Parecer do Comité Económico e Social Europeu Proposta sobre a «Proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 e a Proposta de diretiva do Parlamento Europeu e do Conselho relativa à resiliência das entidades críticas»

[COM(2020) 823 final — 2020/0359(COD) e COM(2020) 829 final — 2020/0365(COD)]

(2021/C 286/28)

Relator: **Maurizio MENSI**

Consulta	Parlamento Europeu, 21.1.2021-11.2.2021
	Conselho, 26.1.2021-19.2.2021
Base jurídica	Artigo 114.º do Tratado sobre o Funcionamento da União Europeia
Competência	Secção dos Transportes, Energia, Infraestruturas e Sociedade da Informação
Adoção em secção	14.4.2021
Adoção em plenária	27.4.2021
Reunião plenária n.º	560
Resultado da votação	
(votos a favor/votos contra/abstenções)	243/0/5

1. **Conclusões e recomendações**

1.1. O CESE congratula-se com os esforços envidados pela Comissão para tornar as entidades públicas e privadas mais resilientes às ameaças dos incidentes, dos ciberataques e dos ataques físicos e concorda com a necessidade de reforçar a indústria e a capacidade de inovação da UE de forma abrangente, mediante uma estratégia assente em quatro pilares, a saber, a proteção dos dados, os direitos fundamentais, a segurança e a cibersegurança.

1.2. No entanto, dada a importância e a sensibilidade dos objetivos perseguidos por ambas as propostas, o CESE assinala que teria sido preferível optar pelo instrumento do regulamento em vez da diretiva. Além disso, não é claro por que razão a Comissão nem sequer equacionou essa hipótese nas várias opções consideradas.

1.3. O CESE observa que algumas disposições das duas propostas de diretiva se sobrepõem, uma vez que ambas estão estreitamente ligadas e são complementares — uma aborda principalmente a cibersegurança e a outra a segurança física. Solicita, por conseguinte, que se pondere fundir as duas propostas num texto único, no interesse da simplificação e da concentração funcional.

1.4. O CESE concorda com a abordagem proposta de acabar com a distinção entre operadores de serviços essenciais e prestadores de serviços digitais inicialmente estabelecida na Diretiva Segurança das Redes e da Informação (Diretiva SRI), mas salienta que, no que diz respeito ao seu âmbito de aplicação, cabe indicar de forma mais precisa e clara as entidades que estão obrigadas a cumprir a diretiva. Em especial, cumpre clarificar a distinção entre entidades «essenciais» e «importantes», bem como os requisitos que cada uma delas deve preencher, a fim de evitar abordagens divergentes a nível nacional que criem obstáculos à concorrência e à livre circulação de bens e serviços, o que pode prejudicar as empresas e pôr em causa as trocas comerciais.

1.5. Dada a complexidade objetiva do sistema delineado nas duas propostas, o CESE reputa importante que a Comissão clarifique com precisão o âmbito de aplicação dos dois atos legislativos, especialmente quando há disposições diferentes que regem a mesma situação ou a mesma entidade.

1.6. O CESE observa que a clareza legislativa é um objetivo primordial, a par da redução da burocracia e da fragmentação através da simplificação dos procedimentos, dos requisitos de segurança e das obrigações em matéria de notificação de incidentes. Para o efeito, poderia ser oportuno e benéfico para os cidadãos e as empresas fundir as duas propostas de diretiva num texto único, evitando um exercício de interpretação e de aplicação, por vezes, complexo.

1.7. O CESE reconhece o papel essencial, salientado na proposta de diretiva, dos órgãos de direção das entidades «essenciais» e «importantes», cujos membros têm de frequentar regularmente ações de formação específicas, a fim de adquirirem os conhecimentos e as competências necessárias para compreender, gerir e avaliar o impacto dos vários riscos cibernéticos. A este respeito, considera que a proposta deve indicar requisitos mínimos em matéria de conhecimentos e competências, a fim de fornecer orientações a nível europeu sobre as competências de formação consideradas adequadas e evitar que o conteúdo das várias ações de formação difira de um país para outro.

1.8. O CESE concorda que a Agência da União Europeia para a Cibersegurança (ENISA) desempenha um papel importante em todo o quadro institucional e operacional da cibersegurança europeia. A este respeito, considera que, para além do relatório bienal sobre o estado da cibersegurança na União, esta agência deve publicar regularmente em linha informações atualizadas sobre os incidentes de cibersegurança, bem como alertas setoriais, a fim de proporcionar mais um instrumento de informação útil que permita às entidades abrangidas pela Diretiva SRI 2 proteger melhor as suas empresas.

1.9. O CESE concorda com a proposta de incumbir a ENISA da criação de um registo europeu de vulnerabilidades e entende que a comunicação de vulnerabilidades e incidentes mais graves deve ser obrigatória e não voluntária, a fim de também se converter num instrumento útil para as entidades adjudicantes no âmbito dos procedimentos de adjudicação de contratos a nível europeu, inclusivamente de produtos e tecnologias 5G.

2. **Observações gerais**

2.1. Em 16 de dezembro de 2020, a nova Estratégia de Cibersegurança da UE foi apresentada juntamente com duas propostas legislativas: a revisão da Diretiva (UE) 2016/1148 ([1]) relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI 2) e uma nova Diretiva relativa à resiliência das entidades críticas. A estratégia, que é um elemento fundamental da Comunicação «Construir o futuro digital da Europa» ([2]), do Plano de Recuperação da Europa e da Estratégia para a União da Segurança, visa reforçar a resiliência coletiva da Europa contra as ciberameaças e garantir que todos os cidadãos e todas as empresas possam beneficiar de serviços e ferramentas digitais fiáveis e seguros.

2.2. Cumpre atualizar as medidas em vigor a nível da UE para proteger os serviços e as infraestruturas críticos contra os riscos cibernéticos e físicos. Os riscos ligados à cibersegurança continuam a evoluir à medida que avança a digitalização e a interconexão. Daí a necessidade de rever o quadro regulamentar em vigor, seguindo a lógica da estratégia da UE para a segurança e superando a dicotomia entre em linha e fora de linha e a abordagem assente em compartimentações rígidas.

2.3. As duas propostas de diretiva abrangem uma vasta gama de domínios e abordam os riscos atuais e futuros, em linha e fora de linha, que decorrem dos ciberataques e ataques criminosos, das catástrofes naturais e de outros incidentes, nomeadamente tirando partido dos ensinamentos da pandemia em curso, que veio pôr em evidência a forma como economias e sociedades cada vez mais dependentes de soluções digitais se encontram vulneráveis e expostas a ciberameaças cada vez mais recorrentes e em rápida evolução, em especial no que toca aos grupos em risco de exclusão social, como as pessoas com deficiência. Esta situação levou a UE a propor medidas para salvaguardar um ciberespaço global e aberto, mas assente em garantias sólidas de segurança, soberania tecnológica e liderança, desenvolvendo capacidades operacionais para prevenir, dissuadir e responder através da cooperação acrescida a eventuais ameaças, no respeito das prerrogativas de segurança nacional dos Estados-Membros.

3. **Proposta de revisão da Diretiva relativa à segurança das redes e da informação**

3.1. A Diretiva (UE) 2016/1148 (Diretiva SRI) foi o primeiro instrumento regulamentar «horizontal» da UE em matéria de cibersegurança e tinha como objetivo reforçar a resiliência das redes e da informação na União contra os riscos cibernéticos. No entanto, apesar dos bons resultados alcançados, a Diretiva SRI evidenciou algumas limitações num momento em que a transformação digital da sociedade, acelerada pela crise da COVID-19, amplificou as ameaças, aumentando a vulnerabilidade das nossas sociedades, que se encontram cada vez mais interdependentes face a riscos graves

([1]) JO L 194 de 19.7.2016, p. 1.
([2]) COM(2020) 67 final.

e imprevistos. Surgiram novos desafios que exigem respostas adequadas e inovadoras. Os resultados da ampla consulta às partes interessadas salientaram um nível de cibersegurança deficiente nas empresas europeias, uma aplicação incoerente das regras pelos Estados nos diferentes setores e uma escassa compreensão das principais ameaças e desafios.

3.2. A proposta de Diretiva SRI 2 está intrinsecamente ligada a duas outras iniciativas, a saber, a proposta de regulamento relativo ao setor financeiro digital (ato relativo à resiliência operacional digital — DORA, na sigla em inglês) e a proposta de diretiva relativa à resiliência das entidades críticas, que alarga o âmbito de aplicação da Diretiva 2008/114/CE ([3]), relativa à energia e aos transportes, a novos setores, centrando-se, por exemplo, no setor da saúde e nas entidades envolvidas na investigação e no desenvolvimento de medicamentos. A proposta de diretiva relativa à resiliência das entidades críticas, cujo âmbito de aplicação setorial é idêntico ao da Diretiva SRI 2 para as entidades essenciais (anexo 1 da Diretiva SRI 2), transfere a sua ênfase da proteção dos ativos físicos para a resiliência das entidades que os gerem e abandona a identificação de infraestruturas críticas europeias com uma dimensão transfronteiras a favor da identificação de infraestruturas críticas a nível nacional. A Diretiva SRI 2 é também coerente com outros instrumentos jurídicos vigentes, complementando-os, como é o caso do Código Europeu das Comunicações Eletrónicas, o Regulamento Geral sobre a Proteção de Dados e o Regulamento eIDAS relativo à identificação eletrónica e aos serviços de confiança.

3.3. Em conformidade com o programa para a adequação e a eficácia da regulamentação (REFIT), a proposta de Diretiva SRI 2 visa reduzir os encargos regulamentares que recaem sobre as autoridades competentes e os custos de conformidade suportados por entidades públicas e privadas e moderniza o quadro jurídico vigente. Reforça igualmente os requisitos de segurança impostos às empresas, aborda a segurança das cadeias de abastecimento, simplifica as obrigações de notificação, introduz medidas de supervisão mais rigorosas para as autoridades nacionais e procura harmonizar os regimes de sanções nos Estados-Membros.

3.4. A Diretiva SRI 2 contribui igualmente para uma maior partilha de informações e para o reforço da cooperação em matéria de gestão de cibercrises a nível nacional e europeu. A distinção entre operadores de serviços essenciais e prestadores de serviços digitais prevista na Diretiva SRI deixa de existir. O seu âmbito de aplicação inclui as empresas de média e grande dimensão em setores identificados com base na sua importância económica e societal. Estas entidades, públicas ou privadas, dividem-se em entidades «essenciais» e «importantes», estando sujeitas a regimes de supervisão distintos. No entanto, é deixada aos Estados-Membros a possibilidade de abranger também entidades de menor dimensão com perfis de risco elevado.

3.5. Prevê-se a criação de uma nova rede de centros de operações de segurança à escala da UE, assentes na inteligência artificial (IA), que constituirão um verdadeiro «escudo de cibersegurança» capaz de detetar sinais de ciberataques com a antecedência suficiente para poder intervir antes de ocorrerem danos. A importância da IA para a cibersegurança é também salientada no relatório sobre inteligência artificial da Comissão de Segurança Nacional para a Inteligência Artificial (NSCAI) dos EUA, apresentado em 1 de março de 2021. Consequentemente, os Estados-Membros e os operadores de infraestruturas críticas terão acesso direto a informações sobre as ameaças («Threat Intelligence») no âmbito de uma rede europeia de segurança.

3.6. A Comissão aborda igualmente a questão da segurança das cadeias de abastecimento e das relações com os fornecedores: os Estados-Membros, em cooperação com a Comissão e a ENISA, podem levar a cabo avaliações coordenadas dos riscos das cadeias de abastecimento críticas, seguindo a abordagem bem-sucedida utilizada para as redes 5G prevista na Recomendação da Comissão, de 26 de março de 2019, «Cibersegurança das redes 5G» ([4]).

3.7. A proposta reforça e racionaliza as obrigações em matéria de segurança e de comunicação de informações a respeitar pelas empresas, impondo uma abordagem comum da gestão dos riscos e estabelecendo uma lista mínima dos elementos essenciais de segurança a aplicar. Preveem-se disposições mais precisas sobre o processo de notificação de incidentes, o conteúdo dos relatórios e os prazos. A este respeito, a proposta define uma abordagem em duas etapas: as empresas dispõem de 24 horas para apresentar um primeiro relatório de síntese, seguido de um relatório final pormenorizado no prazo de um mês.

([3]) JO L 345 de 23.12.2008, p. 75.
([4]) JO L 88 de 29.3.2019, p. 42.

3.8. A proposta prevê que os Estados-Membros designem as autoridades nacionais responsáveis pela gestão de crises e adotem planos específicos e cria uma nova rede de cooperação operacional, a Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe). Reforça o papel do grupo de cooperação na definição das decisões estratégicas e cria um registo das vulnerabilidades detetadas na UE, gerido pela ENISA. Prevê também uma intensificação da partilha de informações e da cooperação entre as autoridades dos Estados-Membros, incluindo a cooperação operacional em matéria de gestão de cibercrises.

3.9. A proposta introduz medidas de supervisão mais rigorosas para as autoridades nacionais e requisitos de execução mais exigentes e procura harmonizar os regimes de sanções em todos os Estados-Membros.

3.10. A este respeito, a proposta de diretiva estabelece uma lista de sanções administrativas em caso de violação das obrigações em matéria de gestão dos riscos de cibersegurança e de comunicação. A proposta prevê disposições sobre a responsabilidade das pessoas singulares com cargos de representação ou de gestão em sociedades abrangidas pela diretiva. Neste sentido, melhora a forma como a UE previne, gere e responde a incidentes e a crises de cibersegurança em grande escala, estabelecendo responsabilidades claras, um planeamento adequado e a cooperação reforçada a nível da UE.

3.11. Os Estados-Membros passam a poder supervisionar conjuntamente a aplicação das regras da UE e a prestar assistência mútua em caso de problemas transfronteiras, a encetar um diálogo mais estruturado com o setor privado, a coordenar a divulgação de vulnerabilidades detetadas em *software* e *hardware* comercializados no mercado interno e a avaliar de forma coordenada os riscos para a segurança e as ameaças relacionadas com as novas tecnologias, como aconteceu com a tecnologia 5G.

4. **Proposta de diretiva relativa à resiliência das entidades críticas**

4.1. Em 2006, a UE estabeleceu o Programa Europeu para a Proteção das Infraestruturas Críticas (PEPIC) e, em 2008, adotou a Diretiva Infraestruturas Críticas Europeias (Diretiva ICE), aplicável aos setores da energia e dos transportes. Tanto a Estratégia para a União da Segurança 2020-2025 ([5]) adotada pela Comissão Europeia, como a Agenda da UE em matéria de Luta contra o Terrorismo adotada recentemente sublinham a importância de garantir a resiliência das infraestruturas críticas face aos riscos físicos e digitais. No entanto, a avaliação realizada em 2019 sobre a aplicação da Diretiva ICE, tal como as conclusões da avaliação de impacto da proposta em apreço demonstraram que as medidas europeias e nacionais em vigor não são suficientes para garantir que os operadores são capazes de fazer face aos riscos atuais, o que levou o Conselho e o Parlamento a solicitar à Comissão uma revisão da atual abordagem em matéria de proteção das infraestruturas críticas.

4.2. Na Estratégia da UE para a União da Segurança, adotada pela Comissão em 24 de julho de 2020, reconhece-se a crescente interligação e interdependência entre as infraestruturas físicas e digitais e salienta-se a necessidade de uma abordagem mais coerente e consistente entre a Diretiva ICE e a Diretiva SRI. Neste sentido, a proposta de diretiva relativa à resiliência das entidades essenciais, cujo âmbito de aplicação é objetivamente idêntico ao da Diretiva SRI 2 no que toca às entidades essenciais, amplia o âmbito de aplicação inicial da Diretiva 2008/114/CE — limitado à energia e aos transportes — aos seguintes domínios: bancos, infraestrutura dos mercados financeiros, saúde, água potável, águas residuais, infraestrutura digital, administração pública e espaço, e estabelece também responsabilidades claras, um planeamento adequado e a cooperação reforçada. A este respeito, cumpre criar um quadro de referência para todos os riscos, sendo necessário apoiar os Estados-Membros nos esforços que desenvolvem para assegurar que as entidades críticas são capazes de prevenir, resistir e absorver as consequências dos incidentes, independentemente de os riscos resultarem de perigos naturais, acidentes, atos terroristas, ameaças internas ou emergências de saúde pública, como a atual.

4.3. Cada Estado-Membro deve adotar uma estratégia nacional para a resiliência das entidades críticas, realizar avaliações de risco regulares e, nessa base, identificar as entidades críticas. Por seu turno, as entidades críticas devem avaliar os riscos, adotar as medidas técnicas e organizativas adequadas para reforçar a resiliência e notificar os incidentes às autoridades nacionais. As entidades que prestam serviços a pelo menos um terço dos Estados-Membros, ou em pelo menos um terço dos Estados-Membros, são objeto de supervisão particular, o que inclui missões específicas de assistência a essas entidades organizadas pela Comissão.

4.4. A proposta de diretiva relativa à resiliência das entidades críticas prevê diferentes formas de apoio aos Estados-Membros e às entidades críticas e apresenta uma panorâmica dos riscos a nível da UE, boas práticas e metodologias, bem como atividades de formação e exercícios para testar a resiliência das entidades críticas. O sistema de cooperação transfronteiras prevê igualmente a constituição de um grupo de peritos específico, o Grupo para a Resiliência das Entidades Críticas, enquanto fórum para a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros.

([5]) COM(2020) 605 final.

5. **Propostas de alteração da proposta legislativa em apreço**

5.1. O CESE congratula-se com os esforços envidados pela Comissão para reforçar a resiliência das entidades públicas e privadas contra as ciberameaças e as ameaças físicas. Trata-se de um aspeto particularmente significativo e pertinente, em especial à luz da rápida transformação digital provocada pelo surto de COVID-19. Concorda igualmente que, tal como referido na Comunicação «Construir o futuro digital da Europa», a Europa deve tirar partido da era digital e reforçar a sua indústria — mormente as pequenas e médias empresas — e a sua capacidade de inovação de forma abrangente, mediante uma estratégia assente em quatro pilares, a saber, a proteção dos dados, os direitos fundamentais, a segurança e a cibersegurança, que são pré-requisitos essenciais para uma sociedade fundada no poder dos dados.

5.2. No entanto, à luz dos resultados da avaliação de impacto e da consulta que precedeu a proposta de Diretiva SRI 2 e tendo em conta o objetivo várias vezes salientado de evitar a fragmentação das regras adotadas a nível nacional, como também pretendido na comunicação de 4 de outubro de 2017 sobre a aplicação da Diretiva SRI ([6]), o CESE observa que não é claro por que razão a Comissão não propôs a adoção de um regulamento em vez de uma diretiva, o qual nem sequer consta das opções consideradas.

5.3. O CESE observa que algumas disposições das duas propostas de diretiva se sobrepõem, uma vez que ambas estão estreitamente ligadas e são complementares — uma aborda principalmente a cibersegurança e a outra a segurança física. Assinala igualmente que as entidades críticas referidas na Diretiva relativa à resiliência das entidades críticas abrangem os mesmos setores e coincidem com as entidades «essenciais» referidas na Diretiva SRI 2 ([7]). Além disso, todas as entidades críticas abrangidas pela Diretiva relativa à resiliência das entidades críticas estão sujeitas às obrigações em matéria de cibersegurança previstas na Diretiva SRI 2. Ademais, ambas as propostas preveem uma série de cláusulas-ponte para assegurar a articulação — disposições relativas ao reforço da cooperação entre as autoridades, ao intercâmbio de informações sobre as atividades de supervisão, à notificação às autoridades designadas nos termos da Diretiva SRI 2 da identidade das entidades críticas previstas na Diretiva relativa à resiliência das entidades críticas —, bem como reuniões regulares (pelo menos uma vez por ano) dos respetivos grupos de cooperação. As duas propostas partilham igualmente a mesma base jurídica, o artigo 114.º do TFUE, que visa o funcionamento do mercado interno mediante a aproximação das regras nacionais, tal como interpretado *ex multis* pelo Tribunal de Justiça da UE no seu acórdão relativo ao processo C-58/08, Vodafone e outros. Solicita-se, por conseguinte, que se pondere fundir as duas propostas num texto único, no interesse da simplificação e da concentração funcional.

5.4. O CESE concorda com a abordagem proposta de acabar com a distinção entre operadores de serviços essenciais e prestadores de serviços digitais inicialmente estabelecida na Diretiva SRI, mas salienta que, no que diz respeito ao seu âmbito de aplicação, cabe indicar de forma mais precisa e clara as entidades que estão obrigadas a cumprir a diretiva. Com efeito, para além das referências constantes dos anexos 1 e 2, a Diretiva SRI 2 elenca uma série de critérios heterogéneos que pressupõem avaliações qualitativas e quantitativas sensíveis suscetíveis de serem efetuadas de forma diferente em cada Estado-Membro, o que pode culminar na situação fragmentada que se pretende evitar com a proposta legislativa em apreço. É importante evitar abordagens divergentes a nível nacional que resultem em obstáculos à concorrência e à livre circulação de bens e serviços, o que pode prejudicar as empresas e pôr em causa as trocas comerciais.

5.5. A Diretiva SRI 2 prevê que as entidades críticas em domínios considerados «essenciais» pela proposta em apreço estejam igualmente sujeitas a obrigações gerais de reforço da resiliência, com especial destaque para os riscos não relacionados com a cibersegurança previstos na Diretiva relativa à resiliência das entidades críticas. No entanto, esta última indica expressamente que não se aplica às questões abrangidas pela Diretiva SRI 2. Com efeito, a Diretiva relativa à resiliência das entidades críticas prevê que, uma vez que a cibersegurança é suficientemente abordada na Diretiva SRI 2, as questões abrangidas por esta última devem ser excluídas do seu âmbito de aplicação, com a exceção do regime especial aplicável às entidades do setor das infraestruturas digitais. A Diretiva relativa à resiliência das entidades críticas explica, em seguida, que as entidades do setor das infraestruturas digitais dependem essencialmente da segurança das redes e da informação, sendo abrangidas pela Diretiva SRI 2, que também aborda a segurança física desses sistemas como parte das obrigações de gestão dos riscos de cibersegurança e de notificação que incumbem a essas entidades. Ao mesmo tempo, a Diretiva relativa à resiliência das entidades críticas não exclui a possibilidade de algumas das suas disposições específicas serem aplicáveis a essas entidades.

5.6. Por conseguinte, neste quadro complexo, o CESE reputa indispensável que a Comissão clarifique com precisão o âmbito de aplicação dos dois atos legislativos, especialmente quando há disposições diferentes que regem a mesma situação ou a mesma entidade.

5.7. A clareza legislativa, nomeadamente em textos tão longos e complexos como os aqui em apreço, deve constituir um objetivo primordial a todos os níveis, a par da redução da burocracia e da fragmentação através da simplificação dos procedimentos, dos requisitos de segurança e das obrigações em matéria de notificação de incidentes. Importa igualmente

([6]) COM(2017) 476 final.
([7]) Anexo 1 (JO L 194 de 19.7.2016, p. 1).

assegurar que a multiplicação de organismos encarregados de tarefas específicas não impede uma identificação clara das suas competências, que ponha em causa os objetivos perseguidos. Por conseguinte, poderia ser oportuno e benéfico para os cidadãos e as empresas fundir as duas propostas de diretiva num texto único, evitando um exercício de interpretação e de aplicação, por vezes, complexo.

5.8. Por várias ocasiões, as disposições de outros instrumentos jurídicos são referidas na Diretiva (UE) 2018/1972 ([8]) que estabelece o Código Europeu das Comunicações Eletrónicas, cuja aplicação se rege pelo princípio da especialidade. Algumas das disposições dessa diretiva são expressamente revogadas (artigos 40.º e 41.º), ao passo que outras devem ser aplicadas em consonância com este princípio, sem qualquer precisão a esse respeito. O CESE espera que sejam dissipadas quaisquer dúvidas sobre esta questão, a fim de evitar problemas de interpretação. Subscreve igualmente o objetivo da Comissão de harmonizar os regimes de sanções em caso de incumprimento na gestão dos riscos, no contexto do reforço da partilha de informações e da cooperação a nível da UE.

5.9. O CESE reconhece o papel essencial, salientado na proposta de diretiva, desempenhado pelos órgãos de direção das entidades «essenciais» e «importantes» na estratégia de cibersegurança e na gestão dos riscos, aos quais incumbe aprovar as medidas de gestão dos riscos, supervisionar a sua aplicação e agir em caso de eventual incumprimento. A este respeito, prevê-se que os membros destes órgãos frequentem regularmente ações de formação específicas, a fim de adquirirem os conhecimentos e as competências necessárias para compreender, gerir e avaliar o impacto dos vários riscos cibernéticos. No entanto, considera-se que a proposta deve indicar os requisitos em matéria de conhecimentos e competências, a fim de fornecer orientações a nível europeu sobre as competências de formação consideradas adequadas para responder às exigências indicadas na proposta e evitar que os requisitos e o conteúdo das várias ações de formação difiram de um país para outro.

5.10. O CESE concorda que a Agência da União Europeia para a Cibersegurança (ENISA) desempenha um papel importante em todo o quadro institucional e operacional da cibersegurança europeia. A este respeito, considera que, para além do relatório sobre o estado da cibersegurança na União, esta agência deve publicar em linha informações atualizadas sobre os incidentes de cibersegurança e alertas setoriais, a fim de proporcionar um instrumento de informação útil que permita às entidades abrangidas pela Diretiva SRI 2 proteger melhor as suas empresas.

5.11. O CESE concorda que o acesso em tempo útil a informações fidedignas sobre as vulnerabilidades dos produtos e serviços de TIC contribui para melhorar a gestão dos riscos de cibersegurança. Nesse contexto, as fontes de informação públicas sobre as vulnerabilidades constituem um instrumento importante para as autoridades nacionais competentes, a rede de equipas de resposta a incidentes de segurança informática (CSIRT), as empresas e os utilizadores. Por este motivo, o CESE concorda com a proposta de incumbir a ENISA da criação de um registo europeu de vulnerabilidades ao qual as entidades essenciais e importantes e os respetivos fornecedores poderão comunicar as informações, de forma a permitir aos utilizadores adotar as medidas de atenuação adequadas. Considera, além disso, que esta comunicação de vulnerabilidades e incidentes mais graves deve ser obrigatória e não voluntária, a fim de também se converter num instrumento útil para as entidades adjudicantes no âmbito dos procedimentos de adjudicação de contratos a nível europeu, inclusivamente de produtos e tecnologias 5G. Esse registo conteria então elementos que poderiam ser utilizados na avaliação das propostas, a fim de verificar a qualidade das mesmas e a fiabilidade dos contratantes europeus e de países terceiros, do ponto de vista da segurança dos produtos e serviços objeto do concurso, em conformidade com a Recomendação da Comissão, de 26 de março de 2019, «Cibersegurança das redes 5G». O registo deve igualmente assegurar que as informações nele contidas são disponibilizadas de forma a evitar qualquer tipo de discriminação.

Bruxelas, 27 de abril de 2021.

A Presidente
do Comité Económico e Social Europeu
Christa SCHWENG

([8]) JO L 321 de 17.12.2018, p. 36.