COMISSÃO
EUROPEIA

Bruxelas, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

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

{SWD(2013) 31 final}
{SWD(2013) 32 final}

EXPOSIÇÃO DE MOTIVOS

A diretiva proposta tem por objetivo garantir um elevado nível comum de segurança das redes e da informação (SRI). Tal implica melhorar a segurança da Internet e das redes e sistemas informáticos privados em que assenta o funcionamento das nossas sociedades e economias. Este objetivo será alcançado exigindo aos Estados-Membros que aumentem o seu nível de preparação e melhorem a cooperação entre si e exigindo aos operadores das infraestruturas críticas, como é o caso da energia, dos transportes e dos principais fornecedores de serviços da sociedade da informação (plataformas de comércio eletrónico, redes sociais, etc.), bem como às administrações públicas, que adotem medidas adequadas para gerir os riscos de segurança e comunicar os incidentes graves às autoridades nacionais competentes.

A presente proposta está relacionada com a Comunicação Conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança sobre uma Estratégia Europeia de Cibersegurança. A estratégia pretende assegurar um ambiente digital seguro e fiável ao mesmo tempo que promove e protege os direitos fundamentais e outros valores fundamentais da UE. A presente proposta é a principal ação da estratégia. As outras ações previstas neste domínio incidem na sensibilização, no desenvolvimento de um mercado interno para os produtos e serviços de cibersegurança e na promoção dos investimentos em I&D. Estas ações serão complementadas por outras no intuito de intensificar a luta contra a cibercriminalidade e de definir uma política internacional de cibersegurança para a UE.

1.1. Justificação e objetivos da proposta

A SRI é cada vez mais importante para a nossa economia e a nossa sociedade. Constitui também uma condição prévia importante para criar um ambiente fiável para o comércio de serviços em todo o mundo. No entanto, os sistemas informáticos podem ser afetados por incidentes relacionados com a segurança, tais como erros humanos, eventos naturais, falhas técnicas ou ataques malévolos. Estes incidentes estão a tornar-se cada vez mais graves, mais frequentes e mais complexos. A consulta pública em linha da Comissão intitulada «Melhorar a segurança das redes e da informação na UE[1]» permitiu constatar que 57 % dos inquiridos tinham sofrido incidentes de SRI durante o ano anterior com um impacto grave nas suas atividades. A falta de segurança pode comprometer serviços vitais, dependendo da integridade das redes e dos sistemas informáticos. Tal pode impedir o funcionamento das empresas, causar prejuízos financeiros consideráveis à economia da UE e prejudicar o bem-estar social.

[1] A consulta pública em linha sobre «Melhorar a segurança das redes e da informação na UE» decorreu de 23 de julho a 15 de outubro de 2012.

Além disso, enquanto instrumentos de comunicação sem fronteiras, os sistemas de informação digitais, em especial a Internet, ligam todos os Estados-Membros e desempenham um papel fundamental na facilitação da circulação transfronteiras de mercadorias, serviços e pessoas. A perturbação significativa destes sistemas num Estado-Membro pode afetar outros Estados-Membros e a UE no seu conjunto. A resiliência e a estabilidade das redes e dos sistemas informáticos é, por conseguinte, essencial para a realização do mercado único digital e o bom funcionamento do mercado interno. A probabilidade e a frequência de incidentes e a incapacidade de garantir uma proteção eficaz também minam a confiança do público nas redes e serviços informáticos: por exemplo, o Eurobarómetro de 2012 sobre a cibersegurança verificou que 38 % dos utilizadores da Internet na UE estão preocupados com a segurança dos pagamentos em linha e alteraram o seu comportamento em virtude de preocupações relacionadas com a segurança: 18 % estão menos dispostos a comprar mercadorias em linha e 15 % estão menos dispostos a utilizar o sistema bancário em linha[2].

A situação atual na UE, que reflete a abordagem puramente voluntária seguida até à data, não proporciona proteção suficiente contra os incidentes e os riscos de SRI em toda a UE. As capacidades e os mecanismos existentes em matéria de SRI são simplesmente insuficientes para fazerem face à rápida evolução das ameaças e garantirem um nível elevado de proteção comum em todos os Estados-Membros.

Apesar das iniciativas empreendidas, os Estados-Membros possuem níveis muito diferentes de capacidades e grau de preparação, o que teve por resultado a adoção de abordagens fragmentadas em toda a UE. Dado o facto de as redes e os sistemas estarem interligados, a SRI geral da UE é enfraquecida pelos Estados-Membros com um nível insuficiente de proteção. Esta situação também dificulta a criação de um clima de confiança entre pares, o que é uma condição prévia para a cooperação e a partilha de informações. A consequência desta situação é que só existe cooperação entre uma minoria de Estados-Membros com um elevado nível de capacidades.

Por conseguinte, não existe atualmente qualquer mecanismo eficaz a nível da UE que assegure uma cooperação e colaboração eficazes e a partilha de informação fiável sobre os incidentes e riscos de SRI entre os Estados-Membros. Esta situação pode ter por resultado intervenções não coordenadas a nível da regulamentação, estratégias incoerentes e normas divergentes, conducentes a uma proteção insuficiente da SRI em toda a UE. Podem também surgir entraves ao mercado interno, o que gera custos de conformidade para as empresas que exercem a sua atividade em mais de um Estado-Membro.

Por último, os intervenientes que gerem as infraestruturas críticas ou prestam serviços essenciais para o funcionamento das nossas sociedades não estão devidamente obrigados a adotar medidas de gestão dos riscos e a proceder ao intercâmbio de informações com as autoridades competentes. Por um lado, as empresas carecem de incentivos eficazes para assegurarem uma verdadeira gestão dos riscos que envolva a sua avaliação e a adoção de medidas adequadas para garantir a segurança das redes e da informação. Por outro, uma grande parte dos incidentes não chega ao conhecimento das autoridades competentes e passa despercebida. No entanto, a informação sobre os incidentes é essencial para que as autoridades públicas possam reagir, tomar as medidas de resolução necessárias e fixar prioridades estratégicas adequadas em matéria de SRI.

O atual quadro regulamentar obriga unicamente as empresas de telecomunicações a adotarem medidas de gestão de riscos e a comunicarem os incidentes graves em matéria de SRI. Contudo, muitos outros setores recorrem às TIC como instrumento de trabalho de base viabilizador, pelo que também deverão estar interessados na SRI. Certos prestadores de

[2] Eurobarómetro 390/2012.

serviços e infraestruturas encontram-se numa situação particularmente vulnerável por estarem fortemente dependentes de redes e sistemas informáticos que funcionem corretamente. Estes setores desempenham um papel fundamental na prestação de serviços essenciais de apoio à nossa economia e à nossa sociedade, revestindo-se a segurança dos seus sistemas de especial importância para o funcionamento do mercado interno. Entre esses setores, contam-se o setor bancário, a bolsa, a produção, transmissão e distribuição de energia, os transportes (aéreos, ferroviários e marítimos), a saúde, os serviços de Internet e as administrações públicas.

Por conseguinte, é necessário proceder a uma mudança radical do modo como a SRI é encarada na UE. São necessárias obrigações regulamentares para estabelecer uma base equitativa e suprir as lacunas legislativas existentes. Numa tentativa de resolver estes problemas e aumentar o nível de SRI na União Europeia, a diretiva proposta tem os objetivos a seguir expostos.

Em primeiro lugar, a proposta exige que todos os Estados-Membros garantam um nível mínimo de capacidades nacionais mediante a criação de autoridades competentes para a SRI e de equipas de resposta a emergências informáticas (CERT) e a adoção de estratégias e planos de cooperação nacionais em matéria de SRI.

Em segundo lugar, as autoridades nacionais competentes devem cooperar numa rede que permita assegurar uma coordenação segura e eficaz, incluindo o intercâmbio coordenado de informações, bem como a deteção e a resposta a nível da UE. Através desta rede, os Estados-Membros devem trocar informações e cooperar para enfrentar as ameaças e os incidentes relativos à SRI com base no plano de cooperação europeia nesta matéria.

Em terceiro lugar, com base no modelo da Diretiva-Quadro das comunicações eletrónicas, a proposta visa garantir o desenvolvimento de uma cultura de gestão dos riscos e a partilha de informação entre os setores público e privado. Será pedido às empresas dos diferentes setores críticos acima referidos e às administrações públicas que avaliem os riscos com que se deparam e adotem medidas adequadas e proporcionadas para garantir a segurança das redes e da informação. Estas entidades serão obrigadas a informar as autoridades competentes sobre todos os incidentes que comprometam seriamente as suas redes e sistemas informáticos e afetem significativamente a continuidade de serviços de importância crítica e o fornecimento de produtos.

1.2. Contexto geral

Já em 2001, na sua Comunicação «Segurança das Redes e da informação: Proposta de abordagem de uma política europeia», a Comissão tinha salientado a importância crescente da SRI[3]. Seguiu-se-lhe a adoção em 2006 de uma estratégia para uma sociedade da informação segura[4], com o objetivo de desenvolver uma cultura de segurança das redes e da informação na Europa. Os seus principais elementos foram aprovados numa resolução do Conselho[5].

A Comissão adotou ainda, em 30 de março de 2009, uma Comunicação sobre a proteção das infraestruturas críticas da informação (PICI)[6], que se concentrava na proteção da Europa contra os ciberataques mediante o aumento da segurança. A Comunicação lançou um plano de ação de apoio aos esforços dos Estados-Membros para garantir a prevenção e a resposta. O plano de ação foi aprovado nas conclusões da Presidência da Conferência Ministerial sobre a proteção das infraestruturas críticas da informação (PICI), realizada em Talin, em 2009. Em

---

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf.
5 2007/068/01.
6 COM(2009) 149.

18 de dezembro de 2009, o Conselho adotou uma resolução sobre «Uma abordagem de colaboração europeia no domínio da segurança das redes e da informação»[7].

A Agenda Digital para a Europa[8] (ADE), adotada em maio de 2010, e as Conclusões do Conselho[9] a ela respeitantes salientaram a visão comum de que a confiança e a segurança são condições prévias fundamentais para a adoção generalizada das TIC e, deste modo, para a consecução dos objetivos da dimensão «crescimento inteligente» da estratégia Europa 2020[10]. No seu capítulo sobre confiança e segurança, a ADE sublinhou a necessidade de todas as partes interessadas se unirem num esforço global para garantir a segurança e a resiliência das infraestruturas TIC, concentrando-se na prevenção, preparação e sensibilização, bem como no desenvolvimento de mecanismos de segurança eficazes e coordenados. Concretamente, a ação-chave 6 da Agenda Digital para a Europa apela à adoção de medidas que visem pôr em prática uma política reforçada e de alto nível em matéria de SRI.

Na sua Comunicação de março de 2011 sobre a PICI, «Proteção das infraestruturas críticas da informação: para uma cibersegurança mundial»[11], a Comissão fez um balanço dos resultados alcançados desde a adoção do plano de ação da PICI em 2009, concluindo que a execução do plano mostrava que as abordagens de resposta puramente nacionais aos desafios da segurança e da resiliência não eram suficientes e que a Europa devia prosseguir os seus esforços para desenvolver uma abordagem coerente e cooperativa em toda a UE. A Comunicação sobre a PICI de 2011 anunciou uma série de ações e instou os Estados-Membros a desenvolverem capacidades e a estabelecerem uma cooperação transfronteiriça em matéria de SRI. Estas ações deviam ter sido, na sua maioria, concluídas até 2012, mas ainda não foram postas em prática.

Nas suas Conclusões de 27 de maio de 2011 sobre a PICI, o Conselho da União Europeia salientou a necessidade imperiosa de tornar as redes e os sistemas TIC resilientes e seguros face a todas as eventuais perturbações acidentais ou intencionais, de desenvolver um nível elevado de capacidade de preparação, segurança e resiliência em toda a UE, de melhorar as competências técnicas para permitir que a Europa responda ao desafio da proteção das redes e das infraestruturas da informação e, por último, de fomentar a cooperação entre os Estados-Membros através do desenvolvimento de mecanismos de cooperação em caso de ocorrência de incidentes.

1.3. Disposições da União Europeia e internacionais em vigor neste domínio

Através do Regulamento (CE) n.º 460/2004, a Comunidade Europeia criou em 2004 a Agência Europeia para a Segurança das Redes e da Informação (ENISA)[12] com o objetivo de contribuir para assegurar um elevado nível e desenvolver uma cultura de segurança na UE. Em 30 de setembro de 2010 foi adotada uma proposta para modernizar o mandato da ENISA[13], que está a ser debatida no Conselho e no Parlamento Europeu. O quadro regulamentar revisto das comunicações eletrónicas[14], em vigor desde novembro de 2009, impõe obrigações de segurança aos fornecedores de comunicações eletrónicas[15]. Estas obrigações tinham de ser transpostas para o direito nacional até maio de 2011.

---

7 2009/C 321/01.
8 COM(2010) 245.
9 Conclusões do Conselho, de 31 de maio de 2010, relativas a uma Agenda Digital para a Europa (10130/10).
10 COM(2010) 2020 e Conclusões do Conselho Europeu de 25 e 26 de março de 2010 (EUCO 7/10).
11 COM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:PT:HTML.
13 COM(2010) 521.
14 Ver http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.
15 Artigos 13.º-A e 13.º-B da Diretiva-Quadro.

Todos os intervenientes responsáveis pelo tratamento de dados (por exemplo, os bancos ou os hospitais) são obrigados pelo quadro regulamentar relativo à proteção de dados[16] a pôr em prática medidas de segurança para proteger os dados pessoais. Do mesmo modo, no âmbito da proposta da Comissão de 2012 relativa a um regulamento geral sobre a proteção de dados[17], os responsáveis pelo tratamento de dados terão de comunicar as violações de dados pessoais às autoridades nacionais de supervisão. Tal significa, por exemplo, que não é necessário notificar uma violação da SRI que afete a prestação de um serviço mas não comprometa os dados pessoais (por exemplo, uma falha das TIC numa companhia elétrica que tenha por resultado uma interrupção brusca de energia elétrica).

Inserido no quadro da Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, o «Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC)[18] define o quadro geral para a proteção das infraestruturas críticas na UE. Os objetivos do PEPIC são plenamente coerentes com a presente proposta e a diretiva deve aplicar-se sem prejuízo da Diretiva 2008/114/CE. O PEPIC não obriga os operadores a comunicarem as infrações significativas em matéria de segurança e não cria mecanismos para os Estados-Membros cooperarem e reagirem aos incidentes.

Os colegisladores estão atualmente a debater a proposta de diretiva, apresentada pela Comissão, relativa a ataques contra os sistemas de informação[19], que tem por objetivo harmonizar a criminalização de determinados tipos de conduta. Esta proposta abrange unicamente a criminalização de tipos específicos de conduta e não aborda a prevenção de riscos e incidentes em matéria de SRI, a resposta a incidentes que afetam a SRI nem a redução do seu impacto. A presente diretiva deverá aplicar-se sem prejuízo da Diretiva relativa a ataques contra os sistemas informáticos.

Em 28 de março de 2012, a Comissão adotou uma Comunicação sobre a criação de um Centro Europeu da Cibercriminalidade (EC3)[20]. Este centro, estabelecido em 11 de janeiro de 2013, faz parte do Serviço Europeu de Polícia (EUROPOL) e funcionará como ponto de contacto na luta contra a cibercriminalidade na UE. O EC3 destina-se a reunir conhecimentos europeus em matéria de cibercriminalidade tendo em vista ajudar os Estados-Membros a desenvolverem capacidades, prestar apoio às investigações de cibercriminalidade empreendidas pelos Estados-Membros e, em estreita colaboração com a Eurojust, tornar-se a voz coletiva dos investigadores de cibercriminalidade europeus junto das autoridades policiais e judiciárias.

As instituições, agências e organismos europeus instituíram as suas próprias equipas de resposta a emergências informáticas, denominadas CERT-UE.

A nível internacional, a UE trabalha na cibersegurança tanto a nível bilateral como multilateral. A Cimeira UE-EUA[21] de 2010 foi assinalada pela criação do Grupo de Trabalho UE-EUA sobre cibersegurança e cibercriminalidade. A UE está igualmente ativa noutros fóruns multilaterais pertinentes, como a Organização de Cooperação e de Desenvolvimento Económicos (OCDE), a Assembleia Geral das Nações Unidas (AGNU), a União Internacional das Telecomunicações (UIT), a Organização para a Segurança e a Cooperação na Europa

16 Diretiva 2002/58/CE de 12 de julho de 2002.
17 COM(2012) 11.
18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.
19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.
20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF.
21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

(OSCE), a Cimeira Mundial sobre a Sociedade da Informação (WSIS) e o Fórum sobre a Governação da Internet (IGF).

2. RESULTADOS DAS CONSULTAS DAS PARTES INTERESSADAS E AVALIAÇÕES DE IMPACTO

2.1. Consulta das partes interessadas e recurso a peritos especializados

Entre 23 de julho e 15 de outubro de 2012 foi efetuada uma consulta pública em linha, intitulada «Melhorar a segurança das redes e da informação na UE». No total, a Comissão recebeu 160 respostas ao questionário em linha.

O principal resultado foi que as partes interessadas manifestaram um apoio generalizado à necessidade de melhorar a SRI em toda a UE. Mais especificamente: 82,8 % dos inquiridos expressaram o ponto de vista de que os governos da UE deviam envidar mais esforços para garantir um elevado nível de segurança das redes e da informação; 82,8 % consideraram que os utilizadores da informação e dos sistemas não tinham conhecimento das ameaças e dos incidentes existentes em matéria de SRI; 66,3 % eram, em princípio, favoráveis à introdução de um requisito regulamentar para gerir os riscos da SRI; e 84,8 % declararam que esses requisitos deviam ser estabelecidos a nível da União Europeia. Um elevado número de inquiridos considerou que seria importante adotar requisitos de SRI, em especial nos seguintes setores: setor bancário e financeiro (91,1 %), energia (89,4 %), transportes (81,7 %), saúde (89,4 %), serviços Internet (89,1 %) e administrações públicas (87,5 %). Os inquiridos consideraram também que se fosse introduzida a obrigatoriedade de comunicação das violações da SRI à autoridade nacional competente, essa medida deveria ser fixada a nível da UE (65,1 %) e afirmaram que as administrações públicas deveriam igualmente ficar a ela sujeitas (93,5 %). Por último, os inquiridos afirmaram que a obrigação de aplicar a gestão dos riscos de SRI de acordo com os progressos da técnica não deveria acarretar custos adicionais significativos (63,4 %) e que a exigência de comunicar as violações da segurança não deveria causar custos adicionais significativos (72,3 %).

Os Estados-Membros foram consultados em várias formações do Conselho pertinentes, no contexto do Fórum Europeu dos Estados-Membros (FEEM), na Conferência sobre a cibersegurança organizada pela Comissão e pelo Serviço Europeu para a Ação Externa em 6 de julho de 2012, bem como nas reuniões bilaterais específicas convocadas a pedido dos diversos Estados-Membros.

Realizaram-se igualmente debates com o setor privado no âmbito da Parceria Público-Privada Europeia para a Resiliência[22] e em reuniões bilaterais. Quanto ao setor público, a Comissão travou conversações com a ENISA e as CERT para as instituições da UE.

2.2. Avaliação de impacto

A Comissão procedeu à avaliação do impacto de três opções estratégicas:

Opção 1: Manutenção do *status quo* (cenário de base) - manutenção da atual abordagem;

Opção 2: Abordagem regulamentar, que consiste numa proposta legislativa que prevê o estabelecimento de um quadro jurídico comum da UE para a SRI no que diz respeito às capacidades dos Estados-Membros, aos mecanismos de cooperação a nível da UE e aos requisitos dos principais intervenientes privados e administrações públicas;

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

Opção 3: Abordagem mista, que combina a possibilidade de iniciativas voluntárias por parte dos Estados-Membros em termos de capacidades e mecanismos de SRI tendo em vista a cooperação a nível da UE com os requisitos regulamentares para os principais intervenientes privados e administrações públicas.

A Comissão concluiu que a opção 2 era a que produzia impactos mais positivos, já que permite melhorar consideravelmente a proteção dos consumidores, das empresas e das administrações da UE contra os incidentes de SRI. Mais concretamente, as obrigações que incumbem aos Estados-Membros asseguram uma preparação adequada a nível nacional, além de contribuírem para a criação de um clima de confiança mútua, o que constitui uma condição prévia para uma cooperação eficaz a nível da UE. A criação de mecanismos de cooperação a nível da UE através da rede garante uma prevenção e capacidade de resposta coerentes e coordenadas aos incidentes e riscos de SRI transfronteiras. A introdução de requisitos para que as administrações públicas e os principais intervenientes privados executem uma gestão dos riscos em matéria de SRI constitui um forte incentivo à gestão eficaz dos riscos de segurança. A obrigação de comunicar incidentes que tenham um impacto significativo na SRI aumenta a capacidade de resposta a incidentes e promove a transparência. Além disso, ao organizar-se internamente, a UE poderá alargar a sua influência internacional e tornar-se um parceiro ainda mais credível no que se refere à cooperação a nível bilateral e multilateral. Deste modo, a UE poderá também ficar em melhor posição para promover os direitos fundamentais e os valores fundamentais da UE no estrangeiro.

A avaliação quantitativa revelou que a opção 2 não impõe uma sobrecarga desproporcionada aos Estados-Membros. Os custos para o setor privado também serão limitados, dado que, em princípio, muitas das entidades em causa já cumprem os requisitos de segurança existentes (nomeadamente a obrigação de os responsáveis pelo tratamento de dados tomarem medidas técnicas e organizacionais para proteger os dados pessoais, incluindo medidas de SRI). As despesas existentes em matéria de segurança no setor privado também foram tidas em conta.

A presente proposta observa os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, em especial o direito ao respeito pela vida e comunicações privadas, 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 deve ser aplicada de acordo com esses direitos e princípios.

3. ELEMENTOS JURÍDICOS DA PROPOSTA

3.1. Base jurídica

A União Europeia tem poderes para adotar medidas que visem criar ou assegurar o funcionamento do mercado interno, em conformidade com as disposições pertinentes dos Tratados (artigo 26.° do Tratado sobre o Funcionamento da União Europeia – TFUE). Nos termos do artigo 114.° do TFUE, a UE pode adotar «medidas relativas à *aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros*, que tenham por objeto o estabelecimento e o funcionamento do mercado interno».

Como já referido, as redes e os sistemas informáticos desempenham um papel essencial na facilitação da circulação transfronteiras de mercadorias, serviços e pessoas. Estão frequentemente interligados e a Internet tem uma natureza global. Dada esta dimensão transnacional intrínseca, uma perturbação num Estado-Membro pode igualmente afetar outros Estados-Membros e a UE no seu conjunto. Por conseguinte, a resiliência e a estabilidade das redes e dos sistemas informáticos é essencial para o bom funcionamento do mercado interno.

Os legisladores da UE já reconheceram a necessidade de harmonizar as regras em matéria de SRI para assegurar o desenvolvimento do mercado interno. Foi este, nomeadamente, o caso do Regulamento (CE) n.º 460/2004, que cria a ENISA[23], que se baseia no artigo 114.º do TFUE.

As disparidades resultantes das capacidades, políticas e nível de proteção da SRI desiguais a nível dos Estados-Membros provocam entraves ao mercado interno e justificam a intervenção da UE.

3.2. Subsidiariedade

A intervenção europeia no domínio da SRI justifica-se pelo princípio da subsidiariedade.

Em primeiro lugar, tendo em conta o caráter transfronteiras da SRI, a não intervenção a nível da UE poderia conduzir a uma situação em que cada Estado-Membro agiria isoladamente, sem ter em conta as interdependências entre as redes e os sistemas informáticos na UE. Um grau apropriado de coordenação entre os Estados-Membros permitirá garantir que os riscos da SRI sejam bem geridos no contexto transfronteiras em que surjam. As divergências dos regulamentos relativos à SRI constituem um entrave para as empresas que pretendem exercer a sua atividade em vários países e à realização de economias de escala a nível mundial.

Em segundo lugar, as obrigações regulamentares a nível da UE são necessárias para criar condições equitativas e colmatar as lacunas legislativas. Uma abordagem numa base puramente voluntária teve por resultado que a cooperação se fizesse unicamente entre uma minoria de Estados-Membros com um elevado nível de capacidades. A fim de fazer participar todos os Estados-Membros, é necessário assegurar que todos tenham o nível mínimo exigido de capacidade. As medidas de SRI adotadas pelos governos têm de ser coerentes entre si e coordenadas a fim de limitar e minimizar as consequências dos incidentes de SRI. No âmbito da rede, através do intercâmbio das boas práticas e da participação constante da ENISA, as autoridades competentes e a Comissão cooperarão par facilitar uma aplicação convergente da diretiva em toda a UE. Além disso, a aplicação de uma política concertada em matéria de SRI pode ter um impacto muito positivo na proteção eficaz dos direitos fundamentais e, mais especificamente, no direito à proteção dos dados pessoais e da privacidade. A ação a nível da UE permitirá, por conseguinte, aumentar a eficácia das políticas nacionais existentes e facilitar o seu desenvolvimento.

As medidas propostas justificam-se também por razões de proporcionalidade. Os requisitos para os Estados-Membros são estabelecidos ao nível mínimo necessário para alcançar um nível adequado de preparação e permitir uma cooperação baseada na confiança. Tal permite também que os Estados-Membros tenham devidamente em conta as especificidades nacionais e assegura que os princípios comuns da UE sejam aplicados adequadamente. O vasto âmbito de aplicação permitirá aos Estados-Membros aplicarem a diretiva tendo em conta os riscos enfrentados atualmente a nível nacional, tal como identificados na estratégia nacional de SRI. Os requisitos para concretizar o objetivo da gestão dos riscos destinam-se unicamente a entidades críticas e impõem medidas que são proporcionais aos riscos. A consulta pública sublinhou a importância de garantir a segurança dessas entidades críticas. As exigências de comunicação só diriam respeito aos incidentes com um impacto significativo. Como já referido, as medidas não imporão custos desproporcionados, visto que muitas destas entidades já são obrigadas pelas atuais regras de proteção de dados a assegurar a proteção dos dados pessoais.

[23] Regulamento (CE) n.° 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação (JO L 77 de 13.3.2004, p. 1).

A fim de evitar impor encargos desproporcionados aos pequenos operadores, em especial às PME, as obrigações são proporcionais aos riscos comportados pela rede ou sistema informático em causa e não se devem aplicar às microempresas. Os riscos terão de ser identificados em primeiro lugar pelas entidades sujeitas a essas obrigações, que terão de decidir sobre as medidas a tomar para reduzir esses riscos.

Os objetivos declarados podem ser mais facilmente alcançados a nível da UE do que a nível dos Estados-Membros, dados os aspetos transfronteiriços dos incidentes e riscos de SRI. Por conseguinte, a UE 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, a diretiva proposta não excede o necessário para alcançar esses objetivos.

A fim de atingir os objetivos, deve ser conferido à Comissão o poder de adotar atos delegados, em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia, que completem ou alterem certos elementos não essenciais do ato legislativo de base. A proposta da Comissão também procura apoiar um processo de proporcionalidade na aplicação das obrigações impostas aos operadores públicos e privados.

A fim de assegurar condições uniformes para a aplicação do ato de base, deverão ser atribuídas competências à Comissão para adotar atos de execução, em conformidade com o artigo 291.º do Tratado sobre o Funcionamento da União Europeia.

Tendo nomeadamente em conta o âmbito de aplicação amplo da diretiva proposta, o facto de esta abordar domínios altamente regulamentados e as obrigações jurídicas decorrentes do seu capítulo IV, a notificação das medidas de transposição deverá ser acompanhada de documentos explicativos. De acordo com a Declaração Política Conjunta dos Estados-Membros e da Comissão sobre os documentos explicativos, de 28 de setembro de 2011, os Estados-Membros assumiram o compromisso de fazer acompanhar, nos casos em que tal se justifique, a comunicação das suas disposições de transposição de um ou mais documentos explicando a relação entre as componentes da diretiva e as partes correspondentes dos instrumentos de transposição nacional. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica.

4. INCIDÊNCIA ORÇAMENTAL

A cooperação e o intercâmbio de informações entre os Estados-Membros deverão assentar em infraestruturas seguras. A proposta só terá implicações para o orçamento da UE se os Estados-Membros optarem por adaptar uma infraestrutura existente (por exemplo, a rede sTESTA) e incumbirem a Comissão de o fazer no âmbito do QFP 2014-2020. Estima-se que o custo único e irrepetível seja de 1 250 000 EUR, a suportar pelo orçamento da UE, rubrica orçamental 09 03 02 (promover a interligação e a interoperacionalidade dos serviços públicos em linha nacionais, bem como o acesso a essas redes — capítulo 09 03, Mecanismo Interligar a Europa (CEF) — redes de telecomunicações), desde que existam fundos disponíveis suficientes no âmbito do CEF. Em alternativa, os Estados-Membros podem partilhar o custo único e irrepetível de adaptar as infraestruturas existentes ou então decidir criar novas infraestruturas suportando os custos correspondentes, estimados em cerca de 10 milhões de EUR por ano.

2013/0027 (COD)

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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

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],

Após consulta da Autoridade Europeia para a Proteção de Dados,

Deliberando de acordo com o processo legislativo ordinário,

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 as atividades económicas e o bem-estar social e, em especial, para o funcionamento do mercado interno.

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

(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.

(4) Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a 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 operadores das infraestruturas críticas de informação, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves.

[1] JO C […] […], p. […].

(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, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro)[2], que estejam sujeitas aos requisitos específicos de segurança e integridade estabelecidos no artigo 13.°-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.

(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 intercâmbio de informações e a coordenação de ações, bem como requisitos mínimos comuns de segurança para todos os operadores do mercado em causa e as administrações públicas.

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

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

(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.

---

[2] JO L 108 de 24.4.2002, p. 33.

(11) Todos os Estados-Membros deverão estar equipados adequadamente, em termos de capacidades técnicas e organizacionais, para impedir, detetar, reagir e reduzir os incidentes e riscos ligados às redes e aos sistemas informáticos. Por conseguinte, devem ser instituídas em todos os Estados-Membros equipas de resposta a emergências informáticas 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.

(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 deverá permitir que o intercâmbio de informações, a deteção e a resposta sejam estruturados e coordenados a nível da União.

(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 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.

(14) Dever-se-á estabelecer uma infraestrutura de partilha de informações segura que permita o intercâmbio de informações sensíveis e confidenciais no âmbito da rede de cooperação. 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.

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

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

(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 para 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.

(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.

(20) Após receção de um alerta precoce e sua avaliação, as autoridades competentes devem chegar a acordo quanto a uma resposta coordenada no âmbito do plano de cooperação da União em matéria de SRI. As autoridades competentes, bem como a Comissão, deverão ser informadas das medidas adotadas a nível nacional em resultado da resposta coordenada.

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

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

(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, 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)[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 devem cingir-se ao setor das comunicações eletrónicas, mas 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, 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[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

[3] JO L 201 de 31.7.2002, p. 37.
[4] JO L 204 de 21.7.1998, p. 37.

nuvem, 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.

(25) As medidas técnicas e organizacionais 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.

(26) As administrações públicas e 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 públicas competentes, independentemente do facto de estes procederem à manutenção das suas redes e sistemas informáticos a nível interno ou de a externalizarem.

(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 deverão esforçar-se por manter canais informais e de confiança para a partilha de informações entre os operadores do mercado e entre o setor público e o setor privado. Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes comunicados às autoridades competentes e o interesse do público em ser informado acerca das ameaças que comportem eventuais danos comerciais e de reputação para as administrações públicas e os operadores do mercado que comunicam esses incidentes. No cumprimento das obrigações de notificação, as autoridades competentes deverão ter em especial atenção a necessidade de manter as informações sobre as vulnerabilidades dos produtos estritamente confidenciais antes da divulgação das medidas de segurança adequadas para as resolver.

(29) As autoridades competentes devem 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 com o objetivo de avaliarem o nível de segurança das redes e dos sistemas informáticos, bem como dados completos e fiáveis sobre eventuais incidentes que tenham tido impacto no seu funcionamento.

(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 e as autoridades policiais e judiciais 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.

(31) Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção dos dados devem cooperar e trocar informações sobre todas as questões pertinentes para combater as violações de dados pessoais resultantes de incidentes. Os Estados-Membros cumprirão a obrigação de notificar os incidentes de segurança de um modo que minimize a carga administrativa caso o incidente em causa constitua também uma violação de dados pessoais, em conformidade com o 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[5]. Em colaboração com as autoridades competentes e as autoridades encarregadas da proteção de dados pessoais, a ENISA poderá dar a sua contribuição desenvolvendo mecanismos de intercâmbio de informações e modelos que evitem a necessidade de dois modelos de notificação. 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.

(32) A normalização dos requisitos de segurança é um processo dirigido pelo mercado. 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, poderá ser necessário elaborar normas harmonizadas, o que deverá ser efetuado em conformidade com o Regulamento (UE) n.° 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.° 1673/2006/CE do Parlamento Europeu e do Conselho[6].

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

(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 Tratado sobre o Funcionamento da União Europeia deve ser delegado à Comissão no que diz respeito à definição dos critérios a cumprir para que um Estado-Membro seja autorizado a participar num sistema seguro de troca de informações, 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.

(35) É particularmente importante que a Comissão proceda a consultas adequadas durante os seus trabalhos preparatórios, incluindo 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, devem ser conferidas competências de execução à Comissão no que diz respeito à cooperação

---

5 SEC(2012) 72 final.

6 JO L 316 de 14.11.2012, p. 12.

com as autoridades competentes no âmbito da rede de cooperação, ao acesso às infraestruturas seguras de partilha de informações, ao plano de cooperação da União em matéria de SRI, aos meios e procedimentos aplicáveis à informação do público sobre a ocorrência de incidentes e às normas e/ou especificações técnicas pertinentes para a SRI. Essas competências deverão ser exercidas em conformidade com o 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[7].

(37) Na aplicação da presente diretiva, a Comissão deve assegurar as ligações adequadas com os comités setoriais pertinentes e os organismos competentes criados a nível da UE, em especial no domínio da energia, transportes e saúde.

(38) As informações que sejam consideradas confidenciais por uma autoridade competente, em conformidade com as regras nacionais e da União em matéria de sigilo comercial, só devem ser trocadas com a Comissão e outras autoridades 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 e adequado ao objetivo dessa comunicação.

(39) A partilha de informações sobre os riscos e incidentes na rede de cooperação e o cumprimento da obrigatoriedade de notificação de incidentes às autoridades nacionais competentes podem requerer o tratamento de dados pessoais. Esse tratamento é necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva e é, pois, legítimo, nos termos do artigo 7.° 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. Na aplicação da presente diretiva, o Regulamento (CE) n.° 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[8], deve aplicar-se conforme adequado. Nos casos em que os dados sejam tratados pelas instituições e órgãos da União, esse tratamento para efeitos de aplicação da presente diretiva deve ser conforme com o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

(40) Atendendo a que os objetivos da presente diretiva, nomeadamente a garantia de um elevado nível de SRI na União, não podem ser suficientemente alcançados pelos Estados-Membros individualmente, podendo contudo, devido aos efeitos da ação considerada, ser mais bem alcançados ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.° 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 esses objetivos.

(41) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, em especial, o direito ao respeito pelas comunicações e vida privadas, a proteção de dados pessoais, a

[7] JO L 55 de 28.2.2011, p. 13.
[8] JO L 145 de 31.5.2001, p. 43.

liberdade de empresa, o direito de propriedade, o direito a recurso judicial e o direito a ser ouvido. A presente diretiva deve ser aplicada de acordo com esses direitos e princípios,

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 (a seguir designada «SRI») na União.

2. Para o 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 aos riscos e incidentes que afetam as redes e os sistemas informáticos;

(c) estabelece requisitos de segurança para os operadores do mercado e as administrações públicas.

3. Os requisitos de segurança previstos no artigo 14.° 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 UE em matéria de luta contra a criminalidade informática nem a 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[9].

5. A presente diretiva também não prejudica a aplicação da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[10], nem da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, nem do Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[11].

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

[9] JO L 345 de 23.12.2008, p. 75.
[10] JO L 281 de 23.11.1995, p. 31.
[11] SEC(2012) 72 final.

para alcançar os objetivos de interesse público prosseguidos pela presente diretiva, deve ser autorizado pelo Estado-Membro em conformidade com o artigo 7.° da Diretiva 95/46/CE e com a Diretiva 2002/58/CE, tal como transpostos para o direito nacional.

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) qualquer dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais efetuam, com base num programa, o tratamento automático dos dados informáticos,

(c) os dados informáticos armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas a) e b) tendo em vista a sua exploração, utilização, proteção e manutenção.

(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;

(3) «Risco»: qualquer circunstância ou evento com um efeito adverso potencial na segurança;

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

(5) «Serviço da sociedade da informação»: um serviço na aceção do artigo 1.º, n.° 2, da Diretiva 98/34/CE;

(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 análise, contenção e resposta em caso de incidente;

(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;

(b) um operador de infraestruturas críticas essenciais para a manutenção de atividades económicas e sociais vitais nos domínios da energia, dos transportes, da banca, da bolsa e da saúde, cuja lista não exaustiva consta do anexo II.

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

(10) «Especificação», uma especificação referida no Regulamento (UE) n.° 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.

CAPÍTULO II

QUADROS NACIONAIS PARA A SEGURANÇA DAS REDES E DA INFORMAÇÃO

Artigo 4.º

Princípio

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.

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 de avaliação dos riscos para identificar os riscos e avaliar os impactos de potenciais incidentes;

(b) A definição das funções e responsabilidades dos diferentes intervenientes envolvidos na execução do plano;

(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 a contar da data da sua adoção.

Artigo 6.º

Autoridade nacional competente em matéria de segurança das redes e dos sistemas informáticos

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

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

3. Os Estados-Membros asseguram que as autoridades competentes 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 através da rede referida no artigo 8.º.

4. Os Estados-Membros asseguram que as autoridades competentes sejam notificadas 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.°.

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

6. Cada Estado-Membro notifica sem demora à Comissão a designação da autoridade competente, as suas funções, bem como quaisquer posteriores alterações. Cada Estado-Membro torna pública a sua designação da autoridade competente.

Artigo 7.º

Equipa de resposta a emergências informáticas

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

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.°.

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 CERT funciona sob a supervisão da autoridade competente, que deve rever periodicamente a adequação dos seus recursos, o seu mandato e a eficácia do seu processo de tratamento de incidentes.

CAPÍTULO III

COOPERAÇÃO ENTRE AUTORIDADES COMPETENTES

Artigo 8.º

Rede de cooperação

1. As autoridades competentes e a Comissão devem constituir uma rede («rede de cooperação») para cooperarem contra os riscos e os incidentes que afetem as redes e os sistemas informáticos.

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

3. No âmbito da rede de cooperação, as autoridades competentes devem:

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

   (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.°, 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 sobre todas as questões pertinentes 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;

   (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.

4. A Comissão deve estabelecer, 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. Os atos de execução correspondentes devem ser adotados em conformidade com o procedimento de consulta referido no artigo 19.º, n.º 2.

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.

2. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 18.° 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.

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.°, n.° 3.

Artigo 10.º

Alerta rápido

1. As autoridades competentes 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 a capacidade nacional de resposta;

   (c) Afetem ou possam afetar mais de um Estado-Membro.

2. Nos alertas rápidos, as autoridades competentes e a Comissão devem comunicar todas as informações pertinentes de que dispõem e possam ser úteis para avaliar o risco ou o incidente.

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.

4. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza criminosa, as autoridades competentes ou a Comissão devem informar o Centro Europeu da Cibercriminalidade na Europol.

5. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 18.º para especificar melhor os riscos e incidentes que desencadeiam o alerta rápido referido no n.º 1.

Artigo 11.º

Resposta coordenada

1. Na sequência de um alerta rápido referido no artigo 10.º, as autoridades competentes devem, após a avaliação das informações pertinentes, chegar a acordo quanto a uma resposta coordenada, conforme com o plano de cooperação da União em matéria de SRI referido no artigo 12.º.

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.°, n.° 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,

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

   (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.

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.

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 para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta os progressos técnicos, essas medidas devem garantir um nível de segurança adequado em função do risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto dos incidentes que afetam a sua rede e sistema informático nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.

2. Os Estados-Membros devem assegurar que as administrações públicas e os operadores do mercado notifiquem às autoridades competentes os incidentes com impacto significativo na segurança dos serviços essenciais que fornecem.

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

4. A autoridade competente pode informar o público ou exigir que as administrações públicas e os operadores do mercado o façam, caso considere que a revelação do 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.

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.

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

7. A Comissão tem poderes para definir, por meio de atos de execução, as modalidades e procedimentos aplicáveis para efeitos do disposto no n.° 2. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.°, n.° 3.

8. Os n.os 1 e 2 não se aplicam às microempresas na aceção da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas[12].

[12] JO L 124 de 20.5.2003, p. 36.

Artigo 15.º

Aplicação e execução

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

2. Os Estados-Membros devem assegurar que as autoridades competentes tenham poderes para exigir aos operadores do mercado e às administrações públicas:

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

   (b) que se submetam a uma auditoria de segurança efetuada por um organismo qualificado independente ou autoridade nacional e coloquem os resultados à disposição da autoridade competente.

3. Os Estados-Membros devem assegurar que as autoridades competentes tenham poderes para emitir instruções vinculativas aos operadores do mercado e às administrações públicas.

4. As autoridades competentes devem notificar os incidentes que se suspeite serem de caráter criminoso grave às autoridades policiais e judiciais.

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

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.

Artigo 16.º

Normalização

1. Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados-Membros devem encorajar a utilização das normas e/ou especificações pertinentes para a segurança das redes e da informação.

2. A Comissão estabelece, por meio de atos de execução, uma lista das normas referidas no n.º 1, que será publicada no Jornal Oficial da União Europeia.

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.

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[13].

Artigo 18.º

Exercício da delegação

1. O poder de adotar os atos delegados conferido à Comissão está sujeito às condições estabelecidas no presente artigo.

2. É conferido à Comissão o poder de adotar os atos delegados referidos nos artigos 9.º, n.º 2, 10.º, n.º 5, e 14.º, n.º 5. A Comissão elabora um relatório sobre a delegação de poderes o mais tardar nove meses antes do final do período de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada período.

3. A delegação de poderes referida nos artigos 9.º, n.º 2, 10.º, n.º 5, e 14.º, n.º 5, pode ser revogada a qualquer momento pelo Parlamento Europeu ou pelo Conselho. Uma decisão de revogação põe termo à delegação dos poderes especificados nessa decisão. A revogação produz efeitos no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou numa data posterior nela indicada. A decisão de revogação não afeta a validade de qualquer ato delegado em vigor.

4. Assim que adotar um ato delegado, a Comissão deve notificá-lo simultaneamente ao Parlamento Europeu e ao Conselho.

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.

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, é aplicável o artigo 4.° do Regulamento (UE) n.° 182/2011.

[13] SEC(2012) 72 final

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

Artigo 20.º

Avaliação

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

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 disposições.

   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 Bruxelas, em

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

ANEXO I

Obrigações a cumprir e tarefas da equipa de resposta a emergências informáticas (CERT)

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 CERT deve garantir uma elevada disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais e dispondo de vários meios para contactar e ser contactada. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos da sua base de clientes e dos parceiros de cooperação.

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

(c) Os gabinetes da CERT e os sistemas informáticos de apoio devem estar situados em locais seguros.

(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:

- Monitorizar os incidentes a nível nacional;
- 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;

– 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.

ANEXO II

Lista de operadores do mercado

Referidos no artigo 3.°, n.° 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.°, n.° 8, alínea b)

1. Energia

- 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
- Oleodutos e armazenamento de petróleo
- Operadores do mercado da eletricidade e do gás
- Operadores da produção de petróleo e gás natural, instalações de refinamento e tratamento

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

3. Setor bancário: instituições de crédito, em conformidade com o artigo 4.º, n.º 1, da Diretiva 2006/48/CE

4. Infraestruturas do mercado financeiro: bolsas e contrapartes centrais

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

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB

1.3. Natureza da proposta/iniciativa

1.4. Objetivos

1.5. Justificação da proposta/iniciativa

1.6. Duração da ação e impacto financeiro

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema de gestão e de controlo

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvidas(s)

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

3.2.2. Impacto estimado nas dotações operacionais

3.2.3. Impacto estimado nas dotações de natureza administrativa

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a União.

1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB[37]

- 09 – Redes de comunicações, conteúdos e tecnologia

1.3. Natureza da proposta/iniciativa

☒ A proposta/iniciativa refere-se a **uma nova ação**

☐ A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**[38]

☐ A proposta/iniciativa refere-se à **prorrogação de uma ação existente**

☐ A proposta/iniciativa refere-se a **uma ação reorientada para uma nova ação**

1.4. Objetivos

1.4.1. Objetivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa

A diretiva proposta tem por objetivo garantir um elevado nível comum de segurança das redes e da informação (SRI) em toda a UE.

1.4.2. Objetivos específicos e atividades ABM/ABB em causa

A proposta estabelece medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas informáticos em toda a União.

Os objetivos específicos são os seguintes:

1. Criar um nível mínimo de SRI nos Estados-Membros e, deste modo, aumentar o nível global de preparação e resposta.

2. Melhorar a cooperação em matéria de SRI a nível da UE de modo a enfrentar eficazmente os incidentes e ameaças transfronteiras. Será estabelecida uma infraestrutura para a partilha segura de informações destinada a permitir a troca de informações sensíveis e confidenciais entre as autoridades competentes.

3. Criar uma cultura de gestão dos riscos e melhorar a partilha de informações entre os setores público e privado.

Atividade(s) ABM/ABB em causa

A diretiva abrange entidades (empresas e organizações, incluindo algumas PME) de vários setores (energia, transportes, instituições de crédito e bolsa, saúde e empresas que asseguram serviços essenciais pela Internet), bem como as administrações públicas. Trata das relações com os serviços repressivos e as autoridades encarregadas da proteção dos dados e dos aspetos das relações externas ligados à SRI.

- 09 - Redes de comunicações, conteúdos e tecnologia

- 02 - Empresas

[37] ABM: *Activity Based Management* (gestão por atividades) – ABB: *Activity Based Budgeting* (orçamentação por atividades).

[38] Tal como referido no artigo 49.º, n.º 6, alíneas a) e b), do Regulamento Financeiro.

- 32 - Energia

- 06 - Mobilidade e Transportes

- Título 17: Saúde e defesa do consumidor

- 18 - Assuntos internos

- 19 - Relações externas

- 33 - Justiça

- 12-Mercado Interno

1.4.3. Resultados e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada

A proteção dos consumidores, empresas e governos na UE contra os incidentes, ameaças e riscos em matéria de SRI melhorará consideravelmente.

Na secção 8.2 (impacto da opção 2 – Abordagem regulamentar) da «Avaliação de impacto», documento de trabalho dos serviços da Comissão que acompanha a presente proposta legislativa, são dadas informações mais pormenorizadas.

1.4.4. Indicadores de resultados e de impacto

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa

Os indicadores para o controlo e a avaliação figuram na secção 10 da Avaliação de impacto.

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidades a satisfazer a curto ou a longo prazo

A cada Estado-Membro será exigido que tenha:

- uma estratégia nacional de SRI;

- um plano de cooperação da União em matéria de SRI;

- uma autoridade nacional competente em matéria de SRI;

- uma equipa de resposta a emergências informáticas (CERT).

A nível da UE, os Estados-Membros serão obrigados a cooperar através de uma rede.

As administrações públicas e os principais intervenientes privados terão de realizar uma gestão dos riscos em matéria de SRI e comunicar às autoridades competentes os incidentes de SRI com impacto significativo.

1.5.2. Valor acrescentado da intervenção da UE

Considerando a natureza transfronteiras da SRI, as divergências nas políticas e legislação pertinentes constituem um obstáculo às empresas para que operem em vários países e realizem economias de escala globais. A falta de intervenção da UE conduziria a uma situação em que cada Estado-Membro deveria atuar sozinho sem ter em conta as interdependências entre as redes e os sistemas informáticos.

Por conseguinte, os objetivos declarados podem ser mais facilmente alcançados através de uma ação a nível da UE em vez de pelos Estados-Membros agindo isoladamente.

1.5.3. Lições tiradas de experiências anteriores semelhantes

A proposta resulta da análise de que as obrigações regulamentares são necessárias para criar condições equitativas e suprir algumas lacunas legislativas. Neste domínio, uma

abordagem puramente voluntária teve por resultado a cooperação unicamente entre uma minoria de Estados-Membros com um elevado nível de capacidades.

1.5.4. Coerência e eventual sinergia com outros instrumentos relevantes

A proposta é totalmente coerente com a Agenda Digital para a Europa e, por conseguinte, com a Estratégia Europa 2020. É também coerente e complementa o quadro regulamentar da UE para as comunicações eletrónicas, a diretiva da UE relativa às infraestruturas críticas europeias e a diretiva relativa à proteção de dados.

A proposta acompanha e constitui uma parte essencial da Comunicação da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança sobre a Estratégia Europeia de Cibersegurança.

1.6. Duração da ação e impacto financeiro

– ☐ Proposta/iniciativa de duração limitada

– ☐ Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA

– ☒ Proposta/iniciativa de duração ilimitada

– O período de transposição terá início imediatamente após a adoção (prevista para 2015) e uma duração de 18 meses. A aplicação da diretiva terá, no entanto, início após a adoção e implicará a criação de infraestruturas seguras, que servirão de suporte à cooperação entre os Estados-Membros.

– Seguir-se-á o funcionamento em pleno.

1.7. Modalidades de gestão previstas[39]

– ☒ Gestão centralizada direta por parte da Comissão

– ☒ Gestão centralizada indireta por delegação de funções de execução:

– ☐nas agências de execução

– ☒ nos organismos criados pelas Comunidades[40]

– ☐ nos organismos públicos nacionais/organismos com missão de serviço público

– ☐ nas pessoas encarregadas da execução de ações específicas por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente na aceção do artigo 49.º do Regulamento Financeiro

– ☐ Gestão partilhada com os Estados-Membros

– ☐ Gestão descentralizada com países terceiros

– ☐ Gestão conjunta com organizações internacionais, incluindo a Agência Espacial Europeia

Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».

Observações:
A ENISA, uma agência descentralizada criada pelas Comunidades, pode assistir os Estados-Membros e a Comissão na aplicação da diretiva com base no seu mandato e pela reafetação dos recursos previstos no âmbito do QFP 2014-2020 para esta agência.

[39] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Referidos no artigo 185.º do Regulamento Financeiro.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições

A Comissão procederá à avaliação periódica do funcionamento da presente diretiva e apresentará um relatório ao Parlamento Europeu e ao Conselho.

A Comissão avaliará igualmente a transposição correta da diretiva pelos Estados-Membros.

A proposta relativa ao CEF prevê também a possibilidade de se avaliarem os métodos de execução dos projetos, bem como o impacto da sua execução, a fim de verificar se os objetivos previstos, nomeadamente no domínio da proteção do ambiente, foram atingidos.

2.2. Sistema de gestão e de controlo

2.2.1. Riscos identificados

- atrasos na execução dos projetos de construção de infraestruturas seguras

2.2.2. Métodos de controlo previstos

Os acordos e decisões de execução das ações no âmbito do CEF deverão prever a supervisão e o controlo financeiro por parte da Comissão, ou por qualquer representante por ela autorizado, bem como a realização de auditorias pelo Tribunal de Contas e de controlos no local pelo Organismo Europeu de Luta Antifraude (OLAF).

2.2.3. Custos e benefícios dos controlos e provável taxa de não cumprimento

Os controlos *ex ante* e *ex post* com base nos riscos e a possibilidade de auditorias no local assegurarão que os custos dos controlos sejam razoáveis.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas

No quadro da execução da ação financiada ao abrigo da presente diretiva, a Comissão deve tomar medidas adequadas que garantam a proteção dos interesses financeiros da União mediante a aplicação de medidas preventivas contra a fraude, a corrupção e outras atividades ilegais, a realização de controlos eficazes e, caso sejam detetadas irregularidades, a recuperação dos montantes pagos indevidamente e, se for caso disso, a aplicação de sanções efetivas, proporcionadas e dissuasivas.

A Comissão, ou os seus representantes, e o Tribunal de Contas podem realizar auditorias com base em documentos e inspeções no local a todos os beneficiários de subvenções, contratantes e subcontratantes que recebam fundos da União ao abrigo do programa.

O Organismo Europeu de Luta Antifraude (OLAF) pode levar a cabo inspeções e verificações no local em relação aos operadores económicos abrangidos direta ou indiretamente por esse financiamento, em conformidade com os procedimentos estabelecidos no Regulamento (Euratom, CE) n.º 2185/96, a fim de investigar a existência de fraudes, atos de corrupção ou quaisquer outras atividades ilegais que prejudiquem os interesses financeiros da União e estejam relacionados com uma

convenção ou decisão de subvenção ou um contrato relativo a um financiamento concedido pela União.

Sem prejuízo dos parágrafos anteriores, os acordos de cooperação com países terceiros e organizações internacionais e as convenções e decisões de subvenção, assim como os contratos resultantes da aplicação desse regulamento, devem autorizar expressamente a Comissão, o Tribunal de Contas e o OLAF a realizar essas auditorias, inspeções e verificações no local.

O CEF prevê que os contratos para as subvenções e os contratos públicos se baseiem em modelos normalizados, que estabelecerão as medidas antifraude geralmente aplicáveis.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvidas(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesa	Participação			
	Número Número [Designação…...….]	DD/DND (41)	dos países da EFTA[42]	dos países candidatos [43]	de países terceiros	na aceção do artigo 18.º, n.º 1, alínea a-a), do Regulamento Financeiro
	09 03 02 Promover a interconexão e a interoperabilidade dos serviços públicos nacionais em linha, assim como o acesso a essas redes	DD	NÃO	NÃO	NÃO	NÃO

- Novas rubricas orçamentais cuja criação é solicitada (não aplicável)

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesa	Participação			
	Número [Designação ……]	DD/DND	dos países da EFTA	dos países candidatos	de países terceiros	na aceção do artigo 18.º, n.º 1, alínea a-a), do Regulamento Financeiro
	[XX.YY.YY.YY]		SIM/ NÃO	SIM/ NÃO	SIM/ NÃO	SIM/ NÃO

41 DD = dotações diferenciadas/DND = dotações não diferenciadas.

42 EFTA: Associação Europeia de Comércio Livre.

43 Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

Em milhões de euros (3 casas decimais)

Rubrica do quadro financeiro plurianual:	1	Crescimento inteligente e inclusivo

DG: <…….>			2015* [44]	Ano **2016**	Ano **2017**	Ano **2018**	Anos seguintes (2019-2021) e posteriormente			**TOTAL**
• Dotações operacionais										
09 03 02	Autorizações	(1)	1,250**	0,000						**1,250**
	Pagamentos	(2)	0,750	0,250	0,250					**1,250**
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos[45]			**0,000**							**0,000**
Número da rubrica orçamental		(3)	**0,000**							**0,000**
TOTAL das dotações para a DG <…….>	Autorizações	= 1 + 1a + 3	1,250	0,000						**1,250**
	Pagamentos	= 2 + 2a +3	0,750	0,250	0,250					**1,250**

• TOTAL das dotações operacionais	Autorizações	(4)	1,250	0,000						**1,250**
	Pagamentos	(5)	0,750	0,250	0,250					**1,250**

[44] O ano N é o do início da aplicação da proposta/iniciativa.

[45] Assistência técnica e/ou administrativa e despesas de apoio à aplicação de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)	**0,000**							
TOTAL das dotações no âmbito da RUBRICA 1 do quadro financeiro plurianual	Autorizações	=4+ 6	1,250	0,000						**1,250**
	Pagamentos	=5+ 6	0,750	0,250	0,250					**1,250**

* O momento exato dependerá da data de adoção da proposta pela autoridade legislativa (ou seja, se a diretiva for aprovada no decurso de 2014, a adaptação de uma infraestrutura existente terá início em 2015, caso contrário, um ano mais tarde).

** Se os Estados-Membros optarem por utilizar uma infraestrutura existente e imputar o custo de adaptação único e irrepetível ao orçamento da UE, tal como exposto nos pontos 1.4.3 e 1.7, o custo da adaptação de uma rede para apoiar a cooperação entre os Estados-Membros, em conformidade com o capítulo III da diretiva (alerta rápido, resposta coordenada, etc.) é estimado em 1 250 000 EUR. Este montante é ligeiramente mais elevado do que o mencionado na avaliação de impacto («cerca de 1 milhão de EUR»), uma vez que assenta numa estimativa mais exata dos elementos de base necessários a essa infraestrutura. Esses elementos e os respetivos custos baseiam-se numa estimativa do JRC, com base na sua experiência no desenvolvimento de sistemas semelhantes para outras áreas, como a saúde pública, e incluirão o seguinte: um sistema de alerta rápido e notificação em matéria de SRI (275 000 EUR); uma plataforma de intercâmbio de informações (400 000 EUR); um sistema de alerta rápido e resposta (275 000 EUR); um centro de crise (300 000 EUR), num total de 1 250 000 EUR. Está previsto um plano de execução mais pormenorizado no próximo estudo de viabilidade no âmbito do contrato específico SMART 2012/0010: «Estudo de viabilidade e atividades preparatórias para a aplicação de um sistema europeu de alerta rápido e resposta contra os ataques e perturbações informáticos».

Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica:

• TOTAL das dotações operacionais	Autorizações	(4)	0,000	0,000						
	Pagamentos	(5)	0,000	0,000						
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)	**0,000**	**0,000**						
TOTAL das dotações no âmbito das RUBRICAS 1 a 4 do quadro financeiro plurianual (quantia de referência)	Autorizações	=4+ 6	1,250	0,000						1,250
	Pagamentos	=5+ 6	0,750	0,250	0,250					1,250

Rubrica do quadro financeiro plurianual	**5**	«Despesas administrativas»

Em milhões de euros (3 casas decimais)

		Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Anos seguintes (2019-2021) e posteriormente			**TOTAL**
DG: CNECT									
• Recursos humanos		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Outras despesas administrativas		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
TOTAL DG CNECT	Dotações	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTAL das dotações no âmbito da RUBRICA 5 do quadro financeiro plurianual	(Total das autorizações = total dos pagamentos)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Em milhões de euros (3 casas decimais)

		Ano **2015**[46]	Ano **2016**	Ano **2017**	Ano **2018**	Anos seguintes (2019-2021) e posteriormente			**TOTAL**
TOTAL das dotações no âmbito das RUBRICAS 1 a 5 do quadro financeiro plurianual	Autorizações	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Pagamentos	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] O ano N é o do início da aplicação da proposta/iniciativa.

3.2.2. Impacto estimado nas dotações operacionais

– ☐ A proposta/iniciativa não acarreta a utilização de dotações operacionais

– ☑ A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

– Dotações de autorização em milhões de euros (3 casas decimais)

Indicar os objetivos e as realizações ⇩			Ano **2015***		Ano **2016**		Ano **2017**		Ano **2018**		Anos seguintes (2019-2021) e posteriormente						**TOTAL**	
			REALIZAÇÕES															
	Tipo[47]	Custo médio	Número	Custo	Número	Custo	Número	Custo	Número	Custo	Número	Custo	Número	Custo	Número	Custo	Número total	Custo total
OBJETIVO ESPECÍFICO N.º 2[48] Infraestrutura de partilha de informações segura																		
- Realização	Adaptar as infra--estruturas																	
Subtotal objetivo específico n.º 2			1	1,250**													1	1,250
CUSTO TOTAL				1,250														1,250

47 As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

48 Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…».

* O momento exato dependerá da data de adoção da proposta pela autoridade legislativa (ou seja, se a diretiva for aprovada no decurso de 2014, a adaptação de uma infraestrutura existente terá início em 2015, caso contrário, um ano mais tarde).

** Ver ponto 3.2.1.

3.2.3. Impacto estimado nas dotações de natureza administrativa

3.2.3.1. Síntese

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– ☑ A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de euros (3 casas decimais)

	Ano **2015**[49]	Ano **2016**	Ano **2017**	Ano **2018**	Anos seguintes (2019-2021) e posteriormente			**TOTAL**
RUBRICA 5 do quadro financeiro plurianual								
Recursos humanos	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Outras despesas administrativas	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Subtotal RUBRICA 5 do quadro financeiro plurianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Com exclusão da RUBRICA 5[50] **do quadro financeiro plurianual**								
Recursos humanos	0,000	0,000						**0,000**
Outras despesas de natureza administrativa								
Subtotal com exclusão da RUBRICA 5 do quadro financeiro plurianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
TOTAL	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

As dotações administrativas necessárias serão cobertas pelas dotações da DG CNECT já afetadas à gestão da ação e/ou reafetadas no interior da DG, se necessário juntamente com eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

49 O ano N é o do início da aplicação da proposta/iniciativa.

50 Assistência técnica e/ou administrativa e despesas de apoio à aplicação de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

A Agência Europeia para a Segurança das Redes e da Informação (ENISA) poderá ajudar os Estados-Membros e a Comissão a aplicarem a diretiva com base no seu mandato e através da reafetação dos recursos ao abrigo do QFP 2014-2020 destinados a esta agência, ou seja, sem quaisquer afetações de recursos orçamentais ou humanos adicionais.

3.2.3.2. Necessidades estimadas de recursos humanos

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos

– ☑ A proposta/iniciativa acarreta a utilização de recursos humanos da Comissão, tal como explicitado seguidamente:

Em princípio, não será necessária mão-de-obra suplementar. Os recursos humanos necessários serão muito limitados e assegurados pelos efetivos da DG já afetados à gestão da ação.

As estimativas devem ser expressas em números inteiros (ou, no máximo, com uma casa decimal)

		Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Anos seguintes (2019-2021) e posteriormente		
• Lugares do quadro do pessoal (funcionários e agentes temporários)								
09 01 01 01 (na sede e nos gabinetes de representação da Comissão)		4	4	4	4	4	4	4
XX 01 01 02 (nas delegações)								
XX 01 05 01 (investigação indireta)								
10 01 05 01 (investigação direta)								
• Pessoal externo (em equivalente a tempo completo: ETC)[51]								
XX 01 02 01 (AC, TT e PND da dotação global)		1	1	1	1	1	1	1
XX 01 02 02 (AC, TT, JPD, AL e PND nas delegações)								
XX 01 04 yy[52]	- na sede[53]							
	- nas delegações							
XX 01 05 02 (AC, TT, PND - investigação indireta)								
XX 01 05 02 (AC, TT e PND - Investigação direta)								
Outras rubricas orçamentais (especificar)								
TOTAL		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX constitui o domínio de intervenção ou título orçamental em causa

As necessidades de recursos humanos devem ser cobertas pelos efetivos da DG CNECT já afetados à gestão da ação e/ou reafetados internamente a nível da DG, completados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

51 AC = agente contratual; TT = trabalhador temporário; JPD = jovem perito nas delegações; AL = agente local; PND = perito nacional destacado.

52 Dentro do limite para o pessoal externo previsto nas dotações operacionais (antigas rubricas «BA»).

53 Essencialmente para os fundos estruturais, o Fundo Europeu Agrícola para o Desenvolvimento Rural (FEADER) e o Fundo Europeu das Pescas (FEP).

A Agência Europeia para a Segurança das Redes e da Informação (ENISA) poderá ajudar os Estados-Membros e a Comissão a aplicarem a diretiva com base no seu atual mandato e através da reafetação dos recursos ao abrigo do QFP 2014-2020 destinados a esta agência, ou seja, sem qualquer afetação de recursos orçamentais ou humanos adicionais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	- Preparar atos delegados em conformidade com o artigo 14.º, n.º 3 - Preparar atos de execução em conformidade com os artigos 8.º, 9.º, n.º 2, 12.°, 14.°, n.° 5, 16.° - Contribuir para a cooperação através da rede a nível estratégico e operacional - Participar em debates internacionais e, possivelmente, concluir acordos internacionais
Pessoal externo	Apoiar todas as tarefas acima mencionadas, conforme for necessário

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

– ☑ A proposta/iniciativa é compatível com o atual quadro financeiro plurianual

– ☐ A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual

O impacto financeiro estimado da proposta nas despesas operacionais verificar-se-á se os Estados-Membros optarem por adaptar uma infraestrutura existente e encarregarem a Comissão de proceder à sua adaptação ao abrigo do QFP 2014-2020. Os respetivos custos únicos e irrepetíveis serão cobertos pelo CEF desde que existam fundos suficientes disponíveis. Em alternativa, os Estados-Membros podem partilhar quer os custos da adaptação da infraestrutura quer os custos da criação de uma nova infraestrutura.

– ☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual[54].

Não aplicável.

3.2.5. Participação de terceiros no financiamento

– A proposta/iniciativa não prevê o cofinanciamento por terceiros.

3.3. Impacto estimado nas receitas

– ☑ A proposta/iniciativa não tem impacto financeiro nas receitas.

[54] Ver pontos 19 e 24 do Acordo Interinstitucional.