



Council of the
European Union

Brussels, 20 July 2023
(OR. en, pt)

12079/23

Interinstitutional File:
2023/0108(COD)

CYBER 193
JAI 1047
TELECOM 239
DATAPROTECT 206
MI 653
IND 411
CODEC 1423

COVER NOTE

From:	The Portuguese Parliament
date of receipt:	17 July 2023
To:	The President of the Council of the European Union
No. prev. doc.:	8511/23 - COM(2023) 208 final
Subject:	Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services [8511/23 - COM(2023)208] - Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion¹ 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: <https://secure.ipex.eu/IPEXL-WEB/document/COM-2023-208>

Parecer
COM(2023)208

Autora: Deputada
Rosário Gambôa

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que altera o Regulamento (UE) 2019/881 no respeitante aos serviços de segurança geridos.

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



ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

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 altera o Regulamento (UE) 2019/881 no respeitante aos serviços de segurança geridos [COM(2023) 208].

Atento o seu objeto, a presente iniciativa foi enviada à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias que a analisou, aprovando o respetivo Relatório que se anexa ao presente Parecer, dele fazendo parte integrante.

PARTE II – CONSIDERANDOS



ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS EUROPEUS

1. A presente iniciativa propõe uma alteração específica ao Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho (Regulamento Cibersegurança)¹ no que concerne aos “serviços de segurança geridos”, de forma a permitir futuramente a adoção de sistemas europeus de certificação para estes serviços, para além dos produtos, serviços e processos de tecnologias de Informação e comunicação (TIC), que já são abrangidos pelo referido Regulamento, e habilita ainda a Comissão a fazê-lo, por meio de atos de execução.

2. Importa evidenciar, que nos termos da definição regulamentar, se entende por «serviços de segurança geridos» os que consistem na realização ou na prestação de assistência para atividades relacionadas com a gestão dos riscos de cibersegurança. Os “serviços de segurança geridos” são, pois, serviços altamente críticos e sensíveis fornecidos por prestadores de serviços de cibersegurança em domínios como a resposta a incidentes, testes de penetração, auditorias e consultoria em matéria de segurança, destinados a ajudar as empresas e outras organizações a prevenir, detetar e reagir a incidentes de cibersegurança, bem como a recuperar dos mesmos. Porém, tem-se verificado que os próprios prestadores de “serviços de segurança geridos” têm sido igualmente alvo de ciberataques, riscos que se tornam mais amplos em virtude da sua estreita integração nas operações dos seus clientes.

¹ Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, 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). Este Regulamento (UE) 2019/881 veio estabelecer um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de tecnologias da Informação e comunicação (TIC) na União Europeia, bem como para evitar a fragmentação do mercado interno no que diz respeito aos sistemas de certificação da cibersegurança na União.



ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS EUROPEUS

Por conseguinte, a presente Iniciativa vem impor que as entidades essenciais e importantes, na aceção da Diretiva SRI 2² (UE) exerçam uma diligência acrescida ao selecionarem um prestador de serviços de segurança geridos, com vista a melhorar a qualidade dos serviços de segurança geridos e aumentar a sua comparabilidade. Acresce apenas referir que a definição de “serviços de segurança geridos” da presente iniciativa é muito semelhante à definição de “prestadores de serviços de segurança geridos” da Diretiva SRI 2. Por estas razões, se considera que a iniciativa em apreço e a referida Diretiva “possuem um alto nível de complementaridade”, tal como se verifica em relação à proposta de Regulamento Cibersolidariedade³, que estabelece um processo para seleccionar os prestadores de serviços que integrarão a reserva de cibersegurança a nível da UE⁴, que deve ter em conta, nomeadamente, se esses fornecedores obtiveram ou não uma certificação da cibersegurança europeia ou nacional.

4. Em suma, os “serviços de segurança geridos” desempenham um papel cada vez mais importante na prevenção e atenuação dos incidentes de cibersegurança, destacando-se que os prestadores de serviços de segurança geridos também desempenharão um papel importante na reserva de cibersegurança a nível da UE, cuja criação progressiva (como já referido) é apoiada pela proposta de Regulamento Cibersolidariedade. Neste contexto, pode concluir-se que a UE tem feito um esforço

² Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 [Diretiva SRI 2].

³ Proposta apresentada paralelamente à presente iniciativa - COM (2023) 209.

⁴ A reserva de cibersegurança a nível da UE deverá ser utilizada para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos e em grande escala.



ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS EUROPEUS

significativo para se tornar mais resiliente e mais reativa face às ciberameaças, desenvolvendo um panorama digital seguro tanto para os cidadãos como para as empresas, bem como para a proteção das entidades críticas e dos serviços essenciais, reforçando simultaneamente a cooperação existente. Motivos pelos quais se assume que a certificação é fundamental para garantir um elevado nível de qualidade e fiabilidade destes serviços de cibersegurança altamente críticos e sensíveis.

4. Por último, tendo em conta que o Relatório apresentado pela Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, reflete o conteúdo da iniciativa com rigor, considera-se que deve, por isso, ser dado por integralmente reproduzido, evitando-se, desta forma, uma repetição de análise e consequente redundância.

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

a) Da Base Jurídica

A presente iniciativa é sustentada, juridicamente, pelo artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que confere competência para adotar medidas adequadas com vista à aproximação das disposições legislativas dos Estados Membros, que tenham por objeto o estabelecimento e o funcionamento do mercado interno. Com efeito, verifica-se que alguns Estados Membros já começaram a adotar sistemas de certificação dos serviços de segurança geridos, pelo que existe um risco concreto de fragmentação do mercado interno destes serviços, risco esse que a presente proposta visa corrigir

b) Do Princípio da Subsidiariedade e da Proporcionalidade



ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS EUROPEUS

No que concerne à verificação do princípio da subsidiariedade, cumpre referir que, atendendo aos objetivos visados pela presente iniciativa de permitir adoção de sistemas europeus de certificação da cibersegurança de “serviços de segurança geridos” e de evitar a fragmentação do mercado, não podem ser suficientemente alcançados pelos Estados Membros, devendo, por conseguinte, ser alcançados a nível da União, em conformidade com o princípio da subsidiariedade previsto no artigo 5.º do Tratado da União Europeia.

No que concerne à observância do princípio da proporcionalidade, cumpre mencionar a presente iniciativa consiste numa alteração específica do Regulamento Cibersegurança, limitando-se ao estritamente necessário para alcançar o seu objetivo.

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.



ASSEMBLEIA DA REPÚBLICA
COMISSÃO DE ASSUNTOS EUROPEUS

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

Palácio de S. Bento, 12 de julho de 2023

A Deputada Autora do Parecer

(Maria do Rosário Gambôa)

O Presidente da Comissão

(Luís Capoulas Santos)

PARTE IV—ANEXO

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



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

RELATÓRIO

COM (2023) 208 final - Proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (UE) 2019/881 no respeitante aos serviços de segurança geridos.

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) 208 final – "Proposta de Regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (UE) 2019/881 no respeitante aos serviços de segurança geridos".

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



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

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 sua base jurídica, o regulamento uniformiza respostas que evitam "a fragmentação do mercado interno, nomeadamente permitindo a adoção de sistemas europeus de certificação da cibersegurança de serviços de segurança geridos. Alguns Estados-Membros começaram a adotar sistemas de certificação dos serviços de segurança geridos, pelo que existe um risco concreto de fragmentação do mercado interno destes serviços, risco esse que a presente proposta visa corrigir. Por conseguinte, o artigo 114.º do TFUE constitui a base jurídica adequada para esta iniciativa."

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) 208 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 específico permitir a "adoção, por meio de atos de execução da Comissão, de sistemas europeus de certificação da cibersegurança dos «serviços de segurança geridos», para além dos produtos, serviços e processos de tecnologias da informação e comunicação (TIC), que já são abrangidos pelo Regulamento Cibersegurança". Importa previamente esclarecer, para melhor enquadramento deste relatório e da sua análise, que, para este efeito, como resulta da própria definição regulamentar, se entendem por «serviços de segurança geridos» os que consistem na realização ou na



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

prestação de assistência para atividades relacionadas com a gestão dos riscos de cibersegurança. Pela relevância cada vez maior que assumem na prevenção e atenuação dos incidentes de cibersegurança, merecem um enquadramento mais formal que, no quadro de matérias transfronteiriças, como é o caso, se possam harmonizar.

Esta necessidade de harmonização, que agora se aplica aos serviços de segurança geridos, resulta da proposta de Regulamento Cibersolidariedade (COM (2023) 209 final). Com efeito, esta proposta de Regulamento Cibersolidariedade estabelece um processo para selecionar os prestadores de serviços que integrarão a reserva de cibersegurança a nível da UE, "que deve ter em conta, nomeadamente, se esses fornecedores obtiveram ou não uma certificação da cibersegurança europeia ou nacional, prevendo que os futuros sistemas de certificação dos serviços de segurança geridos desempenharão, assim, um papel significativo na aplicação do Regulamento Cibersolidariedade".

No seu conjunto, estas propostas, cuja avaliação de princípios é concomitante, procura responder às Conclusões do Conselho de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço. Entre outras, essas conclusões exortam a União e os seus Estados-Membros "a redobram de esforços para aumentar o nível global de cibersegurança, por exemplo facilitando a emergência de prestadores fiáveis de serviços de cibersegurança, e frisou que o incentivo ao desenvolvimento desses prestadores deverá constituir uma prioridade da política industrial da União no domínio da cibersegurança". Ao mesmo tempo, desafiam a Comissão a "propor opções para incentivar a emergência de um setor de serviços fiáveis de cibersegurança". Neste sentido, a certificação dos serviços de segurança geridos revela-se um meio eficaz para reforçar a confiança na qualidade desses serviços, facilitando assim a emergência de um setor europeu de serviços fiáveis de cibersegurança.

Por último, importa salientar que a presente iniciativa complementa a proposta de Regulamento Cibersolidariedade, na medida em que este último estabelece um processo para selecionar os prestadores de serviços que integrarão a reserva de cibersegurança a nível da UE, que deve ter em conta, nomeadamente, se esses fornecedores obtiveram ou não uma certificação da cibersegurança europeia ou nacional, prevendo que os futuros sistemas de certificação dos serviços de segurança geridos desempenharão, assim, um papel significativo na aplicação do Regulamento Cibersolidariedade.



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

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, tomam 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. A crescente preponderância das tecnologias digitais tem aumentado a exposição a incidentes de cibersegurança e os seus potenciais impactos. Efetivamente, os Estados-Membros enfrentam riscos de cibersegurança maiores e um cenário de ameaças global cada vez mais complexo, com forte probabilidade de disseminação dos ciberincidentes de um Estado-Membro para outro. Se é um facto que alguns Estados-Membros adotaram já sistemas de certificação dos serviços de segurança geridos, outros há que ainda não o fizeram ou estão ainda numa fase muito incipiente. Em todo o caso, há um risco cada vez maior de as incoerências entre os diferentes sistemas existentes na União conduzirem à fragmentação do mercado interno desses serviços. Assim, a presente proposta procurar a criação de sistemas europeus de certificação da cibersegurança de serviços de segurança geridos, a fim de evitar essa mesma fragmentação.

Por fim, pese embora a complexidade da regulamentação nesta área, importa destacar neste ponto do relatório, pela sua importância na apreciação da presente iniciativa, o esforço de solidariedade que resulta da COM (2023) 209 final, 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. Como se refere na exposição de motivos dessa proposta, "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



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

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

A natureza transfronteiriça da cibersegurança e o aumento dos riscos de incidentes com alcance transfronteiriço tornam pouco eficazes 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.

Como se transcreve da exposição de motivos, "o objetivo de permitir a adoção de sistemas europeus de certificação da cibersegurança de serviços de segurança geridos e de evitar a fragmentação do mercado interno não pode ser alcançado a nível nacional, mas unicamente a nível da União. Além disso, os serviços de segurança geridos, que são o objeto da alteração proposta, são oferecidos por prestadores que, tal como os seus maiores clientes potenciais, estão ativos em toda a União. A ação a nível da União é, por conseguinte, necessária e mais eficaz do que uma ação a nível nacional".

A experiência recente dos Estados-Membros, vem demonstrando que devem ser criados mecanismos concretos de apoio mútuo. 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, ações não vão além do que é necessário para alcançar os



COMISSÃO DE ASSUNTOS CONSTITUCIONAIS, DIREITOS, LIBERDADES E GARANTIAS

objetivos gerais e específicos do regulamento. Por conseguinte, e como se reconhece na exposição de motivos, a proposta de regulamento cinge-se "ao estritamente necessário para alcançar o seu objetivo, designadamente permitir a adoção de sistemas europeus de certificação da cibersegurança dos serviços de segurança geridos, para além dos produtos, serviços e processos de TIC". 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) 208 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.

Palácio de S. Bento, 21 de junho de 2023

O Deputado Relator,

(Bruno Aragão)

O Presidente da Comissão,

(Fernando Negrão)