

I

(Resoluções, recomendações e pareceres)

PARECERES

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Parecer da Autoridade Europeia para a Proteção de Dados sobre as propostas da Comissão de um Regulamento do Parlamento Europeu e do Conselho relativo ao abuso de informação privilegiada e à manipulação de mercado e para de uma Diretiva do Parlamento Europeu e do Conselho relativa às sanções penais aplicáveis ao abuso de informação privilegiada e à manipulação de mercado

(2012/C 177/01)

A AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS,

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

Tendo em conta a Carta dos Direitos Fundamentais da União Europeia, nomeadamente os seus artigos 7.º e 8.º;

Tendo em conta a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção 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 proteção 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;

ADOTOU O SEGUINTE PARECER:

1. INTRODUÇÃO

1.1. Consulta da AEPD

1. O presente parecer faz parte de um conjunto de 4 pareceres da AEPD relativos ao setor financeiro, todos adotados no mesmo dia ⁽³⁾.
2. Em 20 de outubro de 2011, a Comissão adotou uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao abuso de informação privilegiada e à manipulação de mercado (a «proposta de Regulamento») e uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa às sanções penais aplicáveis ao abuso de informação privilegiada e à manipulação de mercado (a «proposta de Diretiva»). As propostas de Regulamento e de Diretiva (conjuntamente referidas como «as propostas») foram enviadas pela Comissão à AEPD para consulta e recebidas em 31 de outubro de 2011. Em 6 de dezembro de 2011, o Conselho e a União Europeia consultaram a AEPD sobre as propostas.

⁽¹⁾ JO L 281 de 23.11.1995, p. 31.

⁽²⁾ JO L 8 de 12.1.2001, p. 1.

⁽³⁾ Pareceres da AEPD de 10 de fevereiro de 2012 sobre o pacote legislativo relativo à revisão da legislação bancária, às agências de notação de risco, aos mercados de instrumentos financeiros (MiFID/MiFIR — Diretiva relativa aos mercados de instrumentos financeiros/proposta de regulamento relativo aos mercados de instrumentos financeiros) e ao abuso de mercado.

3. A AEPD foi informalmente consultada antes da adoção da proposta de Regulamento. A AEPD observa que várias das suas observações foram tidas em consideração na proposta.
4. A AEPD congratula-se com o facto de ter sido consultada pela Comissão e pelo Conselho.

1.2. Objetivos e âmbito de aplicação das propostas

5. Adotada em inícios de 2003, a Diretiva relativa ao abuso de mercado («DAM») ⁽¹⁾, introduziu um quadro jurídico comum na UE para prevenir, detetar e sancionar o abuso de informação privilegiada e a manipulação de mercado.
6. Após vários anos em vigor, a Comissão avaliou a aplicação da Diretiva DAM e identificou uma série de problemas como, por exemplo lacunas na regulamentação de certos instrumentos e mercados, aplicação efetiva insuficiente (os reguladores não possuem determinadas informações ou competências e as sanções não existem ou não são suficientemente dissuasoras), a falta de clareza de determinados conceitos fundamentais e encargos administrativos dos emitentes.
7. Tendo em conta estes problemas e as mudanças significativas introduzidas no panorama financeiro através das evoluções registadas a nível da legislação, dos mercados e da tecnologia, a Comissão adotou as propostas legislativas para a reformulação da Diretiva relativa ao abuso de mercado, que consistem na proposta de Regulamento e na proposta de Diretiva. Os objetivos políticos da proposta de revisão visam aumentar a confiança dos investidores e a integridade do mercado e acompanhar a evolução do setor financeiro.
8. A proposta de Regulamento, em especial, alarga o âmbito de aplicação do quadro em matéria de abuso de mercado, classifica as tentativas de manipulação do mercado e de abuso de informação privilegiada como infrações específicas, reforça os poderes de investigação das autoridades competentes e introduz regras mínimas aplicáveis a medidas, sanções e coimas administrativas.
9. A proposta de Diretiva exige que os Estados-Membros introduzam sanções penais para o abuso de informação privilegiada e a manipulação de mercado cometidos intencionalmente e para a instigação, o auxílio e a cumplicidade na prática de qualquer uma das infrações ou para a tentativa de cometer essas infrações. Alarga igualmente a responsabilidade às pessoas coletivas, incluindo, sempre que possível, a responsabilidade penal das pessoas coletivas.

1.3. Objetivo do parecer da AEPD

10. Várias das medidas previstas nas propostas para aumentar a integridade do mercado e a proteção dos investidores têm impacto nos direitos das pessoas singulares relacionados com o tratamento dos seus dados pessoais.
11. Em especial, quando as autoridades competentes investigam ou cooperam a fim de detetar, comunicar e/ou sancionar situações de abuso de informação privilegiada ou abuso de mercado, os dados pessoais são recolhidos, processados e partilhados. Além disso, o mecanismo para encorajar as pessoas a comunicar infrações envolve igualmente o tratamento de dados pessoais, quer da pessoa que denuncia as infrações, quer da pessoa «acusada». Por último, o regime de sanções afeta o direito à proteção dos dados pessoais, uma vez que, nos termos da proposta de Regulamento, as sanções que mencionam a identidade da pessoa responsável pela infração serão publicadas.
12. Embora a proposta de Regulamento contenha várias disposições que podem afetar o direito à proteção dos dados pessoais das pessoas singulares, a proposta de Diretiva não envolve, em si mesma, o tratamento de dados pessoais. O presente parecer incidirá, por conseguinte, na proposta de Regulamento, nomeadamente nas seguintes questões: 1. a aplicabilidade da legislação relativa à proteção de dados; 2. as listas de iniciados; 3. os poderes das autoridades competentes; 4. os sistemas atuais de deteção e comunicação de operações suspeitas; 5. o intercâmbio de informações com os países terceiros; 6. a publicação de sanções e a comunicação de violações.

⁽¹⁾ Diretiva 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.

2. ANÁLISE DAS PROPOSTAS

2.1. Aplicabilidade da legislação relativa à proteção de dados

13. Os considerandos ⁽¹⁾ e as disposições ⁽²⁾ da proposta de Regulamento mencionam a Carta dos Direitos Fundamentais, a Diretiva 95/46/CE e o Regulamento (CE) n.º 45/2001. Em especial, o artigo 22.º da proposta de Regulamento prevê explicitamente como regra geral que «no que respeita ao tratamento de dados pessoais efetuado pelos Estados-Membros no quadro do presente regulamento, as autoridades competentes aplicam o disposto na Diretiva 95/46/CE. No que respeita ao tratamento de dados pessoais efetuado pela AEVMM no quadro do presente regulamento, a AEVMM cumpre o disposto no Regulamento (CE) n.º 45/2001». Além disso, a disposição prevê um período de conservação máximo de 5 anos para os dados pessoais.
14. A AEPD acolhe muito favoravelmente a disposição geral e congratula-se pela atenção especial dada à legislação relativa à proteção de dados na proposta de Regulamento. No entanto, a AEPD sugere que a disposição deve ser reformulada com ênfase na aplicabilidade da legislação relativa à proteção de dados existente. Também a referência à Diretiva 95/46/CE deve ser clarificada, especificando que as disposições serão aplicáveis de acordo com as regras nacionais que executam a Diretiva 95/46/CE. A AEPD observa que algumas disposições da proposta de Regulamento referem explicitamente a Diretiva 95/46/CE e/ou o Regulamento (CE) n.º 45/2001. Estas referências sublinham a aplicação das regras relativas à proteção de dados pertinentes em casos específicos, mas tal não significa que as regras não são aplicáveis quando não são explicitamente mencionadas em cada disposição que envolva (potencialmente) o tratamento de dados pessoais.
15. Tal como o considerando 33, outros considerandos devem utilizar de forma consistente a expressão «os Estados-Membros *shall* (devem)» e não «os Estados-Membros *should* (deveriam)» no que se refere à legislação relativa à proteção de dados pertinente, uma vez que esta está em vigor e a sua aplicabilidade é obrigatória.

2.2. Listas de iniciados

16. A proposta de Regulamento obriga os emitentes de um instrumento financeiro ou os participantes no mercado das licenças de emissão a «elaborar uma lista das pessoas que para eles trabalham, ao abrigo de um contrato ou de outra forma, e que têm acesso a informação privilegiada» (artigo 13.º, n.º 1). «Os emitentes de um instrumento financeiro, cujos instrumentos financeiros são admitidos à negociação num mercado de PME em crescimento estão isentos» dessa obrigação, a menos que «tal lhes seja solicitado pelas autoridades competentes» (artigo 13.º, n.º 2).
17. A AEPD reconhece a necessidade dessa lista como um instrumento importante para as autoridades competentes investigarem eventuais situações de abuso de informação privilegiada ou abuso de mercado. Todavia, uma vez que estas listas envolvem o tratamento de dados pessoais, as principais regras e garantias em matéria de proteção de dados devem ser estabelecidas na legislação de base. Por conseguinte, a AEPD recomenda a introdução de uma referência explícita à finalidade dessa lista numa disposição substantiva da proposta de Regulamento. A finalidade é, de facto, um dos elementos essenciais de qualquer processo de tratamento de dados, de acordo com o artigo 6.º da Diretiva 95/46/CE.
18. Nos termos do artigo 13.º, n.º 4, da proposta de Regulamento, a Comissão deve adotar, através de atos delegados, medidas que determinam o conteúdo de uma lista (incluindo dados relativos às identidades das pessoas e aos motivos da sua inclusão numa lista de iniciados) e as condições em que essa lista será elaborada (incluindo as condições para a atualização dessa lista, o período de conservação dos dados e as responsabilidades das pessoas que dela constam). No entanto, a AEPD recomenda:
- a inclusão dos principais elementos da lista (em qualquer circunstância, os motivos da inclusão das pessoas numa lista de iniciados) na proposta de Regulamento,
 - a inclusão de uma referência à necessidade de consultar a AEPD sempre que os atos delegados digam respeito ao tratamento de dados pessoais.

2.3. Poderes das autoridades competentes

19. O artigo 17.º, n.º 2, enumera os poderes mínimos de supervisão e investigação de que dispõem as autoridades competentes para o desempenho das suas funções ao abrigo da proposta de Regulamento.

⁽¹⁾ Ver considerandos 33, 35, 39 e 40 da proposta de regulamento.

⁽²⁾ Ver artigos 17.º, n.º 4, 22.º, 23.º e 29.º, n.º 1, alínea c), da proposta de regulamento.

20. Dois destes poderes, em particular, necessitam de especial atenção devido à sua ingerência nos direitos de privacidade e proteção de dados: o poder de entrar em instalações privadas com o propósito de apreender documentos, independentemente da sua forma, e o poder de solicitar os registos telefónicos e de transmissão de dados existentes.

2.3.1. O poder de entrar em instalações privadas

21. O poder de entrar em instalações privadas com o propósito de apreender documentos, independentemente da sua forma, é altamente intrusivo e interfere com o direito à privacidade. Deve, por conseguinte, ser objeto de condições rigorosas e dotado de garantias adequadas ⁽¹⁾. O artigo 17.º, n.º 2, alínea e), exige que o acesso a instalações privadas seja sujeito a autorização prévia pelas autoridades judiciais dos Estados-Membros em causa nos termos da legislação nacional e à existência de motivos razoáveis para suspeitar que existem documentos relacionados com o objeto da inspeção que podem ser pertinentes para fazer prova de abuso de informação privilegiada ou de manipulação do mercado. A AEPD congratula-se com o facto de o texto qualificar os poderes das autoridades competentes exigindo como condições para entrar em instalações privadas a existência de suspeita razoável de que foi cometida uma infração ao disposto na proposta de Regulamento ou da Diretiva e a autorização prévia por uma autoridade judicial. No entanto, a AEPD considera que essa exigência geral de autorização judicial prévia, independentemente de esta ser exigida ou não pela legislação nacional, se justifica e é necessária tendo em conta o risco de intrusão do poder em causa.
22. O considerando 30 da proposta de Regulamento especifica os casos em que o acesso a instalações privadas é necessário, ou seja, a pessoa a quem foi dirigido um pedido de informação não lhe dá seguimento (total ou parcialmente), ou existem motivos razoáveis para crer que um pedido formulado não seria acatado, ou que os documentos ou a informação a que o pedido diz respeito seriam suprimidos, ilicitamente manipulados ou destruídos. A AEPD congratula-se com estas especificações. No entanto, considera que são necessárias garantias suplementares para assegurar a conformidade com o direito à privacidade e que estas devem ser, por conseguinte, inseridas numa disposição substantiva como condição para acesso a instalações privadas.

2.3.2. O poder de solicitar os registos telefónicos e de transmissão de dados existentes

23. O artigo 17.º, n.º 2, alínea f), dota as autoridades competentes do poder de «solicitar os registos telefónicos e de transmissão de dados existentes na posse de um operador de telecomunicações ou de uma empresa de investimento», clarificando, contudo, que esse pedido é sujeito à existência de «motivos razoáveis para suspeitar que esses registos [...] podem ser pertinentes para fazer prova de abuso de informação privilegiada ou de manipulação de mercado» nos termos da proposta de Regulamento ou da proposta de Diretiva. Esses registos não devem, contudo, incluir o «teor da comunicação com eles relacionada». Além disso, o número 3 do artigo 17.º prevê que os poderes referidos no número 2 devem ser exercidos nos termos da legislação nacional.
24. Os dados relacionados com a utilização de meios de comunicação eletrónica podem transmitir uma grande variedade de informações de carácter pessoal, como a identidade das pessoas que realizam ou recebem a chamada, a hora e a duração da chamada, a rede utilizada, a localização geográfica do utilizador no caso dos dispositivos portáteis, etc. Alguns dados relativos ao tráfego pela Internet e à utilização do correio eletrónico (por exemplo, a lista de sítios *web* visitados) podem revelar, adicionalmente, pormenores importantes do teor da comunicação. Além disso, o tratamento desses dados entra em conflito com o sigilo da correspondência. Tendo isto em conta, a Diretiva 2002/58/CE ⁽²⁾ (a «Diretiva ePrivacidade») estabeleceu o princípio de que os dados de tráfego devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação ⁽³⁾. Nos termos do artigo 15.º, n.º 1, desta Diretiva, os Estados-Membros podem incluir na legislação nacional algumas derrogações para fins concretos e legítimos, mas elas devem constituir uma medida necessária, adequada e proporcionada numa sociedade democrática para atingir esses fins ⁽⁴⁾.

⁽¹⁾ Ver, nomeadamente, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais («CEDH»), de 23 de fevereiro de *Funcke contra França*, 10828/84.

⁽²⁾ Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (JO L 201 de 31.7.2002, p. 37).

⁽³⁾ Ver artigo 6.º, n.º 1, da Diretiva 2002/58/CE (JO L 201 de 31.7.2002, p. 37).

⁽⁴⁾ Artigo 15.º, n.º 1, da Diretiva 2002/58/CE, que dispõe que tais restrições devem constituir «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 deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no artigo 13.º, n.º 1, da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número [...]».

25. A AEPD reconhece que os objetivos prosseguidos pela Comissão na proposta de Regulamento são legítimos. Compreende a necessidade de iniciativas destinadas a reforçar a supervisão dos mercados financeiros, a fim de preservar a sua solidez e proteger melhor os investidores e a economia em geral. Contudo, os poderes de investigação diretamente relacionados com os dados de tráfego, dado o seu carácter potencialmente intrusivo, devem respeitar os requisitos da necessidade e da proporcionalidade, ou seja, serem aptos a realizar o objetivo prosseguido e não irem além do que é necessário para o alcançar ⁽¹⁾. Nesta perspetiva é, portanto, fundamental que eles sejam claramente formulados no que respeita ao seu âmbito de aplicação pessoal e material, bem como às circunstâncias e condições em que podem ser utilizados. Além disso, devem prever-se garantias adequadas contra o risco de abuso.
26. Os registos telefónicos e de transmissão de dados em causa envolvem obviamente dados pessoais na aceção da Diretiva 95/46/CE, da Diretiva 2002/58/CE e do Regulamento (CE) n.º 45/2001. O considerando 31 da proposta de Regulamento refere que: «os registos de tráfego telefónico e de transmissão de dados podem estabelecer a identidade de uma pessoa responsável pela difusão de informações falsas ou enganosas, o estabelecimento de contactos entre duas pessoas numa determinada altura ou a existência de uma relação entre duas ou mais pessoas» ⁽²⁾. Por conseguinte, há que garantir que as condições de tratamento lícito e equitativo dos dados pessoais, estabelecidas nas diretivas e no regulamento, são plenamente respeitadas.

2.3.3. Exigência de uma autorização judicial prévia

27. A AEPD chama a atenção para o facto de, nos termos do disposto no artigo 17.º, n.º 3, este poder ser exercido em conformidade com a legislação nacional sem que haja uma referência explícita à autorização judicial prévia, contrariamente ao que acontece em relação ao poder de entrar em instalações privadas. A AEPD considera que se justificaria uma exigência geral de autorização judicial prévia em todos os casos, independentemente de esta ser exigida ou não pela legislação nacional, tendo em conta o risco de intrusão do poder em causa e no interesse de uma aplicação harmonizada da legislação em todos os Estados-Membros da UE. Também se deveria ter em consideração que várias leis dos Estados-Membros preveem garantias especiais em matéria de inviolabilidade do domicílio contra inspeções, buscas e apreensões desproporcionadas e não adequadamente regulamentadas, em especial quando efetuadas por instituições de natureza administrativa.
28. Além disso, a AEPD recomenda que se introduza o requisito de que as autoridades competentes solicitem os registos telefónicos e de transmissão de dados por meio de uma decisão formal, que especifique a base jurídica e a finalidade do pedido, bem como as informações exigidas, o prazo em que devem ser fornecidas e o direito de recurso da decisão para o Tribunal de Justiça por parte do destinatário.

2.3.4. Definição de registos telefónicos e de transmissão de dados

29. Não existe uma definição de «registos telefónicos e de transmissão de dados» na proposta de Regulamento. A Diretiva 2002/58/CE («ePrivacidade») apenas se refere a «dados de tráfego» e não a «registos telefónicos e de transmissão de dados». Obviamente, a definição exata destes conceitos determina o impacto que o poder de investigação pode ter na proteção da vida privada e dos dados pessoais das pessoas em causa. A AEPD sugere que se utilize a terminologia já em vigor na definição de «dados de tráfego» na Diretiva 2002/58/CE.
30. O artigo 17.º, n.º 2, alínea f), refere «os registos telefónicos e de transmissão de dados existentes na posse de um operador de telecomunicações». A Diretiva ePrivacidade estabelece o princípio de que os dados de tráfego devem ser eliminados quando já não forem necessários para os fins comerciais que motivaram a sua recolha. No entanto, com base no artigo 15.º, n.º 1, da Diretiva ePrivacidade, os Estados-Membros podem estabelecer derrogações a esta obrigação para efeitos de aplicação da lei. A Diretiva relativa à conservação de dados pretende harmonizar as iniciativas dos Estados-Membros com o disposto no artigo 15.º, n.º 1, da Diretiva ePrivacidade, sempre que essas iniciativas digam respeito à conservação de dados para investigação, deteção e repressão de crimes «graves».

⁽¹⁾ Ver, por exemplo, Processos apensos C-92/09 e C-93/09, *Volker und Markus Schecke GbR (C-92/09)*, *Hartmut Eifert (C-92/09)* contra *Land Hessen*, ainda não publicado na Coletânea, ponto 74.

⁽²⁾ Ver também o considerando 12 da exposição de motivos da proposta de Regulamento.

31. A questão reside em saber se os registos telefónicos e de transmissão de dados mencionados no artigo 17.º, n.º 2, alínea f), se referem a dados disponíveis através do armazenamento de dados de tráfego e dos dados de localização regulamentados pela Diretiva ePrivacidade ou a dados suplementares exigidos pela Diretiva relativa à conservação de dados. A última opção suscitaria questões importantes uma vez que as derrogações previstas no artigo 15.º, n.º 1, da Diretiva ePrivacidade (ou seja, a investigação, deteção e repressão de infrações penais) seriam utilizadas no sentido de alargar as finalidades para que foram conservados os dados ao abrigo da Diretiva relativa à conservação de dados (ou seja, investigação, deteção e repressão de crimes «graves»). Por outras palavras, os dados conservados ao abrigo da Diretiva relativa à conservação de dados seriam, deste modo, utilizados para finalidades não previstas nessa diretiva. Esta situação seria um incentivo europeu à utilização do «vazio jurídico» que constitui uma das principais lacunas da atual Diretiva relativa à conservação de dados ⁽¹⁾.
32. Por conseguinte, a AEPD recomenda vivamente que se especifique as categorias de registos telefónicos e de transmissão de dados que as autoridades competentes podem solicitar. Esses dados devem ser adequados, pertinentes e não excessivos em relação aos fins para os quais são acedidos e tratados. Além disso, a AEPD recomenda que se limite o disposto no artigo 17.º, n.º 2, alínea f), aos dados normalmente processados («na posse de») pelos operadores de telecomunicações no âmbito da Diretiva 2002/58/CE (Diretiva ePrivacidade). Esta limitação excluiria, em princípio, o acesso a dados conservados para efeitos da Diretiva relativa à conservação de dados, uma vez que esse acesso não se destinaria a efeitos de investigação, deteção e repressão de crimes «graves» ⁽²⁾.
33. O artigo 17.º, n.º 2, alínea f), prevê o acesso a «registos telefónicos e de transmissão de dados existentes na posse de uma empresa de investimento». O texto deve especificar as categorias de registo e clarificar as empresas que são objeto da disposição. A AEPD parte do princípio que os registos coincidirão com os referidos na proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos mercados de instrumentos financeiros («a proposta MiFID»). A AEPD sublinha que formulou algumas observações sobre esta proposta, nas quais recomendou que se clarificassem também esses conceitos ⁽³⁾. Além disso, na medida em que os dados de tráfego telefónico e de transmissão de dados sejam respeitantes a conversas telefónicas ou comunicações eletrónicas referidas no artigo 16.º, n.º 7, da proposta MiFID, a AEPD recomendou que se definisse a finalidade do registo dessas comunicações e se especificasse que tipo de comunicações e que categorias de dados das comunicações serão gravados ⁽⁴⁾.
34. Por último, a AEPD congratula-se com o facto de o texto exigir como condição para o acesso aos registos a existência de suspeita razoável de que foi cometida uma infração ao disposto na proposta de Regulamento ou na proposta de Diretiva e que exclui explicitamente o acesso ao teor das comunicações pelas autoridades competentes.

2.4. Sistemas atuais de deteção e comunicação de operações suspeitas

35. O artigo 11.º, n.º 1, da proposta de Regulamento prevê que «qualquer pessoa que explore a atividade de uma plataforma de negociação adota e mantém dispositivos e procedimentos eficazes [...] destinados a prevenir e detetar o abuso de mercado». Além disso, o número 2 exige que «qualquer pessoa que, a título profissional, prepare ou execute operações sobre instrumentos financeiros deve dispor de sistemas

⁽¹⁾ Ver sobre esta matéria o parecer da AEPD de 31 de maio de 2011 sobre o relatório de avaliação da Comissão ao Conselho e ao Parlamento Europeu sobre a Diretiva relativa à conservação de dados (Diretiva 2006/24/CE), por exemplo, o número 24.

⁽²⁾ A AEPD gostaria de relembrar os problemas associados à falta de uma definição europeia de «crime grave». A AEPD sublinhou, de facto, que o relatório de avaliação da Comissão sobre a Diretiva relativa à conservação de dados demonstra que a opção de deixar a definição precisa do que constitui um «crime grave» a cargo dos Estados-Membros deu origem a uma grande variedade de finalidades para a utilização dos dados. A Comissão afirmou que «a maior parte dos Estados-Membros que já efetuou a transposição da Diretiva para a respetiva legislação autoriza o acesso e a utilização dos dados conservados para fins que vão mais além dos previstos na Diretiva, incluindo a prevenção e o combate à criminalidade em geral e a prevenção de riscos para a vida e a integridade física das pessoas». Ver sobre esta matéria o parecer da AEPD de 31 de maio de 2011 sobre o relatório de avaliação da Comissão ao Conselho e ao Parlamento Europeu sobre a Diretiva relativa à conservação de dados (Diretiva 2006/24/CE), números 24, 71 e 72.

⁽³⁾ Nos termos do artigo 71.º, n.º 2, alínea d), as autoridades competentes ao abrigo da proposta MiFID são autorizadas a «exigir a consulta dos registos telefónicos e de transmissão de dados existentes detidos por empresas de investimento sempre que exista uma suspeita razoável» de que foi cometida uma infração ao disposto na referida proposta.

⁽⁴⁾ Ver o parecer da AEPD de 10 de fevereiro de 2012 sobre uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos mercados de instrumentos financeiros, que revoga a Diretiva 2004/39/CE do Parlamento Europeu e do Conselho (reformulação) e uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos mercados de instrumentos financeiros, que altera o Regulamento (EMIR) relativo aos derivados OTC, às contrapartes centrais e aos repositórios de transações.

de deteção e comunicação de ordens e operações que possam constituir abuso de informação privilegiada, manipulação de mercado ou tentativas de manipulação de mercado ou de abuso de informação privilegiada». Em caso de suspeita, a autoridade competente deve ser notificada sem demora. A Comissão adotará as normas técnicas de regulamentação, a fim de prever os dispositivos e procedimentos mencionados no número 1 e determinar os sistemas e modelos de notificação mencionados no número 2 (artigo 11.º, n.º 3).

36. Uma vez que estes sistemas não envolverão provavelmente dados pessoais (por exemplo, monitorização de transações efetuadas por pessoas referidas na lista de iniciados), a AEPD gostaria de salientar que estas normas devem ser elaboradas de acordo com o princípio da «privacidade desde a conceção», ou seja, a integração da proteção de dados e da privacidade desde o início dos novos produtos, serviços e procedimentos que impliquem o tratamento de dados pessoais ⁽¹⁾. A AEPD recomenda ainda a inclusão de uma referência à necessidade de consultar a AEPD sempre que estas normas de regulamentação digam respeito ao tratamento de dados pessoais.

2.5. Intercâmbio de informações com países terceiros

37. A AEPD constata a referência à Diretiva 95/46/CE, nomeadamente aos artigos 25.º e 26.º, e as garantias específicas mencionadas no artigo 23.º da proposta de Regulamento relativo à divulgação de dados pessoais a países terceiros. Mais concretamente, a avaliação caso a caso, a garantia da necessidade da transferência, a obrigatoriedade de autorização expressa prévia da autoridade competente para uma nova transferência de dados para um país terceiro e deste para outro país terceiro e a existência de um nível de proteção adequado no país terceiro que recebeu os dados pessoais, constituem garantias adequadas tendo em conta os riscos envolvidos nessas transferências.

2.6. Publicação de sanções

2.6.1. Publicação obrigatória de sanções

38. O disposto no artigo 26.º, n.º 3, da proposta de Regulamento obriga os Estados-Membros a assegurar que as autoridades competentes publicam, sem demora injustificada, as medidas ou sanções administrativas impostas em virtude da violação do disposto na proposta de Regulamento, e incluem, no mínimo, informações sobre o tipo e a natureza da violação e a identidade das pessoas responsáveis, a menos que essa publicação ponha seriamente em risco a estabilidade dos mercados financeiros.
39. A publicação de sanções contribuiria para aumentar o efeito dissuasor, uma vez que os infratores existentes ou potenciais seriam desencorajados de cometer delitos a fim de evitar danos significativos à sua reputação. Aumentaria igualmente a transparência, uma vez que os operadores de mercado teriam conhecimento de que foi cometida uma infração por uma determinada pessoa. Esta obrigação é atenuada apenas nos casos em que a publicação possa provocar danos desproporcionados às partes envolvidas, caso em que as autoridades competentes devem divulgar as sanções ao abrigo do anonimato.
40. A AEPD congratula-se com a referência no considerando 35 à Carta dos Direitos Fundamentais e, em especial, ao direito à proteção dos dados pessoais aquando da adoção e publicação de sanções. Todavia, a AEPD não está convicta de que a publicação obrigatória de sanções, tal como está atualmente formulada, cumpra os requisitos da legislação relativa à proteção de dados, nos termos em que foi clarificada pelo Tribunal de Justiça no acórdão *Schecke* ⁽²⁾. Considera que o objetivo, a necessidade e a proporcionalidade da medida não ficaram suficientemente estabelecidos e que, em qualquer circunstância, devem ser previstas garantias adequadas contra os riscos para os direitos das pessoas singulares.

2.6.2. Necessidade e proporcionalidade da publicação

41. No acórdão *Schecke*, o Tribunal de Justiça anulou as disposições de um regulamento do Conselho e de um regulamento da Comissão que previam a publicação obrigatória das informações relativas aos beneficiários de fundos agrícolas, incluindo a identidade dos beneficiários e os montantes recebidos. O Tribunal decidiu que a referida publicação constituía um tratamento de dados pessoais que integra o âmbito do artigo 8.º, n.º 2, da Carta dos Direitos Fundamentais da União Europeia (a «Carta») e, por conseguinte, uma ingerência nos direitos reconhecidos pelos artigos 7.º e 8.º da Carta.

⁽¹⁾ Ver o parecer da AEPD de 14 de janeiro de 2011 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 proteção de dados pessoais na União Europeia» (JO C 181 de 22.6.2011, p. 1), n.ºs 108 a 115.

⁽²⁾ Processos apensos C-92/09 e C-93/09, *Schecke*, números 56 a 64.

42. Depois de estabelecer que «as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário», o Tribunal analisou o objetivo da publicação e a sua proporcionalidade. Concluiu que, nesse processo, nada indica que o Conselho e a Comissão tenham tomado em consideração, aquando da adoção da legislação em causa, outras formas de publicação de informações relativas aos beneficiários em causa conformes com o objetivo dessa publicação e que fossem ao mesmo tempo menos lesivas dos direitos desses beneficiários.
43. O artigo 26.º n.º 3, da proposta de Regulamento parece encerrar os mesmos vícios apontados pelo Tribunal de Justiça Europeu no acórdão *Schecke*. Importa ter em conta que, para avaliar a conformidade de uma disposição que exija a divulgação pública de informações pessoais com os requisitos relativos à proteção de dados, é essencial ter um objetivo claro e bem definido visado pela publicação de informações pessoais. Apenas com um objetivo claro e bem definido é possível avaliar se a publicação de dados pessoais envolvidos é realmente necessária e proporcionada ⁽¹⁾.
44. Após a leitura da proposta e dos documentos que a acompanham (ou seja, o relatório da avaliação de impacto), a AEPD considera que o objetivo e, conseqüentemente, a necessidade desta medida não estão claramente estabelecidos. Enquanto os considerandos da proposta são omissos quanto a estas questões, o relatório da avaliação de impacto apenas refere os impactos gerais positivos (ou seja, o efeito dissuasor no abuso de mercado, a contribuição para a proteção do investidor, a igualdade de tratamento dos emitentes, o reforço da aplicação), afirmando simplesmente que a publicação de sanções é de grande importância para melhorar a transparência e manter a confiança no mercado financeiro e que a publicação de sanções impostas contribuirá para o objetivo de dissuasão e melhora a integridade do mercado e a proteção do investidor ⁽²⁾. Esta declaração geral não parece ser suficiente para demonstrar a necessidade da medida proposta. Se o objetivo geral consiste em aumentar o efeito dissuasor, parece que a Comissão deveria ter explicado, em especial, por que é que sanções financeiras mais pesadas (ou outras sanções que não a denúncia pública dos incumpridores ou a sua humilhação) não teriam sido suficientes.
45. Além disso, o relatório de avaliação de impacto não parece ter em conta métodos menos invasivos como, por exemplo, decidir a publicação caso a caso. Mais concretamente, a última opção parece ser, *prima facie*, uma solução mais proporcionada, especialmente se se considerar que a própria publicação é já uma sanção nos termos do artigo 26.º n.º 1, alínea d), que, por conseguinte, deve ser avaliada caso a caso, tendo em consideração todas as circunstâncias pertinentes, como a gravidade da infração, o grau de responsabilidade da pessoa singular, a reincidência, os prejuízos causados a terceiros, etc ⁽³⁾.
46. O relatório da avaliação de impacto não explica as razões pelas quais a publicação caso a caso não é uma opção suficiente. Apenas menciona que a publicação das sanções impostas contribui para o objetivo de eliminar opções e faculdades sempre que possível, retirando a atual faculdade de que os Estados-Membros dispõem de não exigir essa publicação ⁽⁴⁾. A AEPD considera que a possibilidade de avaliar o caso à luz das circunstâncias específicas é uma solução mais proporcionada e, por conseguinte, a opção preferida em comparação com a publicação obrigatória em todos os casos. Deixar a decisão ao critério das autoridades competentes permitiria, por exemplo, que estas evitassem a publicação nos casos de infrações menos graves, bem como nos casos em que a infração não tenha causado prejuízos significativos ou em que a pessoa singular responsável tenha colaborado com a autoridade competente, etc. A avaliação efetuada na avaliação de impacto, por conseguinte, não dissipa as dúvidas quanto à necessidade e à proporcionalidade da medida.

2.6.3. A necessidade de garantias adequadas

47. A proposta de Regulamento deveria ter previsto garantias adequadas de modo a assegurar um equilíbrio justo entre os diferentes interesses envolvidos. Em primeiro lugar, são necessárias garantias que assegurem às pessoas acusadas o direito de impugnar judicialmente uma decisão e o princípio da

⁽¹⁾ Ver também sobre esta matéria o parecer da AEPD de 15 de abril de 2011 sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo às disposições financeiras aplicáveis ao orçamento anual da União (JO C 215 de 21.7.2011, p. 13).

⁽²⁾ Ver avaliação de impacto, p. 166.

⁽³⁾ Ou seja, em conformidade com o artigo 27.º da proposta de Regulamento que estabelece os critérios para a determinação de sanções.

⁽⁴⁾ Ver avaliação de impacto, p. 167.

presunção de inocência. Para este efeito, deveria ter sido incluída linguagem específica no texto do artigo 26.º, n.º 3, de modo a obrigar as autoridades competentes a adotar medidas adequadas no que respeita a situações em que a decisão é objeto de recurso ou eventualmente anulada por um tribunal ⁽¹⁾.

48. Em segundo lugar, a proposta de Regulamento deve assegurar que os direitos das pessoas em causa são respeitados de uma forma proativa. A AEPD congratula-se com o facto de a versão final da proposta prever a possibilidade de excluir a publicação nos casos em que esta possa causar danos desproporcionados às partes envolvidas. No entanto, uma abordagem proativa implica que as pessoas em causa sejam previamente informadas de que a decisão que as sanciona será publicada e que têm o direito de oposição nos termos do artigo 14.º da Diretiva 95/46/CE por razões preponderantes e legítimas ⁽²⁾.
49. Em terceiro lugar, embora a proposta de Regulamento não especifique o meio de informação que deve ser utilizado para a publicação, na prática, é de supor que na maioria dos Estados-Membros a publicação será feita através da Internet. As publicações na Internet suscitam questões e riscos específicos, nomeadamente no que respeita à necessidade de assegurar que a informação é mantida em linha apenas durante o tempo necessário e que não pode ser alterada ou manipulada. A utilização de motores de busca externos também implica o risco de que as informações possam ser retiradas do contexto e veiculadas através e fora da *web* de formas que não possam ser facilmente controladas ⁽³⁾.
50. Tendo em conta o acima exposto, é necessário obrigar os Estados-Membros a garantir que os dados das pessoas em causa são mantidos em linha apenas durante um período razoável de tempo, após o qual serão sistematicamente eliminados ⁽⁴⁾. Além disso, os Estados-Membros devem ser obrigados a garantir a aplicação de garantias e medidas de segurança adequadas, nomeadamente para proteger contra os riscos relacionados com a utilização de motores de busca externos ⁽⁵⁾.

2.6.4. Conclusão

51. A AEPD considera que a disposição sobre a publicação obrigatória de sanções, tal como está atualmente formulada, não respeita o direito fundamental da proteção da vida privada e dos dados pessoais. O legislador deve avaliar cuidadosamente a necessidade do sistema proposto e verificar se a obrigação de publicação não excede o necessário para alcançar o objetivo de interesse público previsto e se não existem medidas menos restritivas para alcançar o mesmo objetivo. Sob reserva do resultado desta verificação de proporcionalidade, a obrigação de publicação deve, em qualquer circunstância, ser apoiada por garantias adequadas que assegurem o respeito pelo princípio da presunção de inocência, o direito de oposição da pessoa em causa, a segurança/exatidão dos dados e a sua eliminação após um período de tempo adequado.

2.7. Comunicação das infrações

52. O artigo 29.º da proposta de Regulamento exige que os Estados-Membros criem mecanismos de comunicação de infrações eficazes, também conhecidos como sistemas de denúncia de infrações. Embora possam ser instrumentos eficazes para garantir a conformidade, estes sistemas suscitam questões importantes do ponto de vista da proteção de dados ⁽⁶⁾.

⁽¹⁾ Por exemplo, as medidas seguintes poderiam ter sido consideradas pelas autoridades nacionais: prorrogar a publicação até ser conhecida a decisão sobre o recurso ou, como sugerido no relatório da avaliação de impacto, indicar claramente que a decisão ainda é objeto de recurso e que a pessoa deve ser presumida inocente até que a decisão se torne definitiva ou publicar uma retificação nos casos em que a decisão é anulada por um tribunal.

⁽²⁾ Ver o parecer da AEPD de 10 de abril de 2007 sobre o financiamento da Política Agrícola Comum (JO C 134 de 16.6.2007, p. 1).

⁽³⁾ Ver o documento sobre esta matéria publicado pela autoridade de proteção de dados italiana *Personal Data As Also Contained in Records and Documents by Public Administrative Bodies: Guidelines for Their Processing by Public Bodies in Connection with Web-Based Communication and Dissemination* (Dados pessoais contidos em registos e documentos administrativos de organismos públicos: orientações para o seu tratamento por organismos públicos no que respeita à comunicação e à divulgação na *web*), disponível no sítio *web* da autoridade de proteção de dados italiana, <http://www.garanteprivacy.it/garante/doc.jsp?ID=1803707>

⁽⁴⁾ Estas questões estão também relacionadas com «o direito a ser esquecido», de âmbito mais geral, e cuja inclusão no novo quadro legislativo para a proteção de dados pessoais está em discussão.

⁽⁵⁾ Estas medidas e garantias poderiam consistir, por exemplo, na exclusão da indexação de dados através de motores de busca externos.

⁽⁶⁾ O Grupo de Trabalho do artigo 29.º publicou, em 2006, um parecer sobre os sistemas que tratam dos aspetos relacionados com a proteção de dados deste fenómeno: Parecer 1/2006 sobre a aplicação das regras europeias em matéria de proteção de dados aos sistemas internos de denúncia de infrações nos domínios da contabilidade, dos controlos contabilísticos internos, da auditoria, da luta contra a corrupção e do crime bancário e financeiro (Parecer WP sobre denúncia de infrações). O parecer pode ser consultado na página *web* do Grupo de Trabalho do artigo 29.º: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_pt.htm

53. A AEPD congratula-se com o facto de a proposta de Regulamento conter garantias específicas, que devem ser ainda desenvolvidas a nível nacional, relativamente à proteção das pessoas que comunicam a infração suspeita e, no sentido mais geral, à proteção dos dados pessoais. A AEPD está ciente do facto de que a proposta de Regulamento apenas estabelece os principais elementos do sistema a executar pelos Estados-Membros. Porém, gostaria de chamar a atenção para os seguintes pontos adicionais.
54. A AEPD insiste, tal como no caso dos outros pareceres ⁽¹⁾, na necessidade de introduzir uma disposição específica para garantir a confidencialidade da identidade dos denunciantes e dos informadores. A AEPD frisa que a posição dos denunciantes é 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 infração ⁽²⁾. A confidencialidade da identidade dos denunciantes e informadores deve ser garantida em todas as fases do processo, desde que com isso não se infrinjam as regras nacionais aplicáveis aos processos judiciais. Em especial, poderá ser necessário revelar a identidade dos denunciantes e informadores no âmbito de novos inquéritos ou na sequência de processos judiciais instaurados em resultado dos inquéritos (caso se prove terem prestado declarações intencionalmente falsas a seu respeito) ⁽³⁾. Face ao exposto, a AEPD recomenda a inclusão da disposição seguinte na alínea b) do artigo 29.º, n.º 1: «a identidade destas pessoas deve ser protegida em todas as fases do processo, a menos que a sua divulgação seja exigida pela legislação nacional no âmbito de novos inquéritos ou na sequência de novos processos judiciais».
55. A AEPD congratula-se com o facto de a disposição constante do artigo 29.º, n.º 1, alínea c), exigir aos Estados-Membros a garantia da proteção dos dados pessoais relativos quer à pessoa que comunica a infração quer à pessoa acusada, em conformidade com os princípios consagrados na Diretiva 95/46/CE. Sugere, contudo, a eliminação da expressão «os princípios consagrados» de modo a tornar a referência à Diretiva mais abrangente e vinculativa. No que se refere à necessidade de respeitar a legislação relativa à proteção dos dados na execução prática dos sistemas, a AEPD gostaria de sublinhar, em especial, as recomendações formuladas pelo Grupo de Trabalho do artigo 29.º no seu parecer de 2006 sobre denúncia de infrações. Aquando da execução dos sistemas nacionais, as entidades em causa devem ter em consideração, nomeadamente, a necessidade de respeitar a proporcionalidade, limitando, tanto quanto possível, a categoria de pessoas autorizadas a denunciar, a categoria de pessoas que possam ser incriminadas e as infrações pelas quais possam ser incriminadas; a necessidade de promover a identificação e confidencialidade das denúncias em vez do seu anonimato; a necessidade de divulgação da identidade dos denunciantes em caso de falsa acusação; e a necessidade de cumprimento absoluto dos períodos de conservação dos dados.

3. CONCLUSÕES

56. A AEPD congratula-se com a especial atenção dada à proteção de dados na proposta de Regulamento.
57. A AEPD formula as seguintes recomendações:
- especificar, no artigo 13.º, a finalidade da lista de iniciados,
 - introduzir, no artigo 17.º, n.º 2, alínea e), relativo ao poder de entrar em instalações privadas, a autorização judicial prévia como requisito geral,
 - introduzir, no artigo 17.º, n.º 2, alínea f), relativo ao poder de solicitar os registos telefónicos e de transmissão de dados, uma autorização judicial prévia como requisito geral e a obrigatoriedade de uma decisão formal que especifique: i) a base jurídica, ii) a finalidade do pedido, iii) as informações exigidas, iv) o prazo em que as informações devem ser fornecidas, e v) o direito de recurso da decisão para o Tribunal de Justiça por parte do destinatário,

⁽¹⁾ Ver, por exemplo, o parecer da AEPD sobre as disposições financeiras aplicáveis ao orçamento anual da União de 15 de abril de 2011 e o parecer da AEPD sobre os inquéritos efetuados pelo OLAF de 1 de junho de 2011, ambos disponíveis em <http://www.edps.europa.eu>

⁽²⁾ 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 3 de fevereiro de 2012, 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).

⁽³⁾ Ver parecer sobre as disposições financeiras aplicáveis ao orçamento anual da União de 15 de abril de 2011, disponível em <http://www.edps.europa.eu>

- especificar as categorias de registos telefónicos e de transmissão de dados na posse de um operador de telecomunicações ou de uma empresa de investimento que as autoridades competentes podem solicitar e limitar o disposto no artigo 17.º, n.º 2, alínea f), aos dados normalmente processados («na posse de») pelos operadores de telecomunicações no âmbito da Diretiva 2002/58/CE,
- aditar ao artigo 29.º, n.º 1, alínea b), uma provisão com a seguinte redação: «a identidade destas pessoas deve ser protegida em todas as fases do processo, a menos que a sua divulgação seja exigida pela legislação nacional no âmbito de novos inquéritos ou na sequência de novos processos judiciais»,
- tendo em conta as dúvidas expressas no presente parecer, avaliar a necessidade e a proporcionalidade do sistema proposto para a publicação obrigatória de sanções. Sob reserva do resultado da verificação da necessidade e da proporcionalidade, prever, em qualquer circunstância, garantias adequadas que assegurem o respeito pelo princípio da presunção de inocência e o direito de oposição das pessoas em causa, a segurança/exatidão dos dados e a sua eliminação após um período de tempo adequado.

Feito em Bruxelas, em 10 de fevereiro de 2012.

Giovanni BUTTARELLI
*Autoridade Adjunta Europeia para a Proteção
de Dados*
