ASSEMBLEIA DA REPÚBLICA

COMISSÃO DE ASSUNTOS EUROPEUS

PARECER
COM(2020)823

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

PARTE I - NOTA INTRODUTÓRIA

Nos termos do artigo 7.º da Lei n.º 43/2006, de 25 de agosto, que regula o acompanhamento, apreciação e pronúncia pela Assembleia da República no âmbito do processo de construção da União Europeia, com as alterações introduzidas pelas Lei n.º 21/2012, de 17 de maio, e pela Lei nº 18/2018, de 2 de maio e pela Lei n.º 64/2020, de 2 de novembro, bem como da Metodologia de escrutínio das iniciativas europeias aprovada em 1 de março de 2016, a Comissão de Assuntos Europeus recebeu 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 [COM(2020)823]

A supra identificada iniciativa foi sinalizada à Comissão de Assuntos Constitucionais, Direitos, Liberdade e Garantias, comissão competente em razão da matéria, a qual analisou a referida iniciativa e aprovou o relatório que se anexa ao presente Parecer, dele fazendo parte integrante.

PARTE II – CONSIDERANDOS

1 – A presente iniciativa diz respeito à 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.

2 – Importa começar por relembrar que tal como referido na Comunicação «*Construir o futuro digital da Europa*»[1], é crucial que a Europa tire partido de todos os benefícios da era digital e reforce a sua capacidade industrial e de inovação dentro de limites éticos e seguros. A estratégia europeia para os dados define quatro pilares — a proteção de dados, os direitos fundamentais, a segurança e a cibersegurança —, que constituem condições essenciais para uma sociedade capacitada pela utilização dos dados.

[1] COM(2020) 67 final.

3 – Com efeito, numa Resolução de 12 de março de 2019, o Parlamento Europeu instou «[…] *a Comissão a ponderar a necessidade de alargar o âmbito de aplicação da Diretiva SRI (Diretiva Segurança das Redes e da Informação) a novos setores e serviços críticos que não sejam abrangidos por legislação setorial*»[2].

Também nas suas Conclusões de 9 de junho de 2020, o Conselho congratulou-se com «[…] *os planos da Comissão que visam garantir regras coerentes para os operadores de mercado e facilitar uma partilha de informações segura, sólida e adequada sobre ameaças e incidentes, nomeadamente através de uma revisão da Diretiva Segurança das Redes e da Informação (Diretiva SRI), a fim de encontrar soluções que melhorem a ciber-resiliência e de dar uma resposta mais eficaz aos ciberataques, em particular no contexto das atividades económicas e societais de caráter essencial, sem deixar de respeitar as competências dos Estados-Membros, incluindo a responsabilidade pela sua segurança nacional*»[3].

4 – Nesta sequência, é referido na presente iniciativa que a mesma faz parte de um pacote de medidas destinadas a melhorar a resiliência e a capacidade de resposta a incidentes no domínio da cibersegurança e da proteção de infraestruturas críticas por parte das entidades públicas e privadas, das autoridades competentes e da União no seu conjunto. É consentânea com as prioridades da Comissão no sentido de preparar a Europa para a era digital e criar uma economia pronta para o futuro e que esteja ao serviço dos cidadãos.

A cibersegurança é, pois, uma das áreas prioritárias da resposta da Comissão à crise da COVID-19. O pacote inclui uma nova estratégia em matéria de cibersegurança, com o objetivo de reforçar a autonomia estratégia da União para melhorar a sua resiliência e a sua resposta coletiva, bem como para construir uma Internet aberta e global.

5 - A presente iniciativa tem, assim, por base e revoga a Diretiva (UE) 2016/1148 relativa à segurança das redes e da informação (Diretiva SRI), que constitui o primeiro

[2] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_PT.html.

[3] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/pt/pdf.

ato legislativo à escala da União sobre cibersegurança e que estabelece medidas jurídicas para melhorar o nível geral de cibersegurança na União.

Neste contexto, é relembrado que a Diretiva SRI:

i) contribuiu para melhorar as capacidades de cibersegurança a nível nacional, exigindo que os Estados-Membros adotassem estratégias nacionais de cibersegurança e que designassem autoridades competentes neste domínio;

ii) reforçou a cooperação entre os Estados-Membros a nível da União, criando vários fóruns para facilitar o intercâmbio de informações estratégicas e operacionais;

iii) melhorou a ciber-resiliência de entidades públicas e privadas em sete setores específicos (energia, transportes, serviços bancários, infraestruturas do mercado financeiro, cuidados de saúde, fornecimento e distribuição de água potável, e infraestruturas digitais) e em três serviços digitais (mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem), exigindo que os Estados-Membros se certifiquem de que os operadores de serviços essenciais e os prestadores de serviços digitais estabelecem requisitos de cibersegurança e notificam incidentes.

6 – De facto, desde a entrada em vigor da Diretiva (UE) 2016/1148, foram alcançados progressos significativos no sentido de aumentar a resiliência em matéria da cibersegurança da União Europeia.

A avaliação desta diretiva revelou que a mesma funcionou como um catalisador para a abordagem institucional e regulamentar à cibersegurança na União, abrindo as portas a uma mudança significativa das mentalidades.

Não obstante esses resultados, a avaliação da Diretiva (UE) 2016/1148 revelou deficiências intrínsecas que a impedem de responder de forma eficaz a desafios contemporâneos e emergentes no domínio da cibersegurança.

7 - Neste contexto, é referido que a avaliação da aplicação da Diretiva SRI, realizada para efeitos da avaliação de impacto, identificou as seguintes questões problemáticas:

i) o baixo nível de ciber-resiliência das empresas que operam na UE;

ii) as diferenças em termos de resiliência entre Estados-Membros e setores;

iii) o baixo nível de conhecimento situacional comum e a inexistência de mecanismos de resposta conjunta a situações de crise. Por exemplo, alguns dos principais

hospitais num Estado-Membro não estão abrangidos pelo âmbito da Diretiva SRI e, como tal, não estão obrigados a aplicar as medidas de segurança nela previstas, ao passo que, noutro Estado-Membro, praticamente todos os prestadores de cuidados de saúde do país estão sujeitos aos requisitos de segurança estabelecidos nessa diretiva.

8 – Com efeito, com a rápida transformação digital e interligação da sociedade, nomeadamente nos intercâmbios transfronteiriços, as redes e os sistemas de informação passaram a ocupar um lugar central na vida quotidiana.
Essa evolução originou um alargamento do cenário de ameaças à cibersegurança, criando novos desafios que exigem respostas adaptadas, coordenadas e inovadoras em todos os Estados-Membros.
O número, a amplitude, a sofisticação, a frequência e o impacto dos incidentes de cibersegurança estão a aumentar e constituem uma grave ameaça ao funcionamento das redes e dos sistemas de informação.
Consequentemente, os ciberincidentes podem impedir o exercício de atividades económicas no mercado interno, gerar perdas financeiras, minar a confiança dos utilizadores e causar graves prejuízos à economia e à sociedade da União.
Por conseguinte, a preparação e a eficácia no domínio da cibersegurança nunca foram tão importantes para o bom funcionamento do mercado interno como agora.

9 – Deste modo, a presente iniciativa moderniza o atual quadro jurídico, tendo em conta a crescente digitalização do mercado interno nos últimos anos e a evolução do cenário de ameaças à cibersegurança. Estes dois desenvolvimentos intensificaram-se desde o início da crise da COVID-19, abordando, igualmente, várias deficiências que impediram a Diretiva SRI de concretizar todo o seu potencial.

10 – Nesta sequência, é mencionado que sendo uma iniciativa lançada no âmbito do programa para a adequação e a eficácia da regulamentação (REFIT), a presente iniciativa visa, também, reduzir os encargos regulamentares das autoridades competentes e os custos de conformidade suportados por entidades públicas e privadas.
É, pois, referido que este objetivo é alcançado, em especial, por via da eliminação da obrigação das autoridades competentes de identificarem operadores de serviços

essenciais e de uma maior harmonização dos requisitos de segurança e de notificação, a fim de facilitar a conformidade regulamentar por parte das entidades que prestam serviços transfronteiriços. Simultaneamente, serão também atribuídas novas funções às autoridades competentes, incluindo a supervisão de entidades em setores que até agora não estavam abrangidos pela Diretiva SRI.

11 – Por último, e quanto aos Direitos Fundamentais, é mencionado que a União Europeia está empenhada em assegurar elevados níveis de proteção dos direitos fundamentais. Todos os acordos de partilha de informações a título voluntário entre entidades que esta iniciativa promove seriam aplicados em ambientes de confiança, no pleno respeito das regras da União em matéria de proteção de dados, especialmente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[4].

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

a) Da Base Jurídica

A base jurídica é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, cujo objetivo consiste no estabelecimento e funcionamento do mercado interno por intermédio do reforço de medidas relativas à aproximação das regras nacionais.

b) Do Princípio da Subsidiariedade

A ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de medidas nacionais ou regionais estanques.

Acresce que, desde o início da crise da COVID-19, a economia europeia está mais dependente do que nunca das redes e dos sistemas de informação e a interligação entre setores e serviços é cada vez maior.

Uma intervenção da União que vá além das atuais medidas previstas na Diretiva SRI justifica-se principalmente pelo:

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

i) crescente caráter transfronteiriço das ameaças e dos desafios relacionados com SRI;

ii) potencial da ação da União para melhorar a eficácia e facilitar a coordenação das políticas nacionais;

iii) contributo de ações políticas concertadas e colaborativas para uma proteção eficaz dos dados e da privacidade.

Assim, atendendo a que o objetivo da presente iniciativa, a saber, atingir um elevado nível comum de cibersegurança na União, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido aos efeitos da ação considerada, ser mais bem alcançado a nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia.

É, pois, cumprido e respeitado o princípio da subsidiariedade.

c) Do Princípio da proporcionalidade

As regras propostas na presente iniciativa não excedem o necessário para atingir os objetivos específicos de forma satisfatória. A harmonização e simplificação previstas das medidas de segurança e das obrigações de notificação estão associadas a pedidos formulados pelos Estados-Membros e pelas empresas no sentido de melhorar o quadro atual.

A imposição de requisitos simplificados e coordenados para melhorar o nível de proteção é proporcionada em relação aos riscos cada vez mais elevados que a União enfrenta, incluindo aqueles que apresentam um elemento transfronteiriço.

Assim, em conformidade com o princípio da proporcionalidade consagrado no artigo 5.º do Tratado da União Europeia, a presente iniciativa não excede o necessário para alcançar esse objetivo.

É, pois, cumprido e respeitado o princípio da proporcionalidade.

PARTE III - PARECER

Em face dos considerandos expostos e atento o Relatório da comissão competente, a Comissão de Assuntos Europeus é de parecer que:

1 – A presente iniciativa não viola os princípios da subsidiariedade e da proporcionalidade, na medida em que o objetivo a alcançar será mais eficazmente atingido através de uma ação da União e o proposto não excede o necessário para tal.

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

Palácio de S. Bento, 16 de março de 2021

O Deputado Autor do Parecer	O Presidente da Comissão
(Paulo Moniz)	(Luís Capoulas Santos)

PARTE IV – ANEXO

-Relatório da Comissão de Assuntos Constitucionais, Direitos, Liberdade e Garantias.
-Nota técnica efetuada pelos serviços da Comissão de Assuntos Europeus.

ASSEMBLEIA DA REPÚBLICA

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias

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

COM (2020) 823

Relator:
Deputado José Magalhães

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

I - INTRODUÇÃO

A proposta de Diretiva ora em apreço via proceder à revisão da Diretiva (UE) 2016/1148 (Diretiva SRI) relativa à segurança das redes e da informação, que constituiu o primeiro ato legislativo à escala da União sobre cibersegurança[1]. A diretiva entrou em vigor em agosto de 2016, dando aos Estados Membros 21 meses para a sua transposição para o Direito Interno[2].

Entre a operacionalização da engrenagem pretendida e o momento presente, assistiu-se à explosão de ataques contra sistemas de informação e ao crescimento de cibercrimes. O INTERNET ORGANISED CRIME THREAT ASSESSMENT 2020[3] elaborado pela EUROPOL confirma essa tendência. A recolha de dados para o IOCTA 2020 ocorreu durante o confinamento decretado como resultado da Pandemia Covid-19. A pandemia provocou mudança significativa e inovação criminosa na área do cibercrime. Os criminosos criaram novos *modi operandi* e adaptaram os existentes para explorar a situação, atingindo novos vetores de ataque e novos grupos de vítimas.

Quanto ao pretendido reforço da cibersegurança confirmou-se que a ciber-resiliência não pode ser eficaz em toda a União se for abordada de forma díspar por via de medidas nacionais ou regionais estanques. A Diretiva SRI surgiu para colmatar esta lacuna, estabelecendo um quadro para a segurança das redes e dos sistemas de informação a nível nacional e da União. A primeira avaliação periódica da Diretiva SRI revelou várias deficiências intrínsecas, que

[1] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT

[2] Em Portugal a transposição foi feita sob forma de lei (Lei n.º 46/2018, de 13 de agosto - Regime Jurídico de Segurança do Ciberespaço), porventura para no mesmo ensejo proceder à criação de uma estrutura interinstitucional composta por representantes de departamentos governamentais, elementos das Forças Armadas e dois Deputados (Conselho Nacional para a Segurança do Ciberespaço).

[3] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

acabaram por levar a disparidades consideráveis entre os Estados-Membros em termos de capacidades, planeamento e nível de proteção, e que, ao mesmo tempo, afetam a equidade das condições de concorrência para empresas similares no mercado interno.

Razões estas que bastam para fundamentar uma proposta de significativa revisão.

II – DO OBJETO, CONTEÚDO E MOTIVAÇÃO DA INICIATIVA

1 - 2016/2021: O QUE MUDOU?

Nos termos legais a Comissão procedeu à avaliação *ex-post* da aplicação do diploma, consultou as partes interessadas e mandou proceder a avaliações de impacto da futura diretiva.

a) Avaliações *ex-post*/balanços de qualidade da legislação existente

Segundo a Comissão, as principais constatações da análise feita podem resumir-se nos termos seguintes:

·**O âmbito da Diretiva SRI revelou-se demasiado limitado** em termos dos setores abrangidos, principalmente devido: i) ao aumento da digitalização nos últimos anos e a um maior grau de interligação, ii) ao facto de já não refletir todos os setores digitalizados que prestam serviços fundamentais à economia e à sociedade como um todo.

·**A Diretiva SRI não é suficientemente clara** no que respeita ao âmbito dos operadores de serviços essenciais e as suas disposições não definem com clareza suficiente a competência nacional em relação aos prestadores de serviços digitais.[4]

·**A Diretiva SRI concedeu aos Estados-Membros uma ampla margem de apreciação no estabelecimento dos requisitos em matéria de segurança** e de notificação de incidentes aplicáveis aos operadores de serviços essenciais (a seguir designados por «OSE»). A avaliação revela que, em alguns casos, os Estados-Membros aplicaram estes requisitos de formas muito díspares, criando encargos adicionais para as empresas que operam em mais do que um Estado-Membro.

·**O regime de supervisão e execução coerciva da Diretiva SRI é ineficaz**. Por exemplo, os Estados-Membros têm mostrado grande relutância em aplicar sanções às entidades que não estabeleçam requisitos de segurança ou que não notifiquem

[4] Tal criou uma situação em que "certos tipos de entidades não foram identificadas em todos os Estados-Membros e, como tal, não estão obrigadas a adotar medidas de segurança e a notificar incidentes."

incidentes. Esta situação pode ter consequências negativas para a ciber-resiliência de entidades individuais.

·**Variam muito os recursos financeiros e humanos afetados pelos Estados-Membros ao desempenho das suas funções** (tais como a identificação ou a supervisão de OSE), pelo que são também varáveis os níveis de maturidade na gestão de riscos de cibersegurança. Esta divergência acentua ainda mais as **diferenças** entre o grau de ciber-resiliência dos Estados-Membros.

Tem consequências negativas o facto de os Estados-Membros não partilharem sistematicamente informações entre si. Tal é igualmente válido para a partilha de informações entre entidades privadas e para a relação entre as estruturas de cooperação a nível da UE e as entidades privadas.

b) Consultas realizadas

A Comissão consultou um vasto leque de partes interessadas.

Realizou-se uma consulta pública aberta, inquéritos e debates nas sessões de trabalho organizadas pela empresa Wavestone, pelo CEPE e pela ICF, que a Comissão contratou para a realização de um estudo de apoio à avaliação da Diretiva SRI.

Além disso, a Comissão estabeleceu contacto permanente com as autoridades competentes encarregadas de dar execução à Diretiva SRI.

O grupo de coordenação cobriu exaustivamente vários aspetos transversais e setoriais da execução.

Por último, durante as visitas realizadas aos países em 2019 e 2020 no âmbito da Diretiva SRI, a Comissão entrevistou 154 entidades públicas e privadas, bem como 117 autoridades competentes.

c)Recolha e utilização de conhecimentos especializados

A Comissão contratou um consórcio constituído pela Wavestone, pelo CEPE e pela ICF para a apoiar na avaliação da Diretiva SRI [5] .

Na exposição de motivos da proposta, a Comissão lembra que além de ter contactado as partes interessadas diretamente afetadas pela Diretiva SRI por meio de inquéritos específicos e sessões de trabalho, "o consórcio contratado consultou igualmente um vasto leque de peritos no domínio da cibersegurança, tais como investigadores e profissionais da indústria de cibersegurança".

c) Avaliação de impacto

[5] THE NIS DIRECTIVE AUTHOR AN OVERVIEW OF TRANSPOSITION IN EUROPE FOR OPERATORS OF ESSENTIAL SERVICES - https://tinyurl.com/1lpnlok2

A proposta é acompanhada por uma avaliação de impacto, que foi apresentada ao Comité de Controlo da Regulamentação em 23 de outubro de 2020, tendo recebido um parecer favorável, com observações, em 20 de novembro de 2020.
O CCR recomendou que fossem feitas melhorias em algumas áreas, com vista a:
1)refletir melhor o papel das repercussões transfronteiriças na análise do problema;
2)explicar melhor em que se traduziria o sucesso da iniciativa;
3)justificar mais detalhadamente a lista de opções políticas;
4)esclarecer melhor os custos das medidas propostas.

A avaliação de impacto foi revista para ter em conta estas e outras questões. Passou assim a incluir explicações mais detalhadas sobre o papel das repercussões transfronteiriças no domínio da cibersegurança, uma descrição mais clara da forma como o sucesso pode ser aferido, uma explicação mais detalhada da conceção e da lógica subjacente às diferentes opções políticas e às medidas contempladas no âmbito dessas opções, uma explicação mais detalhada dos aspetos analisados em relação ao âmbito setorial da Diretiva SRI e clarificações adicionais em matéria de custos.

A Comissão ponderou um conjunto de grandes opções políticas para melhorar o quadro jurídico no domínio da ciber-resiliência e da resposta a incidentes. Foram considerados quatro cenários:

cenário I - manutenção do status quo: A Diretiva SRI não seria alterada e não seriam adotadas quaisquer outras medidas de natureza não legislativa para resolver os problemas identificados pela avaliação da referida diretiva.
·cenário II – não seriam introduzidas quaisquer alterações a nível legislativo. Em vez disso, a Comissão emitiria recomendações e orientações (nomeadamente em matéria de identificação de operadores de serviços essenciais, requisitos de segurança, procedimentos de notificação de incidentes e supervisão), após consulta do grupo de coordenação, da Agência da UE para a Cibersegurança (ENISA) e, se pertinente, da rede de equipas de resposta a incidentes de segurança informática (CSIRT).
cenário III -Esta opção implicaria a introdução de alterações específicas na Diretiva SRI, incluindo um alargamento do seu âmbito, e muitas outras alterações que teriam por objetivo garantir certas soluções imediatas para os problemas identificados, proporcionando mais clareza e maior harmonização (tais como disposições para harmonizar os limites de identificação). No entanto, a Diretiva SRI alterada manteria os seus principais elementos constituintes, a sua abordagem e a sua fundamentação lógica.
cenário IV: Este cenário implica alterações sistémicas e estruturais da Diretiva SRI (introduzidas por uma nova diretiva) que visam uma mudança mais profunda da abordagem adotada até agora no sentido de abranger um segmento mais alargado das economias da União, mas com uma supervisão mais direcionada para grandes operadores e operadores fundamentais. Permite igualmente simplificar as

obrigações impostas às empresas e assegurar um nível mais elevado de harmonização das mesmas, criar um quadro mais eficaz para os aspetos operacionais, bem como estabelecer uma base clara para reforçar as responsabilidades partilhadas e a responsabilização das várias partes interessadas em relação a medidas de cibersegurança.

Considera a Comissão, com boa fundamentação, que a avaliação de impacto levou à conclusão de que a opção 4 é a preferida (ou seja, alterações sistémicas e estruturais do quadro para a SRI).

Em termos de eficácia, a opção preferida permite :
- alargar o âmbito da Diretiva SRI, para passar a abranger um segmento mais representativo das economias e sociedades da UE;
-simplificar os requisitos e definir melhor o quadro de supervisão e execução coerciva.

Importa ainda que sejam aprovadas medidas destinadas a melhorar as abordagens ao desenvolvimento de políticas a nível dos Estados-Membros e a *mudar o respetivo paradigma*, bem como a promover *novos quadros de gestão dos riscos* associados às relações com os fornecedores e uma *divulgação coordenada de vulnerabilidades*.

Paralelamente, a opção política preferida permite criar uma base clara para a partilha de responsabilidades e a responsabilização. Importará instituir mecanismos destinados a fomentar a confiança entre os Estados-Membros, (tanto a nível das autoridades como da indústria), para incentivar a partilha de informações e garantir uma abordagem mais operacional, como a assistência mútua e os mecanismos de análise pelos pares. Esta opção também proporcionaria um quadro para a gestão de crises a nível da UE, com base na rede operacional da UE lançada recentemente, e asseguraria um maior envolvimento da ENISA, no âmbito do seu atual mandato, na formação de um conhecimento rigoroso do estado da cibersegurança na União.

É importante notar que a opção preferida:

- implica custos adicionais em matéria de conformidade e de execução coerciva para as empresas e os Estados-Membros, mas conduzirá também a sinergias e soluções de compromissos eficientes, permitindo a uma redução dos custos, tanto para as empresas como para a sociedade[6];

- assegurará a coerência com outros atos legislativos, iniciativas e medidas políticas, nomeadamente com *lex specialis* adotada a nível setorial.

[6] Reconhece a Comissão: "Esta opção política criaria certos encargos administrativos e custos de conformidade adicionais para as autoridades dos Estados-Membros. Porém, de um modo geral, a médio e a longo prazo, traria igualmente benefícios substanciais graças a uma cooperação acrescida entre os Estados-Membros, nomeadamente a nível operacional, e incentivaria um reforço global das capacidades de cibersegurança a nível nacional e regional, por via da assistência mútua, do estabelecimento de mecanismos de análise pelos partes e de uma panorâmica mais informada das empresas-chave, bem como de uma maior interação com estas".

Mais pormenorizadamente:

·Para as entidades essenciais e importantes, o aumento do nível de preparação no domínio da cibersegurança poderá levar à minimização de potenciais perdas de receitas devido a perturbações (incluindo as resultantes de espionagem industrial) e reduzir as elevadas despesas decorrentes de medidas ad hoc de atenuação das ameaças. É provável que tais benefícios compensem os necessários custos.
·Para os Estados-Membros, poderá reduzir ainda mais o risco de aumento das despesas orçamentais com medidas ad hoc de atenuação das ameaças e de custos adicionais em caso de emergências relacionadas com incidentes de cibersegurança.
·Para os cidadãos, a resposta a incidentes de cibersegurança pode fazer diminuir as perdas de rendimento decorrentes de perturbações económicas.

O aumento do nível global de cibersegurança poderá ainda contribuir para a prevenção de riscos/danos ambientais em caso de ataque a um serviço essencial, sobretudo nos setores da energia, do fornecimento e distribuição de água e dos transportes. Se, como é desejável, a transição digital levar à criação de infraestruturas e serviços de TIC de última geração, substituindo infraestruturas pré-existentes ineficientes e menos seguras, haverá redução do número de ciberincidentes dispendiosos.

Concretamente, esta proposta de Diretiva pretende:

a) estabelecer a obrigação de os Estados-Membros adotarem uma estratégia nacional de cibersegurança e designarem autoridades nacionais competentes, pontos de contacto únicos e CSIRT[7];

b) que os Estados-Membros devem impor obrigações de gestão dos riscos de cibersegurança e de notificação às entidades qualificadas como entidades essenciais[8] e como entidades importantes[9];

[7] Equipas de resposta a incidentes de segurança informática.

[8] Entidades essenciais, públicas ou privadas, são as que operam nos setores como energia, transportes, serviços bancários, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, administração pública e espaço.

[9] Entidades importantes são as que operam nos setores como serviços postais e de estafeta, gestão de resíduos, fabrico, produção e distribuição de produtos químicos, produção, transformação e distribuição de produtos alimentares, indústria transformadora e prestadores de serviços digitais.

c) estabelecer que os Estados-Membros devem impor obrigações em matéria de partilha de informações sobre cibersegurança.

d) fixar regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações[10].

Tem, assim, razão a Comissão Europeia quando sustenta que a intervenção da UE, indo além das atuais medidas previstas na Diretiva SRI, tem justificação e principalmente: i) pelo carácter transfronteiriço do problema; ii) pelo potencial da ação da UE para melhorar e facilitar a eficácia das políticas nacionais; iii) pelo contributo de ações concertadas e colaborativas de política em matéria de SRI para uma proteção eficaz dos dados e da privacidade.

Os objetivos enumerados podem ser mais facilmente alcançados por uma ação a nível da UE do que pelos Estados-Membros agindo isoladamente.

2. O LUGAR DA SEGURANÇA NA ESTRATÉGIA PARA A TRANSFORMAÇÃO DIGITAL

A proposta de diretiva é uma componente importante de um conjunto de iniciativas em apreciação nos órgãos da UE. Uma das seis prioridades da Comissão Europeia para 2019-2024 é uma Europa preparada para a era digital, capacitando as pessoas com uma nova geração de tecnologias.

A cibersegurança é hoje uma das principais prioridades da Comissão. Em 16 de dezembro de 2020, foi apresentada a nova Estratégia da UE para a Cibersegurança[11], componente

[10] Considerando (5) da COM (2020) 823.

[11] https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391

fundamental da Comunicação Construir o futuro digital da Europa[12], do Plano de Recuperação para a Europa[13] e da Estratégia da UE para a União da Segurança[14], cujo objetivo é reforçar a resiliência coletiva da Europa contra as ciberameaças e ajudar a garantir que todos os cidadãos e as empresas possam beneficiar plenamente de serviços e ferramentas digitais seguros e fiáveis, mantendo o ciberespaço aberto estável e seguro.

A pandemia COVID 19 veio imprimir ainda maior urgência às linhas de orientação e medidas propostas.

A Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança apresentaram, em dezembro de 2020, a Estratégia de cibersegurança da UE para a década digital [15]na qual se realçou:

A "*pandemia de COVID-19 veio acelerar a digitalização dos modelos de trabalho, tendo 40 % dos trabalhadores da UE passado para o regime de teletrabalho, com prováveis efeitos permanentes na vida quotidiana. Esta mudança aumenta as vulnerabilidades perante ciberataques. Em muitos casos, os objetos conectados são entregues ao consumidor com vulnerabilidades conhecidas, ampliando assim a superfície de ataque das ciberatividades maliciosas. O panorama industrial da UE é cada vez mais digitalizado e conectado, mas tal significa igualmente que os ciberataques podem ter um impacto maior do que nunca nas indústrias e nos ecossistemas.*"

[12] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_pt

[13] https://ec.europa.eu/info/strategy/recovery-plan-europe_pt

[14] https://ec.europa.eu/commission/presscorner/detail/pt/ip_20_1379

[15] Comunicação Conjunta ao Parlamento Europeu e ao Conselho - Estratégia de cibersegurança da UE para a década digital, JOIN/2020/18 final,https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:52020JC0018

Nessa medida, concluiu-se – e bem - que a cibersegurança é essencial para construir uma Europa resiliente, ecológica e digital.

O caminho tem sido lento face ao dinamismo do mundo digital e , como se deixou assinalado, o primeiro ato legislativo horizontal a nível da UE em matéria de cibersegurança, Diretiva (UE) 2016/1148, não permitiu atingir o desejado e desejável nível comum de segurança das redes e dos sistemas de informação em toda a UE.

Também o Regulamento Cibersegurança da UE, em vigor desde 2019[16], dotou a Europa de um quadro para a certificação da cibersegurança de produtos, serviços e processos e reforçou o mandato da Agência da União Europeia para a Cibersegurança (ENISA), sem que tenha sido tenham sido plenamente alcançados os objetivos ambicionados.

O Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC)[17] foi criado em 2006. Deve mencionar-se também a Diretiva 2008/114/CE[18] relativa às infraestruturas críticas europeias em 2008, que se aplica aos setores da energia e dos transportes e vai agora ser revista. .

Por último cumpre lembrar que a iniciativa ora em análise faz parte do conjunto mais amplo de instrumentos legais existentes e iniciativas programadas a nível da União, que visam aumentar a resiliência das entidades públicas e privadas contra ameaças, destacando-se, no domínio da cibersegurança, a Diretiva (UE) 2018/1972 que estabeleceu o Código Europeu das

[16] Revogou o Regulamento (UE) n.º 526/2013

[17] Já não se encontra em vigor. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:l33260&from=PT

[18] Como supra se referiu, esta Diretiva será revista pela Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO relativa à resiliência das entidades críticas COM/2020/829 final - acessível em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0829&from=EN.

Comunicações Eletrónicas [19] e a proposta de regulamento relativo à resiliência operacional digital do setor financeiro.[20]

3. O caso português

No Programa do XXII Governo Constitucional, o 4.º Desafio Estratégico diz respeito a *"Sociedade Digital, da Criatividade e da Inovação – O futuro agora: construir uma sociedade digital"*.

No quadro do trio de Presidências do Conselho da União Europeia entre 1 de julho de 2020 e 31 de dezembro de 2021, que partilha com a Alemanha e a Eslovénia, a República Portuguesa subscreveu a inscrição, no Programa do Trio, do seguinte ponto:

"A transformação digital oferece oportunidades, mas também acarreta desafios no que diz respeito aos direitos e liberdades dos cidadãos. Por conseguinte, é essencial respeitar os direitos fundamentais e os valores comuns no processo de digitalização.

As três Presidências congratulam-se com o Livro Branco da Comissão sobre a inteligência artificial e aguardam com expectativa o seguimento que lhe será dado em todas as suas dimensões, incluindo a investigação e a inovação, as aplicações na educação, os aspetos éticos e antropocêntricos, a sua governação global, o quadro regulamentar baseado nos riscos e o aspeto da responsabilidade em matéria de inteligência artificial. Além disso, o Trio envidará esforços no sentido de uma melhor proteção das nossas sociedades contra as ciberatividades maliciosas, as ameaças híbridas e a desinformação. Procurar-se-á assegurar uma comunicação transparente, atempada e factual, a fim de reforçar a resiliência das nossas sociedades. O futuro ato relativo à resiliência operacional e à ciber-resiliência dos serviços financeiros e a revisão da Diretiva SRI serão passos úteis nesse sentido. O Trio intensificará os

[19] Cujo prazo de transposição – 21.12.20 – está ultrapassado.

[20] https://ec.europa.eu/transparency/regdoc/rep/1/2020/PT/COM-2020-59

esforços a nível europeu para estabelecer um nível mínimo obrigatório de segurança informática a que devem obedecer os dispositivos ligados à Internet".

A transposição da futura directiva permitirá avaliar como decorreu a execução do quadro jurídico em vigor e ajustar a orgânica atual à gravidade das ciberameaças que hoje se apresentam.

4. OUTROS PROCESSOS DE ESCRUTÍNIO[21]

PAÍS		DATA ESCRUTÍNIO	ESTADO DO ESCRUTÍNIO	DOCUMENTOS/OBSERVAÇÕES
Bélgica	Belgian House of Representatives	07.01.2021	Em curso	**Information on parliamentary scrutiny** On January 7th 2021, a flash message was submitted to: - the Home Affairs Committee; - the Justice Committee; - the Foreign Affairs Committee; - the Advisory Committee on European Affairs.
República Checa	Czech Senate	20.01.2021	Em curso	**Information on parliamentary scrutiny**
Finlândia	Finnish Parliament	-	Em curso	**Information on parliamentary scrutiny** Eduskunta dossier TS 96/2020 (in Finnish)
Alemanha	German Bundestag	01.02.2021	Em curso	*Information on parliamentary scrutiny:* **Committee responsible:** Committee on Internal Affairs **Committees asked for an opinion:** Committee on Education, Research and Technology Assessment; Committee on the Affairs of the European Union; Committee on Legal Affairs and Consumer

[21] Quadro da Nota Técnica dos Serviços da 1ª Comissão

PAÍS		DATA ESCRUTÍNIO	ESTADO DO ESCRUTÍNIO	DOCUMENTOS/OBSERVAÇÕES
				Protection; Committee on Transport and Digital Infrastructure; Committee on Economic Affairs and Energy; Defence Committee;
Lituânia	Seimas of the Republic of Lithuania	26.01.2021	Em curso	**Information on parliamentary scrutiny** -
Espanha	Cortes Generales	02.02.2021	Em curso	**Information on parliamentary scrutiny** On 2 February 2021, the Bureau of the Joint Committee for EU Affairs decided to appoint a rapporteur to examine the compliance of the initiative with the principle of subsidiarity.
Suécia	Swedish Parliament	20.01.2021	Em curso	**Information on parliamentary scrutiny** Referred to the Committee on Defence. The Committee will examine whether the draft is in compliance with the principle of subsidiarity. The Committee will report on its findings to the Chamber.

III – CONCLUSÕES

Em face do exposto, a Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias conclui o seguinte:

1. A presente iniciativa respeita o princípio da subsidiariedade e o princípio da proporcionalidade, na medida em que o objectivo a alcançar será mais eficazmente atingido através de uma ação da União;

2. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, dá por concluída a sua intervenção no processo de escrutínio da presente iniciativa, devendo o presente relatório, ser remetido à Comissão de Assuntos Europeus para os devidos efeitos.

IV – ANEXOS

Consta do anexo a nota técnica elaborada pelos serviços da Comissão.

Palácio de S. Bento, 16 de fevereiro de 2021.

O Deputado Relator

(José Magalhães)

O Presidente da Comissão

(Luís Marques Guedes)

COM(2020) 823

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

Data de entrada na CAE: 03-02-2021

Prazo de subsidiariedade: 17-03-2021

Índice

Elaborada por: Gonçalo Sousa Pereira
Data: 10-02-2021

I. OBJETIVO DA INICIATIVA

A presente proposta faz parte de um pacote de medidas destinadas a melhorar a resiliência e a capacidade de resposta a incidentes no domínio da cibersegurança e da proteção de infraestruturas críticas por parte das entidades públicas e privadas, das autoridades competentes e da União.

A proposta de Diretiva ora em crise, tem como propósito a revisão da Diretiva (UE) 2016/1148 (Diretiva SRI), relativa à segurança das redes e da informação, que constituiu o primeiro ato legislativo, à escala da União, sobre cibersegurança e que estabelece medidas jurídicas para melhorar o seu nível na União.

Com esta nova iniciativa, pretende-se abordar as várias deficiências que impediram a Diretiva SRI de concretizar todo o seu potencial bem como modernizar o atual quadro jurídico, tendo em conta a crescente digitalização do mercado interno nos últimos anos e a evolução do cenário de ameaças à cibersegurança, uma vez que estes dois desenvolvimentos intensificaram-se desde o início da crise da COVID-19.

Após uma avaliação de impacto sobre a revisão à Diretiva SRI (Diretiva (UE) 2016/1148), identificaram-se as seguintes questões problemáticas: 1) o baixo nível de ciber-resiliência das empresas que operam na UE; 2) diferenças em termos de resiliência entre Estados-Membros e setores; 3) baixo nível de conhecimento situacional comum e a inexistência de mecanismos de resposta conjunta a situações de crise.

Nessa medida, e considerando os problemas detetados, a proposta em análise visa três objetivos gerais:

1. Aumentar o nível de ciber-resiliência de um conjunto abrangente de empresas que operam na União Europeia em todos os setores importantes, estabelecendo regras que assegurem que todas as entidades públicas e privadas em todo o mercado interno, que desempenham funções importantes para a economia e a sociedade no seu conjunto, sejam obrigadas a tomar medidas de cibersegurança adequadas;
2. Reduzir as diferenças em termos de resiliência no mercado interno nos setores já abrangidos pela Diretiva (UE) 2016/1148, por via de uma maior harmonização: a) do âmbito de aplicação efetivo, b) dos requisitos em matéria de segurança e de comunicação de incidentes, b) das

disposições que regem a supervisão e a execução coerciva a nível nacional, d) das capacidades das autoridades competentes dos Estados-Membros;
3. Melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta, tomando medidas para aumentar o nível de confiança entre as autoridades competentes, partilhando mais informações, e estabelecendo regras e procedimentos em caso de um incidente ou crise em grande escala.[1]

Concretamente, esta proposta de Diretiva pretende:
a) estabelecer a obrigação de os Estados-Membros adotarem uma estratégia nacional de cibersegurança e designarem autoridades nacionais competentes, pontos de contacto únicos e CSIRT[2];
b) que os Estados-Membros devem impor obrigações de gestão dos riscos de cibersegurança e de notificação às entidades qualificadas como entidades essenciais[3] e como entidades importantes[4];
c) estabelecer que os Estados-Membros devem impor obrigações em matéria de partilha de informações sobre cibersegurança.

Acresce que, esta proposta de Diretiva visa igualmente eliminar as divergências entre os Estados-Membros, quanto os requisitos de cibersegurança impostos, estabelecendo regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações[5]. De realçar, no entanto, que esta proposta de Diretiva não afeta a possibilidade de cada Estado-Membro tomar as medidas necessárias para garantir a proteção dos interesses essenciais da sua própria segurança, salvaguardar a ordem e a segurança públicas e permitir a investigação, a deteção e a repressão de infrações penais, em conformidade com o direito da União[6].

[1] Relatório do Resumo da Avaliação de impacto que acompanha 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 (SWD(2020) 344 final).
[2] Equipas de resposta a incidentes de segurança informática.
[3] Entidades essenciais, públicas ou privadas, são as que operam nos setores como energia, transportes, serviços bancários, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, administração pública e espaço.
[4] Entidades importantes são as que operam nos setores como serviços postais e de estafeta, gestão de resíduos, fabrico, produção e distribuição de produtos químicos, produção, transformação e distribuição de produtos alimentares, indústria transformadora e prestadores de serviços digitais.
[5] Considerando (5) da COM (2020) 823.
[6] Considerando (6) da COM (2020) 823.

II. ENQUADRAMENTO LEGAL E DOUTRINÁRIO

A presente proposta tem por base jurídica o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE) que determina que a UE deve adotar medidas de aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros, que tenham por objeto o estabelecimento e o funcionamento do mercado interno na UE.

Uma das seis prioridades da Comissão Europeia para 2019-2024 é uma Europa preparada para a era digital, capacitando as pessoas com uma nova geração de tecnologias. A estratégia digital da UE pretende fazer com que a transformação digital beneficie as pessoas e empresas europeias, contribuindo, simultaneamente, para que a UE possa alcançar o seu objetivo de uma Europa com um impacto neutro no clima até 2050. A abordagem europeia basear-se-á em três pilares principais, a fim de que a Europa possa tirar partido da oportunidade de dar aos cidadãos, empresas e governos a possibilidade de exercerem controlo sobre a transformação digital.

Numa Europa digital e conectada, a cibersegurança é uma das principais prioridades da Comissão. Em 16 de dezembro de 2020, a Comissão apresentou a nova Estratégia da UE para a Cibersegurança, componente fundamental da Comunicação Construir o futuro digital da Europa, do Plano de Recuperação para a Europa e da Estratégia da UE para a União da Segurança, cujo objetivo é reforçar a resiliência coletiva da Europa contra as ciberameaças e ajudar a garantir que todos os cidadãos e as empresas possam beneficiar plenamente de serviços e ferramentas digitais seguros e fiáveis, mantendo o ciberespaço aberto estável e seguro.

Com efeito, a Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, em dezembro de 2020, apresentaram a Estratégia de cibersegurança da UE para a década digital com a apresentação de uma Comunicação Conjunta ao Parlamento Europeu e ao Conselho (JOIN(2020) 18), na qual se realçou que a "*pandemia de COVID-19 veio acelerar a digitalização dos modelos de trabalho, tendo 40 % dos trabalhadores da UE passado para o regime de teletrabalho, com prováveis efeitos permanentes na vida quotidiana. Esta mudança aumenta as vulnerabilidades perante ciberataques. Em muitos casos, os objetos conectados são entregues ao consumidor com vulnerabilidades conhecidas, ampliando assim a superfície de ataque das ciberatividades maliciosas. O panorama industrial da UE é cada vez mais digitalizado e conectado, mas tal significa igualmente que os ciberataques podem ter um impacto*

maior do que nunca nas indústrias e nos ecossistemas." Nessa medida, concluiu-se que a cibersegurança afigurava-se essencial para construir uma Europa resiliente, ecológica e digital.

O primeiro ato legislativo a nível da UE em matéria de cibersegurança, Diretiva (UE) 2016/1148, contribuiu para alcançar um elevado nível comum de segurança das redes e dos sistemas de informação em toda a UE.

Já o Regulamento Cibersegurança da UE, em vigor desde 2019[7], dotou a Europa de um quadro para a certificação da cibersegurança de produtos, serviços e processos e reforçou o mandato da Agência da União Europeia para a Cibersegurança (ENISA).

Com efeito, a UE tem vindo a reconhecer a necessidade de assegurar a resiliência das infraestruturas críticas que prestam serviços essenciais para o bom funcionamento do mercado interno e para a vida e os meios de subsistência dos cidadãos europeus. Por este motivo, a UE criou o Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC)[8] em 2006 e adotou a Diretiva 2008/114/CE[9] relativa às infraestruturas críticas europeias em 2008, que se aplica aos setores da energia e dos transportes.

De referir ainda que, a iniciativa ora em análise, integra-se num conjunto mais amplo de instrumentos legais existentes e iniciativas programadas a nível da União, que visam aumentar a resiliência das entidades públicas e privadas contra ameaças, destacando-se, no domínio da cibersegurança, a Diretiva (UE) 2018/1972 que estabelece o Código Europeu das Comunicações Eletrónicas e a proposta de regulamento relativo à resiliência operacional digital do setor financeiro [COM(2020) 595 final][10], que será considerado uma lex specialis em relação à presente proposta, após a entrada em vigor de ambos os atos. No domínio da segurança física, completa a proposta de diretiva relativa à resiliência de entidades críticas (COM (2020) 829), que revê a Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (Diretiva ICE), que estabelece um processo à escala da União para identificar e designar infraestruturas críticas europeias e define uma abordagem para melhorar a sua proteção.

[7] Revogou o Regulamento (UE) n.º 526/2013
[8] Já não se encontra em vigor.
[9] Como supra se referiu, esta Diretiva será revista pela COM (2020) 829.
[10] Iniciativa que se encontra atualmente em fase de escrutínio por parte da Comissão de Assuntos Europeus.

III. ANTECEDENTES

- Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;
- Regulamento de Execução (UE) 2018/151 da Comissão, de 30 de janeiro de 2018, que estabelece normas de execução da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho;
- Comunicação da Comissão ao Parlamento Europeu e ao Conselho: «Tirar o maior partido da SIR — Para uma execução efetiva da Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União» [COM(2017) 476 final 2 de 4 de outubro de 2017];
- Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala;
- Comunicação conjunta ao Parlamento Europeu e ao Conselho — Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE [JOIN(2017) 450 final de 13 de setembro de 2017];
- Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da EU;
- Decisão do Conselho de 23 de setembro de 2013 (2013/488/UE) relativa às regras de segurança aplicáveis à proteção das informações classificadas da EU;
- Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho;
- Regulamento (UE) n.º 526/2013[11] do Parlamento Europeu e do Conselho, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004;
- Comunicação conjunta da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões «Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido» [JOIN(2013) 1 final de 7 de fevereiro de 2013];

[11] Já não se encontra em vigor.

IV. INICIATIVAS EUROPEIAS SOBRE MATÉRIA RELACIONADA

- Diretiva (UE) 2018/1972 que estabelece o Código Europeu das Comunicações Eletrónicas;
- COM(2020) 595 final proposta de regulamento relativo à resiliência operacional digital do setor financeiro;
- Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias;
- COM (2020) 829 proposta de diretiva relativa à resiliência de entidades críticas;
- Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança);

V. POSIÇÃO DO GOVERNO (QUANDO DISPONÍVEL) E CONTEXTO NACIONAL

No Programa do XXII Governo Constitucional, o 4.º Desafio Estratégico diz respeito a "*Sociedade Digital, da Criatividade e da Inovação – O futuro agora: construir uma sociedade digital*".

Ademais, a República portuguesa, através do seu Governo e no quadro do trio de Presidências do Conselho da União Europeia entre 1 de julho de 2020 e 31 de dezembro de 2021, que partilha com a Alemanha e a Eslovénia, anuiu com a inscrição, no Programa do Trio, do seguinte texto:

A transformação digital oferece oportunidades, mas também acarreta desafios no que diz respeito aos direitos e liberdades dos cidadãos. Por conseguinte, é essencial respeitar os direitos fundamentais e os valores comuns no processo de digitalização.

As três Presidências congratulam-se com o Livro Branco da Comissão sobre a inteligência artificial e aguardam com expectativa o seguimento que lhe será dado em todas as suas dimensões, incluindo a investigação e a inovação, as aplicações na educação, os aspetos éticos e antropocêntricos, a sua governação global, o quadro regulamentar baseado nos riscos e o aspeto da responsabilidade em matéria de inteligência artificial. Além disso, o Trio envidará esforços no sentido de uma melhor proteção das nossas sociedades contra as ciberatividades maliciosas, as ameaças híbridas e a desinformação. Procurar-se-á assegurar uma comunicação transparente, atempada e factual, a fim de reforçar a resiliência das nossas sociedades. O futuro ato relativo à resiliência operacional e à ciber-resiliência dos serviços financeiros e a revisão da Diretiva SRI

serão passos úteis nesse sentido. O Trio intensificará os esforços a nível europeu para estabelecer um nível mínimo obrigatório de segurança informática a que devem obedecer os dispositivos ligados à Internet.

VI. POSIÇÃO DE OUTROS ESTADOS-MEMBROS (IPEX)

PAÍS		DATA ESCRUTÍNIO	ESTADO DO ESCRUTÍNIO	DOCUMENTOS/OBSERVAÇÕES
Bélgica	Belgian House of Representatives	07.01.2021	Em curso	**Information on parliamentary scrutiny** On January 7th 2021, a flash message was submitted to: - the Home Affairs Committee; - the Justice Committee; - the Foreign Affairs Committee; - the Advisory Committee on European Affairs.
República Checa	Czech Senate	20.01.2021	Em curso	**Information on parliamentary scrutiny** -
Finlândia	Finnish Parliament	-	Em curso	**Information on parliamentary scrutiny** Eduskunta dossier TS 96/2020 (in Finnish)
Alemanha	German Bundestag	01.02.2021	Em curso	**Information on parliamentary scrutiny:** **Committee responsible:** Committee on Internal Affairs **Committees asked for an opinion:** Committee on Education, Research and Technology Assessment; Committee on the Affairs of the European Union; Committee on Legal Affairs and Consumer Protection; Committee on Transport and Digital Infrastructure; Committee on Economic Affairs and Energy; Defence Committee;
Lituânia	Seimas of the Republic of Lithuania	26.01.2021	Em curso	**Information on parliamentary scrutiny** -
Espanha	Cortes Generales	02.02.2021	Em curso	**Information on parliamentary scrutiny** On 2 February 2021, the Bureau of the Joint Committee for EU Affairs decided

PAÍS		DATA ESCRUTÍNIO	ESTADO DO ESCRUTÍNIO	DOCUMENTOS/OBSERVAÇÕES
				to appoint a rapporteur to examine the compliance of the initiative with the principle of subsidiarity.
Suécia	Swedish Parliament	20.01.2021	Em curso	**Information on parliamentary scrutiny** Referred to the Committee on Defence. The Committee will examine whether the draft is in compliance with the principle of subsidiarity. The Committee will report on its findings to the Chamber.