COUNCIL OF THE EUROPEAN UNION

Brussels, 11 April 2013

8375/13

Interinstitutional File: 2013/0027 (COD)

TELECOM 71
DATAPROTECT 43
CYBER 6
MI 281
CODEC 793
INST 169
PARLNAT 81

COVER NOTE

from:	Portuguese Parliament
date of receipt:	10 April 2013
to:	The President of the Council of the European Union
Subject:	Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Opinion of the application of the Principles of Subsidiarity and Proportionality[1] **[doc. 6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 - COM(2013) 48 final]** + ADD1 +ADD2

Delegations will find attached for information a copy of the above opinion.

[1] The translation can be found at the Interparliamentary EU information exchange site IPEX at the following address :http://www.ipex.eu/IPEXL-WEB/search.do

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Parecer
COM(2013)48
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

1

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

PARTE I - NOTA INTRODUTÓRIA

Nos termos do artigo 7.º da Lei n.º 43/2006, de 25 de agosto, alterada pela Lei n.º 21/2012, de 17 de maio, que regula o acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, bem como da Metodologia de escrutínio das iniciativas europeias, aprovada em 20 de janeiro de 2010, a Comissão de Assuntos Europeus recebeu a Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União [COM(2013)48].

A supra identificada iniciativa foi enviada às Comissões de Economia e Obras Públicas e para a Ética, a Cidadania e a Comunicação, atento o seu objeto, as quais analisaram a referida iniciativa e aprovaram os Relatórios que se anexam ao presente Parecer, dele fazendo parte integrante

PARTE II – CONSIDERANDOS

1 – A presente iniciativa diz respeito à Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

2 – 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. 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 – É referido na presente iniciativa que 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 - A presente proposta de diretiva, tem, assim, 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.

5 – É referido na presente proposta que 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 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.

6 - É igualmente indicado que 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.

7 - 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.

8 - É igualmente indicado que na presente proposta de diretiva 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.

9 – Quanto à 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 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.

10 – Por último referir que 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.

Atentas as disposições da presente proposta, cumpre suscitar as seguintes questões:

a) Da Base Jurídica

Artigos 26.° e 114.º do Tratado sobre o Funcionamento da União Europeia.

b) Do Princípio da Subsidiariedade

É respeitado e cumprido o princípio da subsidiariedade na medida em que é com uma atuação ao nível da união Europeia como um todo que se asseguram os requisitos comuns a todos os EM, permitindo garantir que os riscos da SRI sejam bem geridos

no contexto transfronteiras em que surjam e aumentando a eficácia das políticas nacionais existentes e facilitando o seu desenvolvimento.

PARTE III - PARECER

Em face dos considerandos expostos e atento os Relatórios das comissões competentes, a Comissão de Assuntos Europeus é de parecer que:

1. A presente iniciativa não viola o princípio da subsidiariedade, na medida em que o objetivo a alcançar será mais eficazmente atingido através de uma ação da União

2. Em relação às iniciativas em análise, o processo de escrutínio está concluido.

Palácio de S. Bento, 9 de abril de 2013

O Deputado Autor do Parecer | **O Presidente da Comissão**

(Duarte Marques) | **(Paulo Mota Pinto)**

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

PARTE IV – ANEXO

Relatório da Comissão de Economia e Obras Públicas

Relatório da Comissão para a Ética, a Cidadania e a Comunicação.

Parecer da Comissão de Economia e Obras Públicas

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

COM (2013) 48

Autor: Deputado

Nuno Matias

ÍNDICE

PARTE I - NOTA INTRODUTÓRIA

1. Nota Preliminar

A Comissão de Assuntos Europeus, nos termos do disposto no artigo 7.º da Lei n.º 43/2006, de 25 de agosto, relativa ao acompanhamento, apreciação, escrutínio e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, remeteu a Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União- COM(2013)48

2. Procedimento adoptado

A supra referida proposta foi distribuída na Comissão de Economia e Obras Públicas, tendo sido nomeado relator o Deputado Nuno Matias, do Grupo Parlamentar do Partido Social Democrata.

PARTE II – CONSIDERANDOS

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.

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.

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.

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 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.

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 %).

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 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 seguintes objetivos:

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.

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;

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.

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.

Ao nível da 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 redes TESTA) 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.

Por fim, 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.

2.1.1. 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.

2.1.2. Princípio da Subsidiariedade e da proporcionalidade

Nos termos do segundo parágrafo do artigo 5.º do Tratado da União Europeia, *"Nos domínios que não sejam das suas atribuições exclusivas, a Comunidade intervém apenas, de acordo com o princípio da subsidiariedade, se e na medida em que os objectivos da acção encarada não possam ser suficientemente realizados pelos Estados – Membros, e possam, pois, devido à dimensão ou aos efeitos da acção prevista, ser melhor alcançados a nível comunitário".*

Este princípio tem como objectivo assegurar que as decisões sejam tomadas o mais próximo possível dos cidadãos, ponderando se a acção a realizar à escala comunitária se justifica face às possibilidades oferecidas a nível nacional, regional ou local. Trata-se de um princípio segundo o qual a União só deve actuar quando a sua acção for mais eficaz do que uma acção desenvolvida pelos Estados – Membros, excepto quando se trate de matérias de competência exclusiva da União.

Para além disso, e nos termos do terceiro parágrafo do artigo 5.º do Tratado da União Europeia, é realçado que "*A ação da Comunidade não deve exceder o necessário para atingir os objectivos do presente Tratado".*

À semelhança do Princípio da Subsidiariedade, o Princípio da Proporcionalidade regula o exercício das competências exercidas pela União Europeia.

Visa delimitar e enquadrar a actuação das instituições comunitárias.

Por força desta regra, a actuação das instituições deve limitar-se ao estritamente necessário para atingir os objectivos dos tratados, por outras palavras, a intensidade da acção deve estar relacionada com a finalidade prosseguida (proibição de excesso).

No caso da iniciativa em apreço:

- Em relação ao Princípio da 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.

- Em relação ao Princípio da proporcionalidade

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.

PARTE III – CONCLUSÕES

1 - A presente iniciativa não viola o princípio da subsidiariedade e assegura a proporcionalidade, na medida em que o objectivo a alcançar será mais eficazmente atingido através de uma ação da União, sem colocar em causa a intervenção, dentro das competências próprias, de cada um dos Estados-membros.

2 - A Comissão de Economia e Obras Públicas dá por concluído o escrutínio da presente iniciativa, devendo o presente parecer, nos termos da Lei n.º 43/2006, de 25 de agosto de 2006, ser remetido à Comissão de Assuntos Europeus para os devidos efeitos.

Palácio de S. Bento, 19 de março de 2013.

O Deputado Relator — O Presidente da Comissão

(Nuno Matias) — (Luis Campos Ferreira)

ASSEMBLEIA DA REPÚBLICA

COMISSÃO PARA A ÉTICA, A CIDADANIA E A COMUNICAÇÃO

Parecer

COM (2013) 48 final

Proposta de DIRETIVA DO PARLAMENTO E DO CONSELHO relativa a medidas destinadas a garantir elevado nível comum de segurança das redes e da informação em toda a União

Autor: Deputado

José Lino Ramos (CDS-PP)

ASSEMBLEIA DA REPÚBLICA

ÍNDICE

2

ASSEMBLEIA DA REPÚBLICA

PARTE I - NOTA INTRODUTÓRIA

Nos termos do artigo 7.º da Lei nº 43/2006, de 25 de Agosto, que regula o acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, a Proposta de DIRETIVA DO PARLAMENTO E DO CONSELHO relativa a medidas destinadas a garantir elevado nível comum de segurança das redes e da informação em toda a União foi enviada à Comissão para a Ética, a Cidadania e a Comunicação, atento o seu objeto, para efeitos de análise e elaboração do presente parecer.

A presente iniciativa 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 Cibesegurança.

PARTE II – CONSIDERANDOS

1. Em geral

- **Objetivo da iniciativa**

A Proposta de Diretiva em apreço visa garantir um elevado nível comum de segurança das redes e da informação (SRI). Tal desígnio exige uma melhoria da segurança da Internet e das redes e sistemas informáticos privados em que assenta o funcionamento das nossas sociedades e economias.

A materialização deste objetivo exige que Estados-Membros aumentem o seu nível de preparação e melhorem a cooperação entre si e exige 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. Esta estratégia visa instituir um ambiente digital seguro e fiável ao mesmo tempo que defende e promove os direitos fundamentais e outros valores fundamentais da UE. A proposta em análise é a principal ação da estratégia. Também se encontram previstas outras ações respeitantes a este domínio, incidindo estas na sensibilização, no desenvolvimento de um mercado interno para os produtos e serviços de cibersegurança e na promoção dos investimentos em I&D. Estas medidas serão complementadas por outras o intuito de fortificar a luta contra a cibercriminalidade e de estabelecer uma política internacional de cibersegurança para a UE.

- **Principais aspetos**

A SRI constitui uma condição imperiosa para o desenvolvimento para a nossa economia e a nossa sociedade. Representa também uma condição prévia importante para criar um ambiente fiável para o comércio de serviços em todo o mundo. Contudo, 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. E 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.

Enquanto instrumentos de comunicação sem fronteiras, os sistemas de informação digitais, em especial a Internet, fazem a ligação entre todos os Estados-Membros, facilitando a circulação transfronteiriças de mercadorias, serviços e possas. A perturbação significativa destes sistemas num Estado-Membro pode afetar outros Estados-Membros e a UE no seu conjunto. Ter a capacidade para superar e estabilizar estabilidade as redes e dos sistemas informáticos é, por conseguinte, essencial para a realização do mercado único digital e o bom funcionamento do mercado interno.

A situação atual na UE, que reflete a abordagem puramente voluntária seguida até à data, não é garantia da 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 meramente insuficientes para fazerem face à rápida evolução das ameaças e garantirem um nível elevado de proteção comum em todos os Estados-Membros.

Não obstante as iniciativas empreendidas, existe um diferencial significativo das capacidades e grau de preparação dos Estados-membros, que resultou na adopção de abordagens fragmentadas em toda a UE. Só têm sido desenvolvidas sinergias e acções de cooperação entre uma minoria de Estados-Membros com elevados níveis de capacidades.

Deste modo, convém destacar que não existe actualmente qualquer mecanismo eficaz ao nível europeu que afirme 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, tendentes a assegurar uma protecção insuficiente da SRI em toda a UE. Entraves ao mercado interno também pode surgir, 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.

Para contrariar a tendência do atual quadro regulamentar que obriga unicamente as empresas de telecomunicações a adotarem medidas de gestão e riscos e a comunicarem os incidentes em matéria de SRI, é necessário proceder a mudança do modo como a SRI é vista pela UE. São necessárias obrigações regulamentares para definir uma base equitativa de resposta a emergências informáticas (CERT) e a adopção de estratégias e planos de cooperação nacionais em matéria de SRI. A diretiva proposta tem os

- Primeiro, a proposta exige que todos os Estados-Membros assegurem um nível mínimo de capacidades nacionais por intermédio da criação de autoridades competentes para SRI e de equipas de resposta a emergências informáticas (CERT) e a adoção de estratégias e planos de cooperação nacionais em matéria de SRI.

- Segundo, as autoridades nacionais 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. Os Estados-Membros, através desta rede, devem trocar informações e cooperar para enfrentar as ameaças e os incidentes relativos à SRI com base no plano de cooperação europeia nesta matéria.

- Por último, 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 assegurar a segurança das redes da informação.

- **Aspetos relevantes**

a) No que respeita aos **resultados das consultas das partes interessadas**, e em particular a consulta das partes interessadas e recursos a peritos especializados, convém notar que entre junho e outubro de 2012 foi efetuada uma consulta pública em linha.

O principal resultado foi que as partes interessadas manifestaram um apoio generalizado à necessidade de melhorar a SRI em toda a UE.

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 e em reuniões bilaterais. Quanto ao setor público, a Comissão estabeleceu contactos com a ENISA e as CERT para as instituições da UE.

b) Em relação à **avaliação de impacto**, destaque-se o recurso da Comissão à avaliação de três opções estratégicas:

I. Opção 1: Manutenção do *status quo* (cenário de base) – manutenção da atual abordagem;
II. Opção 2: Abordagem regulamentar, que consiste numa proposta legislativa prevê o estabelecimento de um quadro jurídico comum da UE para a SRI no que toca às capacidades dos Estados-Membros, aos mecanismos de cooperação ao nível da UE e os requisitos dos principais intervenientes privados e administrações públicas;
III. 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

7

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.

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 protecção de dados pessoais, a liberdade de empresa, o direito de propriedade, o direito a recurso judicial e o direito a ser ouvido. A diretiva em apreço deve ser aplicada em conformidade com esses direitos e princípios.

2. Base jurídica

A adopção de "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" da UE está prevista no artigo 114º do Tratado de Funcionamento da União Europeia.

3. Princípio da Subsidiariedade

A iniciativa respeita o princípio da subsidiariedade na medida em que é com uma actuação ao nível da União Europeia como um todo que se asseguram os requisitos comuns a todos os Estados, permitindo garantir que os riscos da SRI sejam bem geridos no contexto transfronteiras em que surjam e aumentando a eficácia das políticas nacionais existentes e facilitando o seu desenvolvimento.

ASSEMBLEIA DA REPÚBLICA

PARTE III - CONCLUSÕES

Em face do exposto, a Comissão para a Ética, a Cidadania e a Comunicação conclui o seguinte:

1. A iniciativa em análise não viola o princípio da subsidiariedade, na medida em que o objetivo a alcançar será mais eficazmente atingido através de uma ação da União;

2. A análise da presente iniciativa não suscita quaisquer questões que impliquem posterior acompanhamento;

3. A Comissão para a Ética, a Cidadania e a Comunicação dá por concluído o escrutínio da presente iniciativa, devendo o presente parecer, nos termos da Lei n.º 43/2006, de 25 de Agosto de 2006, ser remetido à Comissão de Assuntos Europeus para elaboração do respetivo parecer final.

Palácio de S. Bento, 18 de Março de 2013

O Deputado Autor do Parecer

(José Lino Ramos)

O Vice - Presidente da Comissão

(Jacinto Serrão)

9