PARECERES

AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS

Parecer da Autoridade Europeia para a Protecção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — «A política de luta contra o terrorismo da UE: principais realizações e desafios futuros»

(2011/C 56/02)

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 41.º,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 20 de Julho de 2010, a Comissão adoptou uma Comunicação intitulada «A política de luta contra o terrorismo da UE: principais realizações e desafios futuros» ([3]). A Comunicação pretende descrever «os elementos principais para uma avaliação política da actual Estratégia da UE de luta contra o terrorismo» e também constitui um elemento da Estratégia de Segurança Interna ([4]). Nela se avaliam os resultados obtidos no passado e traçam os desafios e directrizes futuros da política de luta contra o terrorismo da UE.

2. Muitas das iniciativas mencionadas na comunicação já foram objecto de pareceres ou comentários específicos da AEPD. Contudo, a comunicação apresenta uma ampla perspectiva política e orientações a longo prazo que justificam que a AEPD emita um parecer a seu respeito.

3. O presente parecer visa contribuir, assim, para opções políticas mais fundamentais num domínio em que a utilização de informações pessoais é simultaneamente crucial, maciça e particularmente sensível.

4. O parecer não formula quaisquer comentários sobre a mais recente comunicação da Comissão neste domínio, intitulada «Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura» e adoptada em 22 de Novembro de 2010 ([5]). Ela será analisada pela AEPD num outro parecer, no qual se voltará a abordar a necessidade de estabelecer relações claras entre os diferentes documentos.

5. No presente parecer, a AEPD analisa os diversos elementos da comunicação, ao mesmo tempo que formula conselhos e recomendações com o intuito de garantir o direito fundamental à protecção dos dados pessoais no âmbito da política de luta contra o terrorismo da UE, sobretudo ao responder a desafios futuros e ao elaborar novas orientações políticas.

II. ANÁLISE DA COMUNICAÇÃO E QUESTÕES PERTINENTES EM MATÉRIA DE PROTECÇÃO DE DADOS

6. Baseando-se na estrutura da Estratégia da UE de luta contra o terrorismo de 2005 ([6]), a comunicação analisa primeiramente os quatro vectores principais da política de luta contra o terrorismo da UE: prevenir, proteger, perseguir e reagir. Num capítulo específico aborda, seguidamente, algumas questões horizontais, nomeadamente o respeito dos direitos fundamentais, a cooperação internacional e o financiamento.

([1]) JO L 281 de 23.11.1995, p. 31.
([2]) JO L 8 de 12.1.2001, p. 1.
([3]) COM(2010) 386 final.
([4]) Ver página 2 da Comunicação.
([5]) COM(2010) 673 final.
([6]) Documento 14469/4/05, de 30 de Novembro de 2005.

1. **Prevenir, Proteger, Perseguir, Reagir e a necessidade de incorporar os princípios de protecção de dados**

7. «Prevenir» é um vector que engloba um vasto número de actividades, desde a prevenção da radicalização e do recrutamento até ao exame da forma como os terroristas utilizam a Internet. Neste contexto, a comunicação refere entre as principais realizações a Decisão-Quadro relativa à luta contra o terrorismo, adoptada em 2002 ([1]) e alterada em 2008 ([2]).

8. A «protecção» das pessoas e das infra-estruturas também constitui um tema muito vasto, que inclui iniciativas referentes à segurança das fronteiras e dos transportes, ao controlo de substâncias precursoras dos explosivos, à protecção das infra-estruturas críticas e ao reforço da cadeia de abastecimento.

9. Em «perseguir» inclui-se a recolha de informações, a cooperação policial e judiciária, e o combate às actividades terroristas e seu financiamento. Os desafios futuros neste sector são o estabelecimento de um quadro relativo ao registo de identificação dos passageiros (PNR) da UE ([3]), a utilização do artigo 75.º TFUE para desenvolver um quadro relativo ao congelamento de fundos e bens, e o reconhecimento mútuo na obtenção de provas em matéria penal.

10. «Reagir» refere-se à capacidade de resposta às consequências de um atentado terrorista e inclui o apoio às vítimas do terrorismo.

11. Todos estes domínios têm fortes ligações a iniciativas que já foram objecto de uma posição da AEPD: o Programa de Estocolmo, as medidas restritivas e o congelamento de bens, a conservação de dados, os scâneres de segurança, os precursores de armas, os dados biométricos, a Decisão Prüm, os registos de identificação dos passageiros, o Acordo TFTP, o Sistema de Informação de Schengen, o Sistema de Informação sobre Vistos, a gestão integrada das fronteiras, a Estratégia de Gestão da Informação da UE e o intercâmbio transfronteiras de elementos de prova.

12. Os domínios da «prevenção» e da «protecção» são os mais delicados do ponto de vista da protecção de dados, por diversas razões.

13. Em primeiro lugar, são domínios, por definição, baseados em avaliações prospectivas dos riscos, as quais desencadeiam, na maioria dos casos, um tratamento amplo e «preventivo» de grandes volumes de dados pessoais relativos a cidadãos não suspeitos (como, por exemplo, o rastreio da Internet, as «fronteiras electrónicas» (*e-borders*) e os scâneres de segurança).

14. Em segundo lugar, a comunicação prevê um aumento das parcerias entre as autoridades de aplicação da lei e as empresas privadas (como os fornecedores de serviços Internet, as instituições financeiras e as empresas de transportes) tendo em vista o intercâmbio de informações pertinentes e, por vezes, a «delegação» nessas empresas de certos aspectos das funções policiais. Esse aumento implica uma maior utilização pelas autoridades públicas de dados pessoais, recolhidos por empresas privadas para fins comerciais, para efeitos de aplicação da lei.

15. Muitas dessas iniciativas foram frequentemente adoptadas como uma resposta rápida a incidentes terroristas, sem que as eventuais duplicações ou sobreposições com medidas já existentes fossem devidamente tidas em conta. Em alguns casos, apesar de já terem passado vários anos desde que entraram em vigor, ainda não se determinou até que ponto a invasão da privacidade dos cidadãos resultante dessas medidas era realmente necessária.

16. Além disso, a utilização «preventiva» dos dados pessoais é mais susceptível de causar discriminação. A análise preventiva das informações implicaria a recolha e o tratamento de dados pessoais relativos a vastas categorias de indivíduos (por exemplo, todos os passageiros, todos os utilizadores da Internet), independentemente de existirem suspeitas específicas a seu respeito. A análise desses dados — em especial quando associada a técnicas de prospecção de dados — pode levar a que pessoas inocentes sejam assinaladas como suspeitas apenas devido ao facto de terem um perfil (idade, sexo, religião, etc.) e/ou padrões (por exemplo, de viagem, de utilização da Internet, etc.) semelhantes aos de pessoas ligadas, ou suspeitas de estarem ligadas, ao terrorismo. Por conseguinte, sobretudo neste contexto, a utilização ilícita ou inexacta de informações pessoais (por vezes sensíveis), associada aos amplos poderes coercivos das autoridades de aplicação da lei, pode levar à discriminação e à estigmatização de pessoas e/ou grupos de pessoas específicos.

17. Nesta perspectiva, ao garantir um nível elevado de protecção de dados também se está a contribuir para combater o racismo, a xenofobia e a discriminação, sendo que, segundo a comunicação, as iniciativas nesse sentido «podem igualmente contribuir para prevenir a radicalização e o recrutamento para fins terroristas».

2. **Uma abordagem coerente baseada no princípio da necessidade**

18. Uma observação importante de carácter geral tem a ver com a necessidade de assegurar a coerência e relações claras entre todas as comunicações e iniciativas no domínio dos assuntos internos e, em particular, no domínio da segurança interna. Por exemplo, apesar de a estratégia da UE de luta contra o terrorismo estar intimamente ligada à estratégia de gestão da informação, à estratégia relativa à Carta dos Direitos Fundamentais e ao modelo europeu de

([1]) 2002/475/JAI, (JO L 164 de 22.6.2002, p. 3).
([2]) 2008/919/JAI, (JO L 330 de 9.12.2008, p. 21).
([3]) Também anunciado no Plano de Acção de aplicação do Programa de Estocolmo da Comissão COM(2010) 171 final, de 20 de Abril de 2010.

intercâmbio de informações, as relações entre todos estes documentos não são abordadas de forma explícita e exaustiva. Esta situação tornou-se ainda mais evidente com a adopção, em 22 de Novembro de 2010, da Comunicação «Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura» ([1]).

19. A AEPD recomenda, por isso, às instituições da UE que assegurem que as políticas e iniciativas no domínio dos assuntos internos e da segurança interna são concebidas e aplicadas de modo a manterem uma abordagem coerente e relações claras entre si, criando sinergias adequadas e positivas, e evitando a duplicação de tarefas e de esforços.

20. A AEPD recomenda ainda que o princípio da necessidade seja explicitamente tido em conta em cada proposta apresentada neste domínio. Isso exige que se considerem as possíveis sobreposições com instrumentos já existentes e que se limite a recolha e o intercâmbio de dados pessoais ao estritamente necessário para os objectivos pretendidos.

21. Por exemplo, no caso do Acordo relativo ao Programa de Detecção do Financiamento do Terrorismo (TFTP II) celebrado com os EUA, a AEPD questionou em que medida o acordo era realmente necessário para obter resultados que podiam ser obtidos mediante a utilização de instrumentos menos invasivos da vida privada, como os já estabelecidos pelo quadro da UE e internacional existente ([2]). No mesmo parecer, a AEPD questionou a necessidade de enviar dados pessoais por atacado e não de forma mais direccionada.

22. A comunicação menciona que um dos desafios consiste «em assegurar que estes instrumentos cubram as necessidades reais (de aplicação da lei), embora garantindo o pleno respeito do direito à privacidade e das normas em matéria de protecção de dados». A AEPD congratula-se com este reconhecimento explícito e exorta as instituições da UE a avaliarem cuidadosamente até que ponto os instrumentos já existentes, bem como os previstos, cobrem as necessidades reais de aplicação da lei, e a evitarem eventuais sobreposições das medidas, ou restrições desnecessárias à vida privada. Nesta perspectiva, os instrumentos existentes devem provar ser um meio eficaz de combate ao terrorismo, aquando das revisões periódicas.

23. A AEPD tem defendido, em numerosos pareceres e comentários e, com especial ênfase, no recente parecer sobre a comunicação «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça» ([3]), a necessidade de avaliar todos os instrumentos existentes em matéria de intercâmbio de informações, antes de propor outros novos. Na verdade, a avaliação da eficácia das medidas existentes, em paralelo com a análise do impacto das novas medidas previstas na vida privada, é crucial e deve conferir um papel importante à acção da União Europeia neste domínio, em conformidade com a abordagem proposta pelo Programa de Estocolmo.

24. As sobreposições e a falta de eficácia devem conduzir ao ajustamento das opções políticas, ou mesmo à consolidação ou rejeição dos sistemas de recolha e tratamento de dados existentes.

25. A AEPD recomenda que se preste especial atenção às propostas conducentes à recolha dos dados pessoais de todos os cidadãos em geral e não apenas dos suspeitos. Também devem ser especificamente analisados e justificados os casos em que se prevê que os dados pessoais possam ser tratados para outros fins que não aqueles para os quais foram inicialmente recolhidos, como é o caso, por exemplo, do acesso, para fins de aplicação da lei, aos dados pessoais armazenados no sistema Eurodac.

26. A comunicação destaca também que um dos desafios futuros consistirá em garantir uma política eficaz de investigação em matéria de segurança, a qual contribuiria para um elevado nível de segurança. A AEPD subscreve a afirmação da comunicação de que uma investigação eficaz nessa matéria deverá reforçar as relações entre os diversos intervenientes. Deste ponto de vista, é crucial que as competências no domínio da protecção de dados nela sejam integradas desde o início, de modo a orientar as opções políticas e a garantir a máxima incorporação possível da privacidade nas novas tecnologias orientadas para a segurança, em conformidade com o princípio da «privacidade desde a fase de concepção».

3. **Relativamente à utilização de medidas restritivas (congelamento de bens)**

27. No que respeita à utilização de medidas restritivas (congelamento de bens) contra países e suspeitos de terrorismo específicos, a jurisprudência do Tribunal de Justiça tem confirmado, de forma reiterada e coerente, que o respeito dos direitos fundamentais na luta contra o terrorismo é essencial para assegurar o respeito dos direitos dos cidadãos e a legalidade das medidas tomadas.

28. A AEPD já formulou pareceres e comentários neste domínio ([4]), em que destacou, por um lado, as melhorias introduzidas nos procedimentos, mas por outro lado exigiu mais melhorias, principalmente quanto ao direito de informação

([1]) Ver n.º 4 do presente parecer.
([2]) Parecer da AEPD de 22 de Junho de 2010.
([3]) Parecer da AEPD de 30 de Setembro de 2010.

([4]) Parecer de 28 de Julho de 2009, sobre a Proposta de Regulamento do Conselho que altera o Regulamento (CE) n.º 881/2002 que institui certas medidas restritivas específicas contra determinadas pessoas e entidades associadas a Osama Bin Laden, à rede Al-Qaida e aos talibã, (JO C 276 de 17.11.2009, p. 1). Parecer de 16 de Dezembro de 2009 sobre várias propostas legislativas que impõem certas medidas restritivas específicas no que diz respeito à Somália, ao Zimbabué, à República Democrática da Coreia e à Guiné, (JO C 73 de 23.3.2010, p. 1). Ver também a carta da AEPD, de 20 de Julho de 2010, sobre três propostas legislativas referentes a certas medidas restritivas, nomeadamente em relação a Slobodan Milosevic e às pessoas que lhe estão associadas, em apoio do mandato do Tribunal Internacional para a Antiga Jugoslávia, e em relação à Eritreia. Todos os pareceres e comentários da AEPD estão disponíveis no seu sítio *web*: http://www.edps.europa.eu

e de acesso aos dados pessoais, à definição clara das restrições desses direitos e à disponibilidade de vias de recurso judicial eficazes e de um controlo independente.

29. A necessidade de melhorar o procedimento e as garantias ao dispor dos indivíduos constantes das listas foi recentemente confirmada pelo Tribunal Geral no denominado processo «Kadi II» ([1]). O Tribunal salientou, em especial, que era necessário informar a pessoa inscrita na lista de forma pormenorizada sobre os fundamentos da sua inscrição. Isto aproxima-se muito dos direitos de acesso e de rectificação dos dados pessoais de cada indivíduo, nomeadamente quando estes são incorrectos ou desactualizados, consagrados na legislação relativa à protecção de dados. Estes direitos, explicitamente mencionados pelo artigo 8.º da Carta dos Direitos Fundamentais, são elementos essenciais da protecção de dados, que só podem ser objecto de limitações na medida em que essas limitações sejam necessárias, previsíveis e estabelecidas por lei.

30. Nesta perspectiva, a AEPD concorda com a comunicação quando esta afirma que um dos desafios futuros no domínio da política de luta contra o terrorismo será a utilização do artigo 75.º TFUE. Esta nova base jurídica, introduzida pelo Tratado de Lisboa, permite especificamente a adopção de medidas de congelamento dos bens contra pessoas singulares ou colectivas. A AEPD recomenda que esta base jurídica também seja utilizada para estabelecer um quadro para o congelamento de bens inteiramente conforme com o respeito dos direitos fundamentais. A AEPD está disponível para contribuir para o desenvolvimento futuro de instrumentos e procedimentos legislativos pertinentes, e espera ser consultada da forma devida e em tempo útil quando a Comissão — de acordo com o previsto no seu Programa de Trabalho para 2011 — elaborar um regulamento específico neste domínio ([2]).

31. Numa perspectiva mais vasta, é necessário instituir um quadro jurídico para a protecção de dados também aplicável à Política Externa e de Segurança Comum. Na verdade, o artigo 16.º TFUE constitui uma base jurídica para o estabelecimento de normas de protecção de dados também no domínio da PESC. A base jurídica e o procedimento legal diferentes instituídos pelo artigo 39.º TUE apenas são aplicáveis quando os dados pessoais são tratados, neste domínio, pelos Estados-Membros. No entanto, apesar de o Tratado de Lisboa exigir essas normas de protecção de dados e prever os instrumentos necessários para as estabelecer, a recente Comunicação «Uma abordagem global da protecção de dados pessoais na União Europeia» ([3]) ainda não prevê nenhuma iniciativa nesse sentido. Neste contexto, a AEPD insta a Comissão a apresentar uma proposta relativa ao estabelecimento de um quadro jurídico para a protecção de dados no domínio da Política Externa e de Segurança Comum.

([1]) Acórdão de 30 de Setembro de 2010 no processo T-85/09 *Kadi* contra *Comissão Europeia*; ver, em especial, pontos 157 e 177.

([2]) O Programa de trabalho da Comissão para 2011 [COM(2010) 623, de 27 de Outubro de 2010] menciona no seu anexo II (Lista indicativa de iniciativas que poderão ser adoptadas) um «Regulamento que institui um procedimento para o congelamento de fundos das pessoas suspeitas de actividades terroristas na UE».

([3]) Comunicação da Comissão (2010) 609, de 4 de Novembro de 2010.

4. **Respeito dos Direitos Fundamentais e Cooperação Internacional**

32. O capítulo dedicado ao respeito dos direitos fundamentais faz notar que a UE deve constituir um exemplo em matéria de respeito da Carta dos Direitos Fundamentais, a qual deve ser o ponto de referência de todas as suas políticas. A AEPD congratula-se com esta abordagem.

33. A AEPD também apoia a afirmação de que o respeito dos direitos fundamentais não é apenas uma exigência jurídica, mas igualmente uma condição essencial para promover a confiança mútua entre as autoridades nacionais e o público em geral.

34. Neste contexto, a AEPD recomenda uma atitude proactiva e medidas concretas nesse sentido, também como forma de aplicar efectivamente a Carta dos Direitos Fundamentais da UE ([4]).

35. Devem realizar-se avaliações do impacto na privacidade (Privacy Impact Assessments - PIA) e uma consulta precoce das autoridades competentes em matéria de protecção de dados relativamente a todas as iniciativas que afectem a protecção de dados pessoais, independentemente dos seus promotores e do domínio em que são propostas.

36. No seu capítulo sobre a cooperação internacional, a comunicação também destaca a necessidade de criar as «necessárias condições jurídicas e políticas com vista a uma cooperação reforçada com os parceiros externos da UE no domínio do combate do terrorismo».

37. A este respeito, a AEPD lembra a necessidade de assegurar a adopção de garantias adequadas aquando do intercâmbio de dados pessoais com países terceiros e organizações internacionais, a fim de garantir que os direitos de protecção dos dados pessoais dos cidadãos também são adequadamente respeitados no contexto da cooperação internacional.

38. Para esse efeito, há também que promover a protecção de dados em cooperação com os países terceiros e as organizações internacionais, a fim de assegurar o cumprimento das normas da UE. Essa acção está igualmente em sintonia com a intenção da Comissão de elaborar normas jurídicas e técnicas para uma protecção de dados de elevado nível em países terceiros e a nível internacional, bem como de reforçar a cooperação com países terceiros ([5]).

([4]) Ver Comunicação da Comissão (2010) 573, de 19 de Outubro de 2010, «Estratégia para a aplicação efectiva da Carta dos Direitos Fundamentais pela União Europeia».

([5]) Ver Comunicação (2010) 609 «Uma abordagem global da protecção de dados pessoais na União Europeia», páginas 16-17.

39. As medidas restritivas (congelamento de bens) constituem uma clara oportunidade para a acção da União Europeia neste domínio, em que a cooperação intensa com os países terceiros e a Organização das Nações Unidas não deve reduzir o elevado nível de protecção dos direitos fundamentais proporcionado pelo sistema jurídico da UE.

III. **CONCLUSÕES**

40. A AEPD congratula-se com a atenção prestada pela comunicação aos direitos fundamentais e à protecção dos dados, e recomenda que se adoptem outras melhorias concretas no domínio da política de luta contra o terrorismo.

41. A AEPD recomenda que se apoie com iniciativas concretas o respeito dos direitos fundamentais neste domínio, muito em especial o direito à protecção dos dados pessoais, que é indispensável para promover a segurança jurídica, a confiança e a cooperação na luta contra o terrorismo, além de ser uma condição jurídica necessária para o desenvolvimento dos sistemas previstos.

42. A AEPD também subscreve a ideia de que se deve preferir, neste domínio, uma política mais sistemática e menos dirigida para incidentes, em especial quando os incidentes levam à criação de novos sistemas de armazenamento, recolha e intercâmbio de dados sem uma avaliação adequada das alternativas existentes.

43. Nesta perspectiva, a AEPD recomenda às instituições da UE que assegurem que as políticas e iniciativas no domínio dos assuntos internos e da segurança interna são concebidas e aplicadas de modo a manterem uma abordagem coerente e relações claras entre si, criando sinergias adequadas e positivas, e evitando a duplicação de tarefas e de esforços.

44. A AEPD recomenda, assim, que o legislador da UE reforce o papel de protecção de dados através da adopção de acções específicas (e da fixação de prazos), designadamente:

— A avaliação da eficácia das medidas existentes, em paralelo com a análise do seu impacto na vida privada, é crucial e deve conferir um papel importante à acção da União Europeia neste domínio;

— Ao prever novas medidas, há que tomar em consideração as eventuais sobreposições com instrumentos já existentes, ter em conta a sua eficácia, e limitar a recolha e o intercâmbio de dados pessoais ao que é estritamente necessário para os objectivos pretendidos;

— Propor a criação de um quadro jurídico para a protecção de dados também aplicável à Política Externa e de Segurança Comum;

— Propor uma abordagem ampla e global, com base no artigo 75.º TFUE, que garanta, no domínio das medidas restritivas (congelamento de bens), quer a eficácia das medidas de aplicação da lei quer o respeito dos direitos fundamentais;

— Colocar a protecção de dados no centro do debate das medidas neste domínio, assegurando, por exemplo, a realização de avaliações de impacto na privacidade e na protecção de dados e uma consulta oportuna das autoridades competentes em matéria de protecção de dados, quando são apresentadas propostas relevantes;

— Assegurar que as competências no domínio da protecção de dados são integradas, desde o início, na investigação em matéria de segurança, de modo a orientar as acções políticas e a garantir a máxima incorporação possível da privacidade nas novas tecnologias orientadas para a segurança;

— Assegurar a adopção de garantias adequadas quando os dados pessoais são tratados no contexto da cooperação internacional, promovendo simultaneamente o desenvolvimento e a aplicação dos princípios de protecção de dados pelos países terceiros e as organizações internacionais.

Feito em Bruxelas, em 24 de Novembro de 2010.

Peter HUSTINX

Supervisor Europeu para a Protecção de Dados