ASSEMBLEIA DA REPÚBLICA

Comissão para a Ética, a Cidadania e a Comunicação

EXMO. SENHOR
PRESIDENTE DA COMISSÃO DE ASSUNTOS EUROPEUS
DR. PAULO MOTA PINTO

Of. n.º 115/12ª - CPECC/2013

19-03-2013

Assunto: Parecer sobre a COM (2013) 48

Para os devidos efeitos, junto envio a Vossa Excelência o Parecer relativo à **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. Esta iniciativa tem ainda associados dois documentos de trabalho: Avaliação de Impacto [SWD(2013)32] e Resumo da Avaliação de Impacto [SWD(2013)31]", aprovado por unanimidade, verificando-se a ausência do BE, na reunião desta Comissão Parlamentar, realizada em **19 de março de 2013**.

Com os melhores cumprimentos,

O Vice-Presidente da Comissão,

(Jacinto Serrão)

Palácio de S. Bento - 1249-068 LISBOA - PORTUGAL - Telefone: 21 391 96 55 - Fax: 21 391 75 08 - e-mail:

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)

ÍNDICE

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

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.

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)