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 137/12ª - CPECC/2013 08-04-2013

Assunto: Parecer sobre a JOIN(2013)1

Para os devidos efeitos, junto envio a Vossa Excelência o Parecer relativo à **JOIN(2013)1 –** "Relatório da Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido", aprovado por unanimidade, verificando-se a ausência do BE, na reunião desta Comissão Parlamentar, realizada em **9 de abril de 2013**.

Com os melhores cumprimentos,

O Presidente da Comissão,

(José Mendes Bota)

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

Parecer

Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido — **JOIN(2013)1**

Autor: Deputado

Pedro Delgado Alves (PS)

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, Comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido [JOIN(2013)1], foi enviada à Comissão para a Ética, a Cidadania e a Cultura, atento o seu objeto, para efeitos de análise e elaboração do presente parecer.

Esta iniciativa vai ao encontro da Agenda Digital para a Europa que, enquadrada na estratégia Europa 2020, visa estimular a economia digital e responder aos desafios sociais através das Tecnologias de Informação e Comunicação.

PARTE II – CONSIDERANDOS

1. Apreciação geral

A comunicação da Comissão sob escrutínio, pretendendo a edificação de um Estratégia da União Europeia para a cibersegurança, parte de um reconhecimento da centralidade da Internet e do ciberespaço na vida dos cidadãos e das instituições públicas e privadas e da crescente necessidade de criar mecanismos que assegurem que permanecem uma realidade aberta e livre, projectando *"no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico."* Nos considerandos iniciais da comunicação é sublinhado, em particular, que os *"direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço".* Paralelamente, trata-se de uma realidade essencial ao crescimento económico, com particular relevo para setores chave das nossas economias, como as finanças, saúde, energia ou transportes.

A concretização do mercado único digital ou o aprofundamento da comunicação em nuvem, objeto já de análise por esta Comissão no quadro de outras comunicações europeias versando as referidas matérias, revela-se detentora de um imenso potencial de aumento do PIB da União Europeia, sendo essencial assegurar as condições de segurança indispensáveis à sua concretização.

Para o efeito, a Comissão reconhece a necessidade de protecção do ciberespaço contra incidentes, atividades maliciosas e utilizações abusivas, e, em particular, o papel determinante dos governos na operacionalização dessa proteção, em estreita articulação com o setor privado, cujo papel na gestão das redes em questão é incontornável e tem de ser enquadrado em qualquer estratégia eficiente. Nesse sentido, serão eixos relevantes da construção de uma estratégia europeia a necessidade de:

- Salvaguardar o acesso e abertura;
- Respeitar e proteger os direitos fundamentais em linha;
- Manter a fiabilidade e interoperabilidade da internet;

São três os grandes conjuntos de riscos que a Comunicação identifica a título preliminar e que reforçam a necessidade de intervenção neste domínio, a saber:

- O aumento alarmante dos incidentes de cibersegurança, com um potencial de perturbação da prestação de serviços essenciais como a água, a eletricidade ou os cuidados de saúde;

- A cibercriminalidade dirigida ao setor privado e ao setor público, com novos patamares de sofisticação e por vezes associada a fenómenos de espionagem económica ou patrocinada por Estados;

- A utilização abusiva do ciberespaço pelos governos de países que não pertencem à UE para a vigilância e o controlo dos seus próprios cidadãos, domínio no qual a UE pode contrariar esta situação promovendo a liberdade em linha e garantindo o respeito dos direitos fundamentais em linha.

Finalmente, ainda a título de referências iniciais, importa ter em conta quais são os princípios estruturantes a adotar em matéria de cibersegurança por uma futura estratégia da UE:

- Os valores fundamentais da UE aplicam-se tanto no mundo digital como no mundo físico;
- A proteção dos direitos fundamentais, em particular da liberdade de expressão, dos dados pessoais e da privacidade, é essencial à coerência da estratégia;
- Há que assegurar acesso para todos, através do combate à iliteracia digital e da garantia de acesso à Internet;
- A governação desta área tem de atender à presença de diversos agentes, públicos e privados, configurando-se como multilateral, democrática e eficiente;
- É necessária uma responsabilidade partilhada para garantir a segurança.

2. Prioridades estratégicas e ações

A estratégia apresentada na Comunicação sob escrutínio articula-se em cinco prioridades estratégicas, que procuram responder aos desafios diagnosticados inicialmente.

2.1. Garantir a resiliência do ciberespaço

- A Comissão tem vindo a desenvolver uma política de segurança das redes e da informação (SRI). A Agência Europeia para a Segurança das Redes e da Informação, ENISA, foi criada em 2004 e o seu mandato será reforçado e modernizado através de um novo regulamento que está a ser negociado pelo Conselho e pelo Parlamento.

- Ainda se detectando lacunas em toda a UE, nomeadamente em termos de meios disponíveis a nível nacional, de coordenação em caso de incidentes que ultrapassem as fronteiras e de envolvimento e preparação do setor privado, a estratégia sob escrutínio é acompanhada por uma proposta legislativa, que visa:

    a) Estabelecer requisitos mínimos comuns para a SRI (segurança das redes e da informação) a nível nacional;

    b) Criar mecanismos coordenados de prevenção, deteção, atenuação e resposta, que permitam a partilha de informações e a assistência mútua entre as autoridades nacionais competentes em matéria de SRI.

    c) Melhorar o grau de preparação e a participação do setor privado.

- O Mecanismo Interligar a Europa concederá apoio financeiro às infraestruturas fundamentais, ligando as capacidades dos Estados-Membros em matéria de SRI e tornando assim mais fácil a cooperação em toda a EU;

- É essencial realizar exercícios de simulação de incidentes informáticos a nível da UE para treinar a cooperação entre os Estados-Membros e o setor privado.

- Por último, deve ainda merecer destaque a necessidade de reforço de ações de sensibilização dos utilizadores finais.

2.2. Reduzir drasticamente a cibercriminalidade

- A UE e os Estados-Membros devem dotar-se de uma legislação rigorosa e eficaz para combater a cibercriminalidade. A Convenção do Conselho da Europa sobre Cibercriminalidade, também conhecida por Convenção de Budapeste, é um tratado internacional vinculativo que fornece um quadro apropriado para a adoção de legislação nacional.

- A UE já adotou legislação relativa à cibercriminalidade, nomeadamente uma diretiva relativa à luta contra a exploração sexual das crianças em linha e a pornografia infantil. A UE está também prestes a chegar a acordo sobre uma diretiva relativa a ataques contra os sistemas de informação, especialmente através da utilização de «botnets».

- A evolução das técnicas de cibercriminalidade conheceu uma rápida aceleração: as agências responsáveis não podem combater a cibercriminalidade com ferramentas operacionais ultrapassadas, sendo fundamental a disponibilização de meios operacionais acrescidos;

- Finalmente, importa reforçar a coordenação e cooperação a nível da UE, reunindo autoridades judiciais e policiais, e agentes públicos e privados com interesse direto na matéria;

2.3. Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da políica comum de segurança e defesa (PCSD)

- É crítico assegurar uma melhoria das sinergias entre as abordagens civil e militar na proteção dos ativos informáticos críticos. Estes esforços devem ser apoiados pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da UE.

- De forma a evitar duplicações, a UE irá explorar as possibilidades de a UE e a NATO complementarem os seus esforços para aumentar a resiliência das infraestruturas críticas das Administrações, da defesa e outras infraestruturas informáticas.

2.4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança

- Em primeira linha, cumprirá promover um mercado único dos produtos de cibersegurança. Com vista a assegurar a sua concretização, é relevante que sejam implementados ao longo de toda a cadeia de valor dos produtos TIC utilizados na Europa requisitos de desempenho em matéria de cibersegurança. Por outro lado, o setor privado precisa de incentivos para garantir um elevado nível de cibersegurança, devendo igualmente ser estimulada a procura de produtos altamente seguros no mercado europeu.
  Nesse sentido, a Comissão apoiará a elaboração de normas de segurança e colaborará no estabelecimento de sistemas de certificação voluntários no domínio da computação em nuvem em toda a UE, não deixando de ter na devida conta a necessidade de assegurar a proteção dos dados.

- Simultaneamente, importará promover os investimentos em I&D e em inovação. Para o efeito, a UE deve aproveitar da melhor forma o programa-quadro de investigação e inovação Horizonte 202029, que será lançado em 2014.

2.5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

- Na sua política internacional relativa ao ciberespaço, a estratégia constante da comunicação aponta para que a UE promova a abertura e a liberdade da Internet e encoraje os esforços tendentes a estabelecer normas de comportamento e aplicar as leis internacionais em vigor no ciberespaço. Nesse quadro, a UE também tudo deverá fazer para reduzir a clivagem digital e participará ativamente nos esforços internacionais para construir capacidade de cibersegurança.

- Por outro lado, importa neste plano integrar as questões do ciberespaço nas relações externas e na política externa e de segurança comum (PESC) da EU e assegurar o reforço das capacidades em matéria de cibersegurança e desenvolvimento de infraestruturas informáticas resilientes nos países terceiros.

3. Concretização

Finalmente, a definição da estratégia europeia para a cibersegurança pressupõe igualmente a necessidade de coordenação entre os três planos essenciais de intervenção neste domínio, delimitando as esferas de intervenção dos Estados, da União e aquele que fica reservado à coordenação no plano internacional.

Para além da divisão de funções atendendo à prossecução dos objetivos de reforço da cibersegurança resultantes das traves mestras da estratégia, é ainda enfatizada a necessidade de garantia de apoio da UE em caso de incidentes ou ataques informáticos importantes, atento o impacto que podem vir a ter em toda a União.

PARTE III – OPINIÃO DO DEPUTADO AUTOR DO PARECER

Apreciação da Comunicação

A presente comunicação revela-se determinante para a conjugação das diversas intervenções realizadas pela União Europeia até ao momento no domínio da cibersegurança, dotando de coerência e de mecanismos coordenados de implementação os vários domínios diversificados de intervenção da União (que tocam questões que vão desde o funcionamento do mercado interno, à ação externa da União, passando pela tutela de direitos fundamentais e pela coordenação do combate à criminalidade transnacional e ao terrorismo).

Para além de uma estruturada fundamentação da necessidade de ação, colocando a tónica prioritária na indispensabilidade do acesso livre e aberto à Internet como forma de realização de direitos fundamentais, a Estratégia para a Cibersegurança não deixa, no entanto, descurar a sua importância económica e para a segurança interna e externa dos Estados, mobilizando uma variedade significativa de ações de concretização.

A análise da presente iniciativa permite identificar uma necessidade de posterior acompanhamento das iniciativas legislativas de concretização da Estratégia para a Cibersegurança, bem como dos programas a desenvolver na sua execução. Trata-se, aliás, de matéria conexa e de relevante articulação com a Agenda Digital da UE.

Princípio da Subsidiariedade

Tratando-se de uma iniciativa europeia não legislativa, não cabe a apreciação do princípio da subsidiariedade, cuja análise se remeterá para as iniciativas concretizadoras da presente estratégia, a que são feitas inúmeras referências. No entanto, deve sublinhar-se que não só a presente estratégia expressamente aborda a problemática da delimitação das esferas de intervenção da União e dos Estados, como fundamenta de forma clara a necessidade de uma intervenção coordenada em matéria de cibersegurança como caminho para assegurar a eficiência das medidas propostas.

PARTE IV - CONCLUSÕES

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

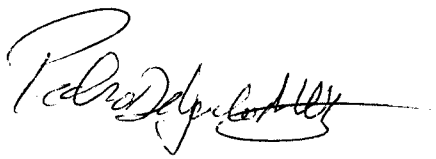
1. Na presente iniciativa não legislativa, não cabe a verificação do cumprimento do princípio da subsidiariedade, apesar dos elementos constantes da Estratégia para a Cibersegurança evidenciarem uma clara e fundamentada delimitação das esferas de intervenção entre União e Estados-membros;

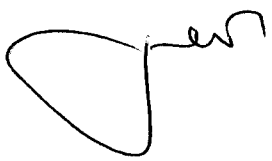
2. A análise da presente iniciativa permite identificar uma necessidade de posterior acompanhamento das iniciativas legislativas de concretização da Estratégia para a Cibersegurança, bem como dos programas a desenvolver na sua execução. Trata-se, aliás, de matéria conexa e de relevante articulação com a Agenda Digital da UE.

3. A Comissão para a Ética, a Cidadania e a Cultura 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, 9 de abril de 2013

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





(Pedro Delgado Alves) | ***(Mendes Bota)***