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

[COM(2017) 477 final/2 — 2017/0225 (COD)]

(2018/C 227/13)

Relator: **Alberto MAZZOLA**

Correlator: **Antonio LONGO**

Consulta	Parlamento Europeu, 23.10.2017
	Conselho da União Europeia, 25.10.2017
Base jurídica	Artigo 114.º do Tratado sobre o Funcionamento da União Europeia
Competência	Secção Especializada de Transportes, Energia, Infraestruturas e Sociedade da Informação
Adoção em secção	5.2.2018
Adoção em plenária	14.2.2018
Reunião plenária n.º	532
Resultado da votação	206/1/2
(votos a favor/votos contra/abstenções)	

1. **Conclusões e recomendações**

1.1. O CESE considera que o novo mandato permanente da ENISA (Agência da União Europeia para a Segurança das Redes e da Informação), tal como proposto pela Comissão, contribuirá significativamente para aumentar a capacidade de resistência dos sistemas europeus. Contudo, o orçamento previsto e os recursos atribuídos à ENISA não serão suficientes para que a agência cumpra o seu mandato.

1.2. O CESE recomenda a todos os Estados-Membros que criem uma entidade homóloga distinta equivalente à ENISA, já que a maioria ainda não o fez.

1.3. O CESE considera também que, no que toca ao reforço das capacidades, a ENISA deve dar prioridade a ações de apoio à administração pública em linha ([1]). Uma identidade digital a nível da UE/mundial para pessoas, organizações e objetos é fundamental, e a prevenção e o combate ao roubo de identidade e à fraude em linha devem ser uma prioridade.

1.4. O CESE recomenda à ENISA que apresente relatórios regulares sobre o estado de preparação cibernética dos Estados-Membros, com particular ênfase nos setores identificados no anexo II da Diretiva relativa à segurança das redes e da informação (Diretiva SRI). Deve ser realizado um exercício anual de cibersegurança a nível europeu, para avaliar a preparação dos Estados-Membros e a eficácia do mecanismo europeu de resposta a cibercrises, devendo ser emitidas recomendações com base no mesmo.

1.5. O CESE apoia a proposta de criar uma rede de competências em matéria de cibersegurança, a ser secundada por um Centro de Investigação e de Competências em matéria de Cibersegurança (CRCC). Esta rede poderá apoiar a soberania digital europeia, desenvolvendo uma base industrial europeia competitiva para as competências tecnológicas fundamentais, com base no trabalho realizado pela parceria público-privada contratual (PPPc), que deverá tornar-se uma empresa comum tripartida.

1.6. O fator humano constitui uma das principais causas dos ciberincidentes. Para o CESE, é necessário construir uma base sólida de competências em matéria de cibersegurança e melhorar a ciber-higiene, nomeadamente através de campanhas de sensibilização dirigidas a pessoas e empresas. O CESE apoia a criação de um programa curricular certificado pela UE para estudantes do ensino secundário e para profissionais.

([1]) Mercado Único Digital — Revisão intercalar.

1.7. O CESE considera que o mercado único digital europeu requer também uma interpretação homogénea das normas de cibersegurança, incluindo o reconhecimento mútuo entre Estados-Membros, e que um quadro de certificação e sistemas de certificação para os diversos setores poderão fornecer uma base de referência comum. Contudo, importa prever diferentes abordagens para os diversos setores em função da forma como funcionam. Por conseguinte, o CESE considera que as agências setoriais da UE (AESA, AFE, EMA, etc.) devem ser associadas ao processo e, nalguns casos, com o acordo da ENISA para garantir a coerência, incumbidas de elaborar os sistemas de certificação. Há que adotar normas mínimas europeias no domínio da segurança informática, em cooperação com os organismos de normalização CEN/CENELEC/ETSI.

1.8. O grupo europeu para a certificação da cibersegurança previsto, apoiado pela ENISA, deverá ser composto por autoridades nacionais supervisoras da certificação, partes interessadas do setor privado, incluindo operadores dos vários domínios de aplicação, e intervenientes da sociedade civil e da comunidade científica.

1.9. O CESE é de opinião que a agência deve, em nome da Comissão, acompanhar o desempenho e a tomada de decisões das autoridades nacionais supervisoras da certificação, através de auditorias e inspeções, e que as responsabilidades e as sanções pelo incumprimento das normas devem ser definidas no regulamento.

1.10. O CESE considera que as atividades de certificação devem incluir um sistema de rotulagem adequado, a ser aplicado também aos produtos importados, para reforçar a confiança dos consumidores.

1.11. A Europa deve aumentar o investimento, fazendo convergir os diferentes fundos da UE, fundos nacionais e investimentos do setor privado em prol de objetivos estratégicos, em forte cooperação público-privada, nomeadamente através da criação de um fundo da UE para a inovação, a investigação e o desenvolvimento no domínio da cibersegurança no âmbito do atual e do futuro Programa-Quadro de Investigação. Além disso, a Europa deveria criar um fundo para a difusão da cibersegurança, abrindo novas perspetivas no atual e futuro Mecanismo Interligar a Europa, bem como no próximo FEIE 3.0.

1.12. O CESE considera que é necessário um nível mínimo de segurança para os dispositivos «normais» da «Internet das pessoas». Neste caso, a certificação é um método fundamental para conferir um nível de segurança mais elevado. A segurança da Internet das coisas deve constituir uma prioridade.

2. **Quadro atual em matéria de cibersegurança**

2.1. A cibersegurança é essencial tanto para a prosperidade e a segurança nacional, como para o próprio funcionamento das nossas democracias, liberdades e valores. O relatório sobre o Índice Global de Cibersegurança das Nações Unidas afirma que a cibersegurança é um ecossistema no qual as leis, organizações, competências, cooperação e implementação técnica devem estar em harmonia para serem mais eficazes, acrescentando que a cibersegurança está cada vez mais presente na mente dos responsáveis políticos a nível nacional.

2.2. A necessidade de um ecossistema seguro está a tornar-se fundamental devido à revolução da Internet. Esta revolução não só ajudou a redefinir o setor dos serviços das empresas aos consumidores (B2C), como é o caso dos serviços de comunicação social, retalhistas e financeiros, mas também está a remodelar os setores da indústria transformadora, da energia, da agricultura, dos transportes e outros setores industriais da economia, que, em conjunto, representam cerca de dois terços do produto interno bruto total, bem como as infraestruturas de serviços e as interações dos cidadãos com a administração pública.

2.3. A Estratégia para o Mercado Único Digital tem como pilares a melhoria do acesso a bens, serviços e conteúdos, a criação de um quadro jurídico adequado para redes e serviços digitais, bem como o aproveitamento dos benefícios de uma economia baseada nos dados. Estima-se que a estratégia possa contribuir com 415 mil milhões de EUR por ano para a economia da UE. Prevê-se que o défice de profissionais com competências de cibersegurança para trabalhar no setor privado, na Europa, chegue aos 350 000 em 2022 ([2]).

([2]) JOIN(2017) 450 final.

2.4. Segundo a estimativa de um estudo de 2014, o impacto económico da cibercriminalidade na União representou 0,41 % do PIB da UE (ou seja, cerca de 55 mil milhões de EUR) em 2013 ([3]).

2.5. De acordo com o Eurobarómetro Especial 464a sobre as atitudes dos europeus em relação à cibersegurança, 73 % dos utilizadores da Internet receiam que as suas informações pessoais em linha possam não estar guardadas em segurança nos sítios Web e 65 % receiam que possam não estar protegidas pelas autoridades públicas. A maioria dos inquiridos está preocupada com a possibilidade de vir a ser vítima de diversas formas de cibercriminalidade, especialmente através de *software* malicioso nos seus dispositivos (69 %), roubo de identidade (69 %) e fraude bancária em linha e com cartões bancários (66 %) ([4]).

2.6. Até à data, nenhum quadro jurídico conseguiu acompanhar o ritmo da inovação digital, mas existem vários textos legislativos que contribuem gradualmente para a criação de um quadro adequado: a revisão do Código das Telecomunicações, o Regulamento geral sobre a proteção de dados (RGPD), a Diretiva relativa à segurança das redes e da informação (Diretiva SRI), o Regulamento relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (Regulamento e-IDAS), o Escudo de Proteção da Privacidade UE-EUA, a Diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, etc.

2.7. Para além da ENISA, a «Agência da UE para a Cibersegurança», existem muitas organizações que lidam com as questões da cibersegurança: a Europol, a CERT-UE (Equipa de Resposta a Emergências Informáticas da União Europeia), o Centro de Situação e de Informações da UE (INTCEN), a Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), os centros de partilha e análise de informações (ISAC), a Organização Europeia de Cibersegurança (ECSO), a Agência Europeia de Defesa (AED), o Centro de Excelência Cooperativo para a Ciberdefesa da OTAN e o Grupo de Peritos Governamentais das Nações Unidas para os progressos da informática e das telecomunicações no contexto da segurança internacional.

2.8. A segurança desde a conceção é fundamental para o fornecimento de bens e serviços de elevada qualidade: os dispositivos inteligentes não são assim tão inteligentes se não forem seguros e o mesmo se aplica aos carros inteligentes, cidades inteligentes e hospitais inteligentes. Todos requerem dispositivos, sistemas, arquiteturas e serviços com segurança integrada.

2.9. Em 19 e 20 de outubro de 2017, o Conselho Europeu solicitou a adoção de uma abordagem comum em matéria de cibersegurança na UE, na sequência do pacote de reformas proposto, apelando para «uma abordagem comum da cibersegurança: o mundo digital requer confiança, e a confiança só se pode alcançar se garantirmos uma segurança mais proativa desde a conceção em todas as políticas digitais, se disponibilizarmos a adequada certificação de segurança dos produtos e serviços, e se aumentarmos a nossa capacidade para prevenir, dissuadir, detetar e debelar os ciberataques» ([5]).

2.10. Na sua resolução de 17 de maio de 2017, o Parlamento Europeu «salienta a necessidade de segurança de ponta a ponta em toda a cadeia de valor dos serviços financeiros; chama a atenção para os elevados e múltiplos riscos decorrentes dos ataques cibernéticos, que visam a infraestrutura, a Internet das Coisas, as moedas e os dados dos nossos mercados financeiros; […] solicita às Autoridades Europeias de Supervisão que […] procedam regularmente a uma revisão das normas operacionais que abrangem os riscos associados às TIC das instituições financeiras; solicita, além disso, que as Autoridades Europeias de Supervisão elaborem orientações relativas à supervisão destes riscos […]; salienta a importância de as Autoridades Europeias de Supervisão disporem de conhecimento técnico» ([6]).

2.11. O CESE já abordou o problema em várias ocasiões ([7]), nomeadamente durante a cimeira de Taline, na conferência sobre o futuro desenvolvimento da administração pública em linha e da cibersegurança ([8]), e criou um Grupo de Estudo Permanente para a Agenda Digital.

([3]) Commission Staff Working Document — Impact Assessment, accompanying the Proposal for a Regulation of the European Parliament and of the Council [Documento de trabalho dos serviços da Comissão — Avaliação de impacto que acompanha a proposta de regulamento do Parlamento Europeu e do Conselho], parte 1/6, p. 21, Bruxelas, 13 de setembro de 2017.

([4]) Special Eurobarometer 464a — Wave EB87.4 — Europeans' attitudes towards cyber security [Eurobarómetro Especial 464a — Wave EB87.4 — Atitudes dos europeus em relação à cibersegurança], setembro de 2017.

([5]) Conclusões do Conselho Europeu de 19 de outubro de 2017.

([6]) Resolução do Parlamento Europeu de 17 de maio de 2017 — A8-0176/2017.

([7]) Mercado Único Digital — Revisão intercalar. (JO C 75 de 10.3.2017, p. 124); (JO C 246 de 28.7.2017, p. 8); (JO C 345 de 13.10.2017, p. 52); (JO C 288 de 31.8.2017, p. 62); (JO C 271 de 19.9.2013, p. 133).

([8]) Comunicado de imprensa do CESE n.º 31/2017 — «Society debates E-government and cybersecurity with incoming Estonian Presidency» [Sociedade civil debate a administração pública em linha e a cibersegurança com a futura Presidência estónia]: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incoming-estonian-Presidency

3. **Propostas da Comissão**

3.1. O Pacote Cibersegurança inclui uma comunicação conjunta que revê a anterior Estratégia Europeia para a Cibersegurança (2013), bem como um Regulamento Cibersegurança, centrado no novo mandato da ENISA e na proposta para um quadro de certificação.

3.2. A estratégia está estruturada em três secções principais: capacidade de resistência, dissuasão e cooperação internacional. A componente da dissuasão centra-se sobretudo nas questões da cibercriminalidade, incluindo a Convenção de Budapeste, e a componente da cooperação internacional incide na ciberdefesa, na ciberdiplomacia e na cooperação com a OTAN.

3.3. A proposta estabelece novas iniciativas, tais como:

— o fortalecimento da Agência da UE para a Cibersegurança;

— a introdução de um sistema de certificação da cibersegurança a nível da UE;

— a rápida execução da Diretiva SRI.

3.4. A componente da capacidade de resistência propõe ações relacionadas com a cibersegurança que abordam, em particular: questões de mercado, a Diretiva SRI, a resposta rápida a emergências, o desenvolvimento de competências na UE, a educação, a formação — em competências de cibersegurança e ciber-higiene — e a sensibilização.

3.5. Em paralelo, o Regulamento Cibersegurança propõe a criação de um quadro europeu de certificação da cibersegurança para produtos e serviços de TIC.

3.6. O Regulamento Cibersegurança também propõe o reforço do papel da ENISA enquanto a Agência da UE para a Cibersegurança, atribuindo-lhe um mandato permanente. Para além das suas atuais responsabilidades, a ENISA terá novas atribuições de apoio e coordenação relacionadas com o apoio à execução da Diretiva SRI, a Estratégia da UE para a Cibersegurança e o respetivo plano de ação, o reforço de capacidades, o conhecimento e a informação, a sensibilização, atribuições relacionadas com o mercado, como o apoio à normalização e à certificação, investigação e inovação, exercícios pan-europeus de cibersegurança, bem como os serviços de secretariado da rede de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT).

4. **Observações na generalidade — Visão geral**

4.1. ***Contexto: Capacidade de resistência***

4.1.1. *Mercado único da cibersegurança*

Dever de diligência: O desenvolvimento do princípio de «dever de diligência» proposto, mencionado na comunicação conjunta para a utilização de processos de desenvolvimento seguros ao longo do ciclo de vida, é um conceito interessante a ser explorado com a indústria da UE, o que poderá levar a uma abordagem abrangente no que respeita ao cumprimento da legislação da UE. A evolução futura deverá ter em conta a segurança por princípio.

Responsabilidade: A certificação facilitará a imputação de responsabilidades em caso de litígio.

4.1.2. *Diretiva SRI*: energia, transportes, serviços bancários/financeiros, saúde, água, infraestruturas digitais, comércio eletrónico.

Para o CESE, a execução plena e eficiente da Diretiva SRI é essencial para garantir a resistência dos setores nacionais fundamentais.

O CESE considera que a partilha de informações entre entidades públicas e privadas deverá ser reforçada através de centros de partilha e análise de informações (ISAC) setoriais. Deve ser desenvolvido um mecanismo adequado para partilhar com segurança informações fiáveis no âmbito de um ISAC e entre CSIRT e ISAC, com base numa análise/avaliação do mecanismo atualmente em uso.

4.1.3. *Resposta rápida a emergências*

A abordagem assente num «plano de ação» constituirá um processo eficaz para uma resposta operacional, a nível da UE e dos Estados-Membros, a incidentes de grande escala. O Comité sublinha a necessidade de envolver o setor privado. Os operadores de serviços essenciais no mecanismo de resposta operacional também deverão ser tidos em consideração, uma vez que poderão fornecer informações importantes sobre ameaças e/ou apoio na deteção e resposta a ameaças e crises de grande escala.

A comunicação conjunta propõe a integração dos ciberincidentes nos mecanismos de gestão de crises da UE. Embora o CESE compreenda a necessidade de uma resposta coletiva e de solidariedade na eventualidade de um ataque, é necessária uma melhor compreensão da sua forma de aplicação, uma vez que as ciberameaças, geralmente, se propagam entre países. As ferramentas utilizadas nas emergências nacionais apenas poderão ser parcialmente partilhadas em caso de necessidade local.

4.1.4. *Desenvolvimento de competências na UE*

Para que a UE possa ser verdadeiramente competitiva a nível mundial e criar uma base tecnológica sólida, é essencial criar um quadro coerente a longo prazo que abranja todas as fases da cadeia de valor da cibersegurança. Neste contexto, promover a cooperação entre os ecossistemas regionais europeus é fundamental para desenvolver uma cadeia de valor da cibersegurança a nível europeu. O CESE congratula-se com a proposta de criar uma rede de competências em matéria de cibersegurança.

Esta rede poderá apoiar a soberania digital europeia, desenvolvendo uma base industrial europeia competitiva e reduzindo a dependência do conhecimento técnico desenvolvido fora da UE para competências tecnológicas fundamentais, fornecer exercícios técnicos, seminários e formação em ciber-higiene para profissionais e não profissionais, bem como, com base no trabalho realizado pela PPPc, fomentar o desenvolvimento de uma rede de organizações nacionais público-privadas para apoiar o desenvolvimento de um mercado na Europa. O avanço da PPPc deverá levar à sua otimização, adaptação ou expansão (programa de trabalho no domínio da cibersegurança do trio de Presidências EE-BG-AT) através da criação de uma empresa comum tripartida (Comissão, Estados-Membros, Empresas).

Para ser eficaz e alcançar os objetivos propostos a nível europeu, a rede deve dispor de um sistema de governação bem definido.

Esta rede será apoiada por um Centro de Investigação e de Competências em matéria de Cibersegurança (CRCC) a nível europeu, interligando os centros de competências nacionais existentes em toda a UE. O CRCC não só será responsável por coordenar e gerir a investigação, tal como acontece noutras empresas comuns, mas também permitirá o desenvolvimento eficaz de um ecossistema da cibersegurança europeu que apoie a implementação e aplicação da inovação na UE.

4.2. ***Contexto: Dissuasão***

4.2.1. O combate à cibercriminalidade é uma das principais prioridades a nível nacional e europeu, que exige um forte empenho político. As atividades de dissuasão devem ser executadas com base numa forte parceria entre os setores público e privado, estabelecendo uma partilha eficiente de informações e conhecimentos especializados a nível nacional e europeu. Poderá prever-se a possibilidade de alargar as atividades da Europol no domínio da informática forense e da monitorização.

4.3. ***Contexto: Cooperação internacional***

4.3.1. Construir e manter uma cooperação de confiança com países terceiros através da ciberdiplomacia e de parcerias comerciais é fundamental para reforçar a capacidade da Europa de prevenir, dissuadir e responder a ataques cibernéticos de grande escala. A Europa deve reforçar a sua cooperação com os EUA, a China, Israel, a Índia e o Japão. A modernização dos mecanismos de controlo das exportações da UE deverá evitar a violação dos direitos humanos e a utilização indevida das tecnologias contra a própria segurança da UE, mas também assegurar que a indústria da UE não é penalizada em relação a ofertas de países terceiros. Deve prever-se uma estratégia específica para os países candidatos à adesão, de forma a prepará-los para o intercâmbio transfronteiras de dados sensíveis, inclusive conferindo a alguns países a possibilidade de participar como observadores nas atividades da ENISA. Esses países devem ser classificados de acordo com a sua vontade de lutar contra a cibercriminalidade, podendo elaborar-se uma lista negra.

4.3.2. O CESE congratula-se com a introdução da ciberdefesa na segunda fase prevista para a possível criação de um futuro centro de competências de cibersegurança da UE. Por esta razão, a Europa poderia, entretanto, equacionar o desenvolvimento de competências duais, nomeadamente tirando partido do Fundo Europeu de Defesa e da criação prevista, até 2018, de uma plataforma de educação e formação em ciberdefesa. Tendo em conta o potencial e as ameaças reconhecidos mutuamente, o CESE reputa necessário desenvolver a cooperação UE-OTAN, e a indústria europeia também deve acompanhar de perto a evolução da cooperação UE-OTAN no que respeita a uma maior interoperabilidade das normas de cibersegurança e outras formas de cooperação no contexto da abordagem da UE em matéria de ciberdefesa.

4.4. ***Quadro europeu de certificação***

4.4.1. O CESE considera que a Europa tem de enfrentar o desafio da fragmentação da cibersegurança através de uma interpretação homogénea das normas, incluindo o reconhecimento mútuo entre Estados-Membros ao abrigo de um quadro unificado para facilitar a proteção de um Mercado Único Digital. Um quadro de certificação poderá fornecer uma base de referência comum (com normas específicas relativas a níveis mais elevados, quando necessário), garantindo sinergias entre setores verticais e reduzindo a atual fragmentação.

4.4.2. O CESE congratula-se com a criação de um quadro europeu de certificação da cibersegurança e de sistemas de certificação para os diversos setores, com base em requisitos adequados e em cooperação com as principais partes interessadas. Contudo, o tempo de lançamento no mercado e os custos de certificação, bem como a qualidade e a segurança, são elementos-chave a ter em conta. Serão criados sistemas de certificação para aumentar a segurança em função das necessidades atuais e do conhecimento sobre ameaças: há que ter em conta a flexibilidade e a capacidade de evolução destes sistemas, a fim de permitir a realização das atualizações necessárias. Importa prever diferentes abordagens para os diversos setores em função da forma como funcionam. Por conseguinte, o CESE considera que as agências setoriais da UE (AESA, EBA, AFE, EMA, etc.) devem ser associadas ao processo e, nalguns casos, com o acordo da ENISA para evitar a duplicação de esforços e a falta de coerência, incumbidas de elaborar os sistemas de certificação.

4.4.3. Para o Comité, é importante que o quadro de certificação assente em normas europeias de cibersegurança e das TIC definidas em conjunto e, na medida do possível, reconhecidas internacionalmente. Considerando os prazos estabelecidos e as prerrogativas nacionais, cumpre adotar normas mínimas europeias no domínio da segurança informática, em cooperação com os organismos de normalização CEN/CENELEC/ETSI. As normas profissionais devem ser consideradas como um elemento positivo, mas não devem ser juridicamente vinculativas nem prejudicar a concorrência.

4.4.4. Torna-se claramente necessário associar as responsabilidades aos diferentes níveis de garantia, em função do impacto das ameaças. O diálogo com as companhias de seguros poderá beneficiar a adoção de requisitos de cibersegurança eficazes dependendo do setor de aplicação. Na opinião do CESE, as empresas que procuram um «nível de garantia elevado» devem ser apoiadas e incentivadas, especialmente no que diz respeito a sistemas e dispositivos vitais.

4.4.5. Tendo em conta o tempo decorrido desde a adoção da Diretiva 85/374/CEE ([9]) e a evolução tecnológica atual, o CESE exorta a Comissão a analisar a pertinência de incluir no âmbito de aplicação da diretiva alguns dos cenários previstos na proposta de regulamento em apreço, a fim de garantir produtos mais seguros, com um elevado nível de proteção.

4.4.6. O CESE considera que o grupo europeu para a certificação da cibersegurança previsto, apoiado pela ENISA, deverá ser composto por autoridades nacionais supervisoras da certificação, partes interessadas do setor privado e operadores dos vários domínios de aplicação, a fim de assegurar a criação de sistemas de certificação abrangentes. Além disso, deve prever-se a cooperação entre este grupo e as associações representativas do setor em questão na UE/EEE (por exemplo, PPPc, setor bancário, transportes, energia, federações, etc.), através da nomeação de peritos. Este grupo deverá ter em conta os resultados alcançados na Europa no domínio da certificação [sobretudo o acordo de reconhecimento mútuo do Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS), sistemas nacionais e proprietários] e procurar preservar as vantagens competitivas europeias.

([9]) JO L 210 de 7.8.1985, p. 29.

4.4.7. O CESE propõe que a responsabilidade pela preparação dos sistemas de certificação seja atribuída a este grupo de partes interessadas, em cooperação com a Comissão Europeia. Os requisitos setoriais também devem ser definidos através de um acordo consensual entre as partes interessadas públicas e privadas (utilizadores e fornecedores).

4.4.8. Além disso, o grupo deve rever regularmente os sistemas de certificação, tendo em conta os requisitos de cada setor, e adaptá-los quando necessário.

4.4.9. O CESE apoia a eliminação progressiva dos sistemas nacionais de certificação quando for introduzido um regime europeu, tal como proposto no artigo 49.º do regulamento. Um mercado único não pode funcionar com regras nacionais diferentes e contraditórias. Para o efeito, o CESE propõe um levantamento de todos os sistemas nacionais.

4.4.10. O CESE propõe que a Comissão lance uma ação para promover a certificação da cibersegurança e os certificados na UE e que vele pelo seu reconhecimento em todos os acordos comerciais internacionais.

4.5. ***ENISA***

4.5.1. O CESE considera que o novo mandato permanente da ENISA, tal como proposto pela Comissão, contribuirá significativamente para aumentar a capacidade de resistência dos sistemas europeus. Contudo, o orçamento previsto e os recursos atribuídos à ENISA reformada podem não ser suficientes para que a agência cumpra o seu mandato.

4.5.2. O CESE incentiva todos os Estados-Membros a criarem uma entidade homóloga distinta semelhante à ENISA, já que a maioria ainda não o fez. Importa promover um programa estruturado para destacar peritos nacionais (PND) para a ENISA, para apoiar o intercâmbio de boas práticas e reforçar a confiança. O Comité recomenda também à Comissão que zele pela recolha e partilha das boas práticas e medidas eficazes atualmente em vigor nos Estados-Membros.

4.5.3. O CESE considera também que, no que toca ao reforço das capacidades, a ENISA deve dar prioridade a ações de apoio à administração pública em linha ([10]). Uma identidade digital a nível da UE/mundial para pessoas, organizações, empresas e objetos é fundamental, e a prevenção e o combate ao roubo de identidade e à fraude em linha, bem como o combate ao roubo de propriedade intelectual e industrial, devem ser uma prioridade.

4.5.4. A ENISA deve também apresentar relatórios regulares sobre o estado de preparação cibernética dos Estados-Membros, com particular ênfase nos setores identificados no anexo II da Diretiva SRI. Deve ser realizado um exercício anual de cibersegurança a nível europeu, para avaliar a preparação dos Estados-Membros e a eficácia do mecanismo europeu de resposta a cibercrises, devendo ser emitidas recomendações com base no mesmo.

4.5.5. O CESE receia que os recursos sejam demasiado limitados no âmbito da cooperação operacional, incluindo a rede de CSIRT.

4.5.6. No que respeita às atribuições relacionadas com o mercado, o CESE considera que o reforço da cooperação com os Estados-Membros e a criação de uma rede formal de agências de cibersegurança poderão ajudar a apoiar a cooperação entre as partes interessadas ([11]). O tempo de lançamento no mercado é muito reduzido e é crucial que as empresas da UE sejam capazes de competir neste domínio; a ENISA deve ser capaz de reagir em conformidade. O CESE considera que, tal como acontece com outras agências da UE, a ENISA poderá, no futuro, aplicar um sistema de taxas e encargos. O CESE manifesta preocupação com a possibilidade de a concorrência por competências entre agências da UE e nacionais, tal como aconteceu noutros domínios, atrasar a criação adequada do quadro regulamentar da UE e prejudicar o mercado único da UE.

4.5.7. O CESE observa que as atribuições relacionadas com a I&D e a cooperação internacional são atualmente mínimas.

([10]) Mercado Único Digital — Revisão intercalar.
([11]) JO C 75 de 10.3.2017, p. 124.

4.5.8. O CESE considera que a cibersegurança deve constituir um tema de debate recorrente nas reuniões regulares conjuntas das agências no domínio da Justiça e dos Assuntos Internos (JAI) e que a ENISA e a Europol devem cooperar regularmente.

4.5.9. Tendo em conta que o mundo cibernético é muito inovador, as normas devem ser cuidadosamente pensadas, de forma a evitar criar entraves à inovação, a qual exige um enquadramento dinâmico. A compatibilidade futura e retroativa deve ser assegurada, na medida do possível, a fim de proteger os investimentos dos cidadãos e das empresas.

4.5.10. Devido à importância das autoridades nacionais supervisoras da certificação, o CESE propõe que o regulamento em apreço estabeleça desde logo uma rede formal de autoridades incumbidas de resolver questões transfronteiras com o apoio da ENISA. A rede poderá, numa fase posterior, transformar-se numa agência única.

4.5.11. A confiança é fundamental, mas a ENISA não pode emitir decisões nem relatórios de auditoria. O CESE é de opinião que a agência deve, em nome da Comissão, acompanhar o desempenho e a tomada de decisões das autoridades nacionais supervisoras da certificação, através de auditorias e inspeções.

4.5.12. A participação no conselho de administração da ENISA deve ser alargada à indústria e às organizações de consumidores enquanto observadores.

4.6. ***Indústria, PME, financiamento/investimento e modelos de negócio inovadores***

4.6.1. *A indústria e o investimento*

Para aumentar a competitividade mundial das empresas da UE que operam no domínio das TIC, as medidas devem ser orientadas para melhor apoiar o crescimento e a competitividade deste setor, nomeadamente das PME.

A Europa deve aumentar o investimento, fazendo convergir os diversos fundos da UE, fundos nacionais e investimentos do setor privado no sentido de objetivos estratégicos, em forte cooperação público-privada. Há que apoiar e aumentar o nível de investimento em domínios essenciais através da criação de um fundo da UE para a inovação, a investigação e o desenvolvimento no domínio da cibersegurança no âmbito do atual e do futuro Programa-Quadro de Investigação. Além disso, a Europa deveria criar um fundo para a difusão da cibersegurança, abrindo novas perspetivas no atual e futuro Mecanismo Interligar a Europa, bem como no próximo FEIE 3.0.

Devem ser criados incentivos para que os Estados-Membros da UE adquiram soluções europeias sempre que possível e selecionem fornecedores europeus, se disponíveis, especialmente no que respeita a aplicações sensíveis. A Europa deve apoiar o crescimento de campeões europeus da cibersegurança capazes de concorrer no mercado mundial.

4.6.2. *As PME*

Devido à fragmentação do mercado, é necessária maior clareza quanto ao que os clientes procuram, de forma a responder melhor às necessidades do mercado. Sem uma procura estruturada, as PME e as empresas em fase de arranque não conseguirão crescer a um ritmo mais rápido. Neste contexto, seria positiva a criação de uma plataforma europeia da cibersegurança para as PME.

As tecnologias de cibersegurança estão em rápida evolução, e as PME, graças à sua agilidade, conseguem fornecer as soluções de vanguarda necessárias para se manterem competitivas. Em comparação com países terceiros, a UE ainda procura um modelo de negócio adequado para as PME.

Poderiam ser concebidos mecanismos específicos para as empresas em fase de arranque e as PME suportarem o custo da certificação, a fim de neutralizar as grandes dificuldades na angariação de fundos para o seu desenvolvimento tecnológico e comercial.

4.7. ***O fator humano: educação e proteção***

4.7.1. O CESE constata que a proposta da Comissão não tem suficientemente em conta o ser humano como motor dos processos digitais, seja como beneficiário, seja como a causa dos principais ciberincidentes.

4.7.2. É necessário construir uma base sólida de competências em matéria de cibersegurança, melhorar a ciber-higiene e sensibilizar as pessoas e as empresas. Para tanto, devem ser equacionados investimentos específicos, tempo para formar instrutores de alto nível e campanhas de sensibilização eficazes. A execução destas três linhas de ação requer a participação das autoridades nacionais e regionais (responsáveis pela criação e investimento em programas educativos eficazes) e das empresas e PME numa abordagem coletiva.

4.7.3. Deve ponderar-se a eventual criação de um programa curricular certificado pela UE para estudantes do ensino secundário e para profissionais, com a participação ativa da ENISA e das suas homólogas nacionais. Além disso, a igualdade de género deve ser tida em consideração no desenvolvimento de programas educativos, para melhorar os níveis de emprego no domínio da cibersegurança.

4.7.4. O CESE considera que o processo de certificação deve incluir um sistema de rotulagem adequado, tanto para o *hardware* como para o *software*, tal como acontece com muitos outros produtos (por exemplo, produtos energéticos). Este instrumento terá a tripla vantagem de reduzir os custos para as empresas, eliminar a atual fragmentação do mercado, decorrente dos diversos sistemas de certificação já adotados a nível nacional, e facilitar a compreensão pelo consumidor da qualidade e das características do produto adquirido. A este respeito, é importante que os produtos importados de países terceiros também estejam sujeitos aos mesmos mecanismos de certificação e rotulagem. Por último, o CESE considera que a criação de um logótipo *ad hoc* poderá ajudar a comunicar rapidamente aos consumidores e utilizadores a fiabilidade dos produtos adquiridos ou dos sítios Web onde se efetuam transações de compra e venda ou que preveem a transmissão de dados sensíveis.

4.7.5. A ENISA deve desenvolver uma atividade fundamental de informação e sensibilização a vários níveis, de forma a reforçar o conhecimento sobre comportamentos digitais «seguros» e a confiança dos utilizadores na Internet. Para o efeito, importa contar com a participação das organizações empresariais, das associações de consumidores e de outras entidades que operem nos serviços digitais.

4.7.6. Em complemento do Regulamento Cibersegurança, tal como já proposto no parecer INT/828, o CESE entende que é fundamental criar um vasto programa europeu dedicado à educação e à formação digitais, de molde a dotar todos os cidadãos das ferramentas necessárias para enfrentar a transição da melhor forma. Em particular, o CESE, embora ciente das competências específicas dos Estados-Membros neste domínio, espera que este programa comece por se aplicar nas escolas, reforçando os conhecimentos dos professores, adaptando os programas de estudo e os métodos pedagógicos às tecnologias digitais (incluindo a aprendizagem eletrónica) e proporcionando a todos os alunos uma formação de elevada qualidade. Este programa terá o seu prolongamento natural na aprendizagem ao longo da vida, a fim de reconverter ou requalificar as competências de todos os trabalhadores ([12]).

5. **Observações na especialidade**

5.1. ***Soluções e tecnologias emergentes: o caso da Internet das coisas***

O número de dispositivos conectados aumenta constantemente, prevendo-se que venha a atingir um múltiplo do número de pessoas que vivem no planeta, graças à digitalização de componentes, sistemas e soluções e a uma melhor conectividade. Esta tendência cria novas oportunidades para os criminosos informáticos, nomeadamente porque, muitas vezes, os dispositivos da Internet das coisas não estão tão bem protegidos como os dispositivos tradicionais.

As normas de segurança europeias nos diferentes setores que utilizam dispositivos ligados à Internet das coisas podem reduzir o esforço de desenvolvimento, tempo e orçamento para todos os participantes industriais na cadeia de valor dos produtos conectados.

Provavelmente será necessário um nível mínimo de segurança para os dispositivos «normais» da «Internet das pessoas», através da Gestão de Identidade e Acesso, correções e gestão de dispositivos. Dado que a certificação é um método fundamental para conferir um nível de segurança mais elevado, a nova abordagem da UE em matéria de certificação deve colocar maior ênfase na segurança da Internet das coisas.

Bruxelas, em 14 de fevereiro de 2018.

O Presidente
do Comité Económico e Social Europeu
Georges DASSIS

([12]) Mercado Único Digital — Revisão intercalar.