Quinta-feira, 13 de março de 2014

P7_TA(2014)0244

Elevado nível comum de segurança das redes e da informação em toda a União ***I

Resolução legislativa do Parlamento Europeu, de 13 de março de 2014, 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))

(Processo legislativo ordinário: primeira leitura)

(2017/C 378/74)

O Parlamento Europeu,

— Tendo em conta a proposta da Comissão ao Parlamento e ao Conselho (COM(2013)0048),

— Tendo em conta o artigo 294.º, n.º 2, e o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, nos termos dos quais a proposta lhe foi apresentada pela Comissão (C7-0035/2013),

— Tendo em conta o artigo 294.º, n.º 3, do Tratado sobre o Funcionamento da União Europeia,

— Tendo em conta o parecer fundamentado apresentado pelo Parlamento sueco, no âmbito do Protocolo n.º 2 relativo à aplicação dos princípios da subsidiariedade e da proporcionalidade, segundo o qual o projeto de ato legislativo não respeita o princípio da subsidiariedade,

— Tendo em conta o parecer do Comité Económico e Social Europeu de 22 de maio de 2013 ([1]),

— Tendo em conta a sua resolução, de 12 de setembro de 2013, sobre a estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido ([2]),

— Tendo em conta o artigo 55.º do seu Regimento,

— Tendo em conta o relatório da Comissão do Mercado Interno e da Proteção dos Consumidores e os pareceres da Comissão da Indústria, da Investigação e da Energia, da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos e da Comissão dos Assuntos Externos (A7-0103/2014),

1. Aprova em primeira leitura a posição que se segue;

2. Requer à Comissão que lhe submeta de novo a sua proposta se pretender alterá-la substancialmente ou substituí-la por outro texto;

3. Encarrega o seu Presidente de transmitir a posição do Parlamento ao Conselho, à Comissão e aos parlamentos nacionais.

P7_TC1-COD(2013)0027

Posição do Parlamento Europeu aprovada em primeira leitura em 13 de março de 2014 tendo em vista a adoção da Diretiva 2014/…/UE 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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

---

([1]) JO C 271 de 19.9.2013, p. 133.
([2]) Textos aprovados, P7_TA(2013)0376.

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Deliberando de acordo com o processo legislativo ordinário ([2]),

Considerando o seguinte:

(1) As redes e os sistemas e serviços informáticos desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais ***para a liberdade e para a segurança geral dos cidadãos da União, bem como*** para as atividades económicas e para o bem-estar social e, em especial, para o funcionamento do mercado interno. **[Alt. 1]**

(2) A amplitude, ~~e~~ a frequência ***e o impacto*** 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 sistemas podem, igualmente, tornar-se um alvo fácil de ações prejudiciais deliberadas, destinadas a danificar ou a interromper a operação dos sistemas.*** Esses incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a confiança dos utilizadores e ***dos investidores, e*** causar graves prejuízos à economia da União, ***e em última instância, pôr em risco o bem-estar dos cidadãos da União e a capacidade de os Estados-Membros garantirem a sua própria proteção, bem como a segurança das infraestruturas críticas***. **[Alt. 2]**

(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.

(3-A) Uma vez que as causas mais comuns de falhas do sistema continuam a ser involuntárias, como causas naturais ou erros humanos, a infraestrutura deverá ser resistente a perturbações voluntárias e involuntárias, e os operadores da infraestrutura crítica deverão conceber sistemas assentes na resiliência. **[Alt. 3]**

(4) Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a ***prevenção,*** deteção e resposta coordenadas a ameaças à segurança das redes e da informação («SRI»). Para que esse mecanismo seja eficaz e inclusivo, é indispensável que todos os Estados-Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de SRI no seu território. Deverão também aplicar-se requisitos mínimos de segurança ~~às administrações públicas e aos~~***, pelo menos a determinados*** operadores ***de mercado*** das infraestruturas ~~críticas~~ de informação, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves. ***As empresas cotadas em bolsa devem ser incentivadas a publicar voluntariamente os incidentes nos seus relatórios financeiros. O quadro jurídico deve basear-se na necessidade de salvaguardar a privacidade e a integridade dos cidadãos. A Rede de Alerta para as Infraestruturas Críticas (RAIC) deverá ser alargada aos operadores de mercado abrangidos pela presente diretiva.*** **[Alt. 4]**

(4-A) Tendo em conta que as administrações públicas, devido à sua missão pública, deverão ser diligentes na gestão e na proteção da sua própria rede e dos seus próprios sistemas informáticos, a presente diretiva deverá centrar-se nas infraestruturas essenciais para a manutenção de atividades socioeconómicas vitais nos domínios da energia, dos transportes, da banca, das infraestruturas de mercado financeiro e da saúde. Os responsáveis pelo desenvolvimento de software e os fabricantes de hardware deverão ser excluídos do âmbito de aplicação da presente diretiva. **[Alt. 5]**

([1]) JO C 271 de 19.9.2013, p. 133.
([2]) Posição do Parlamento Europeu de 13 de março de 2014.

(4-B) A cooperação e a coordenação entre as autoridades pertinentes da União — a Alta Representante/Vice-Presidente, responsável pela Política Externa e de Segurança Comum e pela Política Comum de Segurança e de Defesa, e o Coordenador da luta antiterrorismo da UE — deverão ser garantidas sempre que incidentes com um impacto importante sejam considerados de natureza externa e terrorista. **[Alt. 6]**

(5) No intuito de cobrir todos os incidentes e riscos pertinentes, a presente diretiva deverá aplicar-se a todas as redes e sistemas informáticos. As obrigações que recaem sobre as administrações públicas e os operadores de mercado não deverão, no entanto, aplicar-se às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho ([1]), que estejam sujeitas aos requisitos específicos de segurança e integridade estabelecidos no artigo 13.º-A da referida diretiva, nem se devem aplicar aos prestadores de serviços de confiança.

(6) As capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e da informação na União. Os Estados-Membros possuem níveis muito diversos de preparação que conduzem a abordagens fragmentadas em toda a União. Esta situação conduziria a um nível desigual de defesa dos consumidores e das empresas e compromete o nível global de SRI na União. Por sua vez, a inexistência de requisitos mínimos comuns a respeitar ~~pelas administrações públicas e~~ pelos operadores do mercado torna impossível criar um mecanismo eficaz e global para a cooperação a nível da União. ***As universidades e os centros de investigação desempenham um papel determinante para estimular a investigação, o desenvolvimento e a inovação nessas áreas, e deverão ser dotados de financiamento adequado.*** **[Alt. 7]**

(7) Uma resposta eficaz aos desafios que se colocam à segurança das redes e dos sistemas informáticos exige, assim, uma abordagem global a nível da União, que abranja os requisitos mínimos comuns de desenvolvimento de capacidades e de planificação, ***o desenvolvimento de aptidões de cibersegurança suficientes,*** o intercâmbio de informações e a coordenação de ações, bem como requisitos mínimos comuns de segurança. ***As normas mínimas comuns deverão ser aplicadas de acordo com as recomendações adequadas dos Grupos de Coordenação da Cibersegurança.*** **[Alt. 8]**

(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 Tratado sobre o Funcionamento da União Europeia (TFUE), nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança. ***Além disso, nenhum Estado-Membro é obrigado a divulgar informação classificada da UE, tal como definida na Decisão 2011/292/UE*** ([2])***, informação sujeita a acordos de não divulgação ou a acordos de não divulgação informais, tais como o protocolo relativo a sinalização luminosa.*** **[Alt. 9]**

(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, ***com base nos requisitos mínimos definidos na presente diretiva,*** 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. Os Estados-Membros deverão, por conseguinte, ser obrigados a respeitar as normas comuns relativas ao formato e à intermutabilidade dos dados a partilhar e avaliar. Os Estados-Membros deverão poder solicitar a assistência da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) no quadro da elaboração das suas estratégias nacionais em matéria de SRI, baseadas num plano mínimo comum de estratégia em matéria de SRI.*** **[Alt. 10]**

([1]) Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro) (JO L 108 de 24.4.2002, p. 33).

([2]) ***Decisão 2011/292/UE do Conselho, de 31 de março de 2011, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 141 de 27.5.2011, p. 17).***

(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.

(10-A) Tendo em conta as diferenças nas estruturas governativas nacionais, e a fim de salvaguardar os acordos setoriais pré-existentes ou os organismos de supervisão e regulação da União, bem como evitar duplicações, os Estados--Membros devem poder designar mais do que uma autoridade nacional competente, responsável pelo cumprimento das tarefas associadas à segurança das redes e dos sistemas informáticos dos operadores de mercado, nos termos da presente diretiva. No entanto, para garantir uma boa cooperação e comunicação transfronteiras, é necessário que cada Estado-Membro, sem prejuízo de acordos regulamentares setoriais, designe apenas um balcão único responsável pela cooperação transfronteiras a nível da União. Caso a estrutura constitucional ou outros acordos assim o exijam, um Estado-Membro deve poder designar apenas uma autoridade para levar a cabo as tarefas da autoridade competente e do balcão único. As autoridades competentes e os balcões únicos devem ser entidades civis, sujeitas a controlo integralmente democrático e não devem exercer quaisquer funções no domínio da inteligência, aplicação da lei ou defesa, nem estar associados, de forma alguma, a nível da organização, a organismos ativos nesses domínios. **[Alt. 11]**

(11) Os Estados-Membros ***e os operadores de mercado*** deverão estar equipados adequadamente, em termos de capacidades técnicas e organizacionais, para impedir, detetar, reagir e reduzir***, em qualquer momento,*** os incidentes e riscos ligados às redes e aos sistemas informáticos. ***Os sistemas de segurança das administrações públicas deverão ser seguros e objeto de controlo e análise democráticos. As capacidades e o equipamentohabitualmente exigidos deverão cumprir as normas técnicas aprovadas em comum, bem como os Procedimentos Operativos Normalizados (PON).*** Por conseguinte, devem ser instituídas em todos os Estados-Membros equipas de resposta a emergências informáticas ***(CERT)*** que cumpram as condições essenciais para assegurar capacidades reais e compatíveis para lidar com os incidentes e riscos e garantir uma cooperação eficaz a nível da União. ***Essas CERT devem poder interagir com base nas normas técnicas comuns e nos PON. Tendo em conta as diferentes características das CERT existentes, que correspondem a diferentes intervenientes e necessidades que esta matéria exige, os Estados--Membros devem garantir que cada um dos setores abrangidos, referidos na lista de operadores de mercado estabelecida na presente diretiva, usufrua dos serviços de, pelo menos, uma CERT. Relativamente à cooperação transfronteiras das CERT, os Estados-Membros devem garantir que estas possuam meios suficientes para participar nas redes de cooperação internacionais e da União existentes já em funcionamento.*** **[Alt. 12]**

(12) Aproveitando os progressos significativos realizados no âmbito do Fórum Europeu dos Estados-Membros (FEEM) para promover debates e intercâmbios de boas práticas políticas, incluindo a definição de princípios de cooperação informática europeia em situação de crise, os Estados-Membros e a Comissão deverão formar uma rede para se manterem em comunicação permanente e apoiar a sua cooperação. Este mecanismo de cooperação seguro e eficaz***, incluindo a participação dos operadores de mercado, se adequado,*** deverá permitir que o intercâmbio de informações, a deteção e a resposta sejam estruturados e coordenados a nível da União. **[Alt. 13]**

(13) A ~~Agência Europeia para a Segurança das Redes e da Informação (~~«ENISA») deverá assistir os Estados-Membros e a Comissão através da oferta das suas competências especializadas e aconselhamento e da facilitação do intercâmbio de boas práticas. Em particular, na aplicação da presente diretiva, a Comissão ~~deverá~~ ***e os Estados-Membros deverão*** consultar a ENISA. A fim de garantir a informação eficaz e atempada dos Estados-Membros e da Comissão, os alertas rápidos sobre os incidentes e riscos devem ser notificados à rede de cooperação. Para que os Estados--Membros possam adquirir conhecimentos, a rede de cooperação deverá também servir de instrumento para o intercâmbio de boas práticas, ajudando os seus membros a reforçar as suas capacidades e orientando a organização de avaliações interpares e dos exercícios de SRI. **[Alt. 14]**

(13-A) Se adequado, os Estados-Membros deverão poder utilizar ou adaptar estruturas ou estratégias organizativas existentes aquando da aplicação das disposições da presente diretiva. **[Alt. 15]**

(14) Deverá criar-se uma infraestrutura de partilha de informações segura que permita o intercâmbio de informações sensíveis e confidenciais no âmbito da rede de cooperação. ***As estruturas existentes na União deverão ser plenamente aproveitadas para esse fim.*** Sem prejuízo da sua obrigação de notificar incidentes e riscos de dimensão europeia à rede de cooperação, o acesso às informações confidenciais de outros Estados-Membros só deve ser concedido aos Estados-Membros que demonstrem que os seus recursos e processos técnicos, financeiros e humanos, bem como a sua infraestrutura de comunicação, asseguram uma participação na rede eficaz, eficiente e segura***, utilizando métodos transparentes***. **[Alt. 16]**

(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~~ ***, incluindo a*** troca de ***informações relevantes, de*** apoio operacional ***e de informações analisadas estrategicamente,*** em caso de incidentes. ***Para incentivar efetivamente a partilha de informações e de boas práticas, é essencial assegurar que os operadores de mercado, que participam nos referidos intercâmbios, não fiquem em desvantagem devido à sua cooperação. São necessárias garantias adequadas para assegurar que tal cooperação não exponha estes operadores a um maior risco de incumprimento ou a novas responsabilidades no âmbito, inter alia, da concorrência, propriedade intelectual, proteção dos dados ou legislação em matéria de cibercriminalidade, nem os exponha a maiores riscos operacionais ou de segurança.*** **[Alt. 17]**

(16) Para garantir a transparência e informar devidamente os cidadãos e os operadores do mercado da ~~UE, as autoridades competentes~~ ***União, os balcões únicos*** deverão criar um sítio Web comum ***à escala da União*** para publicar informações não confidenciais sobre os incidente~~s~~ , riscos ***e medidas para atenuar os riscos, e, se necessário, para aconselhar sobre as medidas de manutenção adequadas***. ***A informação contida no sítio Web deverá ser acessível, independentemente do dispositivo utilizado. Os dados pessoais publicados nesse sítio Web deverão restringir-se ao estritamente necessário e deverão ser tão anónimos quanto possível.*** **[Alt. 18]**

(17) Caso as informações sejam consideradas confidenciais em conformidade com as regras nacionais e da União em matéria de sigilo comercial, essa confidencialidade deve ser assegurada no exercício das atividades e no cumprimento dos objetivos estabelecidos pela presente diretiva.

(18) Com base, nomeadamente, nas experiências nacionais de gestão de crises e em cooperação com a ENISA, a Comissão e os Estados-Membros deverão elaborar um plano de cooperação da União em matéria de SRI que defina mecanismos de cooperação***, práticas de excelência e padrões operacionais*** para ***evitar, detetar, relatar e*** fazer face aos riscos e incidentes. Esse plano deverá ser devidamente tido em conta no desencadear de alertas rápidos no âmbito da rede de cooperação. **[Alt. 19]**

(19) A notificação de um alerta precoce na rede deverá ser exigida apenas quando a escala e a gravidade do incidente ou do risco em causa forem ou puderem vir a ser de tal modo significativas que sejam necessárias informações ou a coordenação da resposta a nível da União. Os alertas precoces devem, por conseguinte, limitar-se aos incidentes ou riscos ~~reais ou potenciais~~ que ganhem rapidamente dimensão, excedam a capacidade de resposta nacional ou afetem mais de um Estado-Membro. A fim de permitir uma avaliação adequada, todas as informações relevantes para a avaliação dos riscos ou incidentes deverão ser comunicadas à rede de cooperação. **[Alt. 20]**

(20) Após receção de um alerta precoce e a sua avaliação, ~~as autoridades competentes~~ ***os balcões únicos*** deverão chegar a acordo quanto a uma resposta coordenada no âmbito do plano de cooperação da União em matéria de SRI. ~~As autoridades competentes~~ ***Os balcões únicos, a ENISA*** e a Comissão deverão ser informados das medidas adotadas a nível nacional em resultado da resposta coordenada. **[Alt. 21]**

(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 para promover uma abordagem global comum das questões de SRI. ***Os quadros para essa cooperação internacional deverão estar sujeitos à Diretiva 95/46/CE do Parlamento Europeu e do Conselho*** ([1]) ***e ao Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho*** ([2])**. [Alt. 22]**

(22) A responsabilidade de garantir a SRI recai, em grande medida, ~~às administrações públicas e~~ nos operadores do mercado. Deverá ser promovida e desenvolvida uma cultura de gestão dos riscos, ***cooperação estreita e confiança,*** que abranja a avaliação dos riscos e a implementação de medidas de segurança adequadas aos riscos ~~enfrentados~~ ***e incidentes, deliberados ou acidentais,*** através de requisitos regulamentares adequados e práticas setoriais voluntárias. Estabelecer condições de concorrência equitativas e ***fiáveis*** é também essencial para um funcionamento eficaz da rede de cooperação tendo em vista assegurar a eficácia da cooperação entre todos os Estados-Membros. **[Alt. 23]**

(23) A Diretiva 2002/21/CE exige que as empresas que oferecem redes de comunicações eletrónicas públicas ou serviços de comunicações eletrónicas acessíveis ao público tomem as medidas necessárias para preservar a sua integridade e segurança e introduz requisitos de notificação de quebra de segurança e perda de integridade. A Diretiva 2002/58/ /CE do Parlamento Europeu e do Conselho ([3]) exige que um prestador de um serviço de comunicações eletrónicas acessíveis ao público tome medidas técnicas e organizacionais adequadas para salvaguardar a segurança dos seus serviços.

(24) Essas obrigações não deverão cingir-se ao setor das comunicações eletrónicas, mas ser extensíveis aos ***operadores das infraestruturas que dependem em larga medida das tecnologias da informação e da comunicação, e são essenciais para a manutenção de funções económicas ou sociais essenciais, como a eletricidade e o gás, os transportes, as instituições de crédito, as infraestruturas dos mercados financeiros e a saúde. A perturbação dessas redes e desses sistemas informáticos afetaria o mercado interno. Embora as obrigações estabelecidas na presente diretiva não devam ser extensíveis aos*** principais prestadores de serviços da sociedade da informação, tal como definidos na Diretiva 98/34/CE do Parlamento Europeu e do Conselho ([4]), que estão na base dos serviços da sociedade da informação ou das atividades em linha, como as plataformas de comércio eletrónico, portais de pagamento Internet, redes sociais, motores de pesquisa, serviços de computação em nuvem ***em geral ou*** lojas de aplicações em linha,~~A perturbação destes serviços da sociedade da informação horizontais impede a prestação de outros serviços deste setor que neles se baseiam. Os responsáveis pelo desenvolvimento de *software* e os fabricantes de *hardware* não são prestadores de serviços da sociedade da informação, pelo que são excluídos. Essas obrigações deverão ser também alargadas às administrações públicas e aos operadores das infraestruturas críticas que dependem em larga medida das tecnologias da informação e da comunicação e são essenciais para a manutenção de funções económicas ou sociais vitais como a eletricidade e o gás, os transportes, as instituições de crédito, a bolsa e a saúde. A perturbação dessas redes e sistemas informáticos afetaria o mercado interno~~***, esses fornecedores podem informar, numa base facultativa, a autoridade competente ou o balcão único sobre incidentes de segurança da rede que considerem necessário comunicar***. A ***autoridade competente ou o balcão único devem, se possível, apresentar*** aos operadores ***de mercado que comunicaram o incidente informações analisadas estrategicamente que ajudarão a resolver a ameaça à segurança.*** **[Alt. 24]**

([1]) ***Diretiva 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 (JO L 281 de 23.11.1995, p. 31).***

([2]) ***Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).***

([3]) 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 (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

([4]) Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 204 de 21.7.1998, p. 37).

(24-A) ***Embora os responsáveis pelo desenvolvimento de software e os fabricantes de hardware não sejam operadores de mercado comparáveis aos abrangidos pela presente diretiva, os seus produtos contribuem para a segurança das redes e dos sistemas informáticos. Por conseguinte, têm um papel importante a desempenhar para permitir que os operadores de mercado garantam a segurança das suas redes e infraestruturas de informação. Tendo em conta que os produtos de hardware e software já estão sujeitos às regras existentes em matéria de responsabilidade pelos produtos, os Estados-Membros deverão garantir a aplicação dessas regras.*** **[Alt. 25]**

(25) As medidas técnicas e organizativas impostas ~~às administrações públicas e~~ aos operadores do mercado não deverão exigir que um determinado produto das tecnologias da informação e da comunicação para fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico. **[Alt. 26]**

(26) ~~As administrações Os~~ Os operadores do mercado deverão garantir a segurança das redes e dos sistemas que estão sob o seu controlo. Trata-se principalmente de redes e sistemas privados geridos pelo seu pessoal de TI interno ou cuja segurança tenha sido externalizada. As obrigações em matéria de segurança e notificação deverão aplicar-se aos operadores do mercado pertinentes, ~~e às administrações~~ independentemente do facto de estes procederem à manutenção das suas redes e sistemas informáticos a nível interno ou de a externalizarem. **[Alt. 27]**

(27) A fim de não impor encargos financeiros e administrativos desproporcionados aos pequenos operadores e aos utilizadores, os requisitos devem ser proporcionais ao risco apresentado pela rede ou sistema informático em causa, devendo as medidas ter em conta os mais recentes progressos técnicos. Estes requisitos não serão aplicáveis às microempresas.

(28) As autoridades competentes ***e os balcões únicos*** 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. ***As autoridades competentes e os balcões únicos devem informar os fabricantes de hardware e os prestadores de serviços de TIC afetados acerca de incidentes com um impacto significativo que lhes sejam comunicados.*** Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes comunicados às autoridades competentes e ***aos balcões únicos 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 notificação, as autoridades competentes ***e os balcões únicos*** 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. ***Por norma, os balcões únicos não devem divulgar os dados pessoais de indivíduos envolvidos em incidentes. Os balcões únicos só deverão divulgar dados pessoais caso a divulgação destes seja necessária e proporcional ao objetivo visado.*** **[Alt. 28]**

(29) As autoridades competentes deverão ser dotadas dos meios necessários para desempenharem as suas funções, incluindo o poder de obter informações suficientes dos operadores do mercado, ~~e das administrações públicas~~ a fim de avaliarem o nível de segurança das redes e dos sistemas informáticos, de ***medirem o número, a escala e o âmbito dos incidentes***, bem como dados completos e fiáveis sobre os incidentes que tenham tido impacto no seu funcionamento. **[Alt. 29]**

(30) Em muitos casos, o incidente é causado por atividades criminosas. É possível suspeitar da origem criminosa de um incidente mesmo que não existam provas suficientemente claras desde o início. Neste contexto, a cooperação adequada entre as autoridades competentes***, os balcões únicos*** e as autoridades policiais e judiciais***, bem como a cooperação com o EC3 (Centro Europeu de Cibercriminalidade na Europol) e a ENISA,*** deverá inscrever-se numa resposta global e eficaz à ameaça de incidentes no domínio da segurança. Em especial, a promoção de um ambiente seguro, protegido e mais resiliente requer a notificação sistemática dos incidentes que se suspeite terem uma origem criminosa grave às autoridades responsáveis. O caráter de crime grave atribuído aos incidentes deverá ser avaliado à luz da legislação da UE sobre a cibercriminalidade. **[Alt. 30]**

(31) Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. ***Os Estados-Membros e os operadores de mercado deverão proteger os dados pessoais armazenados, tratados ou transmitidos contra a destruição acidental ou ilícita, a perda ou alteração acidental, o armazenamento, o acesso, a divulgação ou a difusão não autorizados ou ilícitos; devem, ainda, assegurar a implementação de uma política de segurança no domínio do tratamento de dados pessoais.*** Neste contexto, as autoridades competentes***, os balcões únicos*** e as autoridades encarregadas da proteção dos dados deverão cooperar e trocar informações, ~~sobre todas as questões pertinentes para~~***nomeadamente, se adequado, com os operadores de mercado, a fim de*** combater as violações de dados pessoais resultantes de incidentes***, em conformidade com as regras aplicáveis em matéria de proteção de dados***. ~~Os Estados Membros cumprirão~~ A obrigação de notificar os incidentes de segurança ***deve ser concretizada*** de um modo que minimize a carga administrativa caso o incidente em causa constitua também uma violação de dados pessoais ***que tem de ser comunicada*** em conformidade com ~~o Regulamento do Parlamento Europeu e do Conselho relativo à~~ ***a legislação da União em matéria de*** proteção ~~das pessoas singulares no que diz respeito ao tratamento~~ de dados ~~pessoais e à livre circulação desses dados~~ [1]~~. Em colaboração com as autoridades competentes e as autoridades encarregadas da proteção de dados pessoais,~~ . A ENISA ~~poderá~~ ***deverá*** dar a sua contribuição desenvolvendo mecanismos de intercâmbio de informações e ~~modelos que evitem a necessidade de dois modelos de~~ ***um modelo único*** notificação ***que facilitem*** ~~Este único modelo de notificação facilitaria~~ a comunicação de incidentes que comprometam os dados pessoais, aligeirando assim a carga administrativa que recai sobre as empresas e as administrações públicas. **[Alt. 31]**

(32) A normalização dos requisitos de segurança é um processo dirigido pelo mercado***, de natureza voluntária, que deve permitir que os operadores de mercado utilizem meios alternativos para atingir, pelo menos, resultados semelhantes***. A fim de garantir uma aplicação convergente das normas de segurança, os Estados-Membros deverão incentivar o cumprimento ou a conformidade com as normas especificadas para assegurar um elevado nível de segurança a nível da União. Para o efeito, ***deverá ser considerada a aplicação de normas internacionais abertas sobre segurança das redes e da informação ou a criação de tais instrumentos. P***oderá ser necessário ***dar mais um passo para*** elaborar normas harmonizadas, o que deverá ser efetuado em conformidade com o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([2]). ***Em particular, o ETSI, o CEN e o CENELEC devem ser mandatados para sugerir normas europeias de segurança abertas, eficazes e eficientes, em que as preferências tecnológicas sejam evitadas tanto quanto possível, e que devem ser facilmente exequíveis por pequenos e médios operadores de mercado. As normas internacionais relativas à cibersegurança devem ser cuidadosamente aprovadas, a fim de assegurar que não tenham sido comprometidas e que forneçam níveis adequados de segurança, garantindo, assim, que o cumprimento obrigatório das normas relativas à cibersegurança melhore o nível geral da cibersegurança da União, e não o contrário.*** **[Alt. 32]**

(33) A Comissão deverá rever periodicamente a presente diretiva, ***em consulta com todas as partes interessadas,*** nomeadamente para decidir da eventual necessidade de alterações à luz da evolução ***social, política,*** tecnológica ou do mercado. **[Alt. 33]**

(34) A fim de permitir o bom funcionamento da rede de cooperação, o poder de adotar atos em conformidade com o artigo 290.º do TFUE deverá ser delegado na Comissão no que diz respeito ~~à definição dos critérios a cumprir para que um Estado-Membro seja autorizado a participar num sistema seguro~~ ***a um conjunto de normas de interligação e de segurança*** para ***as infraestruturas seguras*** de troca de informações e a uma melhor especificação dos eventos desencadeadores de um alerta rápido ~~e à definição das condições em que os operadores de mercado e as administrações públicas são obrigados a notificar os incidentes~~. **[Alt. 34]**

([1]) ~~SEC(2012) 72 final.~~

([2]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

(35) É particularmente importante que a Comissão proceda a consultas adequadas durante os trabalhos preparatórios, inclusive a nível de peritos. A Comissão, ao preparar e redigir atos delegados, deverá assegurar a transmissão simultânea, atempada e adequada dos documentos relevantes ao Parlamento Europeu e ao Conselho.

(36) A fim de assegurar condições uniformes de aplicação da presente diretiva, deverão ser conferidas competências de execução à Comissão no que diz respeito à cooperação com ~~as autoridades competentes~~ ***os balcões únicos*** no âmbito da rede de cooperação, ***sem prejuízo dos mecanismos de cooperação existentes a nível nacional***, ~~ao acesso às infraestruturas seguras de partilha de informações~~, ao plano de cooperação da União em matéria de SRI, e aos meios e procedimentos aplicáveis à ~~informação do público sobre a ocorrência~~ ***notificação*** de incidentes ~~e às normas e/ou especificações técnicas pertinentes para a SRI~~ ***com um impacto significativo***. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([1]). **[Alt. 35]**

(37) Na aplicação da presente diretiva, a Comissão deverá assegurar as ligações adequadas com os comités setoriais pertinentes e os organismos competentes criados a nível da ~~UE~~ ***União***, em especial no domínio ~~da~~ ***do governo eletrónico, da*** energia, ***dos*** transporte~~s~~***, da*** saúde ***e da defesa***. **[Alt. 36]**

(38) As informações que sejam consideradas confidenciais por uma autoridade competente ***ou por um balcão único***, em conformidade com as regras nacionais e da União em matéria de sigilo comercial, só deverão ser trocadas com a Comissão***, as suas agências relevantes, os balcões únicos e/ou*** e outras autoridades ***nacionais*** competentes nos casos em que tal seja estritamente necessário para a aplicação da presente diretiva. As informações comunicadas deverão limitar-se ao que for pertinente***, necessário*** e adequado ao objetivo dessa comunicação, ***e deverão respeitar os critérios predefinidos para a confidencialidade e a segurança, nos termos da Decisão 2011/292/UE, informação sujeita a acordos de não divulgação ou a acordos de não divulgação informais, tais como o protocolo relativo a sinalização luminosa***. **[Alt. 37]**

(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 o***u aos balcões únicos*** 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 dos dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia. Na aplicação da presente diretiva, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ([2]) deverá 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 deverá ser conforme com o Regulamento (CE) n.º 45/2001. **[Alt. 38]**

(40) Atendendo a que o objetivo da presente diretiva, a saber, garantir um elevado nível de SRI na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação, ser mais bem alcançado a nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para alcançar esse objetivo.

(41) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, nomeadamente o direito ao respeito pelas comunicações e pela vida privada, a proteção de dados pessoais, a liberdade de empresa, o direito de propriedade, o direito a recurso judicial e o direito a ser ouvido. A presente diretiva deverá ser aplicada de acordo com esses direitos e princípios.

([1]) Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

([2]) 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 (JO L 145 de 31.5.2001, p. 43).

(41-A) ***Em conformidade com a declaração política conjunta dos Estados-Membros e da Comissão sobre os documentos explicativos, de 28 de setembro de 2011, os Estados-Membros comprometeram-se a fazer acompanhar a notificação das suas medidas de transposição, quando tal se justifique, de um ou mais documentos que expliquem a relação entre os elementos de uma diretiva e as partes correspondentes dos instrumentos de transposição nacionais. Em relação à presente diretiva, o legislador considera que se justifica a transmissão desses documentos.*** **[Alt. 39]**

(41-B) Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em 14 de junho de 2013 ([1]),

ADOTARAM A PRESENTE DIRETIVA:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. A presente diretiva estabelece medidas destinadas a garantir um elevado nível de segurança das redes e da informação (SRI) na União.

2. Para esse efeito, a presente diretiva:

a) Estabelece obrigações para todos os Estados-Membros relativas à prevenção, ao tratamento e à resposta aos riscos e incidentes que afetam as redes e os sistemas informáticos;

b) Cria um mecanismo de cooperação entre os Estados-Membros a fim de garantir uma aplicação uniforme da presente diretiva na União e, se for caso disso, um tratamento e uma resposta coordenados, ~~e~~ eficazes ***e eficientes*** aos riscos e incidentes que afetam as redes e os sistemas informáticos***, com a participação das partes interessadas pertinentes***; **[Alt. 40]**

c) Estabelece requisitos de segurança para os operadores do mercado~~e as administrações públicas~~. **[Alt. 41]**

3. Os requisitos de segurança previstos no artigo 14.º da presente diretiva não se aplicam às empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público na aceção da Diretiva 2002/21/CE, que devem cumprir os requisitos de integridade e segurança específicos previstos nos artigos 13.º-A e 13.º-B dessa diretiva, nem aos prestadores de serviços de confiança.

4. A presente diretiva não prejudica a legislação da União em matéria de luta contra a criminalidade informática nem a Diretiva 2008/114/CE do Conselho ([2]).

5. A presente diretiva também não prejudica a Diretiva 95/46/CE, a Diretiva 2002/58/CEe o Regulamento ***(CE) n.º 45/2001***. ***Qualquer utilização dos dados pessoais está limitada ao estritamente necessário para efeitos da presente diretiva, devendo esses dados ser o mais anónimos possível, ou mesmo totalmente anónimos.*** **[Alt. 42]**

6. A partilha de informações no quadro da rede de cooperação nos termos do capítulo III e as notificações de incidentes que afetam a SRI ao abrigo do artigo 14.º podem requerer o tratamento de dados pessoais. Esse tratamento, que é necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva, deve ser autorizado pelo Estado-Membro em conformidade com o artigo 7.º da Diretiva 95/46/CE e com a Diretiva 2002/58/CE, tal como transpostos para o direito nacional.

([1]) JO C 32 de 4.2.2014, p. 19.
([2]) Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

Artigo 1.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 [1].

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 são 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. São aplicáveis as notificações de incidentes previstas no artigo 14.º da presente diretiva, 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 da Comissão [2]**. [Alt. 43]**

Artigo 2.º

Harmonização mínima

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.

Artigo 3.º

Definições

Para efeitos da presente diretiva, entende-se por:

1) «Redes e sistemas informáticos»:

a) Uma rede de comunicações eletrónicas na aceção da Diretiva 2002/21/CE;

b) Um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais efetuam, com base num programa, o tratamento automático dos dados ~~informáticos~~ ***digitais***; **[Alt. 44]**

c) Os dados ~~informáticos~~ ***digitais*** armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas a) e b) tendo em vista a sua exploração, utilização, proteção e manutenção; **[Alt. 45]**

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 comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema; ***a «segurança» inclui dispositivos técnicos adequados, soluções e procedimentos operacionais que garantam os requisitos de segurança definidos na presente diretiva;*** **[Alt. 46]**

---

[1] ***Decisão 2009/371/JHA do Conselho, de 6 de Abril de 2009, que cria o Serviço Europeu de Polícia (Europol) (JO L 121 de 15.5.2009, p. 37).***

[2] ***Regulamento (UE) n.º 611/2013 da Comissão, de 24 de junho de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas (JO L 173 de 26.6.2013, p. 2).***

3) «Risco»: Uma circunstância ou um evento ***razoavelmente identificável*** com um efeito adverso potencial na segurança; **[Alt. 47]**

4) «Incidente»: Um ~~circunstância ou~~ evento com um efeito adverso real na segurança; **[Alt. 48]**

~~5) «Serviço da sociedade da informação»: um serviço na aceção do artigo 1.º, n.º 2, da Diretiva 98/34/CE;~~ **[Alt. 49]**

6) «Plano de cooperação em matéria de SRI»: um plano que estabelece o quadro para as funções, responsabilidades e procedimentos organizacionais destinado a manter ou a restabelecer o funcionamento das redes e dos sistemas informáticos, em caso de risco ou incidente que os afetem;

7) «Tratamento de incidentes»: todos os procedimentos de apoio à ***deteção, prevenção,*** análise, contenção e resposta em caso de incidente; **[Alt. 50]**

8) «Operador do mercado»:

~~a) Um fornecedor de serviços da sociedade de informação que permitem a prestação de outros serviços da sociedade da informação, cuja lista não exaustiva consta do anexo II;~~ **[Alt. 51]**

b) Um operador de infraestruturas ~~críticas~~ essenciais para a manutenção de atividades económicas e sociais vitais***, constantes da lista não exaustiva do anexo II,*** nos domínios da energia, dos transportes, da banca, ***das infraestruturas do mercado financeiro, dos nós de comutação*** da ***Internet, da cadeia de abastecimento alimentar*** ~~bolsa~~ e da saúde, ***e*** cuja ~~lista não exaustiva consta do anexo II.~~ ***interrupção ou destruição teria um impacto significativo num Estado-Membro, em resultado da impossibilidade de continuar a assegurar essas funções, na medida em que a rede e os sistemas de informação em causa estão relacionados com os seus serviços essenciais;*** **[Alt. 52]**

8-A) «Incidente com um impacto significativo»: um incidente que afeta a segurança e continuidade de uma rede ou sistema de informação que conduz a uma grande perturbação das funções económicas e sociais vitais; **[Alt. 53]**

9) «Norma», uma norma referida no Regulamento (UE) n.º 1025/2012;

10) «Especificação», uma especificação referida no Regulamento (UE) n.º 1025/2012;

11) «Prestador de serviços de confiança», uma pessoa singular ou coletiva que presta qualquer serviço eletrónico que vise a criação, verificação, validação, tratamento e preservação de assinaturas eletrónicas, selos eletrónicos, carimbos eletrónicos da hora, documentos eletrónicos, serviços de entrega eletrónica, autenticação de sítios Web e certificados eletrónicos, incluindo certificados de assinatura eletrónica e de selos eletrónicos.

11-A) «Mercado regulamentado»: um mercado regulamentado na aceção do artigo 4.º, ponto 14, da Diretiva 2004/39/CE do Parlamento Europeu e do Conselho [1]***,*** **[Alt. 54]**

11-B) «Sistema de negociação multilateral (MTF)»: um sistema de negociação multilateral na aceção do artigo 4.º, ponto 15, da Diretiva 2004/39/CE; **[Alt. 55]**

11-C) «Sistema de negociação organizado»: um sistema ou dispositivo multilateral, que não seja um mercado regulamentado nem um sistema de negociação multilateral ou uma contraparte central, operado por uma empresa de investimento ou um operador de mercado, dentro do qual múltiplos interesses de compra e venda de obrigações, produtos financeiros estruturados, licenças de emissão ou derivados, manifestados por terceiros, podem interagir no sistema para que tal resulte num contrato, em conformidade com o título II da Diretiva 2004/39/CE. **[Alt. 56]**

---

[1] ***Diretiva 2004/39/CE do Parlamento Europeu e do Conselho, de 21 de abril de 2004, relativa aos mercados de instrumentos financeiros (JO L 45 de 16.2.2005, p. 18).***

CAPÍTULO II

QUADROS NACIONAIS PARA A SEGURANÇA DAS REDES E DA INFORMAÇÃO

Artigo 4.º

Princípios

Os Estados-Membros devem garantir um elevado nível de segurança das redes e dos sistemas informáticos no seu território, em conformidade com a presente diretiva.

Artigo 5.º

Estratégia e plano de cooperação nacionais em matéria de SRI

1. Cada Estado-Membro deve adotar uma estratégia nacional de SRI, que defina os objetivos estratégicos e as medidas regulamentares e estratégicas concretas para alcançar e manter um elevado nível de segurança das redes e da informação. A estratégia nacional de SRI deve contemplar, em especial, os seguintes aspetos:

a) A definição dos objetivos e das prioridades da estratégia, com base numa análise atualizada dos riscos e dos incidentes;

b) Um quadro de governação para alcançar os objetivos e as prioridades da estratégia, incluindo uma definição clara das funções e responsabilidades dos organismos governamentais e de outros intervenientes pertinentes;

c) A determinação das medidas gerais para a preparação, resposta e recuperação, incluindo mecanismos de cooperação entre os setores público e privado;

d) A indicação dos programas de ensino, sensibilização e formação;

e) Planos de investigação e desenvolvimento e descrição do modo como estes planos refletem as prioridades estabelecidas.

e-A) Os Estados-Membros podem solicitar a assistência da ENISA para a elaboração das suas estratégias nacionais e dos seus planos de cooperação nacional em matéria de SRI, baseados num plano mínimo comum de estratégia em matéria de SRI. **[Alt. 57]**

2. A estratégia nacional de SRI deve incluir um plano de cooperação nacional em matéria de SRI que cumpra, pelo menos, os seguintes requisitos:

a) Um ~~plano~~ ***quadro*** de ~~avaliação~~ ***gestão*** dos riscos ~~para identificar os riscos e avaliar os~~ ***que estabeleça uma metodologia para a identificação, a definição de prioridades, a avaliação e o tratamento de riscos, a avaliação dos*** impactos de potenciais incidentes***, as opções de prevenção e de controlo, e que defina critérios para a escolha de possíveis contramedidas***; **[Alt. 58]**

b) A definição das funções e responsabilidades ~~dos~~ ***das*** diferentes ***autoridades e de outros*** intervenientes envolvidos na execução do ~~plano~~ ***quadro***; **[Alt. 59]**

c) A definição de processos de cooperação e comunicação que assegurem a prevenção, deteção, resposta, reparação e recuperação, adaptados em função do nível de alerta;

d) Um roteiro para os exercícios e a formação em matéria de SRI, a fim de reforçar, validar e testar o plano. Os ensinamentos retirados devem ser documentados e incorporados nas atualizações do plano.

3. A estratégia e o plano de cooperação nacionais em matéria de SRI devem ser comunicados à Comissão no prazo de ~~um mês~~ ***três meses*** a contar da data da sua adoção. **[Alt. 60]**

Artigo 6.º

~~*Autoridade nacional competente*~~ ***Autoridades nacionais competentes*** e balcões únicos em matéria de segurança das redes e dos sistemas informáticos **[Alt. 61]**

1. Cada Estado-Membro designa uma ~~autoridade nacional competente~~ ***ou mais autoridades nacionais civis competentes*** em matéria de segurança das redes e dos sistemas informáticos («autoridade***(s)*** competente***(s)***»). **[Alt. 62]**

2. As autoridades competentes controlam a aplicação da presente diretiva a nível nacional e contribuem para a sua aplicação coerente em toda a União.

2-A. Sempre que um Estado-Membro designe mais que uma autoridade competente, deve designar uma autoridade nacional civil, por exemplo uma autoridade competente, enquanto balcão único nacional para a segurança das redes e dos sistemas informáticos («balcão único»). Sempre que um Estado-Membro designe apenas uma autoridade competente, esta age também enquanto balcão único. **[Alt. 63]**

2-B. As autoridades competentes e o balcão único do mesmo Estado-Membro cooperam estreitamente no que diz respeito às obrigações previstas na presente diretiva. **[Alt. 64]**

2-C. O balcão único assegura a cooperação transfronteiriça com os outros balcões únicos. **[Alt. 65]**

3. Os Estados-Membros asseguram que as autoridades competentes ***e os balcões únicos*** disponham de recursos técnicos, financeiros e humanos adequados para realizar de modo eficaz e eficiente as tarefas que lhes sejam atribuídas e, deste modo, cumprir os objetivos da presente diretiva. Os Estados-Membros garantem a cooperação eficaz, eficiente e segura ~~das autoridades competentes~~ ***dos balcões únicos*** através da rede referida no artigo 8.º. **[Alt. 66]**

4. Os Estados-Membros asseguram que as autoridades competentes ***e os balcões únicos, se for caso disso nos termos do n.º 2-A do presente artigo,*** sejam ~~notificadas~~ ***notificados*** dos incidentes ocorridos ~~pelas administrações públicas e~~ pelos operadores do mercado, tal como especificado no artigo 14.º, n.º 2, e lhes sejam atribuídos poderes de execução e de repressão, tal como referido no artigo 15.º. **[Alt. 67]**

4-A. Sempre que a legislação da União previr um organismo regulador ou de supervisão da União específico do setor, nomeadamente no que se refere às redes e aos sistemas informáticos, esse organismo recebe as notificações dos incidentes nos termos do artigo 14.º, n.º 2, dos operadores de mercado em causa nesse setor e são-lhe conferidos os poderes de aplicação e de execução referidos no artigo 15.º. Esse organismo da União deve cooperar estreitamente com as autoridades competentes e com o balcão único do Estado-Membro de acolhimento no que se refere a essas obrigações. O balcão único do Estado-Membro de acolhimento representa o organismo da União relativamente às obrigações previstas no capítulo III. **[Alt. 68]**

5. Sempre que necessário, as autoridades competentes ***e os balcões únicos*** consultam as autoridades policiais e judiciais nacionais e as autoridades encarregadas da proteção dos dados, com elas cooperando. **[Alt. 69]**

6. Cada Estado-Membro notifica sem demora a Comissão da designação ~~da autoridade competente~~ ***das autoridades competentes e do balcão único***, das suas funções e de quaisquer alterações posteriores. Cada Estado-Membro torna pública a sua designação ~~da autoridade competente~~ ***das autoridades competentes***. **[Alt. 70]**

Artigo 7.º

Equipa de resposta a emergências informáticas

1. Cada Estado-Membro cria ***pelo menos*** uma equipa de resposta a emergências informáticas (CERT) ***para cada um dos setores enumerados no anexo II***, 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. **[Alt. 71]**

2. Os Estados-Membros asseguram que as CERT disponham dos recursos técnicos, financeiros e humanos adequados de modo a poderem realizar eficazmente as suas funções, tal como definidas no anexo I, ponto 2.

3. Os Estados-Membros asseguram que as CERT possam contar com infraestruturas de comunicação e informação seguras e resilientes a nível nacional, compatíveis e interoperáveis com o sistema seguro de intercâmbio de informações referido no artigo 9.º.

4. Os Estados-Membros informam a Comissão sobre os recursos e o mandato das CERT, bem como sobre o seu processo de tratamento de incidentes.

5. ~~A~~ ***As*** CERT ~~funciona~~ ***funcionam*** sob a supervisão da autoridade competente ***ou do balcão único***, que devem rever periodicamente a adequação dos seus recursos e dos seus ***mandatos,*** e a eficácia do seu processo de tratamento de incidentes. **[Alt. 72]**

5-A. Os Estados-Membros devem assegurar que as CERT possuam recursos humanos e financeiros adequados, de modo a participarem ativamente em redes de cooperação internacionais e, nomeadamente, da União. **[Alt. 73]**

5-B. As CERT devem poder iniciar e participar em exercícios conjuntos com outras CERT, com todas as CERT dos Estados-Membros e com as instituições adequadas dos países terceiros, bem como com as CERT de organismos multinacionais e de instituições internacionais, tais como a Organização do Tratado do Atlântico Norte e a Organização das Nações Unidas, e devem ser incentivadas a fazê-lo. **[Alt. 74]**

5-C. Os Estados-Membros podem solicitar a assistência da ENISA ou de outros Estados-Membros para a criação das suas CERT nacionais. **[Alt. 75]**

CAPÍTULO III

COOPERAÇÃO ENTRE AUTORIDADES COMPETENTES

Artigo 8.º

Rede de cooperação

1. ~~As autoridades competentes e~~ ***Os balcões únicos,*** a Comissão ***e a ENISA*** devem constituir uma rede («rede de cooperação») para cooperarem contra os riscos e os incidentes que afetem as redes e os sistemas informáticos. **[Alt. 76]**

2. A rede de cooperação põe em comunicação permanente a Comissão e ~~as autoridades competentes~~***os balcões únicos***. Quando for solicitada, a ~~Agência Europeia para a Segurança das Redes e da informação (~~«ENISA») apoia a rede de cooperação, fornecendo conhecimentos especializados e aconselhamento. ***Se for caso disso, os operadores de mercado e os fornecedores de soluções de cibersegurança podem igualmente ser convidados a participar nas atividades da rede de cooperação referidas no n.º 3, alíneas (g) e (i).***

Sempre que seja pertinente, a rede de cooperação coopera com as autoridades encarregadas da proteção dos dados.

A Comissão informa regularmente a rede de cooperação sobre a investigação em matéria de segurança e outros programas relevantes do Horizonte 2020. **[Alt. 77]**

3. No âmbito da rede de cooperação, ~~as autoridades competentes~~ ***os balcões únicos*** devem:

a) Difundir alertas rápidos sobre os riscos e os incidentes, em conformidade com o artigo 10.º;

b) Assegurar uma resposta coordenada em conformidade com o artigo 11.º;

c) Publicar periodicamente num sítio Web comum informações não confidenciais sobre alertas rápidos em curso e a resposta coordenada;

d) Debater e avaliar conjuntamente~~, a pedido de um Estado-Membro ou da Comissão~~, uma ou mais estratégias e planos de cooperação nacionais em matéria de SRI referidos no artigo 5.º, no âmbito da presente diretiva;

e) Debater e avaliar conjuntamente, ~~a pedido de um Estado-Membro ou da Comissão,~~ a eficácia das CERT, em particular aquando da realização de exercícios de SRI a nível da União;

f) Cooperar e trocar ~~informações~~ ***conhecimentos especializados*** sobre ~~todas as~~ questões pertinentes ***relativas à segurança das redes e da informação, em especial nos domínios da proteção de dados, energia, transportes, banca, mercados financeiros e saúde*** com o Centro Europeu da Cibercriminalidade na Europol e com outros organismos europeus competentes~~, em especial nos domínios da proteção de dados, energia, transportes, banca, bolsa e saúde~~;

f-A) Se for caso disso, informar o Coordenador da luta antiterrorismo da UE, através de relatórios, existindo a possibilidade de solicitar a sua assistência no quadro de análises, ações e trabalhos preparatórios da rede de cooperação;

g) Proceder ao intercâmbio de informações e de boas práticas entre si e com a Comissão e prestar assistência mútua tendo em vista o desenvolvimento de capacidades em matéria de SRI;

~~h) Organizar análises regulares pelos pares das capacidades e do grau de preparação;~~

i) Organizar exercícios sobre SRI a nível da União e, se tal se afigurar adequado, participar nesse tipo de exercícios a nível internacional;

i-A) Envolver, consultar e trocar informações com os operadores de mercado, sempre que necessário, em matéria de riscos e incidentes que afetem as suas redes e sistemas informáticos;

i-B) Desenvolver, em cooperação com a ENISA, orientações sobre critérios específicos do setor relativos à notificação de incidentes significativos, além dos parâmetros previstos no artigo 14.º, n.º 2, para uma interpretação comum, uma aplicação coerente e uma execução coerente na União. **[Alt. 78]**

3-A. A rede de cooperação publica um relatório anual, com base nas atividades da rede e no relatório resumido, referente aos 12 meses anteriores, apresentado nos termos doartigo 14.º, n.º 4, da presente diretiva. **[Alt. 79]**

4. A Comissão estabelece, por meio de atos de execução, as modalidades necessárias para facilitar a cooperação ~~entre as autoridades competentes e a Comissão~~ referida nos n.os 2 e 3 ***entre os balcões únicos, a Comissão e a ENISA***. Esses atos de execução são adotados pelo procedimento de ~~consulta~~ ***exame*** referido no artigo 19.º, n.º ~~2~~ ***3***. **[Alt. 80]**

Artigo 9.º

Sistema seguro de partilha de informações

1. O intercâmbio de informações sensíveis e confidenciais na rede de cooperação deve ocorrer através de uma infraestrutura segura.

1-A. Os participantes na infraestrutura segura respeitam, nomeadamente, as medidas adequadas de confidencialidade e de segurança nos termos da Diretiva 95/46/CE e o Regulamento (CE) n.º 45/2001, em todas as etapas do tratamento. **[Alt. 81]**

~~2. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 18.º para definir os critérios a cumprir para que um Estado-Membro seja autorizado a participar num sistema de partilha de informações seguro, no que diz respeito:~~

~~a) à disponibilidade de uma infraestrutura de comunicação e informação segura e resiliente a nível nacional, compatível e interoperável com a infraestrutura segura da rede de cooperação em conformidade com o artigo 7.º, n.º 3,~~

~~b) à existência de recursos e processos técnicos, financeiros e humanos adequados para permitir às autoridades competentes e às CERT uma participação eficaz, eficiente e segura no sistema de troca de informações seguro nos termos do artigo 6.º, n.º 3, do artigo 7.º, n.º 2, e do artigo 7.º, n.º 3.~~ **[Alt. 82]**

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. Esses atos de execução devem ser adotados em conformidade com o procedimento de exame referido no artigo 19.º, n.º 3~~ ***delegados, nos termos do artigo 18.º, um conjunto de normas de interligação e de segurança que os balcões únicos devem cumprir antes de trocarem informações sensíveis e confidenciais na rede de cooperação***. **[Alt. 83]**

Artigo 10.º

Alerta rápido

1. ~~As autoridades competentes~~ ***Os balcões únicos*** ou a Comissão devem emitir um alerta rápido na rede de cooperação sobre os riscos e incidentes que preencham, pelo menos, uma das seguintes condições:

a) Aumentem rapidamente ou possam aumentar rapidamente em escala;

~~b) Excedam ou possam exceder~~ ***O balcão único estime que o risco ou incidente é suscetível de exceder*** a capacidade nacional de resposta;

~~c) Afetem ou possam afetar~~ ***Os balcões únicos ou a Comissão considerem que o risco ou incidente afeta*** mais de um Estado-Membro. **[Alt. 84]**

2. Nos alertas rápidos, ~~as autoridades competentes~~ ***os balcões únicos*** e a Comissão devem comunicar ***sem demora injustificada*** todas as informações pertinentes de que dispõem e que possam ser úteis para avaliar o risco ou o incidente. **[Alt. 85]**

~~3. A pedido de um Estado-Membro ou por sua própria iniciativa, a Comissão pode solicitar a um Estado-Membro que forneça todas as informações úteis de que dispõe sobre um determinado risco ou incidente.~~ **[Alt. 86]**

4. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza criminosa~~,, as autoridades competentes ou a Comissão~~ ***e se o operador de mercado em causa tiver comunicado incidentes suspeitos de serem de natureza criminosa grave, conforme referido no artigo 15.º, n.º 4, os Estados-Membros*** devem ~~informar~~ ***assegurar que*** o Centro Europeu da Cibercriminalidade na Europol ***seja informado, sempre que necessário***. **[Alt. 87]**

4-A. Os membros da rede de cooperação não tornam públicas quaisquer informações recebidas relativamente a riscos e incidentes referidos no n.º 1, sem terem recebido aprovação prévia por parte do balcão único notificante.

Além disso, antes de partilhar informação na rede de cooperação, o balcão único notificante comunica a sua intenção ao operador de mercado a que se refere a informação e, caso considere adequado, torna anónima essa informação. **[Alt. 88]**

4-B. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza técnica transfronteiras grave, os balcões únicos ou a Comissão devem informar a ENISA. **[Alt. 89]**

5. A Comissão fica habilitada a adotar atos delegados, nos termos do artigo 18.º, que especifiquem melhor os riscos e incidentes que desencadeiam o alerta rápido referido no n.º 1 do presente artigo.

Artigo 11.º

Resposta coordenada

1. Na sequência de um alerta rápido referido no artigo 10.º, as ~~autoridades competentes~~ ***os balcões únicos*** devem, após a avaliação das informações pertinentes, chegar a acordo ***sem demora injustificada*** quanto a uma resposta coordenada, conforme com o plano de cooperação da União em matéria de SRI referido no artigo 12.º. **[Alt. 90]**

2. As várias medidas adotadas a nível nacional em resultado da resposta coordenada devem ser comunicadas à rede de cooperação.

Artigo 12.º

Plano de cooperação da União em matéria de SRI

1. A Comissão tem poderes para adotar, por meio de atos de execução, um plano de cooperação da União em matéria de SRI. Os referidos atos de execução devem ser adotados em conformidade com o procedimento de exame referido no artigo 19.º, n.º 3.

2. O plano de cooperação da União em matéria de SRI deve prever:

a) Para efeitos do artigo 10.º:

— uma definição do formato e dos procedimentos para a recolha e a partilha ~~pelas autoridades competentes~~ de informações compatíveis e comparáveis sobre os riscos e incidentes ***pelos balcões únicos***, **[Alt. 91]**

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

b) os processos a seguir para as respostas coordenadas ao abrigo do artigo 11.º, incluindo a identificação dos papéis e responsabilidades e os procedimentos de cooperação;

c) um roteiro para os exercícios e a formação em matéria de SRI para reforçar, validar e testar o plano;

d) um programa para a transferência de conhecimentos entre os Estados-Membros no que diz respeito ao reforço das capacidades e à aprendizagem entre pares;

e) um programa de sensibilização e formação entre os Estados-Membros.

3. O plano de cooperação da União em matéria de SRI deve ser adotado o mais tardar um ano após a entrada em vigor da presente diretiva e ser revisto periodicamente. ***Os resultados de cada revisão são comunicados ao Parlamento Europeu.*** **[Alt. 92]**

3-A. Deve ser garantida a coerência entre o plano de cooperação da União em matéria de SRI e as estratégias e os planos de cooperação nacionais em matéria de SRI, tal como previsto no artigo 5.º. **[Alt. 93]**

Artigo 13.º

Cooperação internacional

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 ***e devem especificar o procedimento de controlo a seguir para assegurar a proteção desses dados. O Parlamento Europeu é informado sobre a negociação dos acordos. As transferências de dados pessoais para destinatários em países fora da União são realizadas nos termos dos artigos 25.º e 26.º da Diretiva 95/46/CE e do artigo 9.º do Regulamento (CE) n.º 45/2001***. **[Alt. 94]**

Artigo 13.º-A

Nível de relevância dos operadores de mercado

Os Estados-Membros podem determinar o nível de relevância dos operadores de mercado, tendo em conta as especificidades dos setores, parâmetros como a importância de determinado operador de mercado para a manutenção de um nível suficiente do serviço setorial, o número de intervenientes fornecidos pelo operador de mercado e o período de tempo até a descontinuação dos serviços essenciais do operador de mercado ter um impacto negativo na manutenção de atividades económicas e sociais vitais. **[Alt. 95]**

CAPÍTULO IV

SEGURANÇA DAS REDES E DOS SISTEMAS INFORMÁTICOS DAS ADMINISTRAÇÕES PÚBLICAS E DOS OPERADORES DO MERCADO

Artigo 14.º

Exigências de segurança e notificação de incidentes

1. Os Estados-Membros devem assegurar que ~~as administrações públicas e~~ os operadores do mercado adotem medidas técnicas e organizacionais adequadas ***e proporcionadas*** para ***detetar e*** gerir ***eficazmente*** 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~~ ***o estado da técnica***, essas medidas devem ~~garantir~~ ***assegurar*** um nível de segurança adequado ~~em função do~~ ***ao*** risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a ***segurança das*** suas redes e ~~sistema informático~~ dos seus ***sistemas informáticos*** nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas. **[Alt. 96]**

2. Os Estados-Membros devem assegurar que ~~as administrações públicas e~~ os operadores do mercado notifiquem ***sem demora injustificada*** as autoridades competentes ***ou os balcões únicos*** dos incidentes com impacto significativo na ~~segurança~~ ***continuidade*** dos serviços essenciais que fornecem. ***A notificação não deve expor a parte notificante a responsabilidades acrescidas.***

Para determinar a importância do impacto de um incidente, devem ser tidos em conta, nomeadamente, os seguintes parâmetros: **[Alt. 97]**

a) o número de utilizadores cujo serviço essencial é afetado; **[Alt. 98]**

b) a duração do incidente; **[Alt. 99]**

c) a repartição geográfica no que se refere à área afetada pelo incidente. **[Alt. 100]**

Esses parâmetros devem ser mais bem especificados nos termos do artigo 8.º, n.º 3, alínea i-B). **[Alt. 101]**

2-A. Os operadores do mercado notificam as autoridades competentes ou o balcão único do Estado-Membro em que o serviço essencial é afetado dos incidentes a que se referem os n.os 1 e 2. Quando são afetados serviços essenciais em mais de um Estado-Membro, o balcão único que recebeu a notificação alerta, com base na informação fornecida pelo operador de mercado, os outros balcões únicos afetados. O operador de mercado deve ser informado, o mais rapidamente possível, sobre os outros balcões únicos que foram informados do incidente, bem como das medidas tomadas, resultados ou qualquer informação relevante para o incidente. **[Alt. 102]**

2-B. Sempre que a notificação contenha dados pessoais, só pode ser divulgada a destinatários na autoridade competente ou no balcão único notificado que necessitem de os tratar para o exercício das suas funções, de acordo com as regras aplicáveis em matéria de proteção de dados. Os dados divulgados limitam-se ao estritamente necessário para o exercício das funções dos destinatários. **[Alt. 103]**

2-C. Operadores do mercado não abrangidos pelo anexo II podem notificar incidentes numa base facultativa, tal como especificado no artigo 14.º, n.º 2. **[Alt. 104]**

3. Os n.os 1 e 2 aplicam-se a todos os operadores do mercado que forneçam serviços na União Europeia.

4. ***Após consultar*** a autoridade competente ***e o operador de mercado notificados, o balcão único*** pode informar o público ~~ou exigir que as administrações públicas e os operadores do mercado o façam~~ ***sobre os incidentes ocorridos***, caso ~~considere que a revelação do~~ ***considere que é necessário sensibilizá-lopara evitar um*** incidente ~~é do interesse público. Uma vez por ano, a autoridade competente apresenta à rede de cooperação um relatório resumido sobre as notificações recebidas e as medidas tomadas em conformidade com o presente número~~***ou para fazer face a um incidente em curso, ou caso o operador de mercado, confrontado com um incidente, se tenha recusado a analisar uma vulnerabilidade estrutural grave associada ao incidente, sem demora injustificada***.

Antes de qualquer divulgação pública, a autoridade competente notificada deve assegurar, por um lado, que o operador de mercado em causa tenha a possibilidade de ser ouvido e, por outro, que a decisão de divulgação seja devidamente ponderada com o interesse público.

Sempre que informação sobre incidentes individuais é divulgada publicamente, a autoridade competente ou o balcão único notificados devem assegurar que a informação seja tão anónima quanto possível.

A autoridade competente ou o balcão único devem, se razoavelmente possível, facultar aos operadores de mercado em causa informações que contribuem para resolver de forma eficaz o incidente notificado.

Uma vez por ano, ~~a autoridade competente~~ ***o balcão único*** apresenta à rede de cooperação um relatório resumido sobre as notificações recebidas***, incluindo o número de notificações*** e ***no que diz respeito aos parâmetros do incidente enumerados no n.º 2 do presente artigo, e*** as medidas tomadas em conformidade com o presente número. **[Alt. 105]**

4-A. Os Estados-Membros devem encorajar os operadores de mercado a divulgarem voluntariamente os incidentes que envolvam as suas empresas nos seus relatórios financeiros. **[Alt. 106]**

~~5. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 18.º para definir as circunstâncias em que as administrações públicas e os operadores do mercado são obrigados a notificar incidentes.~~ **[Alt. 107]**

6. ~~Sob reserva de quaisquer atos delegados adotados ao abrigo do n.º 5~~, As autoridades competentes ***ou os balcões únicos*** podem adotar orientações ~~e, se for caso disso, emitir instruções~~ para as circunstâncias em que ~~as administrações públicas e~~ os operadores do mercado são obrigados a notificar incidentes. **[Alt. 108]**

7. A Comissão fica habilitada a definir, por meio de atos de execução, as modalidades e procedimentos aplicáveis para efeitos do n.º 2. Esses atos de execução são adotados pelo procedimento de exame referido no artigo 19.º, n.º 3.

8. Os n.os 1 e 2 não se aplicam às microempresas na aceção da Recomendação 2003/361/CE da Comissão ([1])***, salvo se a microempresa funcionar como filial de um operador de mercado, na aceção do artigo 3.º, n.º 8, alínea b)***. **[Alt. 109]**

8-A. Os Estados-Membros podem decidir aplicar o presente artigo e o artigo 15.º, com as necessárias adaptações, ás administrações públicas. **[Alt. 110]**

Artigo 15.º

Aplicação e execução

1. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham ~~todos~~ os poderes necessários para ~~investigar os casos de incumprimento por parte das administrações públicas ou dos~~ ***assegurar o cumprimento das obrigações que incumbem aos*** 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. **[Alt. 111]**

([1]) Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

Quinta-feira, 13 de março de 2014

2. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham poderes para exigir que os operadores do mercado~~e às administrações públicas~~: **[Alt. 112]**

a) Forneçam as informações necessárias para avaliar a segurança das suas redes e sistemas informáticos, incluindo documentação sobre as políticas de segurança;

b) ***Apresentem provas da aplicação efetiva das políticas de segurança, tais como os resultados de*** a uma auditoria de segurança efetuada por um organismo qualificado independente ou autoridade nacional e coloquem ~~os resultados~~ ***as provas*** à disposição da autoridade competente ***ou do balcão único***. **[Alt. 113]**

Ao transmitir o pedido, as autoridades competentes e os balcões únicos declaram a finalidade do pedido e especificam de forma satisfatória a informação exigida. **[Alt. 114]**

3. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham poderes para emitir instruções vinculativas aos operadores do mercado ~~e às administrações públicas~~. **[Alt. 115]**

3-A. Em derrogação da alínea b) do n.º 2 do presente artigo, os Estados-Membros podem decidir que as autoridades competentes ou os balcões únicos, consoante o caso, devem aplicar um procedimento diferente a operadores de mercado específicos, com base no seu nível de relevância determinado nos termos do artigo 13.º-A. Caso os Estados-Membros assim o decidam:

a) As autoridades competentes ou os balcões únicos, consoante o caso, têm poderes para apresentar um pedido suficientemente específico aos operadores de mercado a solicitar que forneçam provas da aplicação efetiva das políticas de segurança, tais como os resultados de uma auditoria de segurança efetuada por um auditor interno qualificado, e coloquem as provas à disposição da autoridade competente ou do balcão único;

b) Se for caso disso, no seguimento da apresentação pelo operador de mercado do pedido referido na alínea a), a autoridade competente ou o balcão único pode solicitar provas adicionais ou que seja efetuada uma auditoria suplementar pelo organismo qualificado independente ou pela autoridade nacional.

3-B. Os Estados-Membros podem decidir reduzir o número e a intensidade das auditorias a um determinado operador de mercado, se a sua auditoria de segurança tiver demonstrado o cumprimento dos requisitos do capítulo IV de forma coerente. **[Alt. 116]**

4. As autoridades competentes ***e os balcões únicos*** devem ~~notificar~~ ***informar*** os ***operadores de mercado em causa acerca da possibilidade de comunicação de*** incidentes que se suspeite serem de caráter criminoso grave às autoridades policiais e judiciais. **[Alt. 117]**

5. ***Sem prejuízo das regras aplicáveis em matéria de proteção dos dados,*** 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. ***Os balcões únicos e as autoridades responsáveis pela proteção dos dados criam, em cooperação com a ENISA, mecanismos de troca de informações e um modelo único, ambos utilizados para as notificações, nos termos do artigo 14.º, n.º 2, da presente diretiva e da restante legislação da União em matéria de proteção de dados.*** **[Alt. 118]**

6. Os Estados-Membros devem assegurar que todas as obrigações impostas ~~às administrações públicas e~~ aos operadores do mercado ao abrigo do presente capítulo possam ser objeto de avaliação judicial. **[Alt. 119]**

6-A. Os Estados-Membros podem decidir aplicar o presente artigo e o artigo 14.º, com as necessárias adaptações, às administrações públicas. **[Alt. 120]**

Artigo 16.º

Normalização

1. Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados-Membros***, sem exigirem a utilização de qualquer tecnologia em particular,*** devem encorajar a utilização das normas e/ou especificações ***europeias ou internacionais interoperáveis*** pertinentes para a segurança das redes e da informação. **[Alt. 121]**

2. A Comissão ~~estabelece, por meio de atos de execução~~ ***confere um mandato a um organismo europeu de normalização relevante para, após consulta às partes interessadas pertinentes, estabelecer*** uma lista das normas ***e/ou especificações*** referidas no n.º 1, que será publicada no *Jornal Oficial da União Europeia*. **[Alt. 122]**

CAPÍTULO V

DISPOSIÇÕES FINAIS

Artigo 17.º

Sanções

1. Os Estados-Membros determinam o regime de sanções aplicável às violações das disposições nacionais aprovadas em execução da presente diretiva e adotam as medidas necessárias para assegurar a aplicação dessas disposições. As sanções impostas devem ser efetivas, proporcionadas e dissuasivas. O mais tardar até à data da transposição da presente diretiva, os Estados-Membros notificam à Comissão as referidas disposições, devendo notificá-la imediatamente de qualquer alteração posterior das mesmas.

1-A. Os Estados-Membros devem assegurar que as sanções referidas no n.º 1 do presente artigo apenas se aplicam quando o operador de mercado não tiver cumprido as suas obrigações nos termos do capítulo IV, deliberadamente ou por negligência grave. **[Alt. 123]**

2. Os Estados-Membros devem garantir que, quando um incidente de segurança envolver dados pessoais, as sanções previstas sejam coerentes com as sanções previstas no 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 ([1]).

Artigo 18.º

Exercício da delegação

1. O poder de adotar os atos delegados é conferido à Comissão e nas condições estabelecidas no presente artigo.

2. O poder de adotar os atos delegados referido no artigo 9.º, n.º 2, e no artigo 10.º, n.º 5 é conferido à Comissão por um prazo de 5 anos.. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por prazos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

3. A delegação de poderes referida ~~nos artigos~~ ***no artigo*** 9.º, n.º 2~~, 10.º, n.º 5, e 14.º~~, n.º 5, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela . A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor. **[Alt. 124]**

4. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

([1]) SEC(2012) 72 final.

5. Os atos delegados adotados nos termos do artigo 9.º, n.º 2~~, do artigo 10.º, n.º 5, e do artigo 14.º, n.º 5~~, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não têm objeções a formular. O referido prazo pode ser prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho. **[Alt. 125]**

Artigo 19.º

Procedimento de Comité

1. A Comissão é assistida por um comité (Comité de Segurança das Redes e da Informação). Esse Comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se faça referência ao presente número, aplica-se o artigo 4.º do Regulamento (UE) n.º 182/2011.

3. Caso se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

Artigo 20.º

Avaliação

A Comissão avalia periodicamente a aplicação da presente diretiva***, em especial a lista constante do anexo II,*** e apresenta 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 esse efeito, a Comissão pode solicitar que os Estados-Membros lhe forneçam informações sem demora injustificada. **[Alt. 126]**

Artigo 21.º

Transposição

1. Os Estados-Membros devem adotar e publicar as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva o mais tardar até [um ano e meio após a adoção]. Os Estados-Membros devem comunicar imediatamente à Comissão o texto dessas medidas.

Os Estados-Membros devem aplicar as referidas disposições a partir de [um ano e meio após a adoção].

Quando os Estados-Membros aprovarem essas disposições, estas devem incluir uma referência à presente diretiva ou ser acompanhadas dessa referência aquando da sua publicação oficial. As modalidades da referência são estabelecidas pelos Estados-Membros.

2. Os Estados-Membros devem comunicar à Comissão o texto das principais disposições de direito interno que adotarem no domínio abrangido pela presente diretiva.

Artigo 22.º

Entrada em vigor

A presente diretiva entra em vigor no [vigésimo] dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Artigo 23.º

Destinatários

Os destinatários da presente diretiva são os Estados-Membros.

Feito em …,

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

ANEXO I

Obrigações a cumprir e tarefas ~~da equipa~~ ***das equipas*** de resposta a emergências informáticas (CERT) **[Alt. 127]**

As obrigações a cumprir e as tarefas da CERT devem ser definidas de modo claro e adequado e apoiadas por políticas e/ou regulamentação nacionais. Devem incluir os seguintes elementos:

1) Obrigações da CERT:

   ~~a)~~ ~~A~~ **As** CERT ~~deve~~ ***devem*** garantir uma elevada disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais e dispondo de vários meios para ~~contactar e ser contactada~~ ***contactarem e serem contactadas em qualquer momento***. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos da sua base de clientes e dos parceiros de cooperação. **[Alt. 128]**

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

   c) Os gabinetes ~~da~~ ***das*** CERT e os sistemas informáticos de apoio devem estar situados em locais seguros, ***com redes e sistemas informáticos seguros***. **[Alt. 129]**

   d) Deve ser criado um sistema de gestão da qualidade dos serviços para acompanhar o desempenho da CERT e assegurar um processo de melhoria constante. Este sistema deve basear-se em métodos de medição claramente definidos que incluam os níveis de serviço formais e os principais indicadores de desempenho.

   e) Continuidade das atividades:

      — A CERT deve ser equipada com um sistema adequado de gestão e encaminhamento dos pedidos, a fim de facilitar a transferência de responsabilidades;

      — A CERT deve dispor de pessoal suficiente capaz de assegurar a sua operacionalidade a qualquer momento;

      — A CERT deve apoiar-se numa infraestrutura cuja continuidade esteja assegurada. Para o efeito, devem ser criados sistemas redundantes e espaço de trabalho de recurso para que a CERT garanta um acesso permanente aos meios de comunicação.

2) Tarefas da CERT

   a) A CERT deve desempenhar pelo menos as seguintes tarefas:

      — ***Detetar e*** monitorizar os incidentes a nível nacional; **[Alt. 130]**

      — Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, comunicações e fazer a divulgação de informações às partes interessadas relevantes sobre riscos e incidentes;

      — Intervir em caso de incidentes;

      — Proceder à análise dinâmica dos riscos e incidentes e tomar consciência da situação;

      — Sensibilizar o público em geral para os riscos associados às atividades em linha;

      — ***Participar ativamente nas redes de cooperação CERT internacionais e da União;*** **[Alt. 131]**

      — Organizar campanhas sobre a SRI.

   b) A CERT deve estabelecer relações de cooperação com o setor privado.

   c) A fim de facilitar a cooperação, a CERT deve promover a adoção e a utilização de práticas comuns ou normalizadas para:

      — os procedimentos de gestão dos riscos e incidentes;

      — os sistemas de classificação dos incidentes, riscos e informações;

      — as taxonomias para a medição;

      — os formatos de intercâmbio de informações sobre os riscos, os incidentes e as convenções sobre a denominação dos sistemas.

Quinta-feira, 13 de março de 2014

ANEXO II

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~~

~~4. Motores de pesquisa~~

~~5. Serviços de computação em nuvem~~

~~6. Lojas de aplicações em linha~~

~~**Referidos no artigo 3.º, n.º 8, alínea b) [Alt. 132]**~~

1. Energia

a) Eletricidade

— Fornecedores ~~de eletricidade e gás~~

— Operadores da rede de distribuição ~~de gás e/ou eletricidade~~ e retalhistas que vendem aos consumidores finais

— ~~Operadores da rede de transporte de gás natural, operadores de armazenagem e operadores de GNL~~

— Operadores da rede de transporte de eletricidade

b) Petróleo

— Oleodutos e armazenamento de petróleo

— ***Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo***

c) Gás

— ~~Operadores do mercado da eletricidade e do gás~~

— ***Fornecedores***

— ***Operadores da rede de distribuição e retalhistas que vendem aos consumidores finais***

— ***Operadores da rede de transporte de gás natural, operadores de sistemas de armazenamento e operadores de sistemas de gás natural liquefeito***

— Operadores ~~da~~ ***de instalações de*** produção de ~~petróleo e~~ gás natural, ~~instalações de~~ de refinamento e de tratamento, e ***de instalações de armazenamento e transporte***

— ***Operadores do mercado do gás*** **[Alt. 133]**

2. Transportes

— ~~Transportadores aéreos (transporte aéreo de mercadorias e passageiros)~~

— ~~Transportadores marítimos (companhias de transporte marítimo e costeiro de passageiros e companhias de transporte marítimo e costeiro de mercadorias)~~

— ~~Transportes ferroviários (gestores de infraestruturas, empresas integradas e operadores de transportes ferroviários)~~

~~— Aeroportos~~

~~— Portos~~

~~— Operadores de controlo da gestão do tráfego~~

~~— Serviços logísticos auxiliares de: a) depósito e armazenagem; b) movimentação de carga; c) outras atividades auxiliares de transporte~~

a) Transporte rodoviário

i) operadores de controlo da gestão do tráfego

ii) serviços logísticos auxiliares:

— depósito e armazenamento,

— movimentação de carga, e

— outras atividades auxiliares de transporte

b) Transporte ferroviário

i) Transportes ferroviários (gestores de infraestruturas, empresas integradas e operadores de transportes ferroviários)

ii) Operadores de controlo da gestão do tráfego

iii) Serviços logísticos auxiliares:

— depósito e armazenamento,

— movimentação de carga, e

— outras atividades auxiliares de transporte

c) Transporte aéreo

i) Transportadores aéreos (transporte aéreo de mercadorias e passageiros)

ii) Aeroportos

iii) Operadores de controlo da gestão do tráfego

iv) Serviços logísticos auxiliares:

— depósito,

— movimentação de carga, e

— outras atividades auxiliares de transporte

d) Transportes marítimos

i) Transportadores marítimos (companhias de transporte marítimo costeiro e em águas marítimas interiores de passageiros e companhias de transporte marítimo costeiro e em águas marítimas interiores de mercadorias) *[Alt. 134]*

3. Setor bancário: instituições de crédito, nos termos do artigo 4.º, n.º 1, da Diretiva 2006/48/CE do Parlamento Europeu e do Conselho ([1])

([1]) Diretiva 2006/48/CE do Parlamento Europeu e do Conselho, de 14 de Junho de 2006, relativa ao acesso à atividade das instituições de crédito e ao seu exercício (JO L 177 de 30.6.2006, p. 1).

4. Infraestruturas do mercado financeiro: ~~bolsas~~ ***mercados regulamentados, sistemas de negociação multilateral, sistemas de negociação organizados*** e contrapartes centrais **[Alt. 135]**

5. Setor da saúde: instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas) e outras entidades envolvidas na prestação de cuidados de saúde

5-A. Produção e abastecimento de água **[Alt. 136]**

5-B. Cadeia de abastecimento alimentar **[Alt. 137]**

5-C. Nós de comutação da Internet **[Alt. 138]**