**ASSEMBLEIA DA REPÚBLICA**

COMISSÃO DE ASSUNTOS EUROPEUS

---

# Parecer
# JOIN(2013)1
# 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

---

## 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 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].

A supra identificada iniciativa foi enviada às Comissões de Assuntos Constitucionais, Direitos, Liberdades e Garantias; Defesa Nacional 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 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.

2 – A iniciativa em análise traduz a visão global da União Europeia sobre a melhor forma de prevenir e dar resposta às perturbações e ataques na Internet. Assim, para proteger a abertura da rede, a liberdade e as oportunidades em linha, a Comissão Europeia, em colaboração com a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, publicou a sua proposta de estratégia em matéria de cibersegurança.

3 - O documento "Um ciberespaço aberto, seguro e protegido", procura, segundo os seus autores, promover os valores europeus de liberdade e democracia e, ao mesmo tempo, garantir que a economia digital se desenvolva em condições de segurança.
Defende a Comissão que "para que o ciberespaço permaneça aberto e livre devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a União defende para o mundo físico.
Os direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço." Ao mesmo tempo a liberdade em linha exige também segurança e proteção, devendo o ciberespaço ser protegido contra incidentes, atividades maliciosas e utilizações abusivas, tendo os governos um importante papel a desempenhar neste domínio.

4 – É igualmente reconhecido o papel crucial do sector privado que detém e explora partes significativas do ciberespaço e, como tal, a Comissão reconhece que nenhuma iniciativa nesta matéria pode avançar sem o seu contributo.

5 - Tal como realçado na presente iniciativa, é hoje plenamente reconhecido que as tecnologias da informação e das comunicações tornaram-se a "espinha dorsal" do nosso crescimento económico e são um recurso crítico do qual dependem todos os outros sectores.

6 – Importa, ainda, sublinhar que uma vez que seja concretizado o mercado único digital, a Europa poderá aumentar o seu PIB em quase 500 000 milhões de euros por ano, o que representa uma média de 1000 euros por pessoa.
Para que isso aconteça é necessário que os cidadãos europeus tenham confiança na utilização da Internet e sejam ultrapassadas as grandes vulnerabilidades que o mundo digital ainda apresenta.

7 - De facto, os chamados incidentes de cibersegurança[1], quer sejam intencionais ou meramente acidentais, aumentam a um nível preocupante e podem mesmo vir a provocar uma perturbação na prestação dos serviços que entendemos como básicos, como é o caso do abastecimento de água ou eletricidade, os cuidados de saúde ou os serviços de telecomunicações móveis.
Neste caso, as ameaças podem ter origens diversas, nomeadamente ataques criminosos, politicamente motivados, terroristas ou patrocinados por alguns Estados ou catástrofes naturais e até erros humanos involuntários.

8 – É ainda destacado que a economia da União é já bastante afetada pela cibercriminalidade[2] que atinge o sector privado e os particulares. Por outro lado, o aumento da espionagem económica e de atividades patrocinadas por Estados no ciberespaço coloca os governos e as empresas dos países da União ao alcance de uma nova categoria de ameaças.

9 - Assim, tal como já foi referido anteriormente, a presente proposta para uma estratégia da União Europeia nesta matéria pretende clarificar os papéis e as responsabilidades e descreve as ações necessárias para proteger os direitos dos cidadãos a fim de tornar o ambiente em linha na União o mais seguro do mundo.

10 - Para isso a visão da União, vertida nesta proposta, articula-se em torno de cinco grandes prioridades estratégicas:

a) Garantir a resiliência do ciberespaço;

[1] Tal como é referido na Comunicação da Comissão, o termo cibersegurança refere-se, geralmente, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade dessas redes e infraestruturas e a confidencialidade das informações nelas contidas.

[2] A cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infrações nacionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso).

b) Reduzir drasticamente a cibercriminalidade;
c) Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD);
d) Desenvolver os recursos industriais e tecnológicos para a cibersegurança;
e) Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE.

11 – Por último, sublinhar que a presente proposta de estratégia da União Europeia para a cibersegurança, apresentada pela Comissão e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, define a visão da UE e as ações necessárias, fundadas numa proteção e numa promoção eficazes dos direitos dos cidadãos, para tornar o ambiente em linha na UE o mais seguro do mundo[3].

12 – De acordo com o documento em análise, esta visão apenas pode ser concretizada através de uma verdadeira parceria entre os numerosos intervenientes, que assuma a responsabilidade e responda aos desafios que se perfilam.
É igualmente necessário um apoio e empenhamento decididos por parte do setor privado e da sociedade civil, que são atores fundamentais para aumentar o nosso nível de segurança e proteger os direitos dos cidadãos.

[3] O financiamento da estratégia far-se-á dentro dos limites dos montantes previstos para cada um dos domínios políticos relevantes (CEF, Horizonte 2020, Fundo para a Segurança Interna, PESC e Cooperação Externa, nomeadamente o Instrumento de Estabilidade), como indicado na proposta da Comissão relativa ao quadro financeiro plurianual para 2014-2020 (sob reserva da aprovação pela autoridade orçamental e dos montantes definitivos do QFP adotado para 2014-2020). No que respeita à necessidade de assegurar a compatibilidade geral com o número de postos disponíveis para as agências descentralizadas e o subteto máximo para as agências descentralizadas em cada rubrica de despesas do próximo quadro financeiro plurianual, as agências (Academia Europeia de Polícia (CEPOL), a AED, a ENISA, a Eurojust e a Europol/EC3) que passam a assumir novas tarefas nos termos da presente comunicação serão incentivadas a fazê-lo na medida em que tenha sido estabelecida a sua capacidade real para absorver os recursos suplementares e em que tenham sido identificadas todas as possibilidades de reafetação.

## 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. Na presente iniciativa não cabe a apreciação do princípio da subsidiariedade, na medida em que se trata de uma iniciativa não legislativa.

2. No que concerne as questões suscitadas nos considerandos, a Comissão de Assuntos Europeus prosseguirá o acompanhamento do processo referente à presente iniciativa, nomeadamente através de troca de informação com o Governo.

Palácio de S. Bento, 26 de Junho de 2013

**O Deputado Autor do Parecer**

**(Sérgio Azevedo)**

**O Presidente da Comissão**

**(Paulo Mota Pinto)**

## PARTE IV – ANEXO

Relatório da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias.

Relatório da Comissão Defesa Nacional.

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

# ASSEMBLEIA DA REPÚBLICA

## COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

## RELATÓRIO

## 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

### I. Introdução

A Comissão de Assuntos Europeus, em cumprimento com o estabelecido na Lei n.º 43/2006, de 25 de Agosto, alterada pela Lei n.º 21/2012, de 17 de Maio, relativa ao *"Acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia"*, e nos termos previstos no n.º 2 do artigo 7.º da citada Lei, remeteu à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, para a emissão de parecer fundamentado, a JOIN (2013) 1 - 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.

### II. Apreciação da iniciativa

#### 1. Enquadramento

A Comunicação da Comissão insere-se na designada Agenda Digital para a Europa que, enquadrada na estratégia Europa 2020, afirma como objetivo o estímulo da economia digital e a resposta aos desafios sociais através das Tecnologias de Informação e Comunicação.

Reconhecendo a importância da Internet e do ciberespaço na vida dos cidadãos, das instituições e das empresas, bem como a necessidade de assegurar que o ciberespaço permaneça aberto e livre, a Comunicação identifica a necessidade de definição de uma

Estratégia da União Europeia para a cibersegurança, afirmando que *"os direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço"*, devendo aplicar-se *"no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico"*.

Afirma-se simultaneamente que se trata de uma realidade essencial ao crescimento económico, reconhecendo-se mesmo como *"a espinha dorsal do nosso crescimento económico"* e *"um recurso crítico de que todos os setores económicos dependem"*, com destaque para setores fundamentais como as finanças, saúde, energia ou transportes.

A concretização do mercado Único digital ou o aprofundamento da comunicação em nuvem são identificados como objetivos de particular relevância económica, afirmando-se a necessidade de proteção do ciberespaço contra *"ataques criminosos, politicamente motivados, terroristas ou patrocinados por Estados, assim como catástrofes naturais e erros involuntários"*.

Como fundamento da necessidade de intervenção neste domínio, são identificados elementos caracterizadores da evolução da realidade bem como alguns fatores de vulnerabilidade do ciberespaço:

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

b) A repercussão económica da cibercriminalidade contra o setor privado, em crescente sofisticação e por vezes associada a fenómenos de espionagem económica ou até patrocinada por Estados;

c) A utilização abusiva do ciberespaço por governos de países que não pertencentes à UE para vigiar e controlar os seus próprios cidadãos, domínio em que se entende que a UE pode contrariar tal realidade promovendo a liberdade em linha e garantindo o respeito dos direitos fundamentais em linha.

A Comunicação reconhece a ação dos governos ao longo do tempo na adoção de medidas destinadas a garantir a necessária proteção e afirma a necessidade de projetar essas estratégias nacionais de cibersegurança numa dimensão internacional.

Nesse sentido, são apontados como princípios que devem orientar a política de cibersegurança na UE e a nível internacional:

1. Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade;
2. Assegurar a todos o acesso à internet e a um fluxo de informações livre;
3. Assegurar uma governação multilateral, democrática e eficiente;
4. Partilhar a responsabilidade para garantir a segurança.

## 2. Prioridades estratégicas e acões

A estratégia apresentada pela Comissão estrutura-se em cinco prioridades, visando a resposta aos desafios identificados:

1. Garantir a resiliência do ciberespaço
2. Reduzir drasticamente a cibercriminalidade
3. Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD)
4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança
5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE

### 2.1. Garantir a resiliência do ciberespaço

A Comunicação sublinha a importância das medidas de desenvolvimento da política de segurança das redes e da informação (SRI), particularmente pelo seu impacto económico e na segurança interna.

Refere-se igualmente a necessidade de reforço e modernização do mandato da Agência Europeia para a Segurança das Redes e da Informação, ENISA, criada em 2004, através de um novo regulamento que está a ser negociado pelo Conselho e pelo Parlamento. Registando-se as lacunas existentes 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 visando:

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.

É referido o papel do Mecanismo Interligar a Europa que concederá apoio financeiro a infraestruturas fundamentais, ligando as capacidades dos Estados-Membros em matéria de SRI e facilitando a cooperação em toda a UE.

Afirma-se a necessidade de realizar exercícios de simulação de incidentes informáticos ao nível da UE para treinar a cooperação entre os Estados-Membros e o setor privado.

Por fim, refere-se ainda a necessidade de reforço de ações de sensibilização dos utilizadores finais.

## 2.2. Reduzir drasticamente a cibercriminalidade

Neste âmbito sublinha-se a necessidade de a UE e os Estados-Membros se dotarem de uma legislação rigorosa e eficaz para combater a cibercriminalidade. A Convenção do Conselho da Europa sobre Cibercriminalidade – Convenção de Budapeste – é identificada como um tratado internacional que fornece um quadro adequado para a adoção da necessária legislação nacional.

São ainda sublinhadas medidas legislativas como a adoção que se prevê para breve de uma diretiva relativa a ataques contra os sistemas de informação, bem como a adoção de legislação relativa à cibercriminalidade, nomeadamente a 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.

Por outro lado, é identificada a rápida aceleração da evolução das técnicas de cibercriminalidade, reconhecendo-se que as agências responsáveis não conseguem combater a cibercriminalidade com ferramentas operacionais ultrapassadas, pelo que se torna fundamental a disponibilização de meios operacionais acrescidos.

É ainda destacada a necessidade de reforçar a coordenação e cooperação a nível da EU entre autoridades judiciais e policiais e agentes públicos e privados com interesse direto nestas questões.

A Comissão afirma assim a intenção de:

a) Assegurar a transposição e a implementação rápidas das diretivas relativas à cibercriminalidade;

b) Instar os Estados-Membros que ainda não ratificaram a Convenção do Conselho da Europa sobre Cibercriminalidade a ratificarem e aplicarem as suas disposições o mais depressa possível;

c) Através dos seus programas de financiamento, apoiar os Estados-Membros na identificação das lacunas e no reforço da sua capacidade para investigar e combater a cibercriminalidade. Além disso, a Comissão irá apoiar os organismos que fazem a ligação entre a investigação/as universidades, os agentes policiais/judiciais e o setor privado, cujo trabalho tem afinidades com o atualmente realizado pelos centros de excelência para a cibercriminalidade já criados em alguns Estados-Membros e que são financiados pela Comissão;

d) Juntamente com os Estados-Membros, coordenar os esforços para identificar as melhores práticas e as melhores técnicas disponíveis, inclusivamente com o apoio do JRC, para combater a cibercriminalidade (por exemplo, no que diz respeito ao desenvolvimento e à utilização de ferramentas forenses ou à análise das ameaças);

e) Trabalhar em estreita cooperação com o recém-criado Centro Europeu da Cibercriminalidade (EC3), no quadro da Europol e com a Eurojust para harmonizar tais abordagens políticas com as melhores práticas na esfera operacional;

f) Apoiar o recém-criado Centro Europeu da Cibercriminalidade (EC3), enquanto ponto focal europeu no combate à cibercriminalidade. O EC3 fornecerá análises e informações (Intelligence), apoiará as investigações, garantirá investigação forense de elevado nível, facilitará a cooperação, criará canais para a partilha de informações entre as autoridades competentes dos Estados-Membros, o setor privado e outras partes interessadas e assumirá progressivamente o papel de porta-voz das forças policiais.

g) Apoiar os esforços para melhorar a prestação de contas dos agentes de registo de nomes de domínio e garantir a exatidão das informações sobre a propriedade dos sítios Web, nomeadamente com base nas recomendações *Law Enforcement Recommendations* à ICANN (Internet Corporation for Assigned Names and Numbers), em conformidade com o direito da União, incluindo as regras da proteção de dados.

h) Tirar partido da legislação recente para intensificar os esforços da UE no combate aos abusos sexuais de crianças em linha. A Comissão adotou uma estratégia europeia destinada a melhorar a Internet para as crianças e, juntamente com os países da União Europeia e outros, lançou uma aliança mundial contra os abusos sexuais de crianças em linha. A Aliança é um veículo para outras ações dos Estados-Membros apoiadas pela Comissão e pelo Centro Europeu da Cibercriminalidade.

Além disso, a Comissão entende ser necessário junto de outras entidades/instituições solicitar intervenção, nomeadamente:

**A Comissão pede à Europol (EC3) que:**

a) Inicialmente focalize a sua análise e o seu apoio operacional às investigações da cibercriminalidade efetuadas pelos Estados-Membros de modo a ajudar a desmantelar e a desorganizar as redes de cibercriminalidade principalmente nas áreas do abuso sexual de crianças, das fraudes nos pagamentos, dos «*botnets*» e da intrusão.

b) Elabore regularmente relatórios estratégicos e operacionais sobre as tendências e as novas ameaças, para identificar as prioridades e definir alvos para a atividade de investigação das equipas dos Estados-Membros especializadas em cibercriminalidade.

**A Comissão pede à Academia Europeia de Polícia (CEPOL) que, em cooperação com a Europol:**

a) Coordene a conceção e o planeamento de cursos de formação para dotar os órgãos policiais/judiciais dos conhecimentos e competências especializadas necessários para combater eficazmente a cibercriminalidade.

**A Comissão pede à Eurojust que:**

a) Identifique os principais obstáculos à cooperação judiciária em matéria de investigações da cibercriminalidade e à coordenação entre os Estados-Membros e com

os países terceiros e apoie a investigação e a repressão da cibercriminalidade, tanto ao nível estratégico como operacional, assim como as atividades de formação neste domínio.

**A Comissão pede à Eurojust e à Europol (EC3) que:**

Cooperem estreitamente, nomeadamente através do intercâmbio de informações, para aumentar a sua eficácia no combate à cibercriminalidade, de acordo com os respetivos mandatos e competência.

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

A Comissão afirma que os esforços da UE no domínio da cibersegurança devem também envolver a dimensão da ciberdefesa, destacando a necessidade de o desenvolvimento de capacidades de ciberdefesa deve centrar-se na deteção de ameaças informáticas sofisticadas, na resposta a dar e na recuperação posterior.

Afirma ainda a necessidade de melhorar sinergias entre as abordagens civil e militar na proteção dos ativos informáticos críticos, num esforço apoiado pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da UE.

A Comissão afirma pretender 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 das quais dependem os membros de ambas as organizações.

### 2.4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança

A Comissão reconhece que muitos dos líderes mundiais em matéria de produtos e serviços TIC inovadores estão sedeados fora da UE, existindo o risco de a Europa se tornar excessivamente dependente não só de TIC produzidas noutros países mas também de soluções de segurança desenvolvidas fora das suas fronteiras.

A Comunicação sublinha a importância de garantir que os componentes de *hardware* e *software* produzidos na UE e em países terceiros que são utilizados em serviços e infraestruturas críticos, e também em dispositivos móveis, sejam de confiança, seguros e garantam a proteção dos dados pessoais.

A promoção de um mercado único dos produtos de cibersegurança é assim assumida pela Comissão como um passo necessário para atingir aquele objetivo, a par da promoção dos investimentos em I&D e em inovação.

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

Afirmando que a preservação de um ciberespaço aberto, livre e seguro é um desafio de dimensão mundial a que a UE deve responder conjuntamente com os parceiros e organizações internacionais relevantes, com o setor privado e com a sociedade civil, a Comissão diz pretender:

a) promover a abertura e a liberdade da Internet;

b) encorajar os esforços tendentes a estabelecer normas de comportamento e aplicar as leis internacionais em vigor no ciberespaço;

c) tudo fazer para reduzir a clivagem digital e participar ativamente nos esforços internacionais para construir capacidade de cibersegurança.

d) que o envolvimento internacional da UE nas questões que dizem respeito ao ciberespaço pautar-se-á pelos valores fundamentais da UE, a saber, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos fundamentais.

Assim, a Comissão pretende ver integradas as questões do ciberespaço nas relações externas e na política externa e de segurança comum (PESC) da EU, atribuindo uma importância renovada ao diálogo com países terceiros, procurando assegurar um nível elevado de proteção dos dados, nomeadamente em caso de transferência de dados pessoais para um país terceiro.

A UE procurará, nomeadamente, uma cooperação mais estreita com organizações como o Conselho da Europa, a OCDE, a ONU, a OSCE, a NATO, a UA, a ASEAN e OEA. A nível bilateral, a Comissão afirma que a cooperação com os Estados Unidos é particularmente importante e será mais desenvolvida, nomeadamente no contexto do Grupo de Trabalho UE-EUA para a Cibersegurança e a Cibercriminalidade.

Destacando a promoção do ciberespaço enquanto espaço de liberdade e de direitos fundamentais como um dos principais elementos da política internacional da UE no domínio do ciberespaço, a Comissão afirma que o aumento da conectividade mundial não deve ser acompanhado de censura ou de vigilância das populações, pelo que a UE deve promover a responsabilidade social das empresas e lançar iniciativas internacionais para melhorar a coordenação a nível mundial neste domínio.

Assim, a UE não apela à criação de novos instrumentos jurídicos internacionais para as questões do ciberespaço, sublinhando antes a necessidade de respeitar "em linha" as obrigações legais consagradas no Pacto Internacional sobre os Direitos Civis e Políticos, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais da União Europeia.

Destaca-se ainda a necessidade de reforço das capacidades em matéria de cibersegurança e desenvolvimento de infraestruturas informáticas resilientes nos países terceiros.

### 3 – Funções e responsabilidades

Por fim a Comissão destaca a importância de clarificar os papéis e as responsabilidades dos muitos atores envolvidos, afirmando a exigência de coordenação entre três planos de intervenção distintos mas complementares: o dos Estados, o da União e o da coordenação no plano internacional.

Reconhecendo aos governos nacionais melhor posição para organizar a prevenção e a resposta aos incidentes e ataques informáticos e para estabelecer contactos e redes com o setor privado e o grande público através dos canais estabelecidos e dos quadros legais, a Comissão afirma a necessidade de envolvimento da UE como fator de superação de obstáculos resultantes de diferentes quadros legais, devendo tais intervenções articular-se em torno de três pilares fundamentais: a SRI, a repressão e a defesa.

A Comissão desenvolve e caracteriza os diferentes níveis – nacional, da União e internacional – desta coordenação entre as autoridades competentes em matéria de SRI/CERT, as autoridades policiais e o setor da defesa.

Ao nível nacional afirma que os Estados-Membros devem dispor de estruturas preparadas para garantir a resiliência do ciberespaço, combater a cibercriminalidade e prover à defesa e devem atingir o nível de capacidade necessário para lidar com incidentes informáticos, sendo necessário otimizar a coordenação entre os diferentes ministérios. Os Estados-Membros devem definir, nas suas estratégias nacionais de cibersegurança, o papel e as responsabilidades das suas várias entidades nacionais.

A partilha de informações entre as entidades nacionais e com o setor privado deve ser encorajada, devendo prever-se nos planos nacionais de cooperação em matéria de SRI a ativar em caso de incidentes informáticos que os Estados-Membros possam atribuir claramente os papéis e as responsabilidades e otimizar as ações de resposta.

Ao nível da UE, sublinha-se a importância de encorajar a coordenação e a colaboração entre a ENISA, a Europol/EC3 e a AED numa série de domínios em que estão conjuntamente envolvidas, devendo estas agências, conjuntamente com a equipa CERT-UE, a Comissão e os Estados-Membros, apoiar o desenvolvimento de uma comunidade de confiança de peritos técnicos e políticos neste domínio.

Por fim, ao nível internacional a Comissão e a Alta Representante devem procurar garantir uma ação internacional coordenada no domínio da cibersegurança.

## III. Opinião do Relator

A estratégia da União Europeia para a Cibersegurança, apontada na Comunicação da Comissão, assenta na consideração da utilização de dispositivos eletrónicos e sistemas de

comunicação digital como fator de crescimento económico, fonte de lucro, elemento de potencial desenvolvimento de "mercados únicos" ou espaço de disputas económicas entre grandes corporações ou mesmo Estados, desconsiderando o que deveria ser central: os perigos e vulnerabilidades a que os cidadãos são sujeitos em matéria de proteção da reserva e intimidade da vida privada, nomeadamente no que respeita à proteção de dados pessoais.

Afirmando inúmeras preocupações com atividades designadas de "cibercriminosas" – cuja caracterização no entanto nunca é satisfatoriamente efetuada – a Estratégia aborda os problemas decorrentes das quebras ou ataques à segurança das comunicações eletrónicase dos sistemas informáticos primordialmente pelos perigos e riscos que daí decorrem para o funcionamento da economia e do Estado, para o desenvolvimento dos mercados e dos serviços.

A Estratégia foca-se em particular nos riscos e perigos a que estão expostas as grandes corporações e grupos transnacionais nas suas atividades por natureza potencialmente geradoras de maiores proveitos mas igualmente sujeitas a maiores vulnerabilidades.

Não é, assim, de estranhar que na caracterização da situação em matéria de cibersegurança e de evolução do designado cibercrime se "nivelem" as preocupações com as liberdades individuais e de expressão e a "espionagem industrial", ainda que só a final e de forma relativamente superficial se abordem aquelas primeiras preocupações.

Tratando-se os dispositivos eletrónicos e seus sistemas de comunicação digital de sistemas automáticos, passíveis portanto de ser vítimas de ataques massivos, as técnicas de ataque, por serem igualmente automáticas, são de fácil difusão, não carecendo praticamente de especial qualificação para serem aplicadas.

Por outro lado, a amplitude e densidade da informação e o seu valor económico tornam apetecível o mais dispendioso dos ataques, particularmente quando dirigido contra uma base de dados com alguns milhões de entradas uma vez que não só a probabilidade de sucesso do ataque se vê grandemente acrescida, como, e isso é o fundamental, o proveito do mesmo ataque bem sucedido é enormemente recompensado.

O problema é, pois, o de saber qual a eficácia que é possível (ou desejável?) garantir na proteção de direitos, liberdades e garantias dos cidadãos há muito existentes e consagrados, agora no âmbito destes meios digitais de tratamento de informação, sem que os curadores dessa informação sejam, por um lado, obrigados a defender esta informação tão eficazmente quanto o conhecimento e a técnica atuais permitem – impedindo práticas de desproteção para poupança de custos – e, por outro lado, responsabilizados sempre que um ataque é levado a cabo com sucesso e gerando danos por vezes permanentes aos cidadãos a quem a informação violada pertencia.

A realidade tem confirmado estes aspetos como centrais no debate em torno da designada cibersegurança, registando-se a insuficiência de organismos de observação e certificação –

como aliás a Comunicação refere – bem como de legislação e mecanismos preventivos e sancionatórios coerentes e adequados.

Neste quadro, o desafio de garantir aos cidadãos a proteção adequada de direitos que se reconhecem fundamentais é necessariamente contraditório com o desenvolvimento desregulado de novas áreas ou práticas económicas que, a coberto do combate ao cibercrime ou da cibersegurança, pretendem afinal garantir apenas a máxima proteção possível à exploração económica da utilização de dispositivos eletrónicos e sistemas de comunicação digital.

A par da superação de alguma vacuidade na identificação dos objetivos a atingir e meios a mobilizar que sobressaem na análise da referida Estratégia, importará – talvez até de forma prévia – assegurar que o quadro legal, os respetivos mecanismos de proteção dos cidadãos e os organismos de fiscalização não venham a ficar à mercê de quem beneficia com a sua ineficácia ou violação, nomeadamente dos interesses económicos que frequentemente motivam os descritos ciberataques com objetivos de violação da privacidade dos cidadãos ou venda de produtos de cibersegurança.

O que deve motivar o aprofundamento da reflexão em torno do caráter público dos referidos organismos, com a desejada participação das instituições e ensino e investigação mas assegurando também a ligação aos agentes económicos com atuação nesta área.

Tal abordagem permitiria recentrar a abordagem da cibersegurança naqueles que são os direitos fundamentais dos cidadãos, europeus ou não: o direito à privacidade e à reserva da intimidade da vida privada.

## IV – Parecer

### Princípio da subsidiariedade

A Comunicação incide sobre matéria que suscitará, certamente, no futuro intervenção legislativa da União Europeia, sobretudo considerando o conteúdo da estratégia apontada pela Comissão para a cibersegurança em termos de coordenação ao nível da UE e a nível internacional.

No entanto, não se tratando de iniciativa legislativa, não cabe proceder à apreciação do princípio da subsidiariedade.

Face ao exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias é de parecer:

a) Que a *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* não suscita apreciação do princípio da subsidiariedade;

b) Que o presente relatório deve ser remetido à Comissão de Assuntos Europeus.

**Palácio de S. Bento, 12 de Junho de 2013**

**O Deputado Relator**

***(João Oliveira)***

**O Presidente da Comissão**

***(Fernando Negrão)***

ASSEMBLEIA DA REPÚBLICA

Comissão de Defesa Nacional

# Parecer

JOIN (2013) 1 Final

**Autor:** Manuel Correia de Jesus

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

**ÍNDICE**

## PARTE I – CONSIDERANDOS

### 1.1. NOTA PRÉVIA

No âmbito do acompanhamento, apreciação e pronúncia pela Assembleia da República no plano do processo de construção da União Europeia, a Comissão de Defesa Nacional decidiu pronunciar-se sobre a iniciativa europeia JOIN (2013) 1 Final – 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".

### 1.2 Objectivos e conteúdo da proposta

O documento que aqui se analisa traduz a visão global da União Europeia sobre a melhor forma de prevenir e dar resposta às perturbações e ataques na Internet. Assim, para proteger a abertura da rede, a liberdade e as oportunidades em linha, a Comissão Europeia, em colaboração com a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, publicou a sua proposta de estratégia em matéria de cibersegurança.

O documento "Um ciberespaço aberto, seguro e protegido", procura, segundo os seus autores, promover os valores europeus de liberdade e democracia e, ao mesmo tempo, garantir que a economia digital se desenvolva em condições de segurança.

Defende a Comissão que "para que o ciberespaço permaneça aberto e livre devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a União defende para o mundo físico. Os direitos fundamentais, a democracia e o Estado de Direito devem ser protegidos no ciberespaço." Ao mesmo tempo a liberdade em linha exige também segurança e protecção, devendo o ciberespaço ser protegido contra

incidentes, actividades maliciosas e utilizações abusivas, tendo os governos um importante papel a desempenhar neste domínio.

Apesar disso, é também reconhecido o papel crucial do sector privado que detém e explora partes significativas do ciberespaço e, como tal, a Comissão reconhece que nenhuma iniciativa nesta matéria pode avançar sem o seu contributo.

Tal como realçado no documento, é hoje plenamente reconhecido que as tecnologias da informação e das comunicações tornaram-se a "espinha dorsal" do nosso crescimento económico e são um recurso crítico do qual dependem todos os outros sectores.

Uma vez que seja concretizado o mercado único digital, a Europa poderá aumentar o seu PIB em quase 500 000 milhões de euros por ano, o que representa uma média de 1000 euros por pessoa. Para que isso aconteça é necessário que os cidadãos europeus tenham confiança na utilização da Internet e sejam ultrapassadas as grandes vulnerabilidades que o mundo digital ainda apresenta.

De facto, os chamados incidentes de cibersegurança[1], quer sejam intencionais ou meramente acidentais, aumentam a um nível preocupante e podem mesmo vir a provocar uma perturbação na prestação dos serviços que entendemos como básicos, como é o caso do abastecimento de água ou electricidade, os cuidados de saúde ou os serviços de telecomunicações móveis.

Neste caso, as ameaças podem ter origens diversas, nomeadamente ataques criminosos, politicamente motivados, terroristas ou patrocinados por alguns Estados ou catástrofes naturais e até erros humanos involuntários.

[1] Tal como é referido na comunicação da Comissão, o termo cibersegurança refere-se, geralmente, às precauções e acções que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade dessas redes e infraestruturas e a confidencialidade das informações nelas contidas.

Na comunicação é destacado que a economia da União é já bastante afectada pela cibercriminalidade[2] que atinge o sector privado e os particulares. Por outro lado, o aumento da espionagem económica e de actividades patrocinadas por Estados no ciberespaço coloca os governos e as empresas dos países da União ao alcance de uma nova categoria de ameaças.

Assim, tal como já foi referido anteriormente, a presente proposta para uma estratégia da União Europeia nesta matéria pretende clarificar os papéis e as responsabilidades e descreve as acções necessárias para proteger os direitos dos cidadãos a fim de tornar o ambiente em linha na União o mais seguro do mundo.

Para isso a visão da União, vertida nesta proposta, articula-se em torno de cinco grandes prioridades estratégicas:

1. Garantir a resiliência do ciberespaço;
2. Reduzir drasticamente a cibercriminalidade;
3. Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD);
4. Desenvolver os recursos industriais e tecnológicos para a cibersegurança;
5. Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da EU

[2] A cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes actividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infracções nacionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e software malicioso)

Tendo em conta o âmbito de intervenção da Comissão de Defesa Nacional, destacaremos de, entre estes, o ponto três, realçando as passagens que, na proposta, destacam os esforços que têm sido feitos em termos de ciberdefesa.

Assim, considera-se que o desenvolvimento de capacidades de ciberdefesa deve centrar-se na deteção de ameaças informáticas sofisticadas, na resposta a dar a essas ameaças e na recuperação posterior. É importante, para a União, melhorar as sinergias entre as abordagens civil e militar na proteção informática, sendo que os esforços a desenvolver nesta área devem ser acompanhados pela investigação e desenvolvimento e por uma cooperação mais próxima entre os governos dos estados-membros, o sector privado e as universidades.

No sentido de evitar duplicações, a União afirma que irá explorar as possibilidades de complementar os seus esforços com aqueles que são desenvolvidos pela NATO, de forma a aumentarem a resiliência das infraestruturas críticas das administrações, da defesa e outras das quais possam depender os membros destas duas organizações.

Neste campo e tal como é realçado na proposta, a Alta Representante, pedindo a colaboração dos Estados-membros e da Agência Europeia de Defesa, irá centrar os seus esforços nas seguintes actividades consideradas essenciais:

- Avaliar as exigências operacionais da UE em matéria de ciberdefesa e promover o desenvolvimento das capacidades e das tecnologias da UE nessa matéria para abordar todos os aspectos do desenvolvimento de capacidades – incluindo a doutrina, a liderança, a organização, o pessoal, a formação, as tecnologias, as infraestruturas, a logística e a interoperabilidade;

- Desenvolver o quadro político da UE em matéria de ciberdefesa para proteger as redes no quadro das missões e operações da PCSD, incluindo a gestão dinâmica dos riscos, a melhoria da análise das ameaças e a partilha de informações. Melhorar as oportunidades de formação e exercícios de

ciberdefesa para os militares no contexto europeu e multinacional, incluindo a integração de elementos de ciberdefesa nos atuais catálogos de exercícios;

- Promover o diálogo e a coordenação entre os actores civis e militares na UE, com especial enfoque no intercâmbio de boas práticas, no intercâmbio de informações, no alerta precoce, na resposta a incidentes, na avaliação dos riscos, na sensibilização e na atribuição de prioridade à cibersegurança;

- Assegurar o diálogo com os parceiros internacionais, incluindo a NATO, outras organizações internacionais e centros de excelência multinacionais, a fim de garantir capacidades de defesa efectivas, identificar os domínios de cooperação e evitar a duplicação de esforços.

Ao mesmo tempo a proposta afirma que, em cooperação com os Estados-membros, a Comissão e a Alta Representante irão:

- Trabalhar no sentido de definir para a UE uma política internacional coerente em matéria de ciberespaço, que vise aprofundar a colaboração com os principais parceiros e organizações internacionais, integrar as questões do ciberespaço na PESC e melhorar a coordenação das questões da cibersegurança que tenham dimensão mundial;

- Apoiar a elaboração de normas de comportamento e o estabelecimento de medidas que visem reforçar a confiança no campo da cibersegurança. Facilitar o diálogo sobre a forma de aplicar o direito internacional vigente no ciberespaço e promover a Convenção de Budapeste para combater a cibercriminalidade;

- Apoiar a promoção e a proteção dos direitos fundamentais, incluindo o acesso à informação e a liberdade de expressão, com os seguintes enfoques: a) estabelecer novas orientações públicas sobre a liberdade de expressão em

linha e fora de linha; b) controlar a exportação de produtos ou serviços suscetíveis de serem utilizados para a censura ou a vigilância em linha das populações; c) conceber medidas e ferramentas destinadas a alargar o acesso à Internet e a sua abertura e resiliência para resolver o problema da censura ou da vigilância das populações através das tecnologias da comunicação; d) dar autonomia às partes interessadas para utilizarem as tecnologias das comunicações para promoverem os direitos fundamentais;

- Colaborar com os parceiros e as organizações internacionais, o setor privado e a sociedade civil para ajudar os países terceiros a desenvolverem capacidades que permitam melhorar o acesso à informação e a uma Internet aberta, prevenir e combater as ameaças informáticas, incluindo acontecimentos acidentais, a cibercriminalidade e o ciberterrorismo, e reforçar a coordenação entre os doadores para canalizar os esforços nesse sentido;

- Utilizar os diferentes instrumentos de ajuda da UE para a criação de capacidades no domínio da cibersegurança, incluindo a assistência à formação das forças policiais e judiciárias e do pessoal técnico para lidarem com as ciberameaças, assim como apoiar a criação de políticas, estratégias e instituições nacionais neste domínio em países terceiros;

- Intensificar a coordenação das políticas e a partilha de informações através das redes internacionais de proteção das infraestruturas críticas da informação.

A Comissão e a Alta Representante garantem, juntamente com os Estados-membros, a nível internacional, uma acção coordenada no domínio da cibersegurança, defendendo os valores fundamentais da UE e a promoção de uma utilização pacífica, aberta e transparente das cibertecnologias. Fica também salvaguardado que existirá um diálogo político com os parceiros internacionais e com diversas organizações internacionais como o Conselho da Europa, a ONU, a NATO, a OSCE e a OCDE.

## PARTE II - OPINIÃO DO DEPUTADO AUTOR DO PARECER

A iniciativa europeia objecto do presente parecer, sob a epígrafe de "Funções e Responsabilidades", reconhece que "os governos nacionais estão em melhor posição para organizar a prevenção e a resposta aos incidentes e ataques informáticos e para estabelecer contactos e redes com o sector privado e o grande público através dos canais estabelecidos e dos quadros legais", sem prejuízo do necessário envolvimento da União Europeia.

Noutro passo, a iniciativa sublinha a necessária interligação entre os serviços de informações e a ciberdefesa para se poder actuar com eficácia no quadro das novas ameaças.

A este propósito, apraz-me registar que o novo Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de Abril, tenha destacado, na tipologia das ameaças transnacionais, a cibercriminalidade, e tenha reconhecido que, perante o carácter imprevisível, multifacetado e transnacional das novas ameaças, "os serviços de informações constituem-se como incontornáveis instrumentos de identificação e avaliação de ameaças e oportunidades em cenários voláteis e complexos".

É ainda de salientar que o CEDN, no âmbito das respostas a ameaças e riscos, tenha admitido que, no domínio da cibercriminalidade, "impõe-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados" e tenha definido, como linhas de acção prioritárias, as seguintes:

- garantir a protecção das infraestruturas de informação críticas, através da criação de um Sistema de Protecção da Infraestrutura de Informação Nacional (SPIIN);

- definir uma Estratégia Nacional de Cibersegurança;

- montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários;

- sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática;

- levantar a capacidade de ciberdefesa nacional.

Por seu lado, a Resolução do Conselho de Ministros n.º 26/2013, de 19 de Abril, que aprova as linhas de orientação para a execução da reforma estrutural da defesa nacional e das Forças Armadas, inclui, entre as operações específicas a ter em consideração no ciclo de planeamento estratégico, " o levantamento da capacidade de ciberdefesa nacional".

## PARTE III – Conclusões

1. A presente proposta da União Europeia para a cibersegurança, apresentada pela Comissão Europeia e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, define a visão da UE e as acções necessárias, fundadas numa proteção e numa promoção eficazes dos direitos dos cidadãos, para tornar o ambiente em linha na UE o mais seguro do mundo;

2. Esta visão apenas pode ser concretizada através de uma verdadeira parceria entre os diversos intervenientes que permita uma efectiva assumpção de responsabilidades e o encontrar das respostas para os desafios que se perspectivam para o futuro;

3. Face ao exposto, a Comissão de Defesa Nacional é de **Parecer** que o presente Relatório sobre a JOIN (2013) 1 Final deverá ser remetido à Comissão de Assuntos Europeus.

Palácio de S. Bento, 28 de Maio de 2013

**O Deputado autor do Parecer**

***(Correia de Jesus)***

**O Presidente da Comissão**

***(José de Matos Correia)***

**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)***