Parecer do Comité Económico e Social Europeu — 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

[COM(2022) 454 final — 2022/0272 (COD)]

(2023/C 100/15)

Relator: **Maurizio MENSI**

Correlator: **Marinel Dănuț MUREȘAN**

Consulta	Parlamento Europeu, 9.11.2022
	Conselho da União Europeia, 28.10.2022
Base jurídica	Artigo 114.º do Tratado sobre o Funcionamento da União Europeia
Competência	Secção do Mercado Único, Produção e Consumo
Adoção em secção	10.11.2022
Adoção em plenária	14.12.2022
Reunião plenária n.º	574
Resultado da votação	
(votos a favor/votos contra/abstenções)	177/0/0

1. **Conclusões e recomendações**

1.1. O CESE congratula-se com a proposta da Comissão de um ato legislativo sobre a ciber-resiliência (*Cyber Resilience Act*), que visa estabelecer normas mais rigorosas em matéria de cibersegurança, de molde a criar um sistema fiável para os operadores económicos e a garantir aos cidadãos da UE uma utilização segura dos produtos disponíveis no mercado. A iniciativa em apreço enquadra-se na Estratégia Europeia para os Dados, que reforça a segurança dos dados, incluindo os dados pessoais, e os direitos fundamentais, elementos essenciais da nossa sociedade digital.

1.2. O CESE considera essencial reforçar a resposta coletiva aos ciberataques e consolidar o processo de harmonização da cibersegurança a nível nacional no respeitante às regras e instrumentos operacionais, a fim de evitar a criação de insegurança e entraves jurídicos devido a abordagens nacionais distintas.

1.3. O CESE acolhe favoravelmente a iniciativa da Comissão, que não só contribuirá para reduzir os custos significativos incorridos pelas empresas devido aos ciberataques, como também permitirá que os cidadãos/consumidores beneficiem de uma proteção mais eficaz dos seus direitos fundamentais, como a privacidade. Em especial, a Comissão mostra que tem em conta as necessidades específicas das PME no que se refere aos serviços prestados pelas autoridades de certificação. No entanto, o CESE assinala a necessidade de esclarecer os critérios de aplicação.

1.4. O CESE considera importante salientar que, embora seja louvável que o ato legislativo sobre a ciber-resiliência abranja praticamente todos os produtos digitais, a sua aplicação prática pode levantar dificuldades, tendo em conta as atividades importantes e complexas de supervisão e acompanhamento que implica. Por conseguinte, impõe-se reforçar os instrumentos de controlo e verificação.

1.5. O CESE chama a atenção para a necessidade de clarificar de forma precisa o âmbito de aplicação material do ato legislativo sobre a ciber-resiliência, nomeadamente no que diz respeito aos produtos com elementos digitais e ao *software*.

1.6. O CESE observa que os fabricantes serão obrigados a comunicar à Agência da União Europeia para a Cibersegurança (ENISA), por um lado, as vulnerabilidades dos produtos e, por outro, eventuais incidentes de segurança. Neste sentido, importa dotar a ENISA dos recursos necessários para desempenhar atempada e eficazmente as funções importantes e sensíveis que lhe serão confiadas.

1.7. A fim de evitar qualquer dúvida de interpretação, o CESE propõe que a Comissão elabore diretrizes para orientar os produtores e os consumidores sobre as regras e procedimentos específicos aplicáveis, uma vez que, aparentemente, alguns produtos abrangidos pelo âmbito de aplicação da proposta também estão sujeitos a outras disposições regulamentares em matéria de cibersegurança. A este respeito, será igualmente importante que, em particular, as PME e as MPME tenham acesso a apoio especializado qualificado, suscetível de prestar serviços profissionais específicos.

1.8. O CESE observa que a relação entre as autoridades de certificação nos termos do ato legislativo sobre a ciber-resiliência e os demais organismos autorizados a certificar a cibersegurança nos termos de outra legislação não se afigura inteiramente clara. O mesmo problema de coordenação operacional pode surgir entre as autoridades de fiscalização previstas na proposta em apreço e as autoridades já ativas ao abrigo de outras normas aplicáveis aos mesmos produtos.

1.9. O CESE observa que, tendo em conta o número considerável de atividades e responsabilidades que a proposta prevê para as autoridades de certificação, importa acautelar o seu funcionamento prático, evitando também que o ato legislativo sobre a ciber-resiliência conduza a um aumento da burocracia e penalize os fabricantes, que terão de cumprir uma série de requisitos de certificação adicionais para poderem continuar a operar no mercado.

2. **Exame da proposta**

2.1. Com a proposta de um ato legislativo sobre a ciber-resiliência (*Cyber Resilience Act*), a Comissão tenciona racionalizar e redefinir de forma global e horizontal a legislação atual em matéria de cibersegurança e, ao mesmo tempo, atualizá-la à luz das inovações tecnológicas.

2.2. O ato legislativo sobre a ciber-resiliência tem quatro objetivos essenciais: assegurar que os fabricantes melhoram a segurança dos produtos com elementos digitais tanto na fase de conceção e desenvolvimento como durante todo o ciclo de vida; assegurar um quadro normativo coerente em matéria de cibersegurança que facilite a conformidade dos fabricantes de *hardware* e *software*; melhorar a transparência das características de segurança dos produtos com elementos digitais; permitir às empresas e aos consumidores utilizar tais produtos de forma segura. Concretamente, a proposta introduz uma marcação CE em matéria de cibersegurança, exigindo que essa marcação seja aposta em todos os produtos abrangidos pelo ato legislativo sobre a ciber-resiliência.

2.3. Trata-se de uma intervenção horizontal através da qual a Comissão tenciona regular todo este domínio de forma global, uma vez que são incluídos praticamente todos os produtos com elementos digitais. Apenas estão excluídos da proposta os produtos médicos e relativos à aviação civil, os veículos e os produtos militares. A proposta também não abrange os serviços do tipo SaaS — *software* como serviço (nuvem) —, a menos que sejam utilizados no fabrico de produtos com elementos digitais.

2.4. A definição de «produtos com elementos digitais» é muito ampla e abrange qualquer produto de *software* ou *hardware*, incluindo *software* ou *hardware* não incorporados no produto, mas a colocar no mercado separadamente.

2.5. O ato legislativo introduz requisitos obrigatórios em matéria de cibersegurança para os produtos com elementos digitais ao longo de todo o seu ciclo de vida, mas não substitui os requisitos já em vigor. Pelo contrário, os certificados dos produtos que já tenham sido certificados como estando em conformidade com as normas da UE preexistentes serão igualmente considerados «válidos» ao abrigo do novo regulamento.

2.6. O princípio básico geral é de que na Europa apenas são comercializados produtos «seguros» e de que os fabricantes garantem a segurança dos produtos ao longo de todo o seu ciclo de vida.

2.7. Um produto é considerado «seguro» se for concebido e fabricado de tal forma que tenha um nível de cibersegurança adequado aos riscos que a sua utilização comporta, não possua vulnerabilidades conhecidas no momento da venda, tenha uma configuração segura por defeito, esteja protegido contra ligações ilegais, proteja os dados recolhidos e recolha apenas aqueles que são necessários ao seu funcionamento.

2.8. Considera-se que um fabricante está apto a comercializar os seus produtos se divulgar a lista dos componentes de *software* dos seus produtos, fornecer rapidamente soluções gratuitas no caso de novas vulnerabilidades, divulgar e especificar detalhadamente as vulnerabilidades que detetou e resolveu e, por fim, verificar regularmente a «robustez» dos produtos que comercializa. Estas atividades, bem como outras impostas pelo ato legislativo sobre a ciber-resiliência, devem ser realizadas ao longo de toda a vida de um produto ou, pelo menos, durante cinco anos após a sua colocação no mercado. O fabricante é igualmente obrigado a assegurar a eliminação das vulnerabilidades através de atualizações regulares do *software*.

2.9. De acordo com um princípio geral aplicado em vários setores, são impostas as mesmas obrigações aos importadores e distribuidores.

2.10. O ato legislativo sobre a ciber-resiliência prevê uma macrocategoria de produtos e *software* «por defeito», para a qual é suficiente uma autoavaliação do fabricante, como já acontece com outros tipos de certificação através da marcação CE. Segundo a Comissão, 90 % dos produtos no mercado pertencem a esta categoria.

2.11. Os produtos em questão podem ser colocados no mercado na sequência de uma autoavaliação da sua cibersegurança pelo fabricante que apresente a documentação válida estabelecida pelas orientações regulamentares. Em caso de modificação do produto, a avaliação deve ser repetida pelo mesmo fabricante.

2.12. Os restantes 10 % dos produtos repartem-se por duas categorias adicionais (a classe I, para os produtos menos perigosos, e a classe II, para os produtos mais perigosos), cuja colocação no mercado exige maiores cuidados. Trata-se dos chamados «produtos críticos com elementos digitais», cuja falha pode originar outras violações da segurança perigosas e de maior amplitude.

2.13. Para os produtos destas duas classes, as autodeclarações simples só são permitidas se o fabricante puder demonstrar o cumprimento das normas do mercado e das especificações de segurança ou das certificações de cibersegurança previstas pela UE. Se tal não for o caso, o produto pode ser certificado junto de um organismo de certificação acreditado, cuja homologação é obrigatória para os produtos da classe II.

2.14. O sistema de classificação dos produtos em categorias de risco também consta da proposta de regulamento relativo à inteligência artificial (IA). Para que não subsistam dúvidas sobre as disposições aplicáveis, o ato legislativo sobre a ciber-resiliência abrange os produtos com elementos digitais que sejam simultaneamente classificados como «sistemas de IA de risco elevado» na proposta de regulamento relativo à inteligência artificial. Esses produtos cumprem, de modo geral, o procedimento de avaliação de conformidade estabelecido no Regulamento Inteligência Artificial, exceto no caso dos «produtos digitais críticos», aos quais se aplicam as regras de avaliação de conformidade do ato legislativo sobre a ciber-resiliência, bem como os seus requisitos essenciais.

2.15. A fim de assegurar a conformidade com o ato legislativo sobre a ciber-resiliência, cada Estado-Membro designa uma autoridade nacional responsável pela fiscalização do mercado. Em consonância com a legislação respeitante à segurança de outros produtos, se uma dada autoridade nacional verificar que as características de cibersegurança de um produto deixaram de ser válidas, a sua comercialização pode ser suspensa no Estado em questão. A Agência da União Europeia para a Cibersegurança (ENISA) tem competência para efetuar uma avaliação aprofundada de um produto notificado, podendo, caso constate a ausência de segurança do mesmo, determinar a suspensão da sua comercialização na UE.

2.16. O ato legislativo sobre a ciber-resiliência prevê uma série de sanções, consoante a gravidade da infração, que, em caso de violação dos requisitos essenciais em matéria de cibersegurança dos produtos, podem ascender a 15 milhões de euros ou a 2,5 % do volume de negócios do exercício fiscal anterior.

3. **Observações**

3.1. O CESE congratula-se com a iniciativa da Comissão de incluir mais um elemento essencial no quadro legislativo mais vasto em matéria de cibersegurança, que vem coordenar e complementar a Diretiva SRI ([1]) e o Regulamento Cibersegurança ([2]). Com efeito, a adoção de normas estritas em matéria de cibersegurança é fundamental para a criação na UE de um sistema de cibersegurança robusto para todos os operadores económicos, suscetível de garantir que os cidadãos da UE podem utilizar com segurança todos os produtos disponíveis no mercado e de reforçar a sua confiança no mundo digital.

3.2. O ato legislativo aborda duas questões principais: o baixo nível de cibersegurança de muitos produtos e, acima de tudo, o facto de muitos fabricantes não fornecerem atualizações para fazer face a vulnerabilidades. Embora a reputação dos fabricantes de produtos com elementos digitais sofra, por vezes, quando os seus produtos não são seguros, o custo das vulnerabilidades recai principalmente sobre os utilizadores profissionais e os consumidores. Este aspeto reduz os incentivos dos fabricantes para investirem na conceção e no desenvolvimento de produtos seguros e para fornecerem atualizações de segurança. Além disso, as empresas e os consumidores carecem frequentemente de informações suficientes e exatas para a

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

([2]) 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) (JO L 151 de 7.6.2019, p. 15).

escolha de produtos seguros e, muitas vezes, não sabem como garantir que os produtos que adquirem estão configurados de forma segura. As novas normas abordam estes dois aspetos: a questão das atualizações de segurança e do fornecimento de informações atualizadas aos clientes. Neste sentido, o CESE considera que a proposta de regulamento, se devidamente aplicada, pode tornar-se uma referência e um exemplo a nível internacional em matéria de cibersegurança.

3.3. O CESE congratula-se com a proposta de introduzir requisitos de cibersegurança para os produtos com elementos digitais. No entanto, importa evitar sobreposições com outras disposições regulamentares em vigor nesta matéria, como a nova Diretiva SRI 2 ([3]) e o Regulamento Inteligência Artificial.

3.4. O CESE considera importante salientar que, embora seja louvável que o ato legislativo sobre a ciber-resiliência abranja praticamente todos os produtos digitais, a sua aplicação prática pode levantar dificuldades, tendo em conta as atividades consideráveis de supervisão e acompanhamento que implica.

3.5. O âmbito de aplicação material do ato legislativo sobre a ciber-resiliência é vasto, abrangendo todos os produtos com elementos digitais. A definição proposta inclui todos os produtos de *software* e *hardware*, bem como as operações de tratamento de dados conexas. O CESE propõe que a Comissão esclareça se o âmbito de aplicação da proposta de regulamento abrange todos os tipos de *software*.

3.6. Os fabricantes serão obrigados a comunicar, por um lado, as vulnerabilidades ativamente exploradas e, por outro, os incidentes de segurança. Deverão notificar a ENISA de quaisquer vulnerabilidades ativamente exploradas contidas no produto e (separadamente) qualquer incidente que afete a segurança do produto, em ambos os casos, no prazo de 24 horas após tomarem conhecimento dos mesmos. A este respeito, o CESE salienta a necessidade de dotar a ENISA dos recursos adequados, em termos tanto numéricos como de experiência profissional, para que possa desempenhar eficazmente as funções importantes e sensíveis que lhe serão confiadas pelo regulamento.

3.7. O facto de vários dos produtos abrangidos pelo âmbito de aplicação da proposta estarem igualmente sujeitos a outras disposições legislativas em matéria de cibersegurança pode gerar incerteza quanto à legislação aplicável. Embora o ato legislativo sobre a ciber-resiliência acautele a coerência com o atual quadro regulamentar da UE relativo aos produtos e com outras propostas atualmente em curso no contexto da Estratégia Digital da UE, normas como as aplicáveis aos produtos de IA de elevado risco, por exemplo, sobrepõem-se às do Regulamento Geral sobre a Proteção de Dados. A este respeito, o CESE propõe que a Comissão elabore diretrizes específicas para orientar os fabricantes e os consumidores sobre a sua aplicação correta.

3.8. O CESE observa que a relação entre as autoridades de certificação nos termos do ato legislativo sobre a ciber-resiliência e os demais organismos autorizados a certificar a cibersegurança ao abrigo de outra regulamentação igualmente aplicável não se afigura inteiramente clara.

3.9. Além disso, dada a carga de trabalho e as responsabilidades consideráveis dessas mesmas autoridades de certificação, assim como a necessidade de verificar e assegurar o seu funcionamento prático, importa evitar que o ato legislativo sobre a ciber-resiliência aumente a burocracia já prevista a que os fabricantes devem fazer face para operarem no mercado. A este respeito, será igualmente importante que, em particular, as PME e as MPME tenham acesso a apoio especializado qualificado, suscetível de prestar serviços profissionais específicos.

3.10. O ato legislativo sobre a ciber-resiliência prevê que as autoridades de certificação tenham em conta as necessidades específicas das PME ao prestarem os seus serviços. No entanto, o CESE assinala a necessidade de esclarecer os critérios de aplicação.

3.11. Além disso, pode surgir um problema de coordenação entre as autoridades de fiscalização previstas no regulamento em apreço e as autoridades já ativas ao abrigo de outras normas aplicáveis aos mesmos produtos. Por conseguinte, o CESE propõe que a Comissão convide os Estados-Membros a acompanharem e, se necessário, a adotarem medidas para corrigir essa situação.

Bruxelas, 14 de dezembro de 2022.

A Presidente
do Comité Económico e Social Europeu
Christa SCHWENG

([3]) 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) (JO L 333 de 27.12.2022, p. 80).