Council of the European Union

Brussels, 6 November 2018
(OR. en, pt)

13874/18

Interinstitutional File:
2018/0328(COD)

INST 432
CYBER 260
TELECOM 377
CODEC 1885
COPEN 378
COPS 400
COSI 254
CSC 306
CSCI 146
IND 321
JAI 1098
RECH 467
ESPACE 58
PARLNAT 258

COVER NOTE

From:	The Portuguese Parliament
date of receipt:	2 November 2018
To:	The President of the Council of the European Union
No. prev. doc.:	12104/18; COM(2018) 630 final
Subject:	Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [12104/18 - COM(2018) 630 final] - Opinion on the application of the Principles of Subsidiarity and Proportionality[1]

Delegations will find enclosed the opinion of the Portuguese Parliament on the above.

[1] The translation(s) of the opinion may be available on the Interparliamentary EU Information Exchange website (IPEX) at the following address: http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20180630.do

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Parecer

COM(2018)630 final

Proposta de REGULAMENTO DO CONSELHO que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação

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, que regula o acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, com as alterações introduzidas pelas Lei n.º 21/2012, de 17 de maio, e pela Lei nº 18/2018, de 2 de maio, bem como da Metodologia de escrutínio das iniciativas europeias aprovada em 1 de Março de 2016, a Comissão de Assuntos Europeus recebeu a Proposta de REGULAMENTO DO CONSELHO que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação. A presente iniciativa foi distribuída à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, que optou por não se pronunciar sobre a mesma.

PARTE II – CONSIDERANDOS

A presente proposta pretende estabelecer um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança com uma Rede de Centros Nacionais de Coordenação.

Começa-se por fazer referência à dependência das tecnologias digitais e à maior exposição dos cidadãos a "ciberincidentes graves", pelo que a segurança futura depende da capacidade da União em se proteger contra as ciberameaças, já que tanto as infraestruturas civis quanto as capacidades militares dependem de sistemas digitais seguros.

Para dar resposta a estes desafios, afirma-se que a União tem vindo a aumentar as suas atividades nestes domínios, baseando-se na Estratégia para a Cibersegurança de 2013[1] e nos seus objetivos e princípios de forma a fomentar um ambiente de cibersegurança que seja "fiável, seguro e aberto". Além disso, em 2016 a União adotou as primeiras medidas no âmbito da cibersegurança através da Diretiva (UE)

1 COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO: Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido [JOIN(2013) 1 final].

2016/1148 do Parlamento Europeu e do Conselho[2] relativa à segurança das redes e da informação.

O documento faz menção à Comunicação Conjunta[3] intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE», apresentada em setembro de 2017 pela Comissão e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, cujos preceitos se prendiam com (1) o reforço da resiliência e a capacidade de dissuasão e de resposta a ciberataques da União; (2) o reforço da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA); (3) a criação de um quadro de certificação da cibersegurança voluntário a nível da União com o intuito de aumentar a cibersegurança dos produtos e serviços no mundo digital; e (4) a formulação de um plano de ação para uma resposta célere e coordenada a incidentes e crises de cibersegurança em grande escala. Nesta comunicação conjunta foi também reconhecido que a União competir no mercado mundial de cibersegurança, pelo que deve proteger, de forma autónoma, os seus ativos digitais, assegurando que conserva e desenvolve as capacidades tecnológicas necessárias para proteger o seu mercado único digital e especialmente as redes e sistemas de informação críticos.

A proposta alerta que a União é um importador de produtos e soluções de cibersegurança, dependendo largamente de fornecedores não europeus[4], e que o mercado da cibersegurança totaliza 600 mil milhões de EUR, prevendo-se um aumento médio de cerca de 17% ao nível de vendas, número de empresas e postos de trabalho nos próximos 5 anos. Ao mesmo tempo, refere-se que nos 20 países que lideram o mercado da cibersegurança, há apenas seis Estados-Membros[5], mesmo existindo mais de 660 organizações da UE registadas pela Comissão e com elevados conhecimentos especializados no ramo da cibersegurança. No entanto, menciona-se que estes conhecimentos não são aproveitados devido, entre outros fatores, ao fato

2 Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

3 COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO – Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE [JOIN(2017) 450 final].

4 Projeto de relatório final sobre o Estudo do Mercado da Cibersegurança, 2018.

5 Projeto de relatório final sobre o Estudo do Mercado da Cibersegurança, 2018.

dos esforços das comunidades de investigação e industriais estarem fragmentados, carecendo de alinhamento e de uma missão comum. Assim, a competitividade da UE nesta área está comprometida, tendo ainda em conta que os setores e subdomínios relevantes da cibersegurança (por exemplo, energia, espaço, defesa, transportes) são hoje em dia insuficientemente apoiados[6].

Um passo sólido dado, segundo a proposta, foi a criação da parceria público-privada contratual («PPPc») para a cibersegurança na União (2016), que deve proporcionar resultados positivos na investigação e inovação. De todo modo, argumenta-se que a União pode fazer um investimento de uma maior envergadura de forma a criar capacidades duradouras, congregar esforços e competências e estimular "o desenvolvimento de soluções inovadoras que respondam aos desafios industriais da cibersegurança no domínio das tecnologias polivalentes (por exemplo, inteligência artificial, computação quântica, cifragem progressiva — blockchain — e identificação digital segura), bem como em setores críticos (por exemplo, transportes, energia, saúde, finanças, governação, telecomunicações, indústria transformadora, defesa, espaço)".

Ainda relativamente à comunicação conjunta, foi considerada a possibilidade de reforçar a capacidade de cibersegurança da União através de uma rede de centros de competências em cibersegurança com um centro europeu de competências em cibersegurança no seu centro, que "procuraria complementar os esforços existentes de criação de capacidade neste domínio a nível nacional e da União". A avaliação de impacto da estrutura deste centro seria compilada em 2018, tendo a Comissão lançado uma fase-piloto no âmbito do programa *Horizonte 2020*, para "constituir uma rede de centros nacionais com vista a criar uma nova dinâmica em matéria de competências em cibersegurança e de desenvolvimento tecnológico".

No mesmo seguimento foi a declaração dos chefes de Estado e de Governo presentes na Cimeira Digital de Taline, em setembro de 2017, que apelava para que a Comissão se tornasse «um líder mundial em cibersegurança até 2025, para assegurar a

6 Relatório Técnico do JRC: Resultados do Exercício de Levantamento (consultar os anexos 4 e 5 para mais pormenores).

confiança e a proteção dos nossos cidadãos, consumidores e empresas em linha e permitir uma Internet livre e regida pela lei».”

Ao nível das Conclusões do Conselho[7] adotadas em novembro de 2017, refere-se que estas instaram a Comissão a apresentar uma avaliação de impacto sobre as possíveis opções e propor até meados de 2018 o instrumento jurídico relevante para a execução da iniciativa.

A proposta de regulamento agora escrutinada indica que o *Programa Europa Digital* proposto pela Comissão em junho de 2018[8] procura “aumentar e maximizar os benefícios da transformação digital para os cidadãos e empresas europeus em todos os domínios de intervenção relevantes da UE, reforçando as políticas e apoiando as ambições do mercado único digital”, e que propõe uma “abordagem coerente e abrangente para assegurar a melhor utilização de tecnologias avançadas e a combinação certa de capacidade técnica e competências humanas para a transformação digital — não apenas no domínio da cibersegurança, mas também no tocante à infraestrutura inteligente de dados, à inteligência artificial, às competências e aplicações avançadas na indústria e em áreas de interesse público”. É ainda referido que o *Programa Horizonte Europa*[9] será o próximo programa-quadro de I&I da UE e que coloca igualmente a cibersegurança entre as suas prioridades.

No que diz respeito ao modelo de funcionamento do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança com uma Rede de Centros Nacionais de Coordenação, estabelece-se, em primeiro lugar, que o objetivo é estimular o ecossistema industrial e tecnológico europeu no domínio da cibersegurança, e que o Centro de Competências “facilitará e ajudará a coordenar os trabalhos da Rede e enriquecerá a Comunidade de Competências em Cibersegurança, impulsionando a agenda tecnológica neste domínio e facilitando o

7 Conclusões do Conselho sobre a Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE, adotadas pelo Conselho dos Assuntos Gerais em 20 de novembro de 2017.

8 Proposta de Regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027 [COM(2018) 434].

9 Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece o Horizonte Europa – Programa-Quadro de Investigação e Inovação e que define as suas regras de participação e difusão [COM (2018) 435].

acesso aos conhecimentos especializados que forem sendo agregados". Propõe-se que o Centro de Competências seja uma parceria europeia[10] para que haja um investimento conjunto da União, dos Estados-Membros e/ou da indústria tendo em vista os investimentos consideráveis realizados no domínio da cibersegurança noutras regiões do mundo e a necessidade de coordenar esforços de forma conjunta. Pretende-se que os Estados-Membros contribuam com um montante proporcional para as ações do Centro de Competências e da Rede, e refere-se que principal órgão de tomada de decisões será o Conselho de Administração, "no qual todos os Estados-Membros têm assento, embora só os que participem financeiramente tenham direito de voto".

De acordo com a proposta, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança seria o principal órgão de aplicação dos recursos financeiros da UE dedicados à cibersegurança ao abrigo do *Programa Europa Digital* e do *Programa Horizonte Europa* propostos, uma abordagem que permitiria apoiar a cibersegurança de uma forma mais lata, desde a investigação ao apoio à implantação e adoção de tecnologias-chave.

A Organização Europeia de Cibersegurança, atendendo aos seus conhecimentos especializados específicos e à representação ampla e relevante de partes interessadas, deverá ser convidada a contribuir para o trabalho do Centro e da Rede.

É igualmente referido que o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança deve procurar melhorar as sinergias entre as dimensões civil e militar da cibersegurança; apoiar os Estados-Membros ao nível do aconselhamento, da partilha de conhecimentos especializados e da facilitação da colaboração em projetos e ações; e, quando solicitado, atuar como gestor de projetos, particularmente em relação ao Fundo Europeu de Defesa.

---

10 Na aceção da proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação e que define as suas regras de participação e difusão [COM(2018) 435]; e conforme referido na proposta de regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027 [COM(2018) 434].

A presente iniciativa procura resolver 4 problemas identificados:

- Cooperação insuficiente entre as indústrias de procura e de oferta de cibersegurança. Este problema advém do fato das empresas europeias não serem capazes de proteger apropriadamente os seus produtos, serviços e ativos existentes ou de conceber produtos e serviços inovadores seguros, além de que as ligações entre a procura e a oferta do mercado da cibersegurança não estão suficientemente bem desenvolvidas, levando a um "fornecimento deficiente de produtos e soluções europeus adaptados às necessidades dos diferentes setores, bem como em níveis insuficientes de confiança entre os intervenientes do mercado".

- Ausência de um mecanismo de cooperação eficiente entre Estados-Membros para criação de capacidade industrial. A proposta refere que não existe um mecanismo de cooperação entre Estados-Membros que permita a estes trabalharem conjuntamente na inovação em matéria de cibersegurança nos setores industriais e a implantação de soluções de cibersegurança europeias de vanguarda

- Cooperação insuficiente no seio das comunidades de investigação e industriais e entre estas. Existem setores e subsetores de cibersegurança relevantes (por exemplo, energia, espaço, defesa, transportes) que não têm grande apoio da comunidade de investigação ou que são apoiados por um número reduzido de centros (por exemplo, criptografia pós-quântica e quântica, confiança e cibersegurança na IA).

- Cooperação insuficiente entre as comunidades civil e militar de investigação e inovação em matéria de cibersegurança. As sinergias entre as comunidades civil e militar não são devidamente concretizadas devido à ausência de mecanismos de cooperação, que são condição básica para que haja uma cooperação efetiva e que necessitam de mais fundos para a promoção de inovação.

Ao nível da coerência com as disposições em vigor no mesmo domínio de intervenção, a proposta refere que a rede de competências em cibersegurança e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança "atuarão como um apoio adicional às disposições políticas e intervenientes existentes em matéria de cibersegurança", sendo que o mandato do Centro Europeu será

complementar aos esforços da Agência Europeia para a Segurança das Redes e da Informação (ENISA), embora tendo um foco diferente.

A presente iniciativa pretende ampliar a parceria público-privada contratual (PPPc) para a cibersegurança que foi "a primeira tentativa à escala da UE de reunir a indústria da cibersegurança, a procura (compradores de produtos e soluções de cibersegurança, incluindo a administração pública e setores críticos como, por exemplo, os transportes, a saúde, a energia, e o financeiro) e a comunidade de investigação para criar uma plataforma de diálogo sustentável e criar condições para coinvestimento voluntário". Em comparação com os EUA, que investiram 19 mil milhões de dólares em cibersegurança só em 2017, a PPPc foi criada em 2016 e desencadeou 1,8 mil milhões de EUR de investimento até 2020, pelo que se argumenta que a UE tem de fazer mais para alcançar uma "massa crítica de investimento" e superar a fragmentação de capacidades espalhadas por toda a UE.

Relativamente à coerência com outras políticas da União, menciona-se que o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança irá atuar como um órgão de execução único para vários programas da União que apoiam a cibersegurança (Programa *Europa Digital* e *Horizonte Europa*), com vista a reforçar a coerência e as sinergias entre os mesmos. A iniciativa também permitirá prestar contributos para os decisores políticos no domínio da educação, a fim de melhorar as competências em cibersegurança (por exemplo, desenvolvendo conteúdos curriculares de cibersegurança em sistemas educativos civis e militares) para ajudar a desenvolver uma mão de obra qualificada no domínio da cibersegurança na EU.

Em termos da incidência orçamental, a proposta de regulamento refere que o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, em cooperação com a rede de competências em cibersegurança, será o principal órgão de execução dos recursos financeiros da UE dedicados à cibersegurança ao abrigo do Europa Digital e do Horizonte Europa. As implicações orçamentais estão listadas em pormenor na ficha financeira anexada à proposta e a contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação

total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), será proposta pela Comissão durante o processo legislativo.

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

a) Da Base Jurídica

A presente proposta é estabelecida com uma dupla base jurídica, nomeadamente pelo primeiro parágrafo do artigo 188.º Tratado sobre o Funcionamento da União Europeia, que prevê a adoção das medidas previstas no artigo 187.º, que estabelece as estruturas necessárias à boa execução dos programas de investigação, de desenvolvimento tecnológico e de demonstração da União, e permite ao Centro de Competências criar sinergias e reunir recursos para investir nas capacidades necessárias a nível dos Estados-Membros e desenvolver ativos europeus partilhados (por exemplo, mediante processos de aquisição conjunta de infraestruturas de teste e experimentação no domínio da cibersegurança). De todo modo, usar apenas o primeiro parágrafo do artigo 188.º não permitiria que as atividades fossem além da esfera da investigação e desenvolvimento conforme necessário para satisfazer todos os objetivos do Centro de Competências definidos no presente regulamento. Assim, a fim de alcançar esses objetivos, julga-se necessário aditar o artigo 173.º, n.º 3 como base jurídica, permitindo à União prever medidas para apoiar a competitividade da indústria.

b) Do Princípio da Subsidiariedade

Atendendo a que esta iniciativa incide sobre a cibersegurança, questão de interesse comum da União, e particularmente pela dimensão e caráter transfronteiriço de incidentes ocorridos no passado (por exemplo, WannaCry ou NonPetya), pode-se considerar que os objetivos da presente proposta e comunicação não podem ser suficientemente cumpridos pelos Estados-Membros e que podem ser mais bem alcançados a nível da União, pelo que a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Por conseguinte, esta respeita e cumpre o princípio da subsidiariedade.

c) Do Princípio da Proporcionalidade

Atendendo a que a iniciativa não excede o necessário para atingir os objetivos a que se propõe, considera-se que a mesma respeita o princípio da proporcionalidade.

PARTE III - OPINIÃO DA DEPUTADA AUTORA DO PARECER

A autora do presente parecer exime-se de, nesta sede, manifestar a sua opinião, a qual é de "*elaboração facultativa*" nos termos do nº 3 do artigo 137.º do Regimento da Assembleia da República.

PARTE IV – PARECER

Em face dos considerandos expostos, a Comissão de Assuntos Europeus é de parecer que:

1. A presente iniciativa não viola o princípio da proporcionalidade e da subsidiariedade;
2. Em relação à iniciativa em análise, o processo de escrutínio está concluído.

Palácio de S. Bento, 31 de outubro de 2018

A Deputada Autora do Parecer

Isabel Pires

(Isabel Pires)

A Presidente da Comissão

(Regina Bastos)