Council of the European Union

Brussels, 6 July 2023
(OR. en, pt)

11525/23

Interinstitutional File: 2023/0109(COD)

CYBER 179
TELECOM 225
IND 373
FIN 748
BUDGET 20
CADREFIN 100
CODEC 1306
PARLNAT 151
INST 258

COVER NOTE

From:	The Portuguese Parliament
date of receipt:	30 June 2023
To:	The President of the Council of the European Union
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents [8512/23 - COM(2023)209] - Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion[1] of the Portuguese Parliament (Assembleia da República) 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: https://secure.ipex.eu/IPEXL-WEB/document/COM-2023-209

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

Parecer COM(2023)209	Autora: Deputada Rosário Gamboa

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO - que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança.

1

PARTE I - NOTA INTRODUTÓRIA

Nos termos do disposto no 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 pela Lei n.º 21/2012, de 17 de maio, pela Lei n.º 18/2018, de 2 de maio e pela Lei 64/2020, de 2 de novembro, bem como na 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 - que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança [COM(2023) 209].

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, aprovando os respetivos Relatórios que se anexam ao presente Parecer, dele fazendo parte integrante.

PARTE II – CONSIDERANDOS

1. A iniciativa, ora em apreço, tem com objetivo geral reforçar a solidariedade e as capacidades da União Europeia, para detetar e responder a ameaças e incidentes no domínio da cibersegurança.
2. O regresso da guerra à Europa com a invasão da Rússia à Ucrânia levou a uma tomada de consciência a nível europeu da necessidade da UE assumir mais responsabilidade pela sua própria segurança. Também, as atuais alterações geopolíticas vieram ampliar essa necessidade, tornando imperativa a adoção de uma abordagem comum em matéria de segurança e defesa para reforçar a capacidade europeia de defender os seus interesses, nomeadamente no ciberespaço.
3. Neste contexto, tornou-se indubitável que a UE deveria assegurar a sua soberania tecnológica e digital, no domínio da cibernética. Mas, para isso, também precisaria de agir em conjunto para alcançar uma cibersegurança mais forte. Isto mesmo é reconhecido pelo Conselho *"a força da nossa União reside na unidade, na solidariedade e na determinação"*[1].
4. A presente iniciativa, vem, nesta conformidade, responder a este desafio uma vez que visa contribuir para melhorar a deteção e a sensibilização para ameaças e incidentes de cibersegurança, apoiar a preparação das entidades críticas e reforçar a solidariedade, a gestão concertada de crises e as capacidades de resposta em todos os Estados Membros, reforçando assim, a resiliência da União para enfrentar este tipo de riscos. Neste sentido, propõe a criação de

[1] Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, de 23 de maio de 2022.

capacidades a nível da UE de forma a tornar a Europa mais resiliente e mais reativa face às ciberameaças, reforçando simultaneamente o mecanismo de cooperação existente. Além disso, visa contribuir para o desenvolvimento de um panorama digital seguro tanto para os cidadãos como para as empresas, bem como proteger as entidades críticas e os serviços essenciais, como hospitais e serviços públicos.

5. Por conseguinte, para poder detetar as principais ciberameaças de forma rápida e eficaz, a presente iniciativa propõe: i) a criação de um **Escudo de Cibersegurança da UE** através de uma infraestrutura pan-europeia constituída por centros de operações de segurança (SOC)[2] em toda a União Europeia, reunidas em várias plataformas nacionais e transfronteiras[3]; ii) a criação de um **Mecanismo de Ciberemergência** destinado a melhorar a preparação e as capacidades de resposta a incidentes na UE[4]; iii) a criação de um **Mecanismo de Análise de Incidentes de Cibersegurança**, que visa reforçar a resiliência da União, analisando e avaliando incidentes de cibersegurança importantes ou de grande

[2] Do inglês Security Operations Centres

[3] São entidades encarregadas de detetar eventuais ciberameaças e de intervir em conformidade. Estes centros (SOC) recorrerão a tecnologias de ponta, incluindo a inteligência artificial (IA) e técnicas avançadas de análise de dados, para detetar e partilhar atempadamente alertas sobre incidentes e ameaças de cibersegurança de natureza transfronteiras. Permitindo que as autoridades e as entidades competentes possam responder de forma mais eficiente e mais eficaz a incidentes importantes.

[4] Este mecanismo apoiará: i) **Medidas de preparação**, nomeadamente a realização de testes a entidades de setores altamente críticos (saúde, transportes, energia, etc.), com vista a detetar eventuais vulnerabilidades, com base em cenários e metodologias de risco comuns; ii) **Criação de uma nova Reserva de Cibersegurança da UE**, constituída por serviços de resposta a incidentes prestados por fornecedores dignos de confiança pré-contratados e, consequentemente, prontos a intervir, a pedido de um Estado Membro ou de instituições, órgãos e organismos da União, em caso de incidentes de cibersegurança importantes ou de grande escala; iii) **Prestação de apoio financeiro** para assistência mútua, nos casos em que um Estado Membro possa oferecer assistência a outro Estado Membro.

escala após a sua ocorrência[5], retirando ensinamentos e, se for caso disso, formulando recomendações para melhorar a postura da União em matéria de cibersegurança.

De mencionar que o orçamento global previsto para este conjunto de medidas eleva-se a 1,109 mil milhões de euros[6], financiados ao abrigo do objetivo estratégico "Cibersegurança" do Programa Europa Digital (PED).

6. Em suma, a iniciativa proposta pretende reforçar a solidariedade a nível da União, a fim de melhorar a deteção, a preparação e a resposta a incidentes de cibersegurança importantes, ou de grande escala, através da criação de um Escudo de Cibersegurança da UE e de um Mecanismo Global de Ciberemergência. Além do mais, visa que estas ações permitam reforçar a posição competitiva da indústria e das empresas europeias na economia digital e apoiem a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital.

7. Por último, tendo em conta que os Relatórios apresentados pela Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias e pela Comissão de Defesa Nacional, refletem o conteúdo da iniciativa com rigor, considera-se que devem, por isso, ser dados por integralmente reproduzidos, evitando-se desta forma uma repetição de análise e consequente redundância.

---

[5] A pedido da Comissão ou das autoridades nacionais (UE-CyCLONe ou rede de CSIRT), a Agência da UE para a Cibersegurança (ENISA) será responsável pela análise deste tipo de incidentes de cibersegurança recomendações para melhorar a resposta cibernética da União, deverá apresentar um relatório que inclua os ensinamentos retirados e, se for caso disso, formular recomendações para melhorar a postura da União em matéria de cibersegurança.

[6] Incluindo as contribuições dos Estados Membros.

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

a) Da Base Jurídica

A presente iniciativa é sustentada, juridicamente, pelo artigo 173.º, n.º 3, e o artigo 322.º, n.º 1, alínea a) do Tratado sobre o Funcionamento da União Europeia (TFUE).

b) Do Princípio da Subsidiariedade e da Proporcionalidade

No que concerne à verificação do princípio da subsidiariedade, cumpre referir que, atendendo aos objetivos visados pela presente iniciativa, nomeadamente, o reforço da solidariedade à escala da União a fim de melhorar a deteção, a preparação e a resposta a ameaças e incidentes de cibersegurança e aumentar a resiliência da UE perante estes riscos, os objetivos preconizados pela presente iniciativa, devido à sua escala e aos seus efeitos, podem ser melhor alcançados a nível da União, através de regras comuns plenamente harmonizadas em todo o mercado interno e em conformidade com o princípio da subsidiariedade, consagrado no artigo 5.º do Tratado da União Europeia. Além disso, a natureza marcadamente transfronteiriça das ameaças de cibersegurança em geral e o número crescente de riscos e incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos da presente intervenção não podem ser eficazmente alcançados pelos Estados Membros de forma isolada e exigem uma ação comum e solidariedade à escala da União.

No que concerne à observância do princípio da proporcionalidade, cumpre mencionar que a presente iniciativa não excede o necessário para alcançar os seus objetivos. Pois as ações previstas não afetam as responsabilidades dos Estados Membros em matéria de segurança nacional, segurança pública, prevenção, investigação, deteção e repressão de infrações penais.

6

Assim, entende-se que, nas suas vertentes de necessidade, adequação e equilíbrio, o princípio da proporcionalidade se encontra respeitado, tal como consagrado no nº 5 do Tratado da União Europeia.

Pelo exposto, considera-se que a presente iniciativa está em conformidade com o princípio da subsidiariedade e da proporcionalidade.

PARTE III– PARECER

Perante os 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 ao nível da União, e está em conformidade com o princípio da proporcionalidade, na medida em que não excede o necessário para alcançar os respetivos objetivos.

2. Em relação à iniciativa em análise, o processo de escrutínio está concluído.

Palácio de S. Bento, 28 de Junho de 2023

A Deputada Autora do Parecer

(Maria do Rosário Gamboa)

P/ O Presidente da Comissão

(Luís Capoulas Santos)

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

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

RELATÓRIO

COM (2023) 209 final - Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança.

I. Nota Preliminar

Ao abrigo do disposto no n.º 2 do artigo 7.º da Lei n.º 43/2006, de 25 de agosto, alterada pelas Leis n.ºs 21/2012, de 17 de maio, 18/2018, de 2 de maio, e 64/2020, de 2 de novembro, relativa ao "*acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia*", a Comissão de Assuntos Europeus solicitou à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias a emissão de relatório sobre a COM (2023) 209 final – "Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança".

Este relatório analisa a observância do princípio da subsidiariedade, nos termos previstos no Protocolo n.º 2, relativo à aplicação dos princípios da subsidiariedade e da proporcionalidade, anexo ao Tratado da União Europeia (TUE) e ao Tratado do Funcionamento da União Europeia (TFUE).

A proposta é caracterizada por uma opção legislativa que importa antecipada e resumidamente referir, porquanto resultam da complexidade e da especificidade das matérias em discussão. O Parlamento Europeu e o Conselho propõem como instrumento jurídico de harmonização o *regulamento* que, ao contrário da *diretiva,* garante que sejam impostas, de modo uniforme, as mesmas obrigações em toda a UE. Por ser diretamente aplicável, gera maior clareza e segurança jurídica, evitando transposições divergentes nos Estados-

Membros. Este instrumento de harmonização adquire particular relevo nas matérias que agora se regulam. Como se transcrevia a propósito da COM (2022) 454 final, relativa à "proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020", *"o processo de transposição, no caso de uma diretiva relativa a esse tipo de intervenção, poderá deixar uma margem discricionária excessiva a nível nacional, conduzindo potencialmente à falta de uniformidade de certos requisitos essenciais em matéria de cibersegurança, à insegurança jurídica, a uma maior fragmentação ou mesmo a situações discriminatórias transfronteiriças, tanto mais se for tido em conta o facto de os produtos abrangidos poderem ter múltiplas finalidades ou utilizações e de os fabricantes poderem produzir várias categorias desses produtos"*. Acrescente-se que, nas matérias de cibersegurança, tem sido esta a opção jurídica. A proposta é, por isso, juridicamente coerente com o atual quadro regulamentar da UE relacionado com as matérias de cibersegurança, assim como com as recentes propostas legislativas, da qual se destaca o Regulamento Inteligência Artificial (IA). Como se transcreve da proposta de texto, no ponto justificativo da escolha do instrumento jurídico, "trata-se do instrumento [...] mais adequado, dado que só um regulamento, com as suas disposições jurídicas diretamente aplicáveis, pode proporcionar o nível de uniformidade necessário para o estabelecimento e o funcionamento de um ciberescudo e de um mecanismo de ciberemergência europeus, prevendo apoio do Programa Europa Digital para a sua criação, bem como condições claras para a utilização e atribuição desse apoio."

Considerada esta nota de enquadramento preliminar, analisa-se num segundo ponto o objeto desta proposta de regulamento, o seu conteúdo e a motivação da iniciativa que, em todo o caso, não devem substituir a leitura integral da COM (2023) 209 final. No terceiro ponto é analisado o cumprimento do princípio da subsidiariedade e da proporcionalidade. No quarto e último ponto faz-se a conclusão do relatório.

II. Do Objeto, Conteúdo e Motivação da Iniciativa

A proposta de regulamento tem como objetivo central reforçar a posição competitiva dos setores da indústria e dos serviços europeus na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Como instrumento de cibersolidariedade, procura aumentar a resiliência dos cidadãos, das empresas e das

entidades que operam em setores críticos e altamente críticos contra as ameaças crescentes à cibersegurança, cujos impactos sociais e económicos se podem mostrar muito negativos.

Devemos recordar que a natureza transfronteiriça da cibersegurança, a frequência cada vez maior dos incidentes com repercussões que ultrapassam as fronteiras nacionais ou que, afetando inicialmente uma única entidade ou um único Estado-Membro, se propagam rapidamente a todo o mercado interno, tornam difícil, se não mesmo inexequível, que os requisitos de segurança e cibersegurança possam ser eficazmente alcançados pelos Estados-Membros isoladamente. Esta perspetiva de ameaça global impele os Estados-Membros a posições cada vez mais concertadas e articuladas em matérias de cibersegurança. Como se reconhece na exposição de motivos da proposta de regulamento, "a maior adoção das tecnologias digitais aumenta a exposição a incidentes de cibersegurança e os seus potenciais impactos. Ao mesmo tempo, os Estados-Membros enfrentam riscos de cibersegurança crescentes e um cenário de ameaças global complexo, com um claro risco de rápida disseminação dos ciberincidentes de um Estado-Membro para outro".

Foram, neste contexto, definidos três objetivos específicos, que transcrevemos, e que enquadram a proposta de regulamento cujo princípio da subsidiariedade se analisa:

1. *"reforçar a deteção e o conhecimento das situações comuns a nível da UE relativamente a ciberameaças e ciberincidentes, contribuindo assim para a soberania tecnológica europeia no domínio da cibersegurança;*
2. *aumentar o grau de preparação das entidades críticas em toda a UE e reforças a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente ao disponibilizar apoio à resposta a incidentes a países terceiros associados ao Programa Europa Digital;*
3. *reforçar a resiliência da União e contribuir para uma resposta eficaz mediante a análise e avaliação de incidentes significativos ou em grande escala, inclusive retirando ensinamentos e, se for caso disso, formulando recomendações".*

Estes três objetivos balizam os cinco capítulos que, resumidamente, a exposição de motivos da proposta de regulamento apresenta:

- o **Capítulo I** estabelece as disposições gerais, incluindo o objeto e o âmbito de aplicação do regulamento e as definições dos principais termos utilizados no mesmo. É neste capítulo que se estabelecem "os objetivos do regulamento para

reforçar a solidariedade a nível da União a fim de melhor detetar, preparar e responder a ameaças e incidentes de cibersegurança e, em especial, reforçar a deteção e o conhecimento da situação na União relativamente a ciberameaças e ciberincidentes, aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade mediante o desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala e aumentar a resiliência da União mediante a análise e avaliação de incidentes significativos ou em grande escala".

É ainda neste capítulo que são definidas as três grandes ações através das quais os objetivos da proposta de regulamento serão alcançados. Cada uma dessas três grandes ações é densificada nos três capítulos seguintes: a implantação de um ciberescudo europeu (capítulo II), a criação de um mecanismo de ciberemergência (capítulo III) e o estabelecimento de um mecanismo de análise de incidentes de cibersegurança (capítulo IV);

- o **Capítulo II** define e estabelece as condições de implementação do ciberescudo europeu, bem das entidades que o devem constituir e as condições de participação. Por um lado, "anuncia o objetivo geral do ciberescudo europeu, que consiste em desenvolver capacidades avançadas para a União detetar, analisar e tratar dados sobre ciberameaças e ciberincidentes na União, bem como os objetivos operacionais específicos". Por outro lado, define que as entidades que o constituem são os centros de operações de segurança nacionais («SOC nacionais») e os centros de operações de segurança transfronteiriços («SOC transfronteiriços»).

- o **Capítulo III** cria o mecanismo europeu de ciberemergência. Este mecanismo, como se transcreve, procurar "melhorar a resiliência da União a ameaças graves à cibersegurança e preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes ou crises de cibersegurança significativos e em grande escala";

- o **Capítulo IV** define o mecanismo de análise de incidentes de cibersegurança. Como se propõe, "a ENISA deve analisar e avaliar as ameaças, vulnerabilidades e

medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico";

- o **Capítulo V** contém as disposições finais do presente regulamento. Salientam-se particularmente, para efeito deste relatório, alterações ao Regulamento Programa Europa Digital, por ser um instrumento enquadrador nestas matérias e balizar muitas das opções jurídicas da Comissão, como a presente. Destaca-se também neste ponto a obrigação que recai sobre a Comissão de elaborar relatórios periódicos de avaliação e reexame do regulamento, a apresentar ao Parlamento Europeu e ao Conselho.

Por fim, pese embora a complexidade da regulamentação nesta área, importa destacar neste ponto do relatório, pela sua importância, o esforço de solidariedade que resulta desta proposta e que, na essência, lhe dá nome e corpo. Como se refere na exposição de motivos, "no que diz respeito à deteção de ciberameaças e ciberincidentes, é urgente aumentar o intercâmbio de informações e melhorar as nossas capacidades coletivas a fim de reduzir drasticamente o tempo necessário para detetar ciberameaças, antes de estas poderem causar danos e custos em grande escala. Apesar de muitas ameaças e incidentes de cibersegurança terem uma potencial dimensão transfronteiriça, devido à interligação das infraestruturas digitais, a partilha de informações pertinentes entre os Estados-Membros continua a ser limitada". Desenvolvem-se, por isso, mecanismos de solidariedade que criam instrumentos comuns e devidamente articulados com as estratégias de harmonização que vêm sendo implementadas, particularmente o já referido Regulamento Programa Europa Digital e a Estratégia de Cibersegurança da UE, adotada em dezembro de 2020.

III. Princípio da Subsidiariedade e da Proporcionalidade

Como se esclarece na exposição de motivos, "a natureza transfronteiriça da cibersegurança, o aumento dos riscos de incidentes com alcance transfronteiriço e a forte relação entre setores e produtos tornam pouco eficazes, se não mesmo ineficazes, medidas adotadas isoladamente pelos Estados-Membros. Há, por conseguinte, neste domínio, o objetivo de garantir segurança jurídica e, não menos relevante, por força da matéria, segurança dos cidadãos. Estes requisitos podem mais facilmente ser assegurados se os mecanismos de partilha de informação e articulação de respostas garantirem, independentemente da origem, natureza ou destinatários das ameaças, uma partilha solidária

de informação, formalmente regulamentada. Uma iniciativa deste tipo poderá garantir não apenas robustez na resposta, como também, em simultâneo, a complementaridade, não redundante, das capacidades nacionais em matéria de deteção, conhecimento da situação, preparação e resposta a ciberameaças e ciberincidentes.

A experiência recente dos Estados-Membros vem demonstrando "que devem ser criados mecanismos concretos de apoio mútuo, incluindo a cooperação com o setor privado, para alcançar a solidariedade à escala da EU". Por isso mesmo, as Conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço, instam a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança, da qual resulta a presente iniciativa.

Numa última nota, ainda que não se imponha nesta sede a verificação do princípio da proporcionalidade, a sua observância é garantia de maior eficácia na aplicação deste regulamento, o que, numa matéria desta natureza, adquire especial preponderância. Na presente proposta de regulamento, as ações não vão além do que é necessário para alcançar os objetivos gerais e específicos do regulamento. Por conseguinte, e como se reconhece na exposição de motivos, as ações previstas na proposta de regulamento "não afetam as responsabilidades dos Estados-Membros em matéria de segurança nacional, segurança pública, prevenção, investigação, deteção e repressão de infrações penais. Também não afetam as obrigações jurídicas das entidades que operam em setores críticos e altamente críticos de adotarem medidas de cibersegurança". A proposta de regulamento observa, por isso, o princípio da proporcionalidade.

IV. Conclusões

Pelo exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias conclui que:

a) a COM (2023) 209 final – "Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança" não viola o princípio da subsidiariedade;
b) não se impondo nesta sede a verificação do princípio da proporcionalidade, reconhece-se, todavia, a sua observância;
c) o presente relatório deve ser remetido à Comissão de Assuntos Europeus.

ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

Palácio de S. Bento, 21 de junho de 2023

O Deputado Relator,

(Bruno Aragão)

O Presidente da Comissão,

(Fernando Negrão)

7

ASSEMBLEIA DA REPÚBLICA

Comissão de Defesa Nacional

Relatório **COM (2023) 209**	**Autor:** Deputado Miguel dos Santos Rodrigues (PS)

Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança

ÍNDICE

PARTE I – CONSIDERANDOS

1. 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, e pela Lei n.º 18/2018, de 2 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 1 de março de 2016, a Comissão de Assuntos Europeus enviou à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias e à Comissão de Defesa Nacional a Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança COM (2023) 209, atento o seu objeto, para efeitos de análise e elaboração do presente relatório, tendo sido nomeado relator o Deputado autor deste relatório.

2. Enquadramento, motivação e objetivos da proposta

A iniciativa europeia em escrutínio trata uma proposta de regulamento do Parlamento Europeu e do Conselho, que visa reforçar a posição competitiva dos setores da indústria e dos serviços europeus na economia digital, bem como apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital.

A título de enquadramento, refere-se que as ciberoperações estão cada vez mais integradas em estratégias híbridas e de guerra, com efeitos significativos no alvo. Em especial, a agressão militar da Rússia contra a Ucrânia foi precedida e está a ser acompanhada de uma estratégia de ciberoperações hostis, o que constitui um fator de mudança para a perceção e a avaliação do grau de preparação da

UE em matéria de gestão coletiva de crises de cibersegurança e um apelo à adoção de medidas urgentes.

Assim, a ameaça de um eventual incidente em grande escala que cause perturbações e danos consideráveis às infraestruturas críticas exige uma maior preparação a todos os níveis do ecossistema de cibersegurança da UE. Essa ameaça vai além da agressão militar da Rússia contra a Ucrânia e inclui ciberameaças contínuas de intervenientes estatais e não estatais, que provavelmente persistirão, dada a multiplicidade de intervenientes associados ao Estado, criminosos e ativistas háquer envolvidos nas atuais tensões geopolíticas.

Nos últimos anos, o número de ciberataques aumentou drasticamente, incluindo ataques de ciberespionagem, sequestro por programas maliciosos ou perturbação da cadeia de abastecimento. É dado o exemplo do que aconteceu em 2020, com o ataque contra a cadeia de abastecimento da SolarWinds, que afetou mais de 18 000 organizações a nível mundial, incluindo organismos governamentais e grandes empresas.

Pretende-se, assim, aumentar a resiliência dos cidadãos, das empresas e entidades que operam em setores críticos e altamente críticos contra ameaças crescentes à cibersegurança, que podem ter impactos devastadores na sociedade e na economia.

Uma vez que os incidentes de cibersegurança significativos podem ser demasiado disruptivos para que um único ou vários Estados-Membros afetados os possam abordar sozinhos, entende-se que é útil e necessária uma solidariedade reforçada à escala comunitária, que permita uma melhor deteção, preparação e resposta a ameaças e incidentes de cibersegurança.

Destarte, a Comissão apresentou a proposta de Regulamento em referência no título da iniciativa, a fim de melhor detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança através dos seguintes objetivos:

a) reforçar a deteção e o conhecimento da situação comuns a nível da UE relativamente a ciberameaças e ciberincidentes, contribuindo assim para a soberania tecnológica europeia no domínio da cibersegurança;

b) aumentar o grau de preparação das entidades críticas em toda a UE e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente ao disponibilizar apoio à resposta a incidentes a países terceiros associados ao Programa Europa Digital; e reforçar a resiliência da União e contribuir para uma resposta eficaz mediante a análise e avaliação de incidentes significativos ou em grande escala.

Segundo a proposta apresentada, esses objetivos serão concretizados através de ações como a implantação de uma infraestrutura pan-europeia de Centros de Operações de Segurança (SOC, Security Operations Centres), no sentido de criar e reforçar capacidades comuns de deteção e conhecimento da situação, a criação de um mecanismo de ciberemergência para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala e a criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala específicos.

Destaca-se ainda que esta proposta terá por base e apoiará especialmente os quadros de cooperação operacional e de gestão de crises existentes em matéria de cibersegurança, em particular a Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) e a rede de equipas de resposta a incidentes de segurança informática (CSIRT).

Por fim, referir que a presente proposta visa, também, colmatar as lacunas e integrar as informações extraídas de ações como o programa de trabalho em matéria de cibersegurança do Programa Europa Digital para 2021-2022 e o programa de curto prazo para apoiar os Estados-Membros, mediante a afetação de financiamento adicional à Agência da União Europeia para a Cibersegurança

(ENISA), lançado pela Comissão Europeia, a fim de reforçar, a título imediato, a preparação e as capacidades de resposta a ciberincidentes graves.

3. Base jurídica, subsidiariedade e proporcionalidade

A base jurídica da presente proposta é constituída pelo artigo 173.º, n.º 3, e pelo artigo 322.º, n.º 1, alínea a), do Tratado sobre o Funcionamento da União Europeia (TFUE) onde prevê que a União e os Estados-Membros devem zelar por que sejam asseguradas as condições necessárias ao desenvolvimento da capacidade concorrencial da indústria da União bem como pelo facto de conter regras específicas de transição que derrogam o princípio da anualidade estabelecido no Regulamento (UE, Euratom) 2018/1046.

Referir que a iniciativa em análise aplica a Estratégia de Cibersegurança da UE, adotada em dezembro de 2020, que anunciou a criação de um ciberescudo europeu, reforçando as capacidades de deteção de ciberameaças e de partilha de informações na União Europeia através de uma federação de SOC nacionais e transfronteiriços.

Com efeito, no que diz respeito à deteção de ciberameaças e ciberincidentes, era urgente aumentar o intercâmbio de informações e melhorar as capacidades coletivas da União a fim de reduzir drasticamente o tempo necessário para detetar ciberameaças, antes de estas poderem causar danos e custos em grande escala, pois apesar de muitas ameaças e incidentes de cibersegurança terem uma potencial dimensão transfronteiriça, devido à interligação das infraestruturas digitais, a partilha de informações pertinentes entre os Estados-Membros continuava a ser limitada.

Por outro lado, no que diz respeito à preparação e resposta a incidentes de cibersegurança, existe atualmente um apoio limitado à escala da União e uma solidariedade limitada entre os Estados-Membros, tendo as conclusões do Conselho de outubro de 2021 salientado a necessidade de colmatar estas lacunas, convidando a Comissão a apresentar uma proposta relativa a um novo

Fundo de Resposta de Emergência para a Cibersegurança.

Por último, destacar que a presente proposta dá cumprimento ao compromisso, em consonância com a Comunicação Conjunta sobre Ciberdefesa para preparar uma proposta de iniciativa da UE em matéria de cibersolidariedade com os seguintes objetivos: reforçar as capacidades comuns de deteção, conhecimento da situação e resposta da UE, criar progressivamente uma reserva de cibersegurança a nível da UE com serviços de fornecedores privados de confiança e apoiar a avaliação das entidades críticas.

Em matéria de **subsidiariedade**, é de referir que a natureza marcadamente transfronteiriça das ameaças de cibersegurança e o número crescente de riscos e incidentes com repercussões além-fronteiras e entre setores alcançados pelos Estados-Membros de forma isolada e exigem uma ação comum e solidariedade à escala da União.

A experiência no combate a ciberameaças decorrente da guerra contra a Ucrânia, juntamente com os ensinamentos retirados de um exercício de cibersegurança realizado durante a Presidência francesa (EU CyCLES), demonstrou que devem ser criados mecanismos concretos de apoio mútuo, incluindo a cooperação com o setor privado, para alcançar a solidariedade à escala da UE. Perante este cenário, as Conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço convidam a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança.

O apoio e as ações a nível da União que visam uma melhor deteção das ameaças à cibersegurança e um aumento das capacidades de preparação e resposta proporcionam valor acrescentado, uma vez que evitam a duplicação de esforços em toda a União e nos Estados-Membros, conduzindo a uma melhor exploração dos ativos existentes e a uma maior coordenação e intercâmbio de informações sobre os ensinamentos retirados. O mecanismo de ciberemergência prevê igualmente a prestação de apoio a países terceiros

associados ao Programa Europa Digital a partir da Reserva de Cibersegurança da UE.

O apoio prestado através das várias iniciativas a criar e a financiar a nível da União complementará e não duplicará as capacidades nacionais em matéria de deteção, conhecimento da situação, preparação e resposta a ciberameaças e ciberincidentes.

Do ponto de vista da **proporcionalidade**, entende-se que as ações não vão além do que é necessário para alcançar os objetivos gerais e específicos do regulamento. Assim, as ações previstas no regulamento em análise não afetam as responsabilidades dos Estados-Membros em matéria de segurança nacional, segurança pública, prevenção, investigação, deteção e repressão de infrações penais.

As ações abrangidas pelo presente regulamento complementam esses esforços e medidas, apoiando a criação de infraestruturas para uma melhor deteção e análise de ameaças e prestando apoio a ações de preparação e resposta em caso de incidentes significativos ou em grande escala.

PARTE II - OPINIÃO DO DEPUTADO AUTOR DO RELATÓRIO

Sendo a emissão de opinião de caráter facultativo, o deputado autor deste Relatório exime-se de manifestar a sua opinião nesta sede.

PARTE III - CONCLUSÕES

1. Ao abrigo do disposto no n.º 2 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, e pela Lei n.º 18/2018, de 2 maio, relativa 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 que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança COM (2023) 209.

2. Após análise da proposta, conclui-se que os princípios de subsidiariedade e proporcionalidade são respeitados, uma vez que o objetivo estratégico proposto só pode ser conseguido através de uma ação europeia, não abrangendo matérias que não sejam da competência exclusiva da União Europeia, nem excedendo o necessário para cumprir os objetivos a alcançar.

3. A Comissão de Defesa Nacional dá, assim, por concluído, o escrutínio da presente iniciativa, devendo o presente Relatório ser remetido, para os devidos efeitos, à Comissão de Assuntos Europeus.

Palácio de S. Bento, 21 de junho de 2023.

O Deputado Autor do Relatório — **O Presidente da Comissão**

(Miguel dos Santos Rodrigues) — (Marcos Perestrello)