Parecer da Autoridade Europeia para a Protecção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — «A Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura»

(2011/C 101/02)

A AUTORIDADE EUROPEIA PARA A PROTECÇÃO 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 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 emitido nos termos do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho 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 do seu artigo 41.º,

ADOPTOU O SEGUINTE PARECER:

I. INTRODUÇÃO

1. Em 22 de Novembro de 2010, a Comissão adoptou uma Comunicação intitulada *A Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura* (a seguir designada a «Comunicação») [3]. A Comunicação foi enviada à AEPD para consulta.

2. A AEPD congratula-se com o facto de ter sido consultado pela Comissão. Ainda antes da adopção da Comunicação, a AEPD teceu comentários informais sobre o projecto de texto, alguns dos quais foram tidos em conta na versão final da Comunicação.

Contexto da Comunicação

3. A Estratégia de Segurança Interna da UE (a seguir designada ESI), objecto da Comunicação, foi adoptada em 23 de Fevereiro de 2010, sob a Presidência espanhola [4]. A estratégia define um modelo de segurança europeu, que integra, nomeadamente, a acção da cooperação entre autoridades policiais e judiciais, a gestão das fronteiras e a protecção civil, no respeito dos valores comuns europeus, como os direitos fundamentais. Os seus principais objectivos são os seguintes:

— apresentar ao público os instrumentos da UE que já contribuem para garantir a segurança e a liberdade dos cidadãos da UE e a mais-valia que a acção da UE representa neste domínio;

— desenvolver novos instrumentos e políticas comuns que recorram a uma abordagem mais integrada que atenda às causas da insegurança e não apenas aos seus efeitos;

— reforçar a cooperação entre autoridades policiais e judiciais, a gestão das fronteiras, a protecção civil e a gestão de catástrofes.

4. A Estratégia de Segurança Interna pretende responder às ameaças e desafios mais prementes, como a criminalidade grave e organizada, o terrorismo e a cibercriminalidade, a gestão das fronteiras externas da UE e o fomento da capacidade de resistência às catástrofes naturais e de origem humana. A Estratégia fornece orientações, princípios e rumos para a UE dar resposta a estas questões e convida a Comissão a propor acções calendarizadas para a execução da estratégia.

5. Neste contexto, importa ainda referir as conclusões do recente Conselho «Justiça e Assuntos Internos» sobre a criação e implementação de um ciclo político da UE para a criminalidade internacional grave e organizada, adoptadas em 8-9 de Novembro de 2010 [5] (a seguir designadas «conclusões de Novembro de 2010»). Este documento dá seguimento às conclusões do Conselho sobre a arquitectura da segurança interna, de 2006 [6], e apela ao Conselho e à Comissão para definirem uma estratégia global de segurança interna da UE baseada nos valores e princípios comuns consagrados na Carta dos Direitos Fundamentais da UE [7].

[1] JO L 281 de 23.11.1995, p. 31.
[2] JO L 8 de 12.1.2001, p. 1.
[3] COM(2010) 673 final.
[4] Doc. 5842/2/10.
[5] 3043.ª reunião do Conselho «Justiça e Assuntos Internos», 8-10 de Novembro de 2010, Bruxelas.
[6] Doc. 7039/2/06 JAI 86 CATS 34.
[7] O ciclo político da UE para a criminalidade internacional grave e organizada referido nas Conclusões de Novembro de 2010 compreende quatro etapas: 1) Desenvolvimento da política com base numa avaliação da ameaça da criminalidade grave e organizada da União Europeia (AACGO da UE); 2) Definição da política e tomada de decisões mediante a identificação pelo Conselho de um número limitado de prioridades; 3) Implementação e monitorização dos planos de acção operacionais anuais (PAO); 4) No fim do ciclo político, uma avaliação exaustiva que fornecerá igualmente elementos para o novo ciclo político.

6. De entre as orientações e objectivos que devem presidir à execução da Estratégia de Segurança Interna, as conclusões de Novembro de 2010 referem uma reflexão sobre uma abordagem proactiva e baseada na informação, uma estreita cooperação entre as agências da União, nomeadamente graças a um melhor intercâmbio de informações, e a prossecução do objectivo de sensibilizar os cidadãos para a importância do trabalho desenvolvido pela União para os proteger. As conclusões instam ainda a Comissão a desenvolver, juntamente com os peritos dos organismos competentes da UE e dos Estados-Membros, um plano estratégico plurianual (a seguir designado «PEP») para cada prioridade, que defina a estratégia mais adequada para resolver o problema. Por último, insta a Comissão a desenvolver, em consulta com os peritos dos Estados-Membros e dos organismos da UE, um mecanismo independente para avaliar a implementação do PEP. A AEPD voltará a estes temas mais adiante no presente parecer, dado que estes estão estreitamente relacionados com a protecção dos dados pessoais ou com outros direitos e liberdades fundamentais conexos, ou neles têm um impacto significativo.

Conteúdo e objectivo da Comunicação

7. A Comunicação propõe cinco objectivos estratégicos, todos relacionados com a protecção da privacidade e dos dados:

   — desmantelamento das redes internacionais de criminalidade,

   — prevenção do terrorismo e resposta à radicalização e ao recrutamento,

   — reforço dos níveis de segurança para os cidadãos e as empresas no ciberespaço,

   — reforço da segurança através da gestão das fronteiras, e

   — reforço da capacidade de resistência da Europa às crises e às catástrofes.

8. A *Estratégia de Segurança Interna em Acção* apresenta uma agenda comum para os Estados-Membros, o Parlamento Europeu, a Comissão, o Conselho, as agências e outros intervenientes, incluindo a sociedade civil e as autoridades locais, e propõe uma forma para estas entidades, ao longo dos próximos quatro anos, trabalharem em comum para atingir os objectivos da Estratégia de Segurança Interna.

9. A Comunicação assenta no Tratado de Lisboa e reconhece as orientações fornecidas pelo Programa de Estocolmo (e pelo seu plano de acção), que sublinha, no seu ponto 4.1, a necessidade de uma Estratégia de Segurança Interna global, baseada no respeito dos direitos fundamentais, da protecção internacional e do Estado de direito. Além disso, de acordo com o Programa de Estocolmo, o desenvolvimento, o controlo e a implementação da Estratégia de Segurança Interna devem passar a ser uma das tarefas prioritárias do Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna (COSI), criado ao abrigo do artigo 71.º do TFUE. Para assegurar a execução efectiva da Estratégia, este deve ocupar-se igualmente de aspectos de segurança da gestão integrada das fronteiras e, sempre que adequado, da cooperação judiciária em matéria penal necessária para a cooperação operacional no domínio da segurança interna. Importa igualmente referir, neste contexto, que o Programa de Estocolmo advoga uma abordagem integrada da Estratégia de Segurança Interna que tenha igualmente em conta a Estratégia de Segurança Externa desenvolvida pela União, bem como outras políticas da UE, nomeadamente as relativas ao mercado interno.

Objectivo do parecer

10. A Comunicação refere diversas áreas políticas que fazem parte de um conceito geral de «segurança interna» na União Europeia ou nele têm impacto.

11. O objectivo do presente parecer consiste não em analisar a totalidade das áreas políticas e dos tópicos específicos abrangidos pela Comunicação, mas antes em:

   — apreciar os objectivos da Estratégia de Segurança Interna proposta na Comunicação na perspectiva da protecção da privacidade e dos dados e — nessa óptica — destacar as ligações necessárias com outras estratégias actualmente debatidas e adoptadas ao nível da União;

   — enunciar uma série de noções e conceitos relativos à protecção de dados que devem ser tidos em conta na concepção, desenvolvimento e execução da Estratégia de Segurança Interna ao nível da UE;

   — apresentar, quando tal se afigurar útil e adequado, sugestões sobre a melhor forma de ter em conta as preocupações relativas à protecção de dados na execução das acções propostas na Comunicação.

12. A AEPD irá fazê-lo sublinhando, nomeadamente, as relações entre a Estratégia de Segurança Interna e a Estratégia de Gestão da Informação e o trabalho desenvolvido em relação ao quadro geral de protecção de dados. Além disso a AEPD irá referir conceitos, como: as melhores técnicas disponíveis e a «privacidade desde a concepção» («Privacy by design»), a avaliação do impacto da protecção da privacidade e dos dados, e os direitos da pessoa em causa, que têm impacto directo na concepção e na execução da Estratégia de Segurança Interna. O parecer tece ainda observações sobre uma série de áreas políticas, como a gestão integrada das fronteiras, incluindo o Sistema Europeu de Vigilância das Fronteiras (EUROSUR) e o tratamento de dados pessoais pela Frontex, bem como outros domínios, como o ciberespaço e o TFTP.

II. OBSERVAÇÕES DE CARÁCTER GERAL

Necessidade de uma abordagem mais ampla, inclusiva e «estratégica» das estratégias da UE relacionadas com a ESI

13. Estão actualmente a ser discutidas e propostas, ao nível da UE, diversas estratégias baseadas no Tratado de Lisboa e no Programa de Estocolmo que têm um impacto directo ou indirecto na protecção de dados. A Estratégia de Segurança Interna é uma delas e está estreitamente relacionada com outras estratégias (objecto de comunicações recentes da Comissão ou previstas para o futuro próximo), como a Estratégia de Gestão da Informação e o modelo europeu de intercâmbio de informações, a estratégia para a aplicação efectiva da Carta dos Direitos Fundamentais pela União Europeia, a estratégia global de protecção de dados e a política de luta contra o terrorismo da UE. No presente parecer, a AEPD presta especial atenção à relação com a Estratégia de Gestão da Informação e com o quadro geral de protecção de dados baseado no artigo 16.º do TFUE, que, na perspectiva da protecção dos dados, têm relações políticas evidentes com a ESI.

14. Todas estas estratégias constituem um complexo mosaico de directrizes políticas, programas e planos de acção inter-relacionados, que requer uma abordagem global e integrada ao nível da UE.

15. Em termos mais gerais, esta abordagem de «relacionamento das estratégias», se adoptada nas acções futuras, demonstrará a existência de uma visão da UE relativa às suas *estratégias* e que essas estratégias e as comunicações sobre as mesmas recentemente adoptadas estão estreitamente interligadas, sendo o Programa de Estocolmo o ponto de referência comum a todas elas. Resultará ainda em sinergias positivas entre diferentes políticas que se inscrevem no domínio da liberdade, segurança e justiça e evitará a duplicação de trabalho e de esforços neste domínio. O que é igualmente importante, esta abordagem conduzirá a uma aplicação mais eficaz e coerente das regras de protecção de dados no contexto das estratégias interligadas.

16. A AEPD sublinha que um dos pilares da ESI consiste numa gestão eficaz da informação na União Europeia, que deve assentar nos princípios da necessidade e da proporcionalidade para justificar a necessidade de intercâmbio de informações.

17. Além disso, conforme referido no parecer da AEPD relativo à Comunicação sobre a gestão da informação ([8]), a AEPD salienta que todas as novas medidas legislativas que possam facilitar o armazenamento e o intercâmbio de dados pessoais só devem ser propostas quando baseadas em provas concretas da sua necessidade ([9]). Esta obrigação legal deveria ser transformada numa abordagem política proactiva para efeitos de execução da ESI. A necessidade de uma abordagem global da ESI conduz também, inevitavelmente, à necessidade de avaliar todos os instrumentos e ferramentas já existentes no domínio da segurança interna antes de propor novos.

18. Neste contexto, a AEPD sugere igualmente uma aplicação mais frequente das disposições que prevêem a avaliação periódica dos instrumentos existentes, como a constante da Directiva relativa à conservação de dados, que está a ser avaliada ([10]).

A protecção dos dados enquanto objectivo da ESI

19. A Comunicação refere a protecção dos dados pessoais no parágrafo «Políticas de segurança baseadas em valores comuns», onde se afirma que os instrumentos e medidas a utilizar para executar a Estratégia de Segurança Interna devem basear-se em valores comuns, nomeadamente o primado do direito e o respeito dos direitos fundamentais, consagrados na Carta dos Direitos Fundamentais da UE. Neste contexto, a Comunicação estipula que «embora a aplicação eficaz da legislação na UE seja facilitada pelo intercâmbio de informações, devemos igualmente proteger a privacidade dos cidadãos e o seu direito fundamental à protecção dos dados pessoais».

20. Esta é uma declaração que saudamos, embora não possamos considerar que, por si só, constitua uma abordagem suficiente da questão da protecção de dados no âmbito da Estratégia de Segurança Interna. A Comunicação não aprofunda a questão da protecção dos dados ([11]) nem explica de que forma o respeito da privacidade e a protecção dos dados pessoais serão assegurados na prática no âmbito das acções de execução da Estratégia de Segurança Interna.

([8]) Parecer da Autoridade Europeia para a Protecção de Dados, de 30 de Setembro de 2010, sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho — «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça».

([9]) Trata-se de uma obrigação legal; ver, nomeadamente o acórdão do Tribunal de Justiça da União Europeia nos Processos apensos C-92/09 e C-93/09, de 2 de Novembro de 2010. Em contextos mais específicos, a AEPD também tem defendido esta abordagem noutros pareceres sobre propostas legislativas relacionadas com o espaço de liberdade, segurança e justiça, como, por exemplo, o Parecer de 19 de Outubro de 2005 sobre três propostas relativas ao Sistema de Informação de Schengen de segunda geração (SIS II), o Parecer de 20 de Dezembro de 2007 sobre a proposta de decisão-quadro do Conselho relativa à utilização dos dados dos Registos de Identificação dos Passageiros (Passenger Name Record — PNR) para efeitos de aplicação da lei, o Parecer de 18 de Fevereiro de 2009 sobre a proposta de Regulamento relativo à criação do Sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efectiva do Regulamento (CE) n.º […/…] (que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de protecção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida), o Parecer de 18 de Fevereiro de 2009 sobre a proposta de Regulamento que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de protecção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida e o Parecer de 7 de Outubro de 2009 sobre as propostas relativas ao acesso ao Eurodac para fins de aplicação da lei.

([10]) Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE (JO L 105 de 13.4.2006, p. 54).

([11]) A protecção dos dados apenas é referida mais especificamente no contexto do tratamento de dados pessoais pela FRONTEX.

21. A AEPD considera que um dos objectivos da *Estratégia de Segurança Interna em Acção* deveria ser uma *protecção* geral, que assegurasse o *justo* equilíbrio entre, por um lado, a protecção dos cidadãos contra as ameaças existentes e, por outro, a protecção da sua privacidade e o direito à protecção dos dados pessoais. Por outras palavras, as preocupações de segurança e de privacidade deveriam ser tidas em conta da mesma forma no desenvolvimento da Estratégia de Segurança Interna, o que estaria em conformidade com o Programa de Estocolmo e com as Conclusões do Conselho.

22. Em suma, garantir a segurança no pleno respeito da privacidade e da protecção dos dados deveria constituir um objectivo da Estratégia de Segurança Interna da UE, reflectido em todas as acções empreendidas pelos Estados-Membros e pelas instituições da União para executar a Estratégia.

23. Neste contexto, a AEPD remete para a Comunicação (2010) 609, relativa a *Uma abordagem global da protecção de dados pessoais na União Europeia* ([12]). A AEPD emitirá em breve um parecer sobre esta comunicação, mas sublinha desde já que não poderá haver uma Estratégia de Segurança Interna eficaz se esta não for complementada por um sistema de protecção de dados sólido e se não existir confiança mútua e uma maior eficácia.

III. NOÇÕES E CONCEITOS APLICÁVEIS À CONCEPÇÃO E À EXECUÇÃO DA ESTRATÉGIA DE SEGURANÇA INTERNA

24. É evidente que algumas das acções que decorrem dos objectivos da Estratégia de Segurança Interna podem aumentar os riscos para a privacidade dos indivíduos e para a protecção de dados. Para contrabalançar estes riscos, a AEPD gostaria de chamar a atenção para conceitos como os de "privacidade desde a concepção", avaliação do impacto na protecção da privacidade e dos dados, direitos da pessoa em causa e melhores técnicas disponíveis. Todos estes conceitos devem ser tidos em conta na execução da Estratégia de Segurança Interna e podem contribuir para que as políticas neste domínio respeitem mais a privacidade e sejam mais orientadas para a protecção de dados.

«Privacidade desde a concepção»

25. A AEPD já defendeu em diversas ocasiões e em diversos pareceres o conceito de privacidade «integrada» («Privacidade desde a concepção» ou «Privacidade por defeito»). Este conceito, desenvolvido actualmente para os sectores privado e público, deve desempenhar também um papel importante no contexto da segurança interna da UE e no domínio da polícia e da justiça ([13]).

26. A Comunicação não refere este conceito. A AEPD sugere que este conceito seja referido nas acções direccionadas que serão propostas e realizadas para implementar a Estratégia de Segurança Interna, nomeadamente no contexto do Objectivo 4, «Reforçar a segurança através da gestão das fronteiras», em que é feita uma clara referência a uma maior utilização de novas tecnologias para os controlos na fronteira e para a vigilância das fronteiras.

Avaliação do impacto na protecção da privacidade e dos dados

27. A AEPD incentiva a Comissão a reflectir — no âmbito do futuro trabalho de concepção e execução da Estratégia de Segurança Interna com base na Comunicação — sobre aquilo que deve significar uma verdadeira «avaliação do impacto na protecção da privacidade e dos dados» no domínio da liberdade, segurança e justiça e, mais concretamente, da Estratégia de Segurança Interna.

28. A Comunicação refere avaliações de risco e das ameaças, referências com as quais nos congratulamos. No entanto, a Comunicação não refere — em ponto algum — avaliações do impacto na protecção da privacidade e dos dados. O AEPD considera que o trabalho relativo à aplicação da Comunicação sobre a Estratégia de Segurança Interna representa uma boa oportunidade para realizar essas avaliações do impacto na protecção da privacidade e dos dados no contexto da segurança interna. A AEPD nota que nem a Comunicação nem as directrizes da Comissão relativas à avaliação do impacto especificam este aspecto ([14]), tornando-o uma exigência política.

29. A AEPD recomenda, por conseguinte, que na implementação dos futuros instrumentos seja levada a cabo uma avaliação mais específica e rigorosa do respectivo impacto na protecção da privacidade e dos dados, quer como uma avaliação distinta, quer como uma parte da avaliação geral do impacto nos direitos fundamentais realizada pela Comissão. Esta avaliação do impacto não se deve limitar a enunciar princípios gerais ou a analisar opções políticas, como acontece actualmente, devendo igualmente recomendar salvaguardas específicas e concretas.

30. Em consequência, devem ser desenvolvidos indicadores e funções específicos para que todas as propostas no domínio da segurança interna da UE com impacto na protecção da privacidade e dos dados sejam objecto de uma análise aprofundada, que tenha em conta princípios como os da proporcionalidade, da necessidade e da limitação da finalidade.

31. Poderia ainda ser útil, neste contexto, remeter para o artigo 4.º da Recomendação relativa à identificação por radiofrequências (RFID) ([15]), na qual a Comissão convidou os Estados-Membros a assegurarem que as empresas do sector, em colaboração com as partes interessadas da sociedade civil, estabeleçam um quadro para as avaliações do

([12]) Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: «Uma abordagem global da protecção de dados pessoais na União Europeia», COM(2010) 609.

([13]) A AEPD recomendou, no seu parecer sobre a Comunicação da Comissão relativa ao Programa de Estocolmo, a existência de uma obrigação legal, imposta aos criadores e aos utilizadores de sistemas de informação, de utilizar sistemas conformes com o princípio da «privacidade desde a concepção».

([14]) SEC(2009) 92 de 15.1.2009.

([15]) C(2009) 3200 final de 12.5.2009.

impacto na protecção da privacidade e dos dados. Também a Resolução de Madrid, aprovada em Novembro de 2009 pela Conferência Internacional de Comissários para a Protecção da Privacidade e dos Dados, incentiva à realização de avaliações do impacto na protecção da privacidade e dos dados antes da implementação de novos sistemas e tecnologias da informação para o tratamento de dados pessoais ou da introdução de alterações substanciais nos processos de tratamento existentes.

Direitos das pessoas em causa

32. A AEPD nota que a Comunicação não aborda especificamente a questão dos direitos das pessoas em causa, os quais constituem um elemento vital da protecção de dados e deveriam ter impacto na concepção da Estratégia de Segurança Interna. É essencial assegurar que, em todos os diferentes sistemas e instrumentos relacionados com a segurança interna da UE, as pessoas por eles afectadas beneficiem de direitos equivalentes no que respeita à forma como os seus dados pessoais são tratados.

33. Com efeito, muitos dos sistemas mencionados na Comunicação estabelecem regras específicas relativamente aos direitos das pessoas em causa (visando igualmente categorias de pessoas como vítimas, criminosos suspeitos ou migrantes), mas observam-se grandes variações entre os sistemas e instrumentos, sem que exista uma boa justificação para tal.

34. Por esse motivo, a AEPD convida a Comissão a examinar mais atentamente, num futuro próximo, a questão da harmonização a nível da UE dos direitos das pessoas em causa no contexto da Estratégia de Segurança Interna e da Estratégia de Gestão da Informação.

35. Deverá ser prestada particular atenção aos mecanismos de recurso. A Estratégia de Segurança Interna deverá garantir que, sempre que os direitos das pessoas não tenham sido inteiramente respeitados, os responsáveis pelo tratamento dos dados prevejam procedimentos de reclamação facilmente acessíveis, eficazes e a preços razoáveis.

Melhores técnicas disponíveis

36. A execução da Estratégia de Segurança Interna assentará, necessariamente, na utilização de uma infra-estrutura de TI para apoiar as acções previstas na Comunicação. As melhores técnicas disponíveis podem ser consideradas ferramentas que permitem estabelecer o correcto equilíbrio entre a consecução dos objectivos da Estratégia de Segurança Interna e o respeito dos direitos individuais. No contexto actual, a AEPD gostaria de reiterar a recomendação formulada em anteriores pareceres ([16]) relativa à necessidade de a Comissão definir e promover, conjuntamente com interessados do sector, medidas concretas para a aplicação das melhores técnicas disponíveis. Por essa aplicação entende-se o estádio de desenvolvimento mais eficaz e avançado das actividades e dos seus métodos de operação que demonstre a aptidão prática de técnicas específicas para proporcionar os resultados almejados com eficácia e em conformidade com os requisitos do quadro regulamentar da UE em matéria de segurança e de protecção dos dados e da vida privada. Esta abordagem é perfeitamente compatível com a abordagem da "privacidade desde a concepção" acima referida.

37. Sempre que pertinente e exequível, devem ser elaborados documentos de referência sobre as melhores técnicas disponíveis que forneçam orientações e maior segurança jurídica para a execução efectiva das medidas no âmbito da Estratégia de Segurança Interna. Esta prática pode igualmente promover a harmonização dessas medidas nos diferentes Estados-Membros. Por último, mas não menos importante, a definição de privacidade e de melhores técnicas disponíveis compatíveis com a segurança facilitará a tarefa de supervisão das autoridades responsáveis pela protecção dos dados, ao fornecer-lhes referências técnicas compatíveis com a privacidade e a protecção de dados adoptadas pelos responsáveis pelo tratamento de dados.

38. A AEPD nota ainda a importância de um alinhamento correcto da Estratégia de Segurança Interna com as actividades já desenvolvidas no âmbito do sétimo Programa-Quadro de Investigação e Desenvolvimento Tecnológico e do Programa-Quadro de Segurança e Protecção das Liberdades. Uma visão conjunta tendente a facultar as melhores técnicas disponíveis permitirá a inovação nos conhecimentos e capacidades necessários para proteger os cidadãos, no respeito dos direitos fundamentais.

39. Por último, a AEPD chama a atenção para o papel que a Agência Europeia para a Segurança das Redes e da Informação (ENISA) poderá desempenhar na elaboração de orientações e na avaliação das capacidades de segurança necessárias para assegurar a integridade e a disponibilidade dos sistemas de TI, bem como na promoção das melhores técnicas disponíveis. Neste contexto, a AEPD saúda a inclusão da Agência como interveniente principal no reforço das capacidades de resposta a ciberataques e de luta contra a cibercriminalidade ([17]).

Clarificação dos intervenientes e dos respectivos papéis

40. Neste contexto, é necessária uma maior clarificação dos intervenientes que fazem parte ou contribuem para a arquitectura da Estratégia de Segurança Interna. A Comunicação refere diversos intervenientes, como cidadãos, sistema judiciário, agências da União, autoridades nacionais, polícia e empresas. Os papéis e as competências específicas destes

([16]) Parecer da AEPD sobre sistemas de transporte inteligentes, de Julho de 2009, e Parecer da AEPD sobre a Comunicação relativa à identificação por radiofrequências, de Dezembro de 2007; ver igualmente o Relatório Anual da AEPD de 2006, p. 48.

([17]) A AEPD tenciona adoptar, ainda em Dezembro de 2010, um parecer sobre o enquadramento jurídico da ENISA.

intervenientes deverão ser melhor definidos nas acções específicas a propor no âmbito da execução da Estratégia de Segurança Interna.

IV. OBSERVAÇÕES ESPECÍFICAS SOBRE DOMÍNIOS POLÍTICOS RELACIONADOS COM A ESTRATÉGIA DE SEGURANÇA INTERNA

Gestão integrada das fronteiras

41. A Comunicação refere o facto de, com o Tratado de Lisboa, a UE estar em melhores condições de tirar partido das sinergias entre as políticas de gestão das fronteiras no que respeita às pessoas e às mercadorias. Em relação à circulação das pessoas, a Comunicação refere que «a UE pode tratar a gestão da migração e a luta contra a criminalidade como um duplo objectivo da estratégia de gestão integrada das fronteiras». O documento considera a gestão das fronteiras como um meio potencialmente poderoso para desmantelar a criminalidade grave e organizada ([18]).

42. A AEPD nota ainda que a Comunicação identifica três vectores estratégicos: 1) uma maior utilização de novas tecnologias para os controlos na fronteira (a segunda geração do Sistema de Informação de Schengen (SIS II), o sistema de entradas/saídas e o programa de viajantes registados); 2) uma maior utilização de novas tecnologias para a vigilância das fronteiras (Sistema Europeu de Vigilância das Fronteiras, EUROSUR); e 3) uma maior coordenação dos Estados-Membros através da Frontex.

43. A AEPD quer aproveitar a oportunidade proporcionada pelo presente parecer para reiterar o pedido expresso numa série de anteriores pareceres no sentido da definição, ao nível da UE, de uma política clara de gestão das fronteiras, no pleno respeito das regras em matéria de protecção de dados. A AEPD entende que os trabalhos em curso no domínio da Estratégia de Segurança Interna e da Estratégia de Gestão da Informação constituem excelentes ocasiões para tomar medidas mais concretas em favor de uma abordagem política coerente nestas áreas.

44. A AEPD nota que a Comunicação refere não só os sistemas de grande escala existentes e susceptíveis de começar a funcionar num futuro próximo (como o SIS, o SIS II e o VIS), como também, nos mesmos termos, os sistemas que poderão ser propostos pela Comissão no futuro, mas em relação aos quais ainda não foi tomada qualquer decisão (como é o caso do sistema de entradas/saídas e do programa de viajantes registados). Neste contexto, importa lembrar que os objectivos e a legitimidade da introdução destes sistemas devem ainda ser clarificados e demonstrados, nomeadamente à luz dos resultados de avaliações de impacto específicas realizadas pela Comissão. Se tal não acontecer, poderá entender-se que a Comunicação antecipa o processo decisório e, em consequência, não tem em conta o facto de a decisão final relativa à eventual introdução do programa de viajantes registados e do sistema de entradas/saídas na União Europeia ainda não ter sido tomada.

45. Nestas circunstâncias, a AEPD sugere que, nos futuros trabalhos relativos à execução da Estratégia de Segurança Interna, este tipo de antecipação seja evitado. Conforme já se referiu, qualquer decisão relativa à introdução de sistemas de grande escala invasivos da privacidade apenas deve ser tomada após uma avaliação adequada de todos os sistemas existentes, tendo em devida conta os princípios da necessidade e da proporcionalidade.

EUROSUR

46. A Comunicação indica que a Comissão apresentará em 2011 uma proposta legislativa de criação do EUROSUR, no intuito de contribuir para a segurança interna e a luta contra a criminalidade. Afirma ainda que o EUROSUR utilizará novas tecnologias desenvolvidas através das actividades e dos projectos de investigação financiados pela UE, como as imagens de satélite para detectar e seguir alvos nas fronteiras marítimas, por exemplo, acompanhando embarcações rápidas que transportam drogas para a UE.

47. Neste contexto, a AEPD nota que não é claro se e — na afirmativa — em que medida a proposta legislativa relativa ao EUROSUR a apresentar pela Comissão em 2011 contemplará igualmente o tratamento de dados pessoais no âmbito do EUROSUR. A Comissão não toma uma posição clara sobre esta matéria na Comunicação. Esta questão é tanto mais pertinente quanto a Comunicação estabelece uma relação clara entre o EUROSUL e a Frontex, a nível táctico, operacional e estratégico, (ver mais adiante as observações sobre a Frontex), e apela a uma estreita cooperação entre ambos.

O tratamento de dados pessoais pela FRONTEX

48. Em 17 de Maio de 2010 ([19]), a AEPD emitiu um parecer sobre a revisão do regulamento que cria a Frontex em que apela a um verdadeiro debate e a uma reflexão aprofundada sobre a questão da protecção de dados no contexto do reforço das actuais funções da Frontex e da atribuição de novas responsabilidades a esta agência.

49. No Objectivo 4, *Reforçar a segurança através da gestão das fronteiras*, a Comunicação refere a necessidade de melhorar o contributo da Frontex nas fronteiras externas. Neste contexto, a Comunicação indica que, com base na experiência adquirida e no contexto da abordagem global da UE no domínio da gestão da informação, a Comissão considera que autorizar a Frontex a proceder ao tratamento e à utilização destas informações, de forma limitada e em conformidade com regras de gestão de dados pessoais claramente

([18]) Comunicado de imprensa sobre A Estratégia de Segurança Interna da UE em Acção: cinco etapas para uma Europa mais segura, Memo 10/598.

([19]) Parecer da Autoridade Europeia para a Protecção de Dados, de 17 de Maio de 2010, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (CE) n.º 2007/2004 do Conselho que cria uma Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas dos Estados-Membros da União Europeia.

definidas, representará um contributo significativo para o desmantelamento de organizações criminosas. Esta é uma abordagem diferente da adoptada na proposta de revisão do regulamento que cria a Frontex, actualmente em discussão no Parlamento Europeu e no Conselho, que era omissa em relação ao tratamento de dados pessoais.

50. Nestas condições, a AEPD congratula-se com o facto de a Comunicação fornecer algumas indicações sobre as circunstâncias em que o tratamento de dados se pode revelar necessário (por exemplo, para análises de risco, para melhor centrar operações conjuntas ou para intercâmbio de informações com a Europol). Mais concretamente, a Comunicação explica que, actualmente, as informações sobre criminosos envolvidos em redes de tráfico — a que a Frontex tem acesso — não podem ser em seguida utilizadas para análises de risco ou para melhor centrar futuras operações conjuntas. Além disso, os dados relevantes sobre os criminosos suspeitos não são transmitidos às autoridades nacionais competentes nem à Europol tendo em vista uma investigação complementar.

51. No entanto, a AEPD nota que a Comunicação não refere a discussão em curso sobre a revisão do enquadramento jurídico da Frontex, que, conforme já se referiu, aborda este tema no intuito de encontrar soluções legislativas. Acresce que a redacção da Comunicação, que destaca o papel da Frontex no contexto do objectivo de desmantelamento de organizações criminosas, pode ser interpretada como um alargamento das competências da Frontex. A AEPD sugere que este ponto seja tido em conta tanto na revisão do regulamento que cria a Frontex como na execução da Estratégia de Segurança Interna.

52. A AEPD chama ainda a atenção para a necessidade de assegurar que não existe duplicação de tarefas entre a Europol e a Frontex. Neste contexto, a AEPD congratula-se com o facto de a Comunicação referir a necessidade de evitar a duplicação de tarefas entre a Frontex e a Europol. No entanto, esta questão deve ser mais clarificada tanto no regulamento que cria a Frontex revisto como nas acções de execução da Estratégia de Segurança Interna que prevêem uma estreita cooperação entre a Frontex e a Europol. Esta questão assume particular importância do ponto de vista dos princípios da limitação das finalidades e da qualidade dos dados. Esta observação é igualmente aplicável à futura cooperação com agências como a Agência Europeia para a Segurança das Redes e da Informação (ENISA) ou o Gabinete Europeu de Apoio ao Asilo (EASO).

Uso de dados biométricos

53. A Comunicação não aborda especificamente o actual fenómeno do aumento da utilização de dados biométricos no domínio da liberdade, segurança e justiça, incluindo os sistemas informáticos europeus de grande escala e outros instrumentos de gestão das fronteiras.

54. Em consequência, a AEPD aproveita esta oportunidade para reiterar a sua sugestão ([20]) de que esta questão extremamente sensível do ponto de vista da protecção de dados seja tida em devida conta na execução da Estratégia de Segurança Interna, nomeadamente no contexto da gestão das fronteiras.

55. A AEPD recomenda ainda que seja desenvolvida uma política clara e rigorosa sobre o uso de dados biométricos no domínio da liberdade, segurança e justiça, com base numa apreciação séria e numa avaliação caso a caso da necessidade da utilização da biometria no contexto da Estratégia de Segurança Interna, no pleno respeito de princípios fundamentais de protecção de dados, como os princípios da necessidade, da proporcionalidade e da limitação da finalidade.

TFTP

56. A Comunicação anuncia que, em 2011, a Comissão definirá uma política a nível da UE para a extracção e análise da transmissão de dados relativos a mensagens de pagamentos financeiros existentes no seu próprio território. Neste contexto, a AEPD remete para o seu parecer de 22 de Junho de 2010 sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo (TFTP II) ([21]). Todas as observações críticas tecidas nesse parecer são igualmente válidas e aplicáveis no contexto dos trabalhos previstos sobre um enquadramento da UE para dados relativos a mensagens de pagamentos financeiros. Em consequência, essas observações devem ser tidas em conta nas discussões sobre esta matéria. Deverá ser prestada particular atenção à proporcionalidade da extracção e tratamento de grandes quantidades de dados sobre pessoas que não são suspeitas, bem como à questão da supervisão efectiva por autoridades independentes e pelo sistema judiciário.

Segurança para os cidadãos e as empresas no ciberespaço

57. A AEPD congratula-se com a importância conferida às acções preventivas ao nível da UE na Comunicação e considera que o reforço da segurança das redes de TI constitui um factor essencial para o bom funcionamento da sociedade da informação. Além disso, a AEPD apoia as actividades específicas de reforço da capacidade de resposta a ciberataques, de reforço da capacidade das entidades policiais e judiciárias e de criação de parcerias com as empresas para capacitar e proteger os cidadãos e as empresas. É de saudar ainda o papel de facilitador desempenhado pela ENISA em relação a muitas das acções previstas para este objectivo.

([20]) Ver, nomeadamente, o Parecer da Autoridade Europeia para a Protecção de Dados sobre a apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça referido na nota de pé-de-página 8.

([21]) Parecer da Autoridade Europeia para a Protecção de Dados, de 22 de Junho de 2010, sobre a proposta de decisão do Conselho relativa à conclusão do Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo (TFTP II).

58. Contudo, a *Estratégia de Segurança Interna em Acção* não aprofunda as acções de aplicação da lei previstas para o ciberespaço, a forma como essas acções podem pôr em risco os direitos individuais ou as medidas de protecção necessárias. A AEPD insta a uma abordagem mais ambiciosa em relação às garantias adequadas, abordagem que deve ter por objectivo proteger os direitos fundamentais de todos os indivíduos, incluindo aqueles que possam ser afectados por acções destinadas a lutar contra eventuais actividades criminosas neste domínio.

V. **CONCLUSÕES E RECOMENDAÇÕES**

59. O AEPD insta a que, no processo de execução da Estratégia de Segurança Interna, sejam estabelecidas ligações entre diferentes estratégias da UE e diferentes comunicações da Comissão. Esta abordagem deve ser seguida de um plano de acção concreto, apoiado por uma verdadeira avaliação das necessidades, que deverá resultar numa política de segurança interna global, integrada e bem estruturada.

60. A AEPD aproveita ainda esta oportunidade para destacar a importância da obrigação legal de realizar uma verdadeira avaliação de todos os instrumentos existentes a utilizar no contexto da Estratégia de Segurança Interna e do intercâmbio de informações antes de propor novos instrumentos. Neste contexto, é seriamente recomendada a inclusão de disposições que prevejam a avaliação regular da eficácia dos instrumentos pertinentes.

61. A AEPD sugere que, na preparação do plano estratégico plurianual requerido nas Conclusões do Conselho de Novembro de 2010, sejam tidos em conta os trabalhos em curso relativos à preparação de um quadro normativo geral para a protecção de dados com base no artigo 16.º do TFUE, nomeadamente a Comunicação da Comissão (2009) 609.

62. A AEPD formula uma série de sugestões sobre noções e conceitos importantes na perspectiva da protecção de dados que devem ser tidas em conta no domínio da Estratégia de Segurança Interna, como é o caso da privacidade desde a concepção, da avaliação do impacto na protecção da privacidade e dos dados e das melhores técnicas disponíveis.

63. A AEPD recomenda que na implementação dos futuros instrumentos seja levada a cabo uma avaliação do respectivo impacto na protecção da privacidade e dos dados, quer como uma avaliação distinta, quer como uma parte da avaliação geral do impacto nos direitos fundamentais realizada pela Comissão.

64. A AEPD convida ainda a Comissão a desenvolver uma política mais coerente e consistente sobre os requisitos prévios para o uso de dados biométricos no âmbito da Estratégia de Segurança Interna e a garantir uma maior harmonização a nível da UE em termos dos direitos das pessoas em causa.

65. Por último, a AEPD tece uma série de comentários sobre o tratamento de dados pessoais no contexto da gestão das fronteiras, nomeadamente pela Frontex e, eventualmente, no âmbito do EUROSUR.

Feito em Bruxelas, em 17 de Dezembro de 2010.

Peter HUSTINX

Supervisor Europeu para a Protecção de Dados