através da qual a empresa Hansa-Milch AG («Hansa», Alemanha), pertencente a Arla Foods Amba («Arla», Dinamarca), adquire, na acepção do artigo 3.º, n.º 1, alínea b), do Regulamento das concentrações comunitárias, o controlo exclusivo das empresas Allgäuland-Käsereien GmbH e AL Dienstleistungs-GmbH (denominadas conjuntamente «Allgäuland», Alemanha), mediante aquisição de acções.

2. As actividades das empresas em causa são:

- Arla: cooperativa de lacticínios da propriedade dos produtores leiteiros. A empresa dedica-se à produção e venda de uma série de lacticínios. Na Alemanha, a maior parte da sua actividade é exercida principalmente através da sua filial Hansa,
- Allgäuland: cooperativa de lacticínios que produz uma série de queijos de qualidade, bem como outros produtos lácteos, principalmente na Alemanha.

3. Após uma análise preliminar, a Comissão considera que a operação de concentração notificada pode encontrar-se abrangida pelo âmbito de aplicação do Regulamento das concentrações comunitárias. Contudo, a Comissão reserva-se a faculdade de tomar uma decisão final sobre este ponto.

4. A Comissão solicita aos terceiros interessados que lhe apresentem as suas eventuais observações sobre o projecto de concentração em causa.

As observações devem ser recebidas pela Comissão no prazo de 10 dias após a data de publicação da presente comunicação. Podem ser enviadas por fax (+32 22964301), por correio electrónico para COMP-MERGER-REGISTRY@ec.europa.eu ou pelo correio, com a referência COMP/M.6348 — Arla Foods/Allgäuland, para o seguinte endereço:

Comissão Europeia
Direcção-Geral da Concorrência
Registo das Concentrações
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ JO L 24 de 29.1.2004, p. 1 («Regulamento das concentrações comunitárias»).

Notificação prévia de uma concentração**(Processo COMP/M.6392 — Gores/Mexx)****Processo susceptível de beneficiar do procedimento simplificado****(Texto relevante para efeitos do EEE)**

(2011/C 279/10)

1. A Comissão recebeu, em 15 de Setembro de 2011, uma notificação de um projecto de concentração, nos termos do artigo 4.º do Regulamento (CE) n.º 139/2004 do Conselho ⁽¹⁾, através da qual o Gores Group LLC («Gores», EUA) adquire, na aceção do artigo 3.º, n.º 1, alínea b), do Regulamento das concentrações comunitárias, o controlo exclusivo de Mexx European Holding BV («Mexx», Países Baixos), mediante aquisição de acções.

2. As actividades das empresas em causa são:

— Gores: aplicações de capitais de investimento (private equity) nos sectores das tecnologias, telecomunicações, serviços às empresas, da indústria e do vestuário, principalmente nos Estados Unidos e na Europa Ocidental,

— Mexx: venda a retalho de vestuário, calçado e acessórios e venda por grosso de vestuário e calçado na Europa e América do Norte.

3. Após uma análise preliminar, a Comissão considera que a operação de concentração notificada pode encontrar-se abrangida pelo âmbito de aplicação do Regulamento das concentrações comunitárias. Contudo, a Comissão reserva-se a faculdade de tomar uma decisão final sobre este ponto. De acordo com a Comunicação da Comissão relativa a um procedimento simplificado de tratamento de certas operações de concentração nos termos do Regulamento das concentrações comunitárias ⁽²⁾, o referido processo é susceptível de beneficiar da aplicação do procedimento previsto na Comunicação.

4. A Comissão solicita aos terceiros interessados que lhe apresentem as suas eventuais observações sobre o projecto de concentração em causa.

As observações devem ser recebidas pela Comissão no prazo de 10 dias após a data de publicação da presente comunicação. Podem ser enviadas por fax (+32 22964301), por correio electrónico para COMP-MERGER-REGISTRY@ec.europa.eu ou por via postal, com a referência COMP/M.6392 — Gores/Mexx, para o seguinte endereço:

Comissão Europeia
Direcção-Geral da Concorrência
Registo das Concentrações
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ JO L 24 de 29.1.2004, p. 1 («Regulamento das concentrações comunitárias»).

⁽²⁾ JO C 56 de 5.3.2005, p. 32 («Comunicação relativa ao procedimento simplificado»).

Preço das assinaturas 2011 (sem IVA, portes para expedição normal incluídos)

Jornal Oficial da União Europeia, séries L + C, só edição impressa	22 línguas oficiais da UE	1 100 EUR por ano
Jornal Oficial da União Europeia, séries L + C, edição impressa + DVD 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	770 EUR por ano
Jornal Oficial da União Europeia, séries L + C, DVD mensal (cumulativo)	22 línguas oficiais da UE	400 EUR por ano
Suplemento do Jornal Oficial (série S), Adjudicações e Contratos Públicos, DVD, uma edição por semana	Multilingue: 23 línguas oficiais da UE	300 EUR por ano
Jornal Oficial da União Europeia, série C — Concursos	Língua(s) de acordo com o concurso	50 EUR por ano

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 DVD 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 subscrições de diversas publicações periódicas pagas, como a subscrição do *Jornal Oficial da União Europeia*, 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>

