Parecer

COM(2017)477

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativa à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)

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, 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 PARLAMENTO EUROPEU E DO CONSELHO, relativa à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»). **[COM(2017)477]**

Atento o seu objeto, a presente iniciativa foi enviada à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias e à Comissão de Defesa Nacional, que a analisaram e aprovaram os respetivos Relatórios que se subscrevem e anexam ao presente Parecer, dele fazendo parte integrante.

PARTE II – CONSIDERANDOS

"A cibersegurança é uma pedra angular do mundo digital; é nossa responsabilidade comum"

Andrus Ansip, Vice-Presidente da Comissão Europeia

responsável pelo Mercado Único Digital.

A cibersegurança constitui um dos mais importantes desafios que se colocam na era atual. Num mundo cada vez mais tecnológico e em permanente evolução, onde as interações sociais e económicas se desenrolam no ciberespaço, é crucial garantir a segurança e a confiança cibernética a nível da União Europeia, bem como contribuir para a ciberestabilidade global.

A cibercriminalidade constitui hoje, uma das maiores ameaças para a sociedade e para a economia a nível global[1]. Ciente desta realidade e da vulnerabilidade do espaço europeu face a estas ameaças, a UE reconheceu a cibersegurança como uma prioridade política estratégica[2].

Neste domínio são, por isso, de notar os progressos que têm vindo a ocorrer, sobretudo nos últimos três anos, no sentido de aumentar a resiliência e melhorar a cibersegurança europeia. Assim, em 2013, a UE definiu uma estratégia para a cibersegurança[3], lançando

---

[1] Estima-se que as perdas provocadas pelos ciberataques atinjam cerca de 400 mil milhões de euros todos os anos. Alguns estudos sugerem que o impacto económico da cibercriminalidade aumentou cinco vezes, entre 2013 e 2017, podendo quadruplicar até 2019. ["Net Losses: Estimating the Global Cost of Cybercrime" - Centre for Strategic and International Studies, 2014.]

[2] Prioridade claramente assumida, em setembro de 2017, no Discurso do Presidente da Comissão Europeia sobre Estado da União. https://ec.europa.eu/commission/state-union-2017_pt

[3] COM JOIN (2013) 1.

um conjunto ações concretas essenciais para melhorar a ciberresiliência e fomentar um ciberecossistema fiável, seguro e aberto.

Contudo, a ocorrência de ameaças em constante evolução e o seu agravamento têm vindo a exigir a adoção de medidas adicionais. Isso mesmo se encontra refletido na Comunicação da Comissão intitulada "Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora"[4] bem como na Comunicação sobre "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE", de setembro de 2017. Foi neste contexto e na sequência da revisão intercalar da estratégia para o mercado digital, de maio de 2017 que a Comissão propôs a avaliação e revisão do Regulamento relativo a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA)[5], - cujo quadro jurídico atual é complementado pela Diretiva relativa à segurança das redes e da informação "Diretiva SRI"[6]. Essa avaliação foi centrada em torno da análise da relevância, impacto, eficácia, eficiência, coerência e o valor acrescentado para a UE da Agência relativamente ao seu desempenho, governação, estrutura organizacional interna e métodos de trabalho durante o período de 2013-2016. Tendo sido concluído que o desempenho da ENISA havia sido globalmente positivo. Porém, tendo em conta os rápidos desenvolvimentos tecnológicos e as ameaças em constante evolução, bem como os crescentes riscos mundiais de cibersegurança, considerou-se que havia necessidade de reforçar o papel da ENISA e atribuir-lhe uma maior centralidade, sobretudo na certificação de cibersegurança, para que esta pudesse desempenhar plenamente a sua função e assim responder adequada e eficazmente aos desafios atuais e futuros.

---

[4] COM (2016) 410.

[5] REGULAMENTO (UE) N.º 526/2013 DO PARLAMENTO EUROPEU E DO CONSELHO, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004.

[6] 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.

É na decorrência deste enquadramento que a Comissão apresenta a iniciativa em apreço, implicando a revogação do "REGULAMENTO (UE) N.º 526/2013 DO PARLAMENTO EUROPEU E DO CONSELHO, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), e que revoga o Regulamento (CE) n.º 460/2004", propondo a criação da **"Agência da UE para a Cibersegurança"** tendo por base a atual ENISA, atribuindo-lhe um mandato forte e permanente, tendo como objetivo principal apoiar e desenvolver uma cooperação mais estreita entre os Estados membros, com vista a aumentar as suas capacidades e reforçar a confiança na Europa digital.

Acresce mencionar que a presente iniciativa tenciona também resolver o atual problema da forte fragmentação dos sistemas de certificação de produtos e serviços de TIC, resultante da inexistência de um processo-quadro comum, eficaz e juridicamente vinculativo aplicável aos Estados membros, o que cria entraves à criação de um mercado interno para os produtos e serviços de TIC e se repercute negativamente na competitividade da indústria europeia neste setor. Para tal, propõe-se a criação de um quadro comum para a criação de sistemas de certificação da cibersegurança válidos, em toda a UE.

Em termos globais, visa-se melhorar o nível de preparação da UE para reagir através da organização de exercícios anuais de cibersegurança a nível europeu e garantir uma melhor partilha de informações e conhecimentos sobre ameaças, por intermédio da criação de centros de partilha e análise de informações. Pretende-se também apoiar a implementação da Diretiva relativa à segurança das redes e da informação " Diretiva SRI" que contém obrigações de comunicação às autoridades nacionais em caso de incidentes graves, visando além do mais, criar e aplicar um quadro de certificação à escala da UE, que garanta produtos e serviços ciberseguros.

Tendo presente os objetivos gerais enunciados, a iniciativa pretende alcançar os seguintes objetivos específicos: i) aumentar as capacidades e o grau de preparação dos Estados membros e das empresas; ii) melhorar a cooperação e coordenação entre Estados membros e instituições, nas agências e nos organismos da UE; iii) aumentar as capacidades a nível da UE para complementar a ação dos Estados membros, designadamente no caso de cibercrises transfronteiriças; iv) aumentar a sensibilização dos cidadãos e das empresas para as questões da cibersegurança; v) reforçar a confiança no mercado único digital e na inovação digital mediante uma maior transparência da garantia de cibersegurança de produtos e serviços de TIC.

Neste contexto, é relevante referir também que o Conselho Europeu, nas suas conclusões de 20 de outubro de 2017, reconheceu *"a importância da cibersegurança para a prosperidade, o crescimento e a segurança da UE e a integridade das nossas sociedades livres e democráticas e dos processos que lhes estão subjacentes na era digital, ao proteger tanto o Estado de direito como os direitos humanos e as liberdades fundamentais de todas as pessoas."* Reafirmando o seu propósito de *"fazer o que for necessário para que a Europa entre na era digital"*. Defendendo, desde logo, a adoção de *"uma abordagem comum da cibersegurança"*, sublinhando que *"o mundo digital requer confiança, e a confiança só se pode alcançar se garantirmos uma segurança mais proativa desde a conceção em todas as políticas digitais, se disponibilizarmos a adequada certificação de segurança dos produtos e serviços, e se aumentarmos a nossa capacidade para prevenir, dissuadir, detetar e debelar os ciberataques."* Reconhecendo igualmente a necessidade de *"integrar ainda mais a cibersegurança e a ciberdefesa na política comum de segurança e defesa (PCSD) e numa agenda de segurança e defesa mais ampla"*. Isto mesmo foi reafirmado pela Comissão no seu documento de reflexão sobre o futuro da defesa europeia, onde foi salientada a importância da cooperação em matéria de ciberdefesa, nomeadamente a sua intensificação com a NATO em domínios como as ameaças híbridas, a cibersegurança e a segurança marítima.

Considera-se que a UE tem atualmente condições para abordar esta problemática da cibersegurança com êxito, dado o âmbito das suas políticas e os instrumentos, estruturas e capacidades que tem à sua disposição, neste domínio.

Por último, importa referir que a ENISA sediada na Grécia desde a sua instituição em 2004, é o organismo a nível da UE competente em matéria de cibersegurança. Inicialmente, através do Regulamento (EC) Nº 460/2004, foi fixado um mandato por um período de 5 anos. Em 2008, através do Regulamento (EC) Nº 1007/2008 foi atribuída a um novo mandato até março de 2012. Em 2013, com o Regulamento (UE) n.º 526/2013 estabeleceu-se um novo mandato que terminará em 2020. A ENISA é considerada *"uma pequena agência, com um orçamento reduzido e poucos funcionários, comparativamente a todas as agências da UE"*. Além disso, continua a ser a única agência da UE com um mandato fixo, o que limita a sua capacidade de desenvolver uma visão a longo prazo e de apoiar as partes interessadas de um modo sustentável[7].

A ENISA apoia as instituições europeias, os Estados membros e as empresas na análise, na resposta e sobretudo na prevenção de problemas de segurança das redes e da informação. O seu desempenho tem sido bem conseguido ao *"contribuir para uma maior segurança das redes e da informação na Europa"* e ao proporcionar o reforço de capacidades nos 28 Estados membros, melhorando a cooperação entre eles e as partes interessadas na segurança das redes e da informação, bem como a prestação de conhecimentos especializados e o apoio a políticas.

Com a apresentação a da Revisão intercalar da Estratégia para o Mercado Único Digital, de maio de 2017[8], a Comissão propôs a revisão do mandato da ENISA. O objetivo subjacente visa adaptar e definir o seu papel no ecossistema alterado da cibersegurança e a adotar medidas em matéria de normas de cibersegurança, de certificação e de

[7] Isto contrasta com as disposições da Diretiva SRI, que confiam à ENISA funções sem termo.
[8] COM(2017) 228 final

rotulagem para tornar os sistemas baseados nas TIC, sobretudo os objetos conectados, mais ciberseguros.

a) Da Base Jurídica

A base jurídica da presente iniciativa assenta no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que versa a aproximação das legislações dos Estados-Membros a fim de alcançar a realização dos objetivos enunciados no artigo 26.º do TFUE, nomeadamente o bom funcionamento do mercado interno.

a) Do Princípio da Subsidiariedade

No que concerne à verificação do princípio da subsidiariedade cumpre referir que seu cumprimento foi já reconhecido aquando da adoção do Regulamento ENISA em vigor. Porém, importa sublinhar que a cibersegurança é um domínio de interesse comum da União. As interdependências entre redes e sistemas de informação assumem uma dimensão tal, que quer os intervenientes sejam públicos ou privados, não podem enfrentar ameaças, gerir os riscos e os eventuais impactos de ciberincidentes isoladamente. Além do mais, as interdependências entre Estados membros, sobretudo no que concerne ao funcionamento de infraestruturas críticas, como por exemplo: energia, transportes, água, revelam a importância e a necessidade de uma ação a nível da UE.

Por conseguinte, e tendo em conta não apenas contexto atual, como a perspetiva futura da cibersegurança, entende-se que se justifica a ação da UE uma vez que a sua intervenção permitirá robustecer a ciberresiliência coletiva da União. Acresce mencionar que a intervenção a nível da UE é também considerada necessária para resolver a fragmentação dos atuais sistemas de certificação da cibersegurança e beneficiar o mercado interno.

Entende-se assim que os objetivos que a presente iniciativa pretende alcançar não podem ser suficientemente alcançados pelos Estados membros.

Face ao exposto, considera-se que presente iniciativa respeita o princípio da subsidiariedade.

PARTE III – PARECER

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

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

2. No que concerne à presente iniciativa o processo de escrutínio está concluído. Todavia, atendendo à importância da matéria em causa, a Comissão de Assuntos Europeus prosseguirá o acompanhamento do processo legislativo, nomeadamente através de troca de informação com o Governo.

Palácio de S. Bento, 6 de dezembro de 2017

O Deputado Relator

(Vitalino Canas)

A Presidente da Comissão

(Regina Bastos)

PARTE IV – ANEXO

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

ASSEMBLEIA DA REPÚBLICA

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

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

COM (2017) 477 final

Relatora:

Deputada Isabel Moreira

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «*Agência da União Europeia para a Cibersegurança*», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («*Regulamento Cibersegurança*»)

1. Nota introdutória

Em cumprimento do disposto no n.º 1 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 estabelece o regime de acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, foi distribuída à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, a iniciativa europeia *«COM (2017) 477 final – Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)»*, para análise e elaboração de parecer, sendo designada a Deputada Relatora no dia 25 de outubro de 2017.

2. Enquadramento e objeto da iniciativa

A proposta de regulamento em causa surge na sequência da revisão intercalar da estratégia para o mercado único digital, de maio de 2017, no âmbito da qual a Comissão Europeia se comprometeu a proceder à revisão do mandato atribuído à ora designada ENISA – Agência da União Europeia para a Segurança das Redes e da Informação (que funciona nos termos previstos no Regulamento n.º 526/2013[1]), cujo

[1] Em 2004, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 460/2004 , que cria a ENISA, a fim de contribuir para a consecução dos objetivos de garantir um elevado nível de segurança das redes e da informação na União e de desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. Em 2008, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 1007/2008 , que prolonga o mandato da Agência até março de 2012. O Regulamento (CE) n.º 580/2011 prorrogou o mandato da Agência até 13 de setembro de 2013. Em 2013, o Parlamento Europeu e o Conselho adotaram o Regulamento (UE) n.º 526/2013 , relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004, o qual prorrogou o mandato da Agência até junho de 2020

quadro atual se complementa com a Diretiva SRI – relativa à segurança das redes de informação (Diretiva 2016/1148[2]).

O Conselho Europeu, nas suas conclusões de 15 de novembro de 2016, já assumia que «*as ciberameaças e as vulnerabilidades continuam a evoluir e a intensificar-se*» e reconhecia a necessidade de uma «*cooperação contínua e mais estreita, particularmente no tratamento de incidentes transfronteiras de grande escala em matéria de cibersegurança*».

Conforme enfatizam os considerandos da proposta, «*a digitalização e a conectividade estão a tornar-se características centrais num número cada vez maior de produtos e serviços e, com o surgimento da Internet das coisas (IdC), espera-se que milhões, se não mesmo milhares de milhões, de dispositivos digitais conectados sejam implantados em toda a UE durante a próxima década*», reforçando que, «*embora cada vez mais dispositivos estejam conectados à Internet, a segurança e a resiliência não são suficientemente integradas desde a conceção, conduzindo a uma insuficiência de cibersegurança*».

Refere-se que «*neste contexto, a utilização reduzida da certificação leva a que haja informação insuficiente para os utilizadores empresariais e individuais sobre as características de cibersegurança de produtos e serviços de TIC, prejudicando a confiança nas soluções digitais*» e que «*a digitalização e conectividade crescentes conduzem a maiores riscos de cibersegurança, tornando, assim, a sociedade em geral mais vulnerável a ciberameaças e agravando os perigos que as pessoas enfrentam, nomeadamente as pessoas vulneráveis como as crianças*».

Constata-se que «*apesar de os ciberataques terem amiúde uma natureza transfronteiriça, as respostas políticas por parte das autoridades responsáveis pela cibersegurança e as competências de aplicação da lei são predominantemente nacionais*», sendo que esta realidade «*exige uma resposta e uma gestão de crises a*

[2] A Diretiva SRI instituiu requisitos relativos às capacidades nacionais no domínio da cibersegurança, criou os primeiros mecanismos para reforçar a cooperação estratégica e operacional entre Estados-Membros e introduziu obrigações relativas às medidas de segurança e notificações de incidentes nos setores que são vitais para a economia e a sociedade, tais como a energia, os transportes, a água, a banca, as infraestruturas do mercado financeiro, os cuidados de saúde, as infraestruturas digitais, bem como os prestadores de serviços digitais essenciais (motores de pesquisa, serviços de computação em nuvem e mercados em linha).

nível da UE, criando políticas específicas e desenvolvendo instrumentos mais abrangentes que permitam mostrar a solidariedade europeia e prestar assistência mútua».

Consequentemente, a Comissão vem propor, através da iniciativa em apreço, uma revisão da estratégia de Cibersegurança que visa, nomeadamente, os seguintes objetivos:

(i) Aumentar as capacidades e o grau de preparação dos Estados-Membros e das empresas

- *Reforço das capacidades e do grau de preparação dos Estados-Membros em relação à cibersegurança (mediante a análise estratégica de longo prazo das ciberameaças e dos ciberincidentes, orientação e relatórios, corretagem de conhecimentos especializados e boas práticas, disponibilidade de formação e materiais de formação, exercícios «CyberEurope» reforçados);*

- *Reforço das capacidades dos intervenientes privados, graças ao apoio à criação de centros de partilha e análise de informações (ISAC) em vários setores;*

- *Reforço do grau de preparação da UE e dos Estados-Membros em matéria de cibersegurança, com a disponibilidade de planos bem ensaiados e acordados em caso de incidentes de cibersegurança transfronteiriços em grande escala, testados nos exercícios «CyberEurope».*

(ii) Melhorar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE

- *Reforço da cooperação dentro dos setores público e privado e entre estes;*
- *Maior coerência na abordagem à execução da Diretiva SRI entre fronteiras e setores;*
- *Reforço da cooperação no domínio da certificação devido a um quadro institucional que permite o desenvolvimento de sistemas europeus de certificação da cibersegurança e o desenvolvimento de uma política comum neste domínio.*

(iii) Aumentar as capacidades a nível da UE para complementar a ação dos Estados-Membros, designadamente no caso de cibercrises transfronteiriças

- *Reforço da «capacidade operacional da UE» para complementar a ação dos Estados-Membros e apoiá-los, mediante pedido e em relação a serviços limitados e identificados previamente, esperando-se que estes aspetos tenham um impacto positivo no êxito da prevenção, deteção e resposta a incidentes a nível dos Estados-Membros e da União.*

(iv) Aumentar a sensibilização dos cidadãos e das empresas para as questões da cibersegurança

- *Reforço da sensibilização geral dos cidadãos e das empresas para questões da cibersegurança;*
- *Reforço da capacidade de tomar decisões de compra fundamentadas relativamente a produtos e serviços de TIC, graças à certificação da cibersegurança.*

(v) Aumentar a transparência da garantia de cibersegurança de produtos e serviços de TIC, a fim de reforçar a confiança no mercado único digital e na inovação digital

- *Reforço da transparência da garantia de cibersegurança de produtos e serviços de TIC, graças à simplificação de procedimentos para certificação da segurança por meio de um quadro a nível da UE;*
- *Reforço do nível de garantia das propriedades de segurança de produtos e serviços de TIC;*
- *Maior adoção da certificação da segurança, incentivada por procedimentos simplificados, custos reduzidos e pela perspetiva de oportunidades de negócio a nível na UE não entravadas pela fragmentação do mercado;*
- *Reforço da competitividade no mercado da cibersegurança da UE devido à redução de custos e encargos administrativos para as PME e à eliminação de possíveis obstáculos à entrada no mercado causados pela diversidade de sistemas nacionais de certificação.*

(vi) Evitar a fragmentação dos sistemas de certificação na UE e dos requisitos de segurança conexos, bem como dos critérios de avaliação nos Estados-Membros e setores.

Conforme refere a ficha legislativa financeira que acompanha a proposta, pretende-se, em síntese, atribuir à Agência que sucede à ENISA, que se designará por **Agência da União Europeia para a Cibersegurança**, «*um papel mais forte e mais central, nomeadamente no apoio mais ativo aos Estados-Membros no combate a ameaças específicas (capacidade operacional), e torná-la num centro de conhecimentos*

especializados que apoia os Estados-Membros e a Comissão em matéria de certificação de cibersegurança».

Por outro lado, prevê-se um quadro europeu de certificação da cibersegurança de produtos e serviços de TIC, especificando as funções e tarefas essenciais da ENISA no domínio da certificação da cibersegurança.

Este quadro estabelecerá «*disposições e procedimentos comuns que permitem a criação de sistemas de certificação da cibersegurança a nível da UE para produtos/serviços de TIC específicos ou riscos de cibersegurança*», respondendo à atual «*fragmentação do mercado*».

A proposta de Regulamento é composta por 58 artigos, divididos sistematicamente por 4 títulos que tratam, respetivamente, das disposições gerais do regulamento, do regime da Agência da União Europeia para a Cibersegurança (mandato, objetivos e atribuições, organização, orçamento, pessoal), do Quadro de Certificação da Cibersegurança e das disposições finais.

Importa, por último, sinalizar que o Regulamento n.º 526/2013 será revogado com a aprovação do regulamento em apreço, não se encontrando prevista no documento data indicativa para produção de efeitos.

3. Princípio da Subsidiariedade e da Proporcionalidade

A base jurídica invocada, para sustentar a iniciativa, são os artigos 26.º e 114.º do TFUE, com incidência no cumprimento do objetivo da UE de «bom funcionamento do mercado interno», ora validada por decisão do TJUE e pela aprovação do Regulamento ainda em vigor que fixou o atual mandato da agência.

A iniciativa almeja fazer face ao crescendo de desafios e riscos inerentes ao desenvolvimento e aprofundamento do mercado interno, em especial do mercado

digital europeu, reconhecendo as ameaças de dimensão e impacto transfronteiriços, que colocam em causa os direitos e a segurança de pessoas, empresas e instituições, com efeitos económicos nocivos, e que serão mais eficazmente enfrentadas com uma ação concertada e coordenada de Estados-Membros e da União Europeia.

Concorda-se pois com a avaliação subjacente à intervenção em apreço, de que o aumento da «*ciber-resiliência*» da União Europeia não se compadece apenas com a ação isolada de cada um dos Estados-Membros ou uma abordagem fragmentada à realidade da cibersegurança, nomeadamente, ao nível dos sistemas de certificação.

Ainda assim, no processo de transição para o proposto sistema europeu de certificação da cibersegurança, ainda em aberto no documento, conta-se com uma aplicação adequada e articulada com a realidade específica dos sistemas nacionais em vigor e dos interesses em presença.

De resto, o alcance das medidas previstas é apresentado de forma a não exceder o estritamente necessário para a concretização dos objetivos definidos, respeitando o espaço próprio de intervenção dos Estados-Membros que é, pelo contrário, potenciado com a partilha e reforço de capacidades operacionais.

Considera-se assim que a proposta de regulamento em causa não contende com os princípios da subsidiariedade e da proporcionalidade preconizados pelo artigo 5.º do Tratado da União Europeia, considerada a vocação de intervenção supranacional e a abordagem de complementaridade e cooperação ora preservada e preconizada.

4. Parecer

Face ao exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias é de parecer que o presente relatório que aprecia o documento comunitário «*COM (2017) 477 final – Proposta de Regulamento do Parlamento Europeu e do*

ASSEMBLEIA DA REPÚBLICA

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)», seja remetido à Comissão de Assuntos Europeus, nos termos da Lei n.º 43/2006, de 25 de agosto, alterada pela Lei n.º 21/2012, de 17 de maio, para os devidos efeitos.

Palácio de São Bento, 28 de novembro de 2017

A Deputada Relatora,

(Isabel Moreira)

O Presidente da Comissão,

(Pedro Bacelar de Vasconcelos)

ASSEMBLEIA DA REPÚBLICA

Comissão de Defesa Nacional

Exma. Senhora
Dr.ª Regina Bastos
Presidente da Comissão de Assuntos Europeus

Of. N.º 139/3.ªCDN/2017

04-12-2017

Assunto: Envio de Relatório - (COM(2017)477 - Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento . (UE) n.º 526/2013 («Regulamento Cibersegurança»)

Para os devidos efeitos, junto se envia o relatório sobre a iniciativa europeia COM (COM(2017)477 - Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»), que, submetido á votação nas partes regimentalmente votáveis, foi aprovado por unanimidade, na reunião de 30 de novembro de 2017 da Comissão de Defesa Nacional.

Com os melhores cumprimentos,

O Presidente da Comissão,

(Marco António Costa)

Palácio de S. Bento - 1249-068 LISBOA - PORTUGAL - Telefone: 21 391 9602
3CDN@.parlamento.pt

Relatório
COM (2017) 477 final

Autor: Deputado
Miranda Calha (PS)

COM (2017) 477 final - Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»)

ÍNDICE

PARTE I – NOTA INTRODUTÓRIA

PARTE II – CONSIDERANDOS

PARTE III – CONCLUSÕES

PARTE I – NOTA INTRODUTÓRIA

No cumprimento da Lei n.º 43/2006, de 25 de agosto, com as alterações introduzidas pela Lei n.º 21/2012, de 17 de maio, referente ao *"Acompanhamento, Apreciação e Pronúncia pela Assembleia da República no âmbito do Processo de Construção da União Europeia"*, a Comissão de Assuntos Europeus enviou à Comissão de Defesa Nacional a Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO, relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»), acompanhada do documento de trabalho {SWD(2017) 500 final} {SWD(2017) 501 final} {SWD(2017) 502 final}, para efeito de análise e elaboração do presente relatório, tendo sido designado como Relator o Deputado Miranda Calha.

PARTE II – CONSIDERANDOS

1- Exposição de motivos

1. A COM (2017) 477 final diz respeito à Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO, relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»).

2. Na base da Proposta de Regulamento em apreciação está a revisão da estratégia para o mercado único digital, que data de maio de 2017, e que corresponde ao compromisso da Comissão Europeia de rever o mandato atribuído à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA).

3. Em 2013, foi adotada a primeira Estratégia da UE para a Cibersegurança e foram então definidos objetivos estratégicos e ações concretas, no sentido de alcançar resiliência,

reduzir a cibercriminalidade, desenvolver a política e as capacidades de ciberdefesa, desenvolver recursos industriais e tecnológicos e estabelecer uma política internacional coerente em matéria de ciberespaço para a UE, merecendo destaque importantes desenvolvimentos, particularmente, o segundo mandato da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e a adoção da Diretiva relativa à segurança das redes e da informação («Diretiva SRI»), que constituem a base da proposta em apreço.

4. Mais tarde, em 2016, foram anunciadas outras medidas para instituir a cooperação e o intercâmbio de informações e conhecimentos e para reforçar a resiliência e a preparação da UE. Para tanto, a União Europeia adotou uma comunicação intitulada «*Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora*», considerando a possibilidade de ocorrência de incidentes em grande escala e uma eventual crise pan-europeia de cibersegurança.

5. A aprovação do regulamento em análise implica a revogação do Regulamento n.º 526/2013 do Parlamento Europeu e do Conselho, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004.

6. Nesta sede, importará ter presente que nas conclusões do Conselho Europeu, de 15 de novembro de 2016, se constata a efetiva preocupação com as questões ora levantadas, lendo-se que «*as ciberameaças e as vulnerabilidades continuam a evoluir e a intensificar-se*», e o reconhecimento da sua premência, pela invocação da necessidade de uma cooperação contínua e mais estreita, em especial no tratamento de incidentes transfronteiras de grande escala em matéria de cibersegurança.

7. Neste contexto, na Proposta é sublinhado que «*apesar de os ciberataques terem amiúde uma natureza transfronteiriça, as respostas políticas por parte das autoridades responsáveis pela cibersegurança e as competências de aplicação da lei são predominantemente nacionais*». Assim, exige-se uma resposta que aconteça a nível da UE, pela criação de políticas concretas e pelo desenvolvimento de instrumentos de maior abrangência «*que permitam mostrar a solidariedade europeia e prestar assistência mútua*».

8. A proposta da Comissão apresenta uma análise prévia de um conjunto diversificado de medidas, que se reporta a ações anteriores e promove os objetivos que seguem:

   - **Aumentar as capacidades e o grau de preparação dos Estados-Membros e das empresas,** pelo reforço das capacidades e do grau de preparação dos Estados-Membros em relação à cibersegurança (mediante a análise estratégica de longo prazo das ciberameaças e dos ciberincidentes, orientação e relatórios, corretagem de conhecimentos especializados e boas práticas, disponibilidade de formação e materiais de formação, exercícios «CyberEurope» reforçados), das capacidades dos intervenientes privados, graças ao apoio à criação de centros de partilha e análise de informações (ISAC) em vários setores e do grau de preparação da UE e dos Estados-Membros em matéria de cibersegurança, com a disponibilidade de planos bem ensaiados e acordados em caso de incidentes de cibersegurança transfronteiriços em grande escala, testados nos exercícios «CyberEurope»;

   - **Melhorar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da EU,** reforçando a cooperação dentro dos setores público e privado e entre estes, a coerência na abordagem à execução da Diretiva SRI entre fronteiras e setores e a cooperação no domínio da certificação devido a um quadro institucional que permite o desenvolvimento de sistemas europeus de certificação da cibersegurança e o desenvolvimento de uma política comum neste domínio;

   - **Aumentar as capacidades a nível da UE para complementar a ação dos Estados-Membros, designadamente no caso de cibercrises transfronteiriças,** o que passa pelo reforço da «capacidade operacional da UE» para complementar a ação dos Estados-Membros e apoiá-los, mediante pedido e em relação a serviços limitados e identificados previamente, esperando-se que estes aspetos tenham um impacto positivo no êxito da prevenção, deteção e resposta a incidentes a nível dos Estados-Membros e da União;

   - **Aumentar a sensibilização dos cidadãos e das empresas para as questões da cibersegurança,** pela sensibilizando geral dos cidadãos e das empresas para questões da cibersegurança e reforço da capacidade de tomar decisões de compra

fundamentadas relativamente a produtos e serviços de TIC, graças à certificação da cibersegurança;

- **Aumentar a transparência da garantia de cibersegurança de produtos e serviços de TIC, a fim de reforçar a confiança no mercado único digital e na inovação digital**, aumentando a transparência da garantia de cibersegurança de produtos e serviços de TIC, graças à simplificação de procedimentos para certificação da segurança por meio de um quadro a nível da EU, elevando o nível de garantia das propriedades de segurança de produtos e serviços de TIC, garantindo uma maior adoção da certificação da segurança, incentivada por procedimentos simplificados, custos reduzidos e pela perspetiva de oportunidades de negócio a nível na UE não entravadas pela fragmentação do mercado e reforçando a competitividade no mercado da cibersegurança da UE devido à redução de custos e encargos administrativos para as PME e à eliminação de possíveis obstáculos à entrada no mercado causados pela diversidade de sistemas nacionais de certificação;
- **Evitar a fragmentação dos sistemas de certificação na UE e dos requisitos de segurança conexos, bem como dos critérios de avaliação nos Estados-Membros e setores.**

9. Em suma, está em consideração a atribuição à Agência da União Europeia para a Cibersegurança de uma posição «*mais forte e mais central, nomeadamente no apoio mais ativo aos Estados-Membros no combate a ameaças específicas (capacidade operacional), e torná-la num centro de conhecimentos especializados que apoia os Estados-Membros e a Comissão em matéria de certificação de cibersegurança*».

10. No sentido de definir «*disposições e procedimentos comuns que permitem a criação de sistemas de certificação da cibersegurança a nível da UE para produtos/serviços de TIC específicos ou riscos de cibersegurança*», em resposta à fragmentação do mercado, antevê-se um enquadramento europeu de certificação da cibersegurança de produtos e serviços de TIC, especificando as funções e tarefas essenciais da ENISA.

11. Em termos de sistemática, a proposta de Regulamento COM (2017) 477 final - Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, «Agência

da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança») trata, em 4 títulos, as disposições gerais do regulamento, do regime da Agência da União Europeia para a Cibersegurança, o Quadro de Certificação da Cibersegurança e as disposições finais, compondo um articulado, constituído por 58 artigos.

2- Princípio da Subsidiariedade

A proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»), referente à promoção de «*ciber-resiliência*» e de confiança no seio da União da União Europeia em matéria de cibersegurança, compreendendo a premente necessidade de assegurar o normal funcionamento do mercado interno, respeita o princípio da subsidiariedade, preconizado pelo artigo 5.º do Tratado da União Europeia. Com efeito, os objetivos preconizados pressupõem uma abordagem política necessariamente colaborativa, que não se confina às fronteiras nacionais, podendo ser conseguidos se abordados numa perspetiva de complementaridade e cooperação a nível europeu.

PARTE III – CONCLUSÕES

No âmbito do processo de escrutínio previsto na Lei n.º 43/2006, de 25 de agosto, com as alterações da Lei n.º 21/2012, de 17 de maio, a Comissão de Defesa Nacional é de parecer que o presente relatório seja, para os efeitos devidos, remetido à Comissão de Assuntos Europeus.

Palácio de S. Bento, 30 de novembro de 2017.

O Deputado Relator

(Miranda Calha)

O Presidente da Comissão

(Marco António Costa)