Parecer da Autoridade Europeia para a Protecção de Dados sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)

(2011/C 101/04)

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 pedido de parecer apresentado nos termos do artigo 28.º, n.º 2, do 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 [2],

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

Descrição da proposta

1. Em 30 de Setembro de 2010, a Comissão adoptou uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA) [3].

2. A ENISA foi criada em Março de 2004, por um período inicial de cinco anos, pelo Regulamento (CE) n.º 460/2004 [4]. Em 2008, o Regulamento (CE) n.º 1007/2008 [5] prorrogou o mandato até Março de 2012.

3. Como decorre do artigo 1.º, n.º 1, do Regulamento (CE) n.º 460/2004, a Agência foi constituída a fim de garantir na União um nível de segurança das redes e da informação elevado e eficaz, contribuindo assim para o normal funcionamento do mercado interno.

4. A proposta da Comissão pretende modernizar a Agência, reforçar as suas competências e estabelecer um novo mandato para um período de cinco anos que possibilitará a continuidade da Agência para além de Março de 2012 [6].

5. A proposta de regulamento tem a sua base jurídica no artigo 114.º do TFUE [7], que confere à União competência para adoptar medidas com o objectivo de estabelecer ou assegurar o funcionamento do mercado interno. O artigo 114.º do TFUE é o sucessor do artigo 95.º do Tratado CE no qual se baseavam os anteriores regulamentos relativos à ENISA [8].

6. A Exposição de Motivos que acompanha a proposta refere o facto de a prevenção e o combate à criminalidade se terem tornado uma competência partilhada na sequência da entrada em vigor do Tratado de Lisboa. Esta situação criou uma oportunidade para que a ENISA funcione como uma plataforma relativamente aos aspectos de segurança das redes e da informação (SIR) da luta contra a cibercriminalidade, e para que proceda a um intercâmbio de ideias e melhores práticas com as autoridades responsáveis pela ciberdefesa, a aplicação da lei e a protecção dos dados.

7. Entre várias opções, a Comissão decidiu propor um alargamento das funções da ENISA e a integração das autoridades responsáveis pela aplicação da lei e pela protecção dos dados como membros de pleno direito do seu grupo permanente de partes interessadas. A nova lista de funções não inclui funções operacionais, mas actualiza e reformula as actualmente existentes.

Consulta da AEPD

8. Em 1 de Outubro de 2010, a proposta foi enviada à AEPD para consulta, em conformidade com o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001. A AEPD congratula-se por ter sido consultada sobre o tema em apreço e recomenda que seja feita referência a esta consulta nos considerandos da proposta, como habitualmente acontece nos textos legislativos sobre os quais foi chamada a pronunciar-se, nos termos do dito regulamento.

9. A AEPD foi consultada a título informal, antes da adopção da proposta, e formulou várias observações a esse título. Todavia, nenhuma delas foi tida em conta na versão final da proposta.

Avaliação geral

10. A AEPD salienta que a segurança do tratamento de dados é um elemento fundamental da protecção de dados [9]. A este respeito, congratula-se com o objectivo da proposta de reforçar as competências da Agência, para que esta possa desempenhar mais eficazmente as suas tarefas e atribuições actuais e expandir, simultaneamente, o seu domínio de

(1) JO L 281 de 23.11.1995, p. 31.
(2) JO L 8 de 12.1.2001, p. 1.
(3) COM(2010) 521 final.
(4) JO L 77 de 13.3.2004, p. 1.
(5) JO L 293 de 31.10.2008, p. 1.
(6) A fim de evitar um vazio jurídico, caso o processo legislativo no Parlamento Europeu e no Conselho se prolongasse para além do termo da vigência do mandato actual, a Comissão, em 30 de Setembro de 2010, adoptou uma segunda proposta de alteração do Regulamento (CE) n.º 460/2004 com o único intuito de prorrogar o mandato actual por mais dezoito meses. Ver COM(2010) 520 final.
(7) Cf. supra.
(8) Em 2 de Maio de 2006, o Tribunal de Justiça negou provimento ao recurso de anulação do anterior Regulamento (CE) n.º 460/2004, que contestava a sua base jurídica (Processo C-217/04).
(9) Os requisitos de segurança constam dos artigos 22.º e 35.º do Regulamento (CE) n.º 45/2001, dos artigos 16.º e 17.º da Directiva 95/46/CE e dos artigos 4.º e 5.º da Directiva 2002/58/CE.

actividade. A AEPD congratula-se ainda com a inclusão das autoridades responsáveis pela protecção de dados e dos organismos responsáveis pela aplicação da lei como partes interessadas de pleno direito. Considera que o alargamento do mandato da ENISA é uma forma de incentivar, a nível europeu, uma gestão profissional e simplificada das medidas de segurança aplicáveis aos sistemas de informação.

11. A avaliação global da proposta é positiva. Todavia, a proposta de regulamento é pouco clara ou incompleta relativamente a diversos aspectos, o que suscita preocupações do ponto de vista da protecção de dados. Essas questões serão explicitadas e analisadas no próximo capítulo do presente parecer.

II. **COMENTÁRIOS E RECOMENDAÇÕES**

As funções alargadas que a ENISA deverá exercer não são suficientemente claras

12. As funções alargadas da Agência que estão relacionadas com o envolvimento dos organismos responsáveis pela aplicação da lei e das autoridades responsáveis pela protecção de dados são formuladas em termos muito genéricos no artigo 3.º da proposta. A Exposição de Motivos é mais explícita a esse respeito, referindo que a ENISA estabelece uma interface com os organismos responsáveis pela aplicação da lei na luta contra a cibercriminalidade e desempenha funções não operacionais nessa luta. Contudo, essas funções não foram incluídas, ou apenas foram mencionadas em termos muito vagos no artigo 3.º.

13. A fim de evitar toda e qualquer insegurança jurídica, a proposta de regulamento deve descrever as funções da ENISA de forma clara e inequívoca. Como já foi dito, a segurança do tratamento de dados é um elemento fundamental da protecção de dados, e a ENISA irá desempenhar um papel cada vez mais importante nesse domínio. Os cidadãos, as instituições e os organismos devem compreender claramente que tipo de actividades a ENISA pode desenvolver. Essa dimensão ainda se torna mais importante se as funções alargadas da ENISA incluírem o tratamento de dados pessoais (ver n.os 17 a 20).

14. O artigo 3.º, n.º 1, alínea k), da proposta afirma que a Agência desempenha qualquer outra função que lhe seja conferida por um acto legislativo da União. Esta cláusula indeterminada suscita preocupação à AEPD, visto criar uma eventual lacuna que pode afectar a coerência do instrumento jurídico e conduzir a um «desvirtuamento da função» da Agência.

15. Uma das funções a que o artigo 3.º, n.º 1, alínea k), da proposta se refere está contida na Directiva 2002/58/CE [1], que obriga a Comissão a consultar a Agência sobre as medidas técnicas de execução aplicáveis às notificações em casos de violação de dados. A AEPD recomenda que esta actividade da Agência seja descrita com mais pormenor e delimitada ao domínio da segurança. Dado o eventual impacto que a ENISA poderá ter na elaboração de políticas nesse domínio, esta actividade deve ocupar uma posição mais clara e destacada na proposta de regulamento.

16. A AEPD recomenda ainda que se inclua uma referência à Directiva 1999/5/CE [2] no considerando 21, dada a função específica da ENISA, referida no artigo 3.º, n.º 1, alínea c), da presente proposta, de prestar assistência aos Estados-Membros e às instituições e organismos europeus nos seus esforços para recolher, analisar e difundir dados sobre a segurança das redes e da informação. Essa inclusão favoreceria as actividades desenvolvidas pela ENISA para promover as melhores práticas e técnicas de SRI (segurança das redes e da informação), uma vez que exemplifica melhor as possíveis interacções construtivas entre a Agência e os organismos de normalização.

Deve ser esclarecido se a Agência irá ou não tratar dados pessoais

17. A proposta não especifica se as funções atribuídas à Agência poderão incluir o tratamento de dados pessoais. Não contém, por isso, uma base jurídica específica para esse tratamento, na acepção do artigo 5.º do Regulamento (CE) n.º 45/2001.

18. Contudo, algumas das funções atribuídas à Agência podem implicar (pelo menos até certo ponto) o tratamento de dados pessoais. Não está, por exemplo, excluído que a análise dos incidentes de segurança e dos casos de violação de dados ou a execução de funções não operacionais na luta contra a cibercriminalidade possam envolver a recolha e a análise de dados pessoais.

19. O considerando 9 da proposta refere as disposições contidas na Directiva 2002/21/CE [3] segundo as quais a Agência deve, se for caso disso, ser notificada pelas autoridades reguladoras nacionais em caso de violação da segurança. A AEPD recomenda que a proposta indique com mais pormenor que notificações devem ser enviadas para a ENISA e a forma como a ENISA lhes deve responder. Do mesmo modo, a proposta deve abordar as implicações em matéria de tratamento de dados pessoais que poderão resultar da análise dessas notificações (se as houver).

---

[1] 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.

[2] Directiva 1999/5/CE do Parlamento Europeu e do Conselho, de 9 de Março de 1999, relativa aos equipamentos de rádio e equipamentos terminais de telecomunicações e ao reconhecimento mútuo da sua conformidade, JO L 91 de 7.4.1999, p. 10, e em especial o seu artigo 3.º, n.º 3, alínea c).

[3] 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.

20. A AEPD convida o legislador a esclarecer se algumas, e quais, das actividades da ENISA enumeradas no artigo 3.º incluirão o tratamento de dados pessoais.

Devem ser especificadas regras de segurança interna para a ENISA

21. Não obstante a ENISA desempenhar um papel importante no debate sobre a segurança das redes e da informação na Europa, a proposta é quase omissa a respeito da instituição de medidas de segurança para a própria Agência (relacionadas ou não com o tratamento de dados pessoais).

22. A AEPD entende que a Agência estará numa posição ainda melhor para promover as boas práticas em relação à segurança do tratamento de dados, se essas medidas de segurança forem firmemente aplicadas a nível interno pela própria Agência. Isso contribuirá para o seu reconhecimento não só como um centro especializado, mas também como um ponto de referência na aplicação prática das melhores técnicas disponíveis no domínio da segurança. A busca da excelência na execução das práticas de segurança deve estar, por isso, inscrita no regulamento relativo ao funcionamento interno da Agência. A AEPD sugere, assim, que se acrescente à proposta uma disposição neste sentido, exigindo, por exemplo, que a Agência aplique as melhores técnicas disponíveis, ou seja, os procedimentos de segurança mais eficazes e avançados e os seus métodos de operação.

23. Esta abordagem permitirá que a Agência preste aconselhamento sobre a aptidão prática de determinadas técnicas para fornecer as garantias de segurança necessárias. Além disso, a aplicação das melhores técnicas disponíveis deve dar prioridade às que permitam garantir a segurança minimizando simultaneamente, o mais possível, o impacto sobre a privacidade. Devem escolher-se as técnicas mais compatíveis com o conceito de «privacidade desde a concepção» (*privacy by design*).

24. Mesmo que a abordagem seja menos ambiciosa, a AEPD recomenda, no mínimo, que o regulamento contenha os seguintes requisitos: i) a criação de uma política de segurança interna, após uma avaliação dos riscos exaustiva e tendo em conta as normas internacionais e as melhores práticas utilizadas nos Estados-Membros, ii) a nomeação de um responsável pela segurança encarregado de aplicar essa política, com os recursos e a autoridade adequados, iii) a aprovação da política, após um exame atento dos riscos residuais e dos controlos propostos pelo Conselho de Administração, e iv) uma revisão periódica da política, com uma periodicidade e objectivos claramente definidos.

Os canais de cooperação com as autoridades responsáveis pela protecção de dados (incluindo a AEPD) e o Grupo de Trabalho do artigo 29.º devem ser melhor definidos

25. Como já foi dito, a AEPD congratula-se com o alargamento do mandato da Agência e considera que as autoridades responsáveis pela protecção de dados podem beneficiar muito com a sua existência (e a Agência com a experiência dessas autoridades). Na verdade, dada a convergência natural e lógica entre a segurança e a protecção de dados, é inevitável que a Agência e as autoridades responsáveis pela protecção de dados tenham de colaborar estreitamente.

26. Os considerandos 24 e 25 contêm uma referência à proposta de directiva da UE relativa à cibercriminalidade e mencionam que a Agência deve colaborar com os organismos responsáveis pela aplicação da lei e também com as autoridades responsáveis pela protecção de dados, no que respeita aos aspectos da luta contra a cibercriminalidade que estão relacionados com a segurança da informação [1].

27. A proposta também deve prever canais e mecanismos de colaboração concretos que i) garantam a *coerência* das actividades da Agência com as das autoridades responsáveis pela protecção de dados e que ii) permitam uma *estreita cooperação* entre a Agência e essas autoridades.

28. No que diz respeito à *coerência*, o considerando 27 refere explicitamente que as funções da Agência não devem entrar em conflito com as autoridades responsáveis pela protecção de dados dos Estados-Membros. A AEPD congratula-se com esta referência, mas constata que a AEPD e o Grupo do Artigo 29.º não são referidos. Recomenda, assim, ao legislador que também inclua na proposta uma disposição de não interferência similar em relação a estas duas entidades. Desse modo, criar-se-á um ambiente de trabalho mais claro para todas as partes e delinear-se-ão os canais e mecanismos de colaboração necessários para que a Agência possa prestar assistência às diversas autoridades responsáveis pela protecção de dados e ao Grupo do Artigo 29.º.

29. Assim, no que respeita à *cooperação estreita*, a AEPD congratula-se com a inclusão de uma representação das autoridades responsáveis pela protecção de dados no grupo permanente de partes interessadas que aconselhará a Agência no exercício das suas actividades. Recomenda que seja explicitamente mencionado que essa representação deve ser nomeada pela Agência com base numa proposta do Grupo do Artigo 29.º. Considera também conveniente incluir uma referência à participação da AEPD, enquanto tal, nas reuniões onde sejam debatidas questões relevantes para a cooperação com a AEPD. Além disso, recomenda que a Agência (após consulta ao grupo permanente de partes interessadas e com a aprovação do Conselho de Administração) crie grupos de trabalho *ad hoc* para os diversos temas em que a protecção dos dados e a segurança se sobrepõem, a fim de preparar esse esforço de estreita cooperação.

[1] Proposta de Directiva do Parlamento Europeu e do Conselho relativa a ataques contra os sistemas de informação e que revoga a Decisão-Quadro 2005/222/JAI do Conselho, COM(2010) 517 final.

30. Por último, a fim de evitar mal-entendidos, a AEPD recomenda que se utilize o termo «autoridades responsáveis pela protecção de dados» em lugar de «autoridades responsáveis pela protecção da privacidade» e que se esclareça quem são essas autoridades através da inclusão de uma referência ao artigo 28.º da Directiva 95/46/CE e à AEPD nos termos do Capítulo V do Regulamento (CE) n.º 45/2001.

Não é claro que beneficiários podem solicitar a assistência da ENISA

31. A AEPD observa uma incoerência na proposta de regulamento no que diz respeito às entidades que podem solicitar a assistência da ENISA. Depreende-se, dos considerandos 7, 15, 16, 18 e 36 da proposta, que a ENISA tem capacidade para prestar assistência aos organismos dos Estados-Membros e à União em geral. Porém, o artigo 2.º, n.º 1, apenas refere a Comissão e os Estados-Membros, ao passo que o artigo 14.º restringe a capacidade de apresentar pedidos de assistência às seguintes entidades: i) Parlamento Europeu, ii) Conselho, iii) Comissão e iv) qualquer organismo competente designado por um Estado-Membro, deixando de fora algumas das instituições, organismos, agências e serviços da União.

32. O artigo 3.º da proposta é mais específico e prevê diversos tipos de assistência, consoante o tipo de beneficiários: i) recolha e análise de dados sobre a segurança da informação (no caso dos Estados-Membros e das instituições e organismos europeus), ii) análise do estado da segurança das redes e da informação na Europa (no caso dos Estados-Membros e das instituições europeias), iii) promoção da utilização de boas práticas de gestão dos riscos e de segurança (na União e nos Estados-Membros), iv) desenvolvimento da detecção em relação à segurança das redes e da informação (nas instituições e organismos europeus) e v) colaboração no diálogo e na cooperação com países terceiros (no caso da União).

33. A AEPD convida o legislador a corrigir esta incoerência e a harmonizar as disposições acima mencionadas. A este respeito, a AEPD recomenda que o artigo 14.º seja alterado de forma a incluir efectivamente todas as instituições, organismos, serviços e agências da União e a esclarecer o tipo de assistência que pode ser solicitada pelas diferentes entidades da União (caso esta diferenciação seja prevista pelo legislador). No mesmo sentido, recomenda-se que certas entidades públicas e privadas possam solicitar a assistência da Agência, se o apoio pedido demonstrar um claro potencial do ponto de vista europeu e estiver de acordo com os objectivos da Agência.

Funções do Conselho de Administração

34. A Exposição de Motivos prevê um reforço das competências do Conselho de Administração no que respeita ao seu papel de supervisão. A AEPD congratula-se com esse reforço e recomenda que se incluam vários aspectos relativos à protecção de dados nas funções do Conselho de Administração. Recomenda, ainda, que o regulamento especifique inequivocamente a quem compete: i) estabelecer medidas de aplicação do Regulamento (CE) n.º 45/2001 pela Agência, designadamente no que respeita à nomeação do responsável pela protecção de dados, ii) aprovar a política de segurança e as revisões periódicas subsequentes, e iii) definir o protocolo de cooperação com as autoridades responsáveis pela protecção de dados e os organismos responsáveis pela aplicação da lei.

Aplicabilidade do Regulamento (CE) n.º 45/2001

35. Ainda que já seja exigida pelo Regulamento (CE) n.º 45/2001, a AEPD sugere que se inclua no artigo 27.º a nomeação do responsável pela protecção de dados, visto revestir-se de especial importância e dever ser acompanhada pela rápida adopção das regras de execução relativas ao âmbito das competências e funções que lhe deverão ser confiadas, em conformidade com o artigo 24.º, n.º 8, do Regulamento (CE) n.º 45/2001. Mais concretamente, o artigo 27.º poderá ter a seguinte redacção:

1. As informações tratadas pela Agência em conformidade com o presente regulamento estão sujeitas ao 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. O Conselho de Administração estabelece medidas de aplicação do Regulamento (CE) n.º 45/2001 pela Agência, nomeadamente em relação ao responsável pela protecção de dados da Agência.

36. Caso seja necessária uma base jurídica específica para o tratamento de dados pessoais, como se analisa nos n.os 17-20, ela também deve prever especificações a respeito das garantias, limitações e condições necessárias e adequadas para esse tratamento ter lugar.

III. **CONCLUSÕES**

37. A avaliação global da proposta é positiva, e a AEPD congratula-se com o alargamento do mandato da Agência e a extensão das suas funções mediante a inclusão das autoridades responsáveis pela protecção de dados e dos organismos responsáveis pela aplicação da lei como partes interessadas de pleno direito. A AEPD considera que a continuidade da Agência irá incentivar, a nível europeu, uma gestão profissional e simplificada das medidas de segurança aplicáveis aos sistemas de informação.

38. A AEPD recomenda que, a fim de evitar toda e qualquer insegurança jurídica, a proposta seja clarificada no tocante à extensão das funções da Agência, sobretudo das relacionadas com o envolvimento dos organismos responsáveis pela aplicação da lei e das autoridades responsáveis pela protecção de dados. Além disso, a AEPD chama a atenção para a eventual lacuna criada pela inclusão, na proposta, de uma disposição que permite que qualquer outro acto legislativo da União atribua novas funções à Agência sem estabelecer restrições adicionais.

39. A AEPD convida o legislador a esclarecer se algumas, e quais, das actividades da ENISA incluirão o tratamento de dados pessoais.

40. A AEPD recomenda a inclusão de disposições relativas ao estabelecimento de uma política de segurança da própria Agência, a fim de reforçar o seu papel de promoção da excelência nas práticas de segurança, bem como da privacidade desde a concepção, conciliando a utilização das melhores técnicas de segurança disponíveis com o respeito pelos direitos de protecção dos dados pessoais.

41. Os canais de cooperação com as autoridades responsáveis pela protecção de dados, incluindo a AEPD e o Grupo do Artigo 29.º, devem ser definidos de forma mais precisa, a fim de garantir a coerência e uma estreita cooperação.

42. A AEPD convida o legislador a solucionar algumas incoerências no que respeita às restrições expressas no artigo 14.º quanto à capacidade de solicitar a assistência da Agência. Em especial, a AEPD recomenda que essas restrições sejam postas de parte e que todas as instituições, organismos, agências e serviços da União possam solicitar a assistência da Agência.

43. Por último, a AEPD recomenda que, nas competências alargadas do Conselho de Administração, se incluam elementos concretos que reforcem a garantia de que na Agência se aplicam boas práticas em matéria de segurança e protecção de dados. Propõe-se, nomeadamente, a inclusão da nomeação de um responsável pela protecção de dados e a aprovação das medidas necessárias para a correcta aplicação do Regulamento (CE) n.º 45/2001.

Feito em Bruxelas, em 20 de Dezembro de 2010.

Giovanni BUTTARELLI

Autoridade Adjunta Europeia para a Protecção de Dados