



PARLAMENTO EUROPEU

2009 - 2014

---

*Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos*

---

**2013/0027(COD)**

15.1.2014

## **PARECER**

da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

dirigido à Comissão do Mercado Interno e da Proteção dos Consumidores

sobre a 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  
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Relator de parecer: Carl Schlyter

PA\_Legam

## JUSTIFICAÇÃO SUCINTA

A diretiva proposta tem por objetivo garantir um elevado nível de segurança das redes e da informação na UE. O relator apoia os objetivos da proposta, pelo que recomenda alterações para melhorar a segurança jurídica, reforçar as salvaguardas e a proteção dos indivíduos e da sua privacidade, de forma a garantir o controlo dos seus dados pessoais e a confiança no ambiente digital, a criação de uma cultura de gestão de risco e uma melhor partilha de informação entre entidades privadas e públicas.

As alterações propostas visam reforçar a referência à legislação em matéria de proteção de dados, deixar claro que a «infraestrutura crítica» não deve incluir redes sociais e lojas de aplicações em linha (ver lista atualizada no Anexo II) e, ainda, garantir o respeito da proporcionalidade, destacando a vertente civil da tarefa: a maioria das perturbações e as causas mais comuns de falhas do sistema não são ataques cibernéticos por parte de terroristas, criminosos ou espões estrangeiros, mas sim causas não intencionais, erros humanos e causas naturais. É fundamental que a UE estabeleça a diferença entre a aplicação da legislação proposta e qualquer forma de militarização deste assunto, excluindo os objetivos da indústria da segurança e vigilância, tendo em conta o contexto de um mercado digital mundializado.

Uma das preocupações importantes gira em torno da relação entre o sistema proposto e o sistema de notificação proposto pelo regulamento geral sobre proteção dos dados, assim como da coexistência eficaz de ambos, uma das razões pelas quais destacamos que qualquer legislação da UE em matéria de cibersegurança só deve ser adotada após o regulamento geral sobre proteção dos dados, e não precedê-lo. Além disso, devem ser tidas em conta as verdadeiras implicações financeiras e administrativas, incluindo a totalidade dos custos societários e não apenas os custos de uma notificação. As empresas que são descuidadas na forma como elaboram os seus programas informáticos, poupando, assim, dinheiro mas expondo os seus clientes, nem sempre podem invocar as condições normais de utilização para se exonerarem da responsabilidade pelo mau funcionamento dos seus programas. Estas empresas devem beneficiar de incentivos para garantir que os programas sejam razoavelmente seguros. Por fim, devem ser esclarecidos, e não deixados à interpretação dos Estados-Membros, certos conceitos centrais (como, por exemplo, o significado de «administrações públicas», «impacto significativo» e uma definição concreta de «cibercrime»).

## ALTERAÇÕES

A Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos insta a Comissão do Mercado Interno e da Proteção dos Consumidores, competente quanto à matéria de fundo, a incorporar as seguintes alterações no seu relatório:

### **Alteração 1**

#### **Proposta de diretiva**

#### **Considerando 1**

*Texto da Comissão*

(1) As redes e os sistemas e serviços informáticos desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para as atividades económicas e o bem-estar social e, em especial, para o funcionamento do mercado interno.

*Alteração*

(1) As redes e os sistemas e serviços informáticos desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para as atividades económicas e o bem-estar social e para as comunicações *e os intercâmbios entre as pessoas, as organizações da sociedade civil e as empresas, bem como para a proteção e o respeito da vida privada e dos dados pessoais.*

**Alteração 2**

**Proposta de diretiva  
Considerando 2**

*Texto da Comissão*

(2) A amplitude e a frequência de incidentes de segurança deliberados ou acidentais está a aumentar e constitui uma importante ameaça para o funcionamento das redes e dos sistemas informáticos. Esses incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a confiança dos utilizadores e causar graves prejuízos à economia da União.

*Alteração*

(2) A amplitude e a frequência de incidentes de segurança deliberados ou acidentais está a aumentar e constitui uma importante ameaça para o funcionamento das redes e dos sistemas informáticos. Esses incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a confiança dos utilizadores e causar graves prejuízos à economia da União. *Há um reconhecimento cada vez mais amplo de que os sistemas de controlo são vulneráveis a ataques informáticos de várias origens, incluindo governos hostis, grupos terroristas e outros intrusos maliciosos. A realização de ataques inteligentes e coordenados pode ter um impacto considerável na estabilidade, desempenho e situação económica das infraestruturas.*

**Alteração 3**

**Proposta de diretiva  
Considerando 3**

*Texto da Comissão*

(3) Enquanto instrumentos de comunicação sem fronteiras, os sistemas de informação digitais, e essencialmente a Internet, desempenham um papel crucial na facilitação da circulação transfronteiras de mercadorias, serviços e pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas num Estado-Membro podem igualmente afetar outros Estados-Membros e a União no seu conjunto. Por consequência, a resiliência e a estabilidade das redes e dos sistemas informáticos é essencial para o bom funcionamento do mercado interno.

*Alteração*

(3) Enquanto instrumentos de comunicação sem fronteiras, os sistemas de informação digitais, e essencialmente a Internet, desempenham um papel crucial na facilitação da circulação transfronteiras de mercadorias, serviços e pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas num Estado-Membro podem igualmente afetar outros Estados-Membros e a União no seu conjunto. Por consequência, a resiliência e a estabilidade das redes e dos sistemas informáticos é essencial para o bom funcionamento do mercado interno *e para as comunicações e os intercâmbios entre as pessoas, as organizações da sociedade civil e as empresas.*

**Alteração 4**

**Proposta de diretiva  
Considerando 3-A (novo)**

*Texto da Comissão*

*Alteração*

*(3-A) Uma vez que as causas mais comuns de falhas do sistema continuam a ser não intencionais, como causas naturais ou erros humanos, a infraestrutura deve ser resiliente a perturbações voluntárias e involuntárias, e os operadores da infraestrutura crítica devem conceber sistemas assentes na resiliência que se mantenham operacionais mesmo que falhem outros sistemas fora do seu controlo.*

**Alteração 5**

**Proposta de diretiva  
Considerando 6-A (novo)**

*Texto da Comissão*

*Alteração*

***(6-A) O reconhecimento da incerteza inerente aos sistemas complexos que nos sustentam é fundamental. Tal exige um melhor entendimento comum sobre o que é essencial entre os que protegem uma organização e os que definem a sua direção estratégica.***

## **Alteração 6**

### **Proposta de diretiva Considerando 8**

*Texto da Comissão*

*Alteração*

(8) As disposições da presente diretiva devem ser interpretadas sem prejuízo da possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos seus interesses essenciais em matéria de segurança, proteger a ordem e a segurança públicas e permitir a investigação, deteção e sanção das infrações penais. Nos termos do artigo 346.º do TFUE, nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança.

(8) As disposições da presente diretiva devem ser interpretadas sem prejuízo da possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos seus interesses essenciais em matéria de segurança, proteger a ordem e a segurança públicas e permitir a investigação, deteção e sanção das infrações penais, ***desde que tal não lhes sirva de pretexto para não cumprirem as obrigações de caráter mais geral em matéria de respeito da proteção da vida privada e dos dados pessoais.*** Nos termos do artigo 346.º do TFUE, nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança.

## **Alteração 7**

### **Proposta de diretiva Considerando 9**

*Texto da Comissão*

*Alteração*

(9) A fim de atingir e manter um nível elevado comum de segurança das redes e

(9) A fim de atingir e manter um nível elevado comum de segurança das redes e

dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes.

dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes, ***respeitando e protegendo a vida privada e os dados pessoais.***

## Alteração 8

### Proposta de diretiva Considerando 10

#### *Texto da Comissão*

(10) Para permitir a aplicação eficaz das disposições adotadas ao abrigo da presente diretiva, em cada Estado-Membro deverá ser criada ou designada uma entidade responsável pela coordenação das questões da SRI e que sirva de ponto focal para a cooperação transfronteiras a nível da União. Estas entidades deverão dispor de recursos técnicos, financeiros e humanos adequados para garantir a realização eficaz e eficiente das tarefas que lhes sejam atribuídas e assim alcançar os objetivos da presente diretiva.

#### *Alteração*

(10) Para permitir a aplicação eficaz das disposições adotadas ao abrigo da presente diretiva, em cada Estado-Membro deverá ser criada ou designada uma autoridade ***nacional competente sob controlo civil e operacionalmente sujeita a supervisão e transparência integralmente democráticas, que seja*** responsável pela coordenação das questões da SRI e que sirva de ponto focal para a cooperação transfronteiras a nível da União. Estas entidades deverão dispor de recursos técnicos, financeiros e humanos adequados para garantir a realização eficaz e eficiente das tarefas que lhes sejam atribuídas e assim alcançar os objetivos da presente diretiva.

## Alteração 9

### Proposta de diretiva Considerando 14-A (novo)

***(14-A) Outros setores recorrem a serviços em nuvem nos seus ambientes informáticos, nomeadamente serviços de TI que operam infraestruturas críticas. São necessárias medidas de segurança suficientes para garantir a confidencialidade, a integridade e a disponibilidade das informações registadas em nuvem. O alojamento de serviços de infraestruturas e o armazenamento de dados sensíveis em ambiente de nuvem acarretam exigências em termos de segurança e de resiliência a que os atuais serviços em nuvem não estão em condições de dar resposta. Por conseguinte, é necessário garantir que o ambiente informático em nuvem pode proteger devidamente os dados sensíveis das infraestruturas críticas.***

## Alteração 10

### Proposta de diretiva Considerando 15

(15) Uma vez que a maioria das redes e dos sistemas informáticos é explorada pelo setor privado, a cooperação entre este setor e o setor público é essencial. Os operadores do mercado deverão ser encorajados a prosseguir os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e da informação. Deverão também cooperar com o setor público e partilhar informações e boas práticas em troca de apoio operacional em caso de incidentes.

(15) Uma vez que a maioria das redes e dos sistemas informáticos é explorada pelo setor privado, a cooperação entre este setor e o setor público é essencial. Os operadores do mercado deverão ser encorajados a prosseguir os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e da informação. Deverão também cooperar com o setor público e partilhar ***mutuamente*** informações e boas práticas, ***além de apoio operacional recíproco, necessário*** em caso de incidentes.

## Alteração 11

### Proposta de diretiva Considerando 15-A (novo)

*Texto da Comissão*

*Alteração*

***(15-A) Os mecanismos de cooperação nacionais entre os operadores públicos e privados já em aplicação devem ser integralmente respeitados, sempre que possível e de acordo com a Diretiva 95/46/CE, e as disposições da presente diretiva não devem pôr em causa essas disposições de cooperação vigentes.***

## Alteração 12

### Proposta de diretiva Considerando 16

*Texto da Comissão*

*Alteração*

(16) Para garantir a transparência e informar devidamente os cidadãos e os operadores do mercado da UE, as autoridades competentes deverão criar um sítio Web comum para publicar informações não confidenciais sobre os incidentes e riscos.

(16) Para garantir a transparência e informar devidamente os cidadãos e os operadores do mercado da UE, as autoridades competentes deverão criar um sítio Web comum para ***publicação atempada e exaustiva de*** informações não confidenciais sobre os incidentes e riscos.

## Alteração 13

### Proposta de diretiva Considerando 21

*Texto da Comissão*

*Alteração*

(21) Dado o caráter global dos problemas de SRI, é necessário reforçar a cooperação internacional para melhorar as normas de segurança e o intercâmbio de informações e promover uma abordagem comum global das questões de SRI.

(21) Dado o caráter global dos problemas de SRI, é necessário reforçar a cooperação internacional para melhorar as normas de segurança e o intercâmbio de informações e promover uma abordagem comum global das questões de SRI, ***desde que os Estados com os quais está prevista esta cooperação estejam dotados de***

*instrumentos de controlo e de proteção dos dados que garantam o mesmo nível de qualidade dos da UE.*

## Alteração 14

### Proposta de diretiva Considerando 22

#### *Texto da Comissão*

(22) As responsabilidades na garantia da SRI incumbem, em grande medida, às administrações públicas e ***aos operadores do mercado***. Dever-se-á promover e desenvolver uma cultura de gestão dos riscos, que abranja a avaliação dos riscos e a implementação de medidas de segurança ***adequadas aos riscos enfrentados*** através de requisitos regulamentares adequados e práticas setoriais voluntárias. Estabelecer condições de concorrência equitativas é também essencial para um funcionamento eficaz da rede de cooperação tendo em vista assegurar a eficácia da cooperação entre todos os Estados-Membros.

#### *Alteração*

(22) As responsabilidades na garantia da SRI incumbem, em grande medida, às administrações públicas e ***às empresas***. Dever-se-á promover e desenvolver uma cultura de gestão dos riscos que abranja a avaliação dos riscos e a implementação de medidas de segurança ***procurando antever os incidentes de segurança, deliberados ou acidentais***, através de requisitos regulamentares adequados e práticas setoriais apropriadas. ***Onde já estiver implantada – e sobretudo se assentar em práticas voluntárias –, essa cultura de gestão dos riscos deve ser apoiada, reforçada e partilhada***. Estabelecer condições de concorrência equitativas é também essencial para um funcionamento eficaz da rede de cooperação tendo em vista assegurar a eficácia da cooperação entre todos os Estados-Membros.

## Alteração 15

### Proposta de diretiva Considerando 22-A (novo)

#### *Texto da Comissão*

#### *Alteração*

***(22-A) As administrações públicas e as empresas privadas, incluindo os prestadores de serviços de redes, de informações e de software, devem encarar a proteção dos seus sistemas de informação e dos dados contidos nos mesmos como inerentes ao seu dever de***

*diligência. Devem ser oferecidos níveis de proteção adaptados contra ameaças razoavelmente identificáveis. Os custos e peso dessa proteção devem refletir os danos prováveis sofridos pelas pessoas afetadas na sequência de um ataque informático.*

## Alteração 16

### Proposta de diretiva Considerando 26-A (novo)

*Texto da Comissão*

*Alteração*

*(26-A) As crianças estão expostas desde muito novas à Internet e a outras novas tecnologias, bem como às ameaças delas decorrentes. A boa administração de um espaço em linha seguro para as crianças é fundamental para minimizar os danos e garantir que a proteção das crianças e dos seus direitos não seja comprometida;*

## Alteração 17

### Proposta de diretiva Considerando 28

*Texto da Comissão*

*Alteração*

(28) As autoridades competentes deverão esforçar-se por manter canais informais e de confiança para a partilha de informações entre os operadores do mercado e entre o setor público e o setor privado. ***Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes comunicados às autoridades competentes e o interesse do público em ser informado acerca das ameaças que comportem eventuais danos comerciais e de reputação para as administrações públicas e os operadores do mercado que comunicam esses incidentes. No cumprimento das obrigações de***

(28) As autoridades competentes deverão esforçar-se por manter canais informais e de confiança para a partilha de informações entre os operadores do mercado e entre o setor público e o setor privado. ***Na publicidade dada aos incidentes comunicados às autoridades competentes, o interesse do público em ser informado acerca das ameaças deve ter primazia sobre considerações económicas de curto prazo.***

*notificação, as autoridades competentes deverão ter em especial atenção a necessidade de manter as informações sobre as vulnerabilidades dos produtos estritamente confidenciais antes da divulgação das medidas de segurança adequadas para as resolver.*

## **Alteração 18**

**Proposta de diretiva  
Considerando 29-A (novo)**

*Texto da Comissão*

*Alteração*

*(29-A) Uma utilização fraudulenta da Internet dá ao crime organizado a possibilidade de expandir as suas atividades em linha para fins de lavagem de dinheiro e de contrafação, além de outras violações do direito de propriedade intelectual, bem como de testar novas atividades criminosas, revelando assim uma assustadora capacidade de adaptação às novas tecnologias;*

## **Alteração 19**

**Proposta de diretiva  
Considerando 30-A (novo)**

*Texto da Comissão*

*Alteração*

*(30-A) A cibercriminalidade provoca cada vez mais danos económicos e sociais, afetando milhões de consumidores e originando perdas anuais estimadas em 290 mil milhões de euros<sup>4a</sup>;*

---

*<sup>4-A</sup> Segundo o relatório Norton sobre cibercriminalidade, de 2012.*

## Alteração 20

### Proposta de diretiva Considerando 33

#### *Texto da Comissão*

(33) A Comissão deverá rever periodicamente a presente diretiva, nomeadamente para decidir da eventual necessidade de alterações à luz da evolução tecnológica ou do mercado.

#### *Alteração*

(33) A Comissão deverá rever periodicamente a presente diretiva, nomeadamente para decidir da eventual necessidade de alterações à luz da evolução tecnológica ou do mercado *e das obrigações que visam o nível máximo de segurança e de integridade das redes e da informação e da proteção da vida privada e dos dados pessoais.*

## Alteração 21

### Proposta de diretiva Considerando 39

#### *Texto da Comissão*

(39) A partilha de informações sobre os riscos e incidentes na rede de cooperação e o cumprimento da obrigatoriedade de notificação de incidentes às autoridades nacionais competentes podem requerer o tratamento de dados pessoais. Esse tratamento é necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva *e é, pois*, legítimo, nos termos do artigo 7.º da Diretiva 95/46/CE. Não *constitui, em relação a estes objetivos legítimos, uma interferência desproporcionada e intolerável que lese a própria essência do* direito à proteção de dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais. Na aplicação da presente diretiva, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da

#### *Alteração*

(39) A partilha de informações sobre os riscos e incidentes na rede de cooperação e o cumprimento da obrigatoriedade de notificação de incidentes às autoridades nacionais competentes podem requerer o tratamento de dados pessoais. *Se* esse tratamento *for* necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva *pode ser* legítimo, nos termos do artigo 7.º da Diretiva 95/46/CE. Não *obstante*, não *dispensam as autoridades competentes de interferência proporcionada que não seja suscetível de lesar o* direito à proteção dos dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais. Na aplicação da presente diretiva, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão<sup>8</sup>,

Comissão<sup>8</sup>, deve aplicar-se conforme adequado. Nos casos em que os dados sejam tratados pelas instituições e órgãos da União, esse tratamento para efeitos de aplicação da presente diretiva deve ser conforme com o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

---

<sup>8</sup> JO L 145 de 31.5.2001, p. 43.

deve aplicar-se conforme adequado. Nos casos em que os dados sejam tratados pelas instituições e órgãos da União, esse tratamento para efeitos de aplicação da presente diretiva deve ser conforme com o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

---

<sup>8</sup> JO L 145 de 31.5.2001, p. 43.

## Alteração 22

### Proposta de diretiva Considerando 41-A (novo)

*Texto da Comissão*

*Alteração*

***(41-A) Considerando que em todas as medidas é necessário assegurar a proteção dos direitos humanos fundamentais, em particular dos direitos referidos na CEDH (artigo 8º, respeito pela vida privada), e garantir o cumprimento do «princípio da proporcionalidade».***

## Alteração 23

### Proposta de diretiva Artigo 1 – n.º 5

*Texto da Comissão*

*Alteração*

5. A presente diretiva ***também não prejudica a aplicação*** da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados

5. A presente diretiva ***respeita integralmente as disposições*** da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados

personais e à livre circulação desses dados<sup>10</sup>, **nem** da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, **nem** do Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados<sup>11</sup>.

<sup>10</sup> JO L 281 de 23.11.1995, p. 31.

<sup>11</sup> SEC(2012) 72 final.

personais e à livre circulação desses dados, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, e do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, **de 18 de dezembro de 2000**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais **pelas instituições e pelos órgãos comunitários** e à livre circulação desses dados.

<sup>8</sup> JO L 281 de 23.11.95, p. 31.

<sup>11</sup> SEC(2012) 72 final.

## Alteração 24

### Proposta de diretiva Artigo 2

#### *Texto da Comissão*

Os Estados-Membros não devem ser impedidos de adotar ou manter disposições que assegurem um nível de segurança superior, desde que tal não prejudique o cumprimento das obrigações que lhes incumbem por força da legislação da União.

#### *Alteração*

Os Estados-Membros não devem ser impedidos de adotar ou manter disposições que assegurem um nível de segurança superior, desde que tal não prejudique o cumprimento das obrigações que lhes incumbem por força da legislação da União; **contudo, tais disposições devem observar as expectativas mínimas comuns que sejam aplicáveis neste caso e estejam consagradas na presente diretiva.**

## Alteração 25

### Proposta de diretiva Artigo 3 – n.º 2

#### *Texto da Comissão*

(2) «Segurança»: a capacidade de uma rede ou sistema informático para resistir, **com um dado nível de confiança**, a eventos acidentais ou a ações dolosas que

#### *Alteração*

(2) «Segurança»: a capacidade de uma rede ou sistema informático para resistir a eventos acidentais ou a ações dolosas que comprometem a disponibilidade,

comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema;

autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema;

## Alteração 26

### Proposta de diretiva Artigo 3 – n.º 2 – alínea a) (nova)

*Texto da Comissão*

*Alteração*

***a) «Resiliência cibernética»: a capacidade de uma rede ou de um sistema informático resistir e recuperar a plena capacidade operacional após incidentes, incluindo, entre outros: avarias técnicas, falhas de energia ou incidentes relacionados com a segurança;***

## Alteração 27

### Proposta de diretiva Artigo 3 – n.º 4

*Texto da Comissão*

*Alteração*

4. «Incidente»: qualquer circunstância ou evento com um efeito adverso real na segurança;

4. «Incidente»: qualquer circunstância ou evento com um efeito adverso real na segurança ***e na prestação de serviços essenciais;***

## Alteração 28

### Proposta de diretiva Artigo 3 – n.º 8 – alínea b)

*Texto da Comissão*

*Alteração*

(b) um operador de infraestruturas críticas essenciais para a manutenção de atividades ***económicas e sociais*** vitais nos domínios da energia, dos transportes, da banca, da

(b) um operador de infraestruturas críticas essenciais para a manutenção de atividades ***sociais e económicas*** vitais nos domínios da energia, dos transportes, da banca, da

bolsa e da saúde, cuja lista não exaustiva consta do anexo II.

bolsa, *da cadeia de abastecimento alimentar* e da saúde, cuja lista não exaustiva consta do anexo II.

## Alteração 29

### Proposta de diretiva Artigo 5 – n.º 2 – alínea a)

#### *Texto da Comissão*

(a) Um plano de avaliação dos riscos para identificar os riscos e avaliar os impactos de potenciais incidentes;

#### *Alteração*

(a) Um ***quadro de gestão dos riscos que inclua, pelo menos, uma avaliação regular*** dos riscos para identificar os riscos e avaliar os impactos de potenciais incidentes ***e medidas de salvaguarda da segurança e, da integridade e da informação, incluindo um alerta rápido;***

#### *Justificação*

*Um plano de avaliação é insuficiente e não inclui outras medidas necessárias à gestão dos riscos em matéria de segurança das redes e da informação. A AEPD recomenda que seja estabelecido um quadro de gestão de riscos, que inclua uma avaliação do risco.*

## Alteração 30

### Proposta de diretiva Artigo 5 – n.º 3

#### *Texto da Comissão*

3. A estratégia e o plano de cooperação nacionais em matéria de SRI devem ser comunicados à Comissão no prazo de um mês a contar da data da sua adoção.

#### *Alteração*

3. A estratégia e o plano de cooperação nacionais em matéria de SRI devem ser comunicados à Comissão, ***ao Parlamento Europeu, ao Conselho e à Autoridade Europeia para a Proteção de Dados***, no prazo de um mês a contar da data da sua adoção, ***que deverá ter lugar o mais tardar 12 meses após a entrada em vigor da presente diretiva.***

## Alteração 31

### Proposta de diretiva

## Artigo 5 – n.º 3-A (novo)

*Texto da Comissão*

*Alteração*

***3-A. A Comissão deve elaborar uma súmula das estratégias em matéria de SRI de todos os Estados-Membros e transmitir a mesma aos Estados-Membros de uma forma organizada.***

*Justificação*

*Seria útil que todos os Estados-Membros vissem os planos uns dos outros. Tal contribuiria para determinar as respetivas abordagens, sendo inclusivamente suscetível de criar oportunidades de intercâmbio das melhores práticas.*

## Alteração 32

**Proposta de diretiva**

**Artigo 5 – n.º 3-B (novo)**

*Texto da Comissão*

*Alteração*

***3-B. No prazo de seis meses a contar da data de adoção da presente diretiva, a Comissão deve compilar um guia para a estrutura da estratégia em matéria de SRI. O objetivo consiste em ajudar os Estados-Membros a elaborar e a adotar documentos com aproximadamente a mesma estrutura.***

*Justificação*

*O trabalho de organização e de resumo a nível da Comissão pode ser mais eficaz se os 28 documentos que estão na base do trabalho aderirem a uma determinada estrutura geral. Embora não seja vinculativo, o guia da Comissão teria, ainda assim, o efeito de induzir os Estados-Membros a aderir a este modelo/estrutura recomendado quando redigirem as suas próprias estratégias nacionais.*

### Alteração 33

#### Proposta de diretiva

##### Artigo 6 – n.º 1

###### *Texto da Comissão*

1. Cada Estado-Membro designa uma autoridade nacional competente em matéria de segurança das redes e dos sistemas informáticos («autoridade competente»).

###### *Alteração*

1. Cada Estado-Membro designa uma autoridade *civil* nacional competente em matéria de segurança das redes e dos sistemas informáticos («autoridade competente»).

### Alteração 34

#### Proposta de diretiva

##### Artigo 6 – n.º 5

###### *Texto da Comissão*

5. Sempre que necessário, as autoridades competentes consultam as autoridades policiais e judiciais nacionais e as autoridades encarregadas da proteção dos dados, com elas cooperando.

###### *Alteração*

5. Sempre que necessário *e atendendo ao princípio da proporcionalidade*, as autoridades competentes consultam as autoridades policiais e judiciais *competentes* nacionais e as autoridades encarregadas da proteção dos dados, com elas cooperando *estritamente*.

### Alteração 35

#### Proposta de diretiva

##### Artigo 6 – n.º 5-A (novo)

###### *Texto da Comissão*

###### *Alteração*

*5-A. As autoridades competentes devem, no que diz respeito à informação recolhida, tratada e comunicada, respeitar os requisitos relativos à proteção de dados pessoais previstos no artigo 17.º da Diretiva 95/46/CE.*

### Alteração 36

#### Proposta de diretiva

## Artigo 7 – n.º 1

### *Texto da Comissão*

1. Cada Estado Membro cria **uma equipa** de resposta a emergências informáticas (a seguir **designada** por «CERT»), **responsável** pelo tratamento de incidentes e riscos de acordo com um processo bem definido, que deve cumprir as condições estabelecidas no anexo I, ponto 1. A CERT **pode ser** estabelecida no âmbito da autoridade competente.

### *Alteração*

1. Cada Estado Membro cria **equipas** de resposta a emergências informáticas (a seguir **designadas** por «CERT»), **responsáveis** pelo tratamento de incidentes e riscos de acordo com um processo bem definido, que deve cumprir as condições estabelecidas no anexo I, ponto 1. **Quando adequado**, a CERT **é** estabelecida no âmbito da autoridade competente.

## Alteração 37

### Proposta de diretiva

#### Artigo 8 – n.º 2

### *Texto da Comissão*

2. A rede de cooperação põe em comunicação permanente a Comissão e as autoridades competentes. Quando for solicitada, a Agência Europeia para a Segurança das Redes e da informação («ENISA») apoiará a rede de cooperação, fornecendo **conhecimentos especializados e aconselhamento**.

### *Alteração*

2. A rede de cooperação põe em comunicação permanente a Comissão e as autoridades competentes. Quando for solicitada, a Agência Europeia para a Segurança das Redes e da informação («ENISA») apoiará a rede de cooperação, fornecendo **orientações tecnológicas neutras com medidas adequadas para os setores público e privado**.

## Alteração 38

### Proposta de diretiva

#### Artigo 9 – n.º 2 – alínea b-A) (nova)

### *Texto da Comissão*

### *Alteração*

**(b-A) Os critérios de participação dos Estados-Membros no sistema de partilha de informações devem garantir a observação de um elevado nível de segurança e de resiliência por todos os participantes, em todas as etapas do tratamento, inclusive através de medidas adequadas de confidencialidade e de**

*segurança, em conformidade com os artigos 16.º e 17.º da Diretiva 95/46/CE e os artigos 21.º e 22.º do Regulamento (CE) n.º 45/2001.*

### **Alteração 39**

#### **Proposta de diretiva**

#### **Artigo 9 – n.º 3**

##### *Texto da Comissão*

*3. A Comissão adota, por meio de atos de execução, decisões sobre o acesso dos Estados-Membros a esta infraestrutura segura, de acordo com os critérios referidos nos n.ºs 2 e 3. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.º, n.º 3.*

##### *Alteração*

**Suprimido**

### **Alteração 40**

#### **Proposta de diretiva**

#### **Artigo 12 – n.º 2 – alínea a) – travessão 2**

##### *Texto da Comissão*

– uma definição dos **procedimentos e** critérios para a avaliação pela rede de cooperação dos riscos e incidentes;

##### *Alteração*

– uma definição dos critérios para a avaliação pela rede de cooperação dos riscos e incidentes;

### **Alteração 41**

#### **Proposta de diretiva**

#### **Artigo 13**

##### *Texto da Comissão*

Sem prejuízo da possibilidade de a rede de cooperação manter uma cooperação informal a nível internacional, a União pode concluir acordos internacionais com países terceiros ou organizações internacionais, que permitam e organizem

##### *Alteração*

Sem prejuízo da possibilidade de a rede de cooperação manter uma cooperação informal a nível internacional, a União pode concluir acordos internacionais com países terceiros ou organizações internacionais, que permitam e organizem

a sua participação em algumas atividades da rede de cooperação. Esses acordos **devem ter em conta a necessidade de** assegurar uma proteção adequada **dos** dados pessoais que circulam na rede de cooperação.

a sua participação em algumas atividades da rede de cooperação. Esses acordos **só são concluídos se for possível** assegurar **um nível** de proteção **adequado e comparável ao da União para os** dados pessoais que circulam na rede de cooperação.

## Alteração 42

### Proposta de diretiva

#### Artigo 14 – n.º 1

##### *Texto da Comissão*

1. Os Estados-Membros devem assegurar que as administrações públicas e os operadores do mercado adotem medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta os progressos técnicos, essas medidas devem garantir um nível de segurança adequado **em função do** risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a sua rede e sistema informático nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.

##### *Alteração*

1. Os Estados-Membros devem assegurar que as administrações públicas e os operadores do mercado adotem medidas técnicas e organizacionais adequadas para **detetar**, gerir **e limitar** efetivamente os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta os progressos técnicos, essas medidas devem garantir um nível de segurança adequado **e proporcional ao** risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a sua rede e sistema informático nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços, **bem como a segurança dos dados**, assentes nessas redes e sistemas.

## Alteração 43

### Proposta de diretiva

#### Artigo 14 – n.º 2 – alínea a) (nova)

##### *Alteração*

**(a) Em caso de negligência grosseira em matéria de proteção e segurança, os responsáveis pelo desenvolvimento de software comercial serão**

***responsabilizados independentemente das cláusulas de exoneração de responsabilidade constantes dos acordos de licença dos utilizadores.***

#### *Justificação*

*No acordo de licença, os responsáveis pelo desenvolvimento de software exoneram-se das responsabilidades que possam resultar de uma atitude displicente em termos de segurança e de uma programação de fraca qualidade. Para incentivar o investimento dos responsáveis pelo desenvolvimento de software em medidas de segurança, é necessária uma cultura diferente. Isso só será possível se os responsáveis pelo desenvolvimento de software forem responsabilizados pelas falhas de segurança.*

#### **Alteração 44**

##### **Proposta de diretiva**

##### **Artigo 14 – n.º 3**

###### *Texto da Comissão*

3. As exigências previstas nos n.ºs 1 e 2 aplicam-se a todos os operadores do mercado que fornecem serviços na União Europeia.

###### *Alteração*

3. As exigências previstas nos n.ºs 1 e 2 aplicam-se a todos os operadores do mercado ***e responsáveis pelo desenvolvimento de programas informáticos*** que fornecem serviços na União Europeia.

#### **Alteração 45**

##### **Proposta de diretiva**

##### **Artigo 14 – n.º 6**

###### *Texto da Comissão*

***6. Sob reserva de quaisquer atos delegados adotados ao abrigo do n.º 5, as autoridades competentes podem adotar orientações e, se for caso disso, emitir instruções sobre as circunstâncias em que as administrações públicas e os operadores do mercado são obrigados a notificar incidentes.***

###### *Alteração*

***Suprimido***

## Alteração 46

### Proposta de diretiva Artigo 15 – n.º 1

#### *Texto da Comissão*

1. Os Estados-Membros devem assegurar que as autoridades competentes tenham **todos** os poderes necessários para investigar os casos de incumprimento por parte das administrações públicas ou dos operadores do mercado das obrigações que lhes incumbem por força do artigo 14.º, bem como os efeitos desse incumprimento na segurança das redes e sistemas informáticos.

#### *Alteração*

1. Os Estados-Membros devem assegurar que as autoridades competentes tenham os poderes necessários para investigar os casos de incumprimento por parte das administrações públicas ou dos operadores do mercado das obrigações que lhes incumbem por força do artigo 14.º, bem como os efeitos desse incumprimento na segurança das redes e sistemas informáticos.

## Alteração 47

### Proposta de diretiva Artigo 15 – n.º 5

#### *Texto da Comissão*

5. As autoridades competentes devem trabalhar em estreita colaboração com as autoridades responsáveis pela proteção dos dados pessoais quando tratarem de incidentes de que resultou a violação desses dados.

#### *Alteração*

**5. Sem prejuízo da legislação aplicável em matéria de proteção dos dados e em consulta aprofundada aos responsáveis pelo tratamento dos dados e respetivos subcontratantes**, as autoridades competentes **e os balcões únicos** devem trabalhar em estreita colaboração com as autoridades responsáveis pela proteção dos dados pessoais quando tratarem de incidentes de que resultou a violação desses dados.

## Alteração 48

### Proposta de diretiva Artigo 19-A (novo)

#### *Texto da Comissão*

#### *Alteração*

#### **Artigo 19.º-A**

*Proteção e tratamento de dados pessoais*

*1. O tratamento de dados pessoais nos Estados-Membros ao abrigo da presente diretiva é efetuado em conformidade com a Diretiva 95/46/CE e com a Diretiva 2002/58/CE.*

*2. O tratamento de dados pessoais pela Comissão e a ENISA ao abrigo do presente regulamento é efetuado em conformidade com o Regulamento (CE) n.º 45/2001.*

*3. O tratamento de dados pessoais pelo Centro Europeu da Cibercriminalidade no seio da Europol para os fins previstos na presente diretiva é efetuado em conformidade com a Decisão 2009/371/JAI.*

*4. O tratamento de dados pessoais deve ser justo, lícito e limitar-se estritamente aos dados mínimos necessários para o fim para que são tratados. Os dados pessoais devem ser conservados de forma a permitir a identificação dos titulares de dados, mas unicamente durante o período necessário para atingir os fins para que são tratados.*

*5. As notificações de incidentes previstas no artigo 14.º são aplicáveis, sem prejuízo das disposições e obrigações relativas à notificação de violações de dados pessoais estabelecidas no artigo 4.º da Diretiva 2002/58/CE e no Regulamento (UE) n.º 611/2013.*

*6. As remissões para a Diretiva 95/46/CE serão consideradas remissões para o Regulamento [xxx] do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento geral sobre a proteção de dados), assim que o mesmo entrar em vigor.*

## Alteração 49

### Proposta de diretiva

#### Artigo 20 – parágrafo 1 (novo)

##### *Texto da Comissão*

A Comissão deve avaliar periodicamente a aplicação da presente diretiva e apresentar um relatório ao Parlamento Europeu e ao Conselho. O primeiro relatório deve ser apresentado no prazo de *três* anos após a data de transposição referida no artigo 21.º. Para o efeito, a Comissão pode solicitar aos Estados-Membros que lhe forneçam informações sem demora injustificada.

##### *Alteração*

A Comissão deve avaliar periodicamente a aplicação da presente diretiva e apresentar um relatório ao Parlamento Europeu e ao Conselho. O primeiro relatório deve ser apresentado no prazo de *dois* anos após a data de transposição referida no artigo 21.º. Para o efeito, a Comissão pode solicitar aos Estados-Membros que lhe forneçam informações sem demora injustificada.

## Alteração 50

### Proposta de diretiva

#### Anexo 1 – ponto 1 – alínea b)

##### *Texto da Comissão*

(b) A CERT deve implementar e gerir medidas de segurança destinadas a garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações que recebe e trata.

##### *Alteração*

(b) A CERT deve implementar e gerir medidas de segurança destinadas a garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações que recebe e trata, ***garantindo a proteção dos dados.***

## Alteração 51

### Proposta de diretiva

#### Anexo 2 – parágrafo 1

##### *Texto da Comissão*

Lista de operadores do mercado  
Referidos no artigo 3.º, n.º 8, alínea a)  
1. Plataformas de comércio eletrónico  
2. Portais de pagamento pela Internet  
**3. Redes sociais**

##### *Alteração*

Lista de operadores do mercado  
Referidos no artigo 3.º, n.º 8, alínea a)  
1. Plataformas de comércio eletrónico  
2. Portais de pagamento pela Internet

- 4. Motores de pesquisa
- 5. Serviços de computação em nuvem

**6. Lojas de aplicações em linha**

**Alteração 52**

**Proposta de diretiva**

**Anexo 2 – parágrafo 2 – ponto 5-A (novo)**

*Texto da Comissão*

- 3. Motores de pesquisa
- 4. Serviços de computação em nuvem ***que armazenam dados sensíveis de infraestruturas críticas da União Europeia***

*Alteração*

**5-A. Cadeia de abastecimento alimentar**

## PROCESSO

<b>Título</b>	Elevado nível comum de segurança das redes e da informação em toda a União			
<b>Referências</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)			
<b>Comissão competente quanto ao fundo</b> Data de comunicação em sessão	IMCO 15.4.2013			
<b>Parecer emitido por</b> Data de comunicação em sessão	LIBE 15.4.2013			
<b>Comissões associadas - data de comunicação em sessão</b>	12.9.2013			
<b>Relator(a) de parecer</b> Data de designação	Carl Schlyter 7.3.2013			
<b>Exame em comissão</b>	25.4.2013	18.9.2013	4.11.2013	13.1.2014
<b>Data de aprovação</b>	13.1.2014			
<b>Resultado da votação final</b>	+: -: 0:	36 6 0		
<b>Deputados presentes no momento da votação final</b>	Jan Philipp Albrecht, Roberta Angelilli, Edit Bauer, Rita Borsellino, Arkadiusz Tomasz Bratkowski, Philip Claeys, Frank Engel, Cornelia Ernst, Tanja Fajon, Monika Flašíková Beňová, Kinga Gál, Kinga Göncz, Salvatore Iacolino, Sophia in 't Veld, Timothy Kirkhope, Juan Fernando López Aguilar, Baroness Sarah Ludford, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu Houillon, Anthea McIntyre, Nuno Melo, Roberta Metsola, Claude Moraes, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Csaba Sógor, Renate Sommer, Axel Voss, Renate Weber, Josef Weidenholzer, Cecilia Wikström, Tatjana Ždanoka, Auke Zijlstra			
<b>Suplente(s) presente(s) no momento da votação final</b>	Monika Hohlmeier, Jean Lambert, Ulrike Lunacek, Jan Mulder, Carl Schlyter, Marco Scurria			
<b>Suplente(s) (nº 2 do art. 187º) presente(s) no momento da votação final</b>	Katarína Neved'alová			