Síntese do parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação Conjunta da Comissão e da Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança intitulada «Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido», e sobre a proposta da Comissão para uma Diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

(O texto integral do presente parecer está disponível em EN, FR e DE no sítio Web da AEPD em http://www.edps.europa.eu)

(2014/C 32/10)

1. **Introdução**

1.1. *Consulta da AEPD*

1. Em 7 de fevereiro de 2013, a Comissão e a Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança adotaram uma Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões intitulada «Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido» ([1]) (a seguir «a Comunicação Conjunta», «a Estratégia para a cibersegurança» ou «a Estratégia»).

2. Na mesma data, a Comissão adotou uma proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União ([2]) (a seguir «a proposta de Diretiva» ou «a Proposta»). Esta Proposta foi enviada à AEPD para consulta em 7 de fevereiro de 2013.

3. Antes da adoção da Comunicação Conjunta e da Proposta, a AEPD teve a oportunidade de apresentar observações informais à Comissão. A AEPD congratula-se com o facto de algumas das suas observações terem sido tomadas em consideração na Comunicação Conjunta e na Proposta.

4. **Conclusões**

74. A AEPD congratula-se com o facto de a Comissão e a Alta Representante da UE para os Negócios Estrangeiros e a Política de Segurança terem apresentado uma Estratégia para a cibersegurança abrangente, complementada por uma proposta de Diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação (SRI) em toda a UE. A Estratégia complementa as medidas políticas já desenvolvidas pela UE no domínio da segurança das redes e da informação.

75. A AEPD congratula-se com o facto de a Estratégia ir além da abordagem tradicional de opor a segurança à privacidade, optando antes pelo reconhecimento explícito da privacidade e da proteção de dados como valores fundamentais que devem orientar a política sobre cibersegurança na UE e a nível internacional. A AEPD sublinha que a Estratégia para a cibersegurança e a proposta de Diretiva no domínio da SRI podem dar um contributo fundamental para a garantia da proteção dos direitos das pessoas à privacidade e à proteção dos dados no ambiente em linha. Simultaneamente, importa assegurar que não conduzirão a medidas que constituiriam ingerências ilícitas nos direitos à privacidade e à proteção de dados.

76. A AEPD congratula-se ainda com o facto de a proteção de dados ser várias vezes mencionada ao longo da Estratégia e ser tomada em consideração na proposta de Diretiva sobre SRI. No entanto, lamenta que a Estratégia e a proposta de Diretiva não deem maior destaque ao contributo da atual e futura legislação sobre proteção de dados para a segurança e não assegurem plenamente a complementaridade entre as obrigações resultantes da proposta de Diretiva ou de outros elementos da Estratégia e as obrigações em matéria de proteção de dados, evitando sobreposições e contradições entre as mesmas.

77. Além disso, a AEPD salienta que a Estratégia para a cibersegurança não toma plenamente em consideração outras iniciativas paralelas da Comissão e processos legislativos em curso, tais como a Reforma da Proteção de Dados e a proposta de Regulamento relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas, o que a impede de traçar um quadro verdadeiramente abrangente e

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

holístico da cibersegurança na UE e contribui para perpetuar uma abordagem fragmentada e compartimentalizada. A AEPD sublinha igualmente que a proposta de Diretiva sobre SRI também ainda não permite uma abordagem exaustiva da segurança na UE e que a obrigação estabelecida na legislação sobre proteção de dados é provavelmente a obrigação mais abrangente em matéria de redes e segurança prevista na legislação da UE.

78. A AEPD lamenta ainda que o importante papel que as autoridades de proteção de dados desempenham na aplicação e execução das obrigações em matéria de segurança e no reforço da cibersegurança também não seja devidamente considerado.

79. No que respeita à Estratégia para a cibersegurança, a AEPD sublinha que:

— é particularmente importante dispor de uma definição clara dos termos «resiliência do ciberespaço», «cibercrime» e «ciberdefesa», dado que são utilizados como justificação para a adoção de certas medidas especiais suscetíveis de interferir nos direitos fundamentais, nomeadamente nos direitos à privacidade e à proteção dos dados. Porém, as definições de «cibercrime» dadas na Estratégia e na Convenção sobre o Cibercrime são ainda muito latas. Seria aconselhável adotar uma definição clara e *restrita* de «cibercrime» ao invés de uma definição geral;

— a legislação sobre proteção de dados deve aplicar-se a todas as ações da Estratégia sempre que digam respeito a medidas que impliquem o tratamento de dados pessoais. Embora a legislação sobre proteção de dados não seja especificamente mencionada nas secções relacionadas com cibercrime e ciberdefesa, a AEPD sublinha que muitas das ações programadas nestes domínios envolveriam o tratamento de dados pessoais e, como tal, estariam sujeitas à legislação aplicável em matéria de proteção de dados. A AEPD observa ainda que muitas ações consistem na criação de mecanismos de cooperação, que exigirão a implementação de salvaguardas adequadas em matéria de proteção dos dados relativamente às modalidades de intercâmbio de dados pessoais;

— as autoridades de proteção dos dados (APD) desempenham um importante papel no contexto da cibersegurança. Enquanto guardiãs dos direitos à privacidade e à proteção dos dados das pessoas, as APD promovem ativamente a proteção dos seus dados pessoais, tanto em linha (*online*) como não em linha (*offline*). Por conseguinte, na qualidade de entidades supervisoras, devem participar, de forma adequada, na aplicação de medidas que envolvam o tratamento de dados pessoais (tais como o lançamento do projeto-piloto da UE para combater os *botnets* e o *malware*). Outros intervenientes no campo da cibersegurança também devem cooperar com as APD no desempenho das suas funções, nomeadamente no intercâmbio de melhores práticas e em ações de sensibilização. A AEPD e as APD nacionais devem igualmente participar, a um nível adequado, na conferência de alto nível que será organizada em 2014, a fim de avaliar os progressos alcançados na implementação da Estratégia.

80. No que respeita à proposta de Diretiva sobre SRI, a AEPD aconselha os legisladores a:

— conferir maior clareza e segurança jurídica à definição de operadores de mercado abrangidos pela Proposta, que consta do artigo 3.º, n.º 8, e elaborar uma lista exaustiva de todas as partes interessadas relevantes, com vista a assegurar uma abordagem totalmente harmonizada e integrada à segurança dentro da UE;

— esclarecer, no artigo 1.º, n.º 2, alínea c), que a proposta de Diretiva é aplicável às instituições e organismos da UE, e incluir uma referência ao Regulamento (CE) n.º 45/2001 no artigo 1.º, n.º 5, da Proposta;

— reconhecer um papel mais horizontal a esta Proposta em matéria de segurança, estabelecendo expressamente no artigo 1.º que é aplicável sem prejuízo de regras mais detalhadas, atuais ou futuras, em domínios específicos (tais como aquelas a que estarão sujeitos os prestadores de serviços de confiança nos termos da proposta de Regulamento relativo à identificação eletrónica);

— aditar um considerando que explique a necessidade de incorporar a proteção de dados de raiz e por defeito numa fase precoce da conceção dos mecanismos estabelecidos na Proposta e ao longo de todo o ciclo de vida dos processos, procedimentos, organizações, técnicas e infraestruturas envolvidos, tomando em consideração a proposta de Regulamento relativo à proteção de dados;

— clarificar as definições de «redes e sistemas informáticos» no artigo 3.º, n.º 1, e de «incidente» no artigo 3.º, n.º 4, e substituir, no artigo 5.º, n.º 2, a obrigação de elaborar um «plano de avaliação dos riscos» pela «criação e manutenção de um quadro de gestão dos riscos»;

— especificar, no artigo 1.º, n.º 6, que o tratamento de dados pessoais seria justificado ao abrigo do artigo 7.º, alínea e), da Diretiva 95/46/CE, na medida em que fosse necessário para alcançar os objetivos de interesse público prosseguidos pela proposta de Diretiva. Contudo, importa assegurar o respeito pelos princípios da necessidade e da proporcionalidade, a fim de que apenas sejam tratados os dados estritamente necessários para o objetivo a alcançar;

— definir, no artigo 14.º, os casos em que é necessária uma notificação, bem como o conteúdo e o formato da mesma, incluindo os tipos de dados pessoais que devem ser notificados e se a notificação e os documentos que a acompanham incluirão ou não (e em que medida) informações sobre os dados pessoais afetados por um incidente específico de segurança (tais como endereços IP). Importa ter em conta o facto de que as autoridades competentes em matéria de SRI só devem ser autorizadas a recolher e tratar dados pessoais no contexto de um incidente de segurança quando tal for estritamente necessário. Devem ser igualmente estabelecidas na Proposta salvaguardas apropriadas para garantir uma proteção adequada dos dados tratados pelas autoridades competentes em matéria de SRI;

— esclarecer, no artigo 14.º, que as notificações de incidentes previstas no n.º 2 são aplicáveis sem prejuízo das obrigações de notificação de violações de dados pessoais previstas na legislação aplicável em matéria de proteção de dados. Devem ser estabelecidos na Proposta os principais aspetos do procedimento de cooperação entre as autoridades competentes em matéria de SRI e as APD nos casos em que o incidente de segurança envolva a violação de dados pessoais;

— alterar o artigo 14.º, n.º 8, para que a exclusão das microempresas do âmbito da notificação não seja aplicável aos operadores que desempenhem um papel crucial na prestação de serviços da sociedade da informação, nomeadamente face à natureza das informações que tratam (por exemplo, dados biométricos ou dados sensíveis);

— aditar à Proposta disposições que regulem o posterior intercâmbio de dados pessoais entre as autoridades competentes em matéria de SRI e outros destinatários, a fim de assegurar que i) os dados pessoais serão unicamente divulgados a destinatários que necessitem de proceder ao seu tratamento para o desempenho das suas funções em conformidade com uma base jurídica adequada e ii) tais informações limitar-se-ão ao que for necessário para o desempenho das suas funções. Deve ser igualmente ponderado o modo como as entidades que fornecem dados à rede de partilha de informações asseguram a conformidade com o princípio da limitação da finalidade;

— especificar o prazo máximo de conservação de dados pessoais para os efeitos estabelecidos na proposta de Diretiva, em especial no que diz respeito à conservação desses dados pelas autoridades competentes em matéria de SRI e dentro da infraestrutura segura da rede de cooperação;

— relembrar às autoridades competentes em matéria de SRI o seu dever de fornecer às pessoas em causa informações adequadas sobre o tratamento de dados pessoais, publicando, por exemplo, uma política de privacidade no seu sítio Web;

— aditar uma disposição sobre o nível de segurança que as autoridades competentes em matéria de SRI devem cumprir em relação às informações recolhidas, tratadas e trocadas. Deve ser feita expressamente referência aos requisitos de segurança previstos no artigo 17.º da Diretiva 95/46/CE relativamente à proteção de dados pessoais pelas autoridades competentes em matéria de SRI;

— esclarecer, no artigo 9.º, n.º 2, que os critérios de participação de um Estado-Membro no sistema seguro de partilha de informações devem assegurar a garantia de um elevado nível de segurança e resiliência por todos os participantes no sistema em todas as etapas do tratamento. Estes critérios devem incluir medidas de confidencialidade e segurança adequadas, em conformidade com os artigos 16.º e 17.º da Diretiva 95/46/CE e dos artigos 21.º e 22.º do Regulamento (CE) n.º 45/2001. A Comissão deve estar expressamente vinculada a esses critérios em relação à sua participação no sistema seguro de partilha de informações na qualidade de responsável pelo tratamento;

— incluir, no artigo 9.º, uma descrição das funções e responsabilidades da Comissão e dos Estados-Membros na criação, gestão e manutenção do sistema seguro de partilha de informações, e estabelecer que a conceção do sistema deve obedecer aos princípios da proteção de dados, de raiz e por defeito, e aos da segurança, de raiz; e

— especificar, no artigo 13.º, que as transferências de dados pessoais para destinatários localizados em países fora da UE devem cumprir o disposto nos artigos 25.º e 26.º da Diretiva 95/46/CE e no artigo 9.º do Regulamento (CE) n.º 45/2001.

Feito em Bruxelas, em 14 de junho de 2013.

Peter HUSTINX

Autoridade Europeia para a Proteção de Dados