

MESTRADO EM DIREITO
CIÊNCIAS JURÍDICO-POLÍTICAS

**CIBERSEGURANÇA NA UNIÃO EUROPEIA
E OS DESAFIOS PARA A SUA EFICÁCIA**
PERSPETIVAS, PANORAMA ESTRATÉGICO E
INSTRUMENTOS JURÍDICOS

GABRIELLA FRANÇA HERMENEGILDO

M
2020

Gabriella França Hermenegildo. CIBERSEGURANÇA NA
UNIÃO EUROPEIA E OS DESAFIOS PARA A SUA EFICÁCIA

M.FDUP 2020

**CIBERSEGURANÇA NA UNIÃO EUROPEIA E OS
DESAFIOS PARA A SUA EFICÁCIA**
PERSPETIVAS, PANORAMA ESTRATÉGICO E INSTRUMENTOS
JURÍDICOS

Gabriella França Hermenegildo.

FACULDADE DE DIREITO



Cibersegurança na União Europeia e os Desafios para a sua Eficácia

Perspetivas, Panorama Estratégico e Instrumentos Jurídicos

Gabriella França Hermenegildo

Dissertação elaborada sob orientação da Professora
Doutora Maria da Graça Jerónimo Enes Ferreira
conducente à obtenção do grau de Mestre em Direito
na Área de Especialização em Ciências Jurídico
Políticas

Faculdade de Direito da Universidade do Porto

Porto, 2020

RESUMO: Os desafios para a construção de um espaço digital seguro a nível da UE demandam uma complexidade de ações para garantir a eficácia das medidas de cibersegurança adotadas, dada a transversalidade desta matéria. A ciberdependência é um caminho sem volta, e por este motivo, o combate as ciberameaças passaram a fazer parte das prioridades da agenda política da UE. Devido ao aumento da preocupação com as ameaças híbridas, os ativos que carregam maior grau de importância na estratégia atual são as infraestruturas críticas, essenciais para o funcionamento da sociedade, e a construção de ciber-resiliência, elemento fundamental para a confiança e segurança do mercado interno e para o aproveitamento dos benefícios trazidos pelas transformações digitais. Desta forma, o presente trabalho se propõe a analisar o panorama estratégico da UE neste domínio, com o objetivo de verificar os principais desafios para a eficácia das medidas de cibersegurança, a partir da perspectiva adotada pela UE. Para isso, serão introduzidas noções de cibersegurança, de ciberameaça e de ferramentas de avaliação de riscos e ameaças, e, levantadas questões sobre a falta de padronização terminológica e de abordagens, associadas às diferentes perspectivas do enfoque dado a esta matéria na tomada de decisão. Posteriormente, será analisado o caminho escolhido pela UE e as diferentes perspectivas para lidar com o tema ao longo do tempo, para, em seguida, abordar o panorama geral da estratégia adotada e os principais instrumentos jurídicos vigentes. Ao final serão apresentados os principais desafios para a eficácia da política de cibersegurança a partir da perspectiva adotada pela UE para lidar com esta temática, com a finalidade de levantar algumas questões relacionadas à adequação do panorama estratégico adotado em relação aos objetivos traçados.

Palavras-chave: Direito e Cibersegurança, Cibersegurança na União Europeia, Ciberameaças na UE, Estratégia de Cibersegurança da UE, Eficácia da Cibersegurança.

ABSTRACT: The challenges for building a secure cyberspace at EU's level require a complexity of actions to ensure the effectiveness of cybersecurity measures adopted, given the cross-cutting nature of this matter. Cyberdependence is an irreversible path, therefore, because of that, combating cyber threats has become a high priority on the EU's political agenda. Due to the growing concerns about hybrid threats, the assets that carry the greatest degree of importance in the current strategy are critical infrastructures, which are essential for the functioning of society, and the construction of cyber-resilience, fundamental element for the confidence and security of the internal market and to take advantage of the benefits brought by the digital transformations. In this way, the present work proposes to analyze the current strategic overview of the EU in this field, with the objective of examine the main challenges for the effectiveness of cybersecurity measures, considering the perspective adopted by the EU. For this purpose, the concepts of cybersecurity, cyber threat and risk and threat assessment tools will be analysed. Also some issues will be raised regarding the lack of terminological and approaches standardization, associated with the different perspectives of the focus given to this matter in the decision making process. Subsequently, it will be verified the path chosen by the EU and the different approaches to deal with the cybersecurity problem along the time, and next, it will be addressed the general situation of the adopted strategy and the main legal instruments in force. At the end, will be presented the challenges for the effectiveness of the cybersecurity policy from the perspective adopted by the EU to deal with this issue, in order to raise some questions related to the adequacy of the strategical approach adopted in relation to the outlined objectives.

Keywords: Law and Cybersecurity, Cybersecurity in the European Union, Cyber Threats in the EU, Cybersecurity Strategy in the EU, Cybersecurity Effectiveness.

Lista de Tabelas e Figuras

Tabela 1 – Domínios de atuação na proteção do ciberespaço.....	7
Tabela 2 – Fases das abordagens e perspectivas da UE para a Cibersegurança.....	26
Figura 1 – Sistema simplificado de avaliação de ameaças.....	13

Lista de Siglas e Abreviaturas

CERT	Centro de Estudos para Resposta e Tratamento de Incidentes
CSIRT	Equipas de Resposta a Incidentes de Segurança Informática
EC3	Centro Europeu da Cibercriminalidade
EM	Estado Membro
ENISA	Agência da União Europeia para a Cibersegurança
EUROPOL	Serviço Europeu de Polícia (Agência)
NATO	Organização do Tratado do Atlântico Norte
OCDE	Organização de Cooperação e de Desenvolvimento Económicos
OSE	Operadores de Serviços Essenciais
PSD	Prestadores de Serviços Digitais
SRI	Segurança das Redes e Sistemas de Informação
TCE	Tribunal de Contas Europeu
TFUE	Tratado sobre o Funcionamento da União Europeia
TI	Tecnologias da Informação
TIC	Tecnologias da Informação e da Comunicação
TUE	Tratado da União Europeia
UE	União Europeia
UIT	União Internacional de Telecomunicações

ÍNDICE

1 INTRODUÇÃO.....	1
2 CIBERSEGURANÇA: TERMINOLOGIA E ENQUADRAMENTO.....	4
2.1 As Ciberameaças.....	9
2.2 Impactos das Ciberameaças na UE.....	14
3 A UE EM MATÉRIA DE CIBERSEGURANÇA.....	17
3.1 O Caminho Escolhido pela UE.....	18
3.2 Panorama Geral da Cibersegurança na EU.....	27
4 PRINCIPAIS INSTRUMENTOS JURÍDICOS.....	31
4.1 A Diretiva SRI.....	31
4.2 O Regulamento da Cibersegurança da UE.....	35
4.3 Base Jurídica, Subsidiariedade e Proporcionalidade.....	37
5 DESAFIOS PARA EFICÁCIA DA CIBERSEGURANÇA NA UE.....	42
6 CONCLUSÃO.....	53
REFERÊNCIAS.....	55

1 INTRODUÇÃO

A Cibersegurança é um tema que tem ocupado grande espaço nos debates académicos multidisciplinares devido à crescente digitalização da vida e à necessidade de utilização segura de toda informação que transita na dimensão virtual. As infraestruturas que dão suporte a esta nova dinâmica da sociedade impõem novos desafios para a segurança dos dados e informações, uma vez que a conectividade é progressivamente ampliada e, com ela, os riscos e ameaças a toda informação que transita no espaço cibernético. De acordo com o glossário do CNCS¹, Cibersegurança é:

O conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Desse modo, a Cibersegurança, é um termo amplamente utilizado para designar todas as medidas e garantias necessárias com o objetivo de proteger o conjunto de dispositivos, equipamentos, serviços e dados associados a esses sistemas (que vão desde aparelhos telefónicos de uso pessoal, até centrais de geração de energia elétrica, ou mesmo hospitais). Contudo, a cibersegurança não se restringe às tecnologias destinadas a proteger os equipamentos e dados em si, mas também a um conjunto de políticas e estratégias para lidar com a ocorrência de ataques e danos causados por atividades ilícitas que envolvam a utilização de meios informáticos. Além disso, na ocorrência de ciberincidentes, também envolve a capacidade de recuperação dos sistemas afetados e de uma resposta eficaz. Nesse sentido, o processo de construção de um ambiente ciberseguro se torna, particularmente, desafiador na medida em que um número crescente de equipamentos passam a ser ciberdependentes e interconectados, o que aumenta a preocupação com as consequências de incidentes a nível nacional, europeu e até mesmo mundial.

As ameaças relacionadas aos ciberataques e seus potenciais impactos no funcionamento da sociedade entraram na agenda da União Europeia e assumiram elevada importância na elaboração de políticas para a garantia de um nível mais elevado de cibersegurança. De acordo com a Estratégia da UE para cibersegurança, lançada em 2013, o objetivo estratégico geral da UE é o de se tornar o ambiente em linha mais seguro do mundo². No entanto, o ciberespaço

¹ Centro Nacional de Cibersegurança – CNCS – Portugal. **Glossário do Curso Cidadão Ciberseguro**. Disponível em: <https://lms.nau.edu.pt/courses/course-v1:CNCS+CC101+2018_T1/about>. 2018. Acesso em Dez.2019.

² COMUNICAÇÃO CONJUNTA JOIN(2013) 1 final - **Estratégia da União Europeia para a cibersegurança**: Um ciberespaço aberto, seguro e protegido. Bruxelas, 7.2.2013. Item 1.1. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52013JC0001>>. Acesso em Fev.2020.

surge como um novo *locus* de atuação que transcende a conceção de governação tradicional para a criação de políticas e regulamentação, onde a segurança, a privacidade, a soberania e as fronteiras assumem uma nova dimensão³. Neste sentido, ao estabelecer uma estratégia a nível da UE, deve-se considerar a natureza complexa e multilateral da cibersegurança, altamente dependente de cooperação institucional e de confiança mútua a nível nacional e internacional, do setor público e privado.

Por este motivo, é pertinente avaliar a adequação da estratégia da UE neste campo que está em constante transformação. Na comunicação de 2013 sobre a estratégia da União Europeia para a Cibersegurança, foi ressaltada sua importância para a concretização do mercado único digital assim como a compreensão de que os benefícios trazidos pela digitalização vêm acompanhados de vulnerabilidades, com destaque para a crescente ocorrência de incidentes:

Os incidentes de cibersegurança, intencionais ou acidentais, estão a aumentar a um ritmo alarmante e poderão perturbar a prestação de serviços essenciais que consideramos garantidos, como a água, os cuidados de saúde, a eletricidade ou os serviços móveis. As ameaças podem ter origens diversas — nomeadamente ataques criminosos, politicamente motivados, terroristas ou patrocinados por Estados, assim como catástrofes naturais e erros involuntários.⁴

Uma vez que os riscos e ameaças são transfronteiriços, os desafios para a construção de um espaço digital seguro a nível da UE demandam uma complexidade de ações para garantir a eficácia das medidas de cibersegurança adotadas dada a transversalidade desta matéria (referente aos meios necessários para avaliação dos riscos e alcance dos objetivos), o que abrange além da segurança das redes e sistemas de informação propriamente dita, a proteção de infraestruturas críticas para o funcionamento da sociedade, a ciberdefesa, a cibercriminalidade e a desinformação⁵. Desta forma, o presente trabalho se propõe a uma análise da estratégia adotada pela União Europeia em matéria de cibersegurança até o presente momento, bem como avaliar os principais instrumentos jurídicos vigentes neste domínio, com o objetivo de aferir a adequação das medidas da UE em relação às novas ameaças potenciadas pelo ciberespaço.

Para isso, como ponto de partida, será feita uma elucidação terminológica sobre o termo cibersegurança, seus desdobramentos e perspetivas quanto ao enfoque dado a esta matéria do ponto de vista da tomada de decisão, o que servirá de recorte da política e das motivações

³ BELÁZ, Annamaria. (2019). *The changing role of the EU in cybersecurity*. 1. 17-30. Biztonságtudományi Szemle Safety and Security Sciences Review 2019, I. évf. 1-2. Szám. Disponível em: <https://www.researchgate.net/publication/334173763>. Acesso em Jun.2020.

⁴ JOIN(2013) 1 final. Op.cit. Item 1.1.

⁵ TRIBUNAL DE CONTAS EUROPEU - TCE. **Documento de análise n.º 02/2019**: Desafios à eficácia da política de cibersegurança da UE. 2019. Disponível em: <https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=49416>. Acesso em Jan.2020.

estratégicas da UE que se pretende analisar. Em seguida, será feita uma breve explicação sobre os tipos de ameaças e uma noção geral dos impactos relativos aos riscos associados a cibersegurança para a UE. Posteriormente, será analisado o caminho escolhido pela UE e abordados alguns instrumentos e medidas complementares com o objetivo de fornecer um panorama geral da estratégia adotada em matéria de cibersegurança, bem como serão analisados os principais instrumentos jurídicos vigentes, que são:

1. a Diretiva (UE) 2016/1148⁶ sobre a segurança das redes e da informação, SRI, que estabelece a adoção de uma estratégia de cibersegurança pelos Estados-Membros (EM) e a designação de uma autoridade competente em cada EM para lidar com esta matéria específica, bem como institui requisitos de segurança e de notificação de incidentes para operadores que prestam serviços essenciais (em setores críticos como a energia, os transportes, a saúde e as finanças) e pelos prestadores de serviços digitais;
2. o Regulamento (UE) 2019/881⁷, de Cibersegurança, que cria um sistema de certificação europeu e um mandato permanente para a ENISA com a reestruturação de suas atribuições⁸.

Na última parte, será feito levantamento dos principais desafios para a eficácia da política de cibersegurança a partir da perspectiva adotada pela UE e colocar algumas questões relacionadas à adequação do panorama estratégico em relação aos objetivos traçados. O objetivo geral deste trabalho é o de transmitir a noção de cibersegurança e de ciberameaças, e buscar perceber a perspectiva adotada pela UE no processo de desenvolvimento das estratégias para lidar com essas questões, para, ao final, levantar as problemáticas para a eficácia das medidas de uma maneira geral e, a partir disso, compreender as soluções atualmente consagradas e perspetivar as soluções futuras. Dessa forma, este trabalho tem o intuito de servir como uma base crítica para compreensão do tema e de como ele se insere no contexto atual, com vistas a contribuir com a produção académica nesta matéria dada a sua relevância e atualidade, e também, dada à carência de pesquisas em língua portuguesa relacionadas ao tema.

⁶ DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 – DIRETIVA SRI - Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

⁷ REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEU E DO CONSELHO de 17 de abril de 2019 – REGULAMENTO DA CIBERSEGURANÇA - Relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013.

⁸ ENISA (AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA) Disponível em: <https://www.enisa.europa.eu/>. Acesso em Jan.2020.

2 CIBERSEGURANÇA: TERMINOLOGIA E ENQUADRAMENTO

Não existe um padrão universalmente reconhecido para conceituar o termo ‘Cibersegurança’. Para compreender a origem do termo, deve fazer-se uma distinção entre o prefixo ‘ciber~cyber’ e a raiz ‘segurança’. O termo ‘cyber’, conforme explica Dunn (2005, p. 3), deriva da palavra ‘cybernetics’ que possuía o sentido geral de “*through the use of a computer*” e é frequentemente usado como sinônimo de ‘ciberespaço~cyberspace’. O autor explica que o termo foi cunhado por William Gibson e se popularizou em seu livro ‘Neuromancer’, e foi utilizado pela primeira vez para se referir à Internet em 1991. Para Dunn, o termo ‘ciberespaço’ conota:

The fusion of all communication networks, databases, and sources of information into a huge, tangled, and diverse blanket of electronic interchange. Thus, a “network ecosystem” is created, a place that is not part of the normal, physical world. It is “virtual”, a “bioelectronic environment” that is literally universal, that exists wherever there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves. This environment is inhabited by knowledge, existing in electronic form. Virtually any element of cyberspace can be at risk, and the degree of interconnection of those elements can make it difficult to determine the extent of the security measures needed. (DUNN, 2005, p. 3)

Apesar de a palavra ‘segurança’ possuir uma vasta gama de significados, segundo Dunn (2005, p. 3), em geral, é sinônimo de “estar seguro”, mas tecnicamente significa não apenas que algo é seguro, mas que está protegido/ assegurado. A junção dos termos que formam a palavra cibersegurança traz a noção de tornar o ciberespaço seguro de ameaças, ou seja, livre de ‘ciberameaças~ cyber-threats’. Para o autor, a noção de ciberameaças “*is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors*”.

De acordo com o CNCS (supracitado), no sentido lato, a cibersegurança se refere às medidas necessárias para proteger os sistemas informáticos e os utilizadores de acessos não autorizados, ataques e danos, de forma a assegurar a confidencialidade, a integridade e a disponibilidade dos dados, informações, redes e equipamentos interconectados. Dunn (2005, p.4) explica que a confidencialidade refere-se à proteção das informações contra o acesso e divulgação a terceiros não autorizados; a integridade refere-se à proteção contra alteração ou dano provocado por partes não autorizadas; e a disponibilidade significa que a informação e os equipamentos devem estar disponíveis para as partes autorizadas quando solicitadas.

Para Beláz, (2019, p. 28) “*cybersecurity is an activity, ability or capability to protect information and communications systems and the data/information contained therein*”. Já no dicionário ‘Infopédia’, o termo cibersegurança aparece como o “estado de proteção contra

ciberataques ou qualquer atividade criminosa feita através de redes informáticas”⁹. Porém, mantendo a noção ampla, importa fazer referência à definição que consta no Regulamento da Cibersegurança de 2019 (Artigo 2º, n. 1), correspondente à perspectiva atual da UE, como: “todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas”. Por outro lado, de acordo com a União Internacional de Telecomunicações (UIT) – a agência das Nações Unidas que trata das questões sobre tecnologias da informação e comunicação – no sentido de estabelecer padronizações, medidas e intercâmbio de informações neste setor, define cibersegurança como:

*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.*¹⁰

Apesar do conceito amplo e genérico da UE, pode-se verificar que o conceito da UIT, embora também seja amplo, é mais detalhado e adequado. Assim, a cibersegurança é um termo “guarda-chuva” que abrange **todas** as medidas destinadas a uma utilização segura do ciberespaço de forma a evitar danos aos sistemas informáticos e ativos conexos que sejam provocados por atividades ilícitas ou incidentais através da utilização de tecnologias digitais. A partir desta noção temos que tais atividades ilícitas vêm acompanhadas de novos tipos de ciberconflituidade que trazem à luz a necessidade da instituição de contramedidas de cibersegurança em diferentes domínios de atuação associados à segurança e à defesa a nível nacional, regional e mundial.

Porém, a problemática da terminologia ‘cibersegurança’ reside em como a mesma é percebida e definida por diferentes atores (*stakeholders*) com interesses divergentes, pois como inexiste um conceito *standard*, pode significar coisas diferentes para países, organizações, especialistas de TIC, cidadãos, etc. Van der Meulen, A Jo e Soesanto (2015, p. 20) explicam que para os atores da área de segurança da informação “*the uptake of the term cybersecurity is an undesirable development brought about by policymakers who have little knowledge of the subject matter*”. Isto porque existe uma desconexão entre os atores responsáveis pela elaboração de políticas públicas e a comunidade tecnológica, onde nesta, os termos ‘segurança da

⁹ *cibersegurança* in Dicionário infopédia da Língua Portuguesa [em linha]. Porto: Porto Editora, 2003-2020. Disponível na Internet: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/ciberseguranca>. Acesso em Mai.2020.

¹⁰ Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity. Disponível em: <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>. Acesso em Mai.2020.

informação' e 'segurança das redes' são mais comuns. Os autores também revelam que a falta de definição “*especially in connection to its transformation into a national security concern, may lead to ‘drastic solutions’ like network monitoring as opposed to ‘practical solutions’ that are more respectful of citizens’ rights*”. Além disso, a falta de consenso e a adoção de um conceito “guarda-chuva” para a cibersegurança, de acordo com o que frisa Silva (2013, p. 3-4), “não somente debilita o valor e a aplicação do termo, mas também abre possibilidades para que a 'segurança cibernética' seja usada para fins múltiplos e indiscriminados”.

Ou seja, a adoção de um conceito muito aberto e abrangente repercute na forma de alocação de responsabilidades entre os *stakeholders* e na elaboração de um plano de ação coerente. No atual estágio de desenvolvimento tecnológico de ampliação da ciberdependência, onde a cibersegurança passa a compor uma prioridade nas estratégias políticas, com o envolvimento de diversos *stakeholders* com interesses distintos, e até mesmo conflituosos, a falta de uma definição comumente aceite, conforme frisa Van der Meulen, A Jo e Soesanto (2015, p. 25), também impede o estabelecimento de um sistema universalmente aceite de categorização de ameaças, pois leva à variabilidade do que deve ser incluído nas avaliações de ameaças potenciais, o que será visto mais adiante neste trabalho.

A partir desta noção geral, importa compreender que a cibersegurança entrou na agenda da UE através do que Dunn denomina de ‘*threat politics*’ que significa: “*a political process by which threats are introduced to and removed from the political agenda, or by which the face of threats on the political agenda is altered*”¹¹. Ou seja, tomando em consideração a perspectiva da UE sobre as ciberameaças como resultado de um processo político, podemos caracterizar o enfoque e o peso das contramedidas e estratégias adotadas.

Santos, Bravo e Nunes (2012, p. 164) informam a existência de **três domínios de atuação** (entendidos como a prossecução de um objetivo por um conjunto de meios técnicos, humanos e legais) face ao fenómeno das ciberameaças: o da proteção simples, o da prossecução criminal e o da defesa de Estado. Os autores explicam que cada domínio corresponde a uma perspectiva em relação as ciberameaças “a qual determina diferenças relevantes relativas ao que significa cibersegurança, aos objetivos a atingir, aos principais atores envolvidos, aos meios técnicos disponíveis e ao enquadramento jurídico aplicável” (ver Tabela 1 abaixo).

¹¹ Dunn, M. (2005, p.2) - *A Comparative Analysis of Cybersecurity Initiatives Worldwide*. Technical report, ITU - WSIS Thematic Meeting on Cybersecurity.

	Proteção Simples	Prosecução criminal	Defesa do Estado
Caracterização	Os ciberataques são vistos como ameaças à disponibilidade, integridade e confidencialidade da informação e de outros ativos.	Os ciberataques são vistos como atos criminalmente relevantes.	Os ciberataques são vistos como um ato de Guerra, pondo em risco a existência do Estado.
Objetivos	Proteger potenciais alvos contra ciberataques.	Prevenir crimes e identificar e condenar os responsáveis.	Eliminar uma ameaça que coloque em causa a Soberania Nacional ou ganhar uma vantagem competitiva sobre outro Estado.
Aspetos legais e constitucionais	Salvaguarda dos direitos individuais e da privacidade dos cidadãos.	Atuação dentro do quadro da legislação aplicável e segundo as regras do sistema judicial	Atuação sujeita à Constituição da República, Lei do Estado de Sítio e do Estado de Guerra, bem como ao Direito Internacional dos Conflitos Armados e dos Direitos Humanos.
Atores	Técnicos de sistemas e de redes, Indústria TIC, autoridades reguladoras sectoriais, CSIRT, utilizadores TIC.	Órgãos de polícia criminal, Ministério Público e Magistrados Judiciais.	Forças Armadas e Serviços de Informações.

Tabela 1 – Domínios de atuação na proteção do ciberespaço¹²

Por outro lado, também podemos avaliar as medidas de cibersegurança sob o ponto de vista de como a temática da cibersegurança é **percebida pelos atores responsáveis pela tomada de decisão** na elaboração de iniciativas e políticas. Dunn (2005, p. 20) caracteriza quatro tipologias de perspetivas sobre como esta matéria pode ser tratada:

1. **A cibersegurança é uma questão de segurança de TI:** a cibersegurança pode ser abordada como uma questão de segurança de TI ou segurança da informação, com forte foco em segurança da Internet. Assim, as políticas visam combater as ameaças à infraestrutura de informações por meios técnicos, como firewalls, software antivírus ou software de deteção de intrusão. Os principais atores são profissionais de segurança de TI. As principais ameaças percebidas variam de acidentes, falhas no sistema, programação incorreta e falhas humanas a ataques de hackers.
2. **A cibersegurança é uma questão econômica:** a cibersegurança é vista como relevante para a continuidade dos negócios, e especialmente para os negócios eletrónicos, que exigem acesso permanente às infraestruturas de TIC e processos de negócios permanentemente disponíveis para garantir um desempenho comercial satisfatório. Os principais atores são representantes do setor privado. As principais ameaças são vírus e worms, falhas humanas, mas também ataques de hackers de todos os tipos e atos de crimes cibernéticos.
3. **A cibersegurança é uma questão de prossecução criminal:** a cibersegurança é vista como relevante ao crime (cibernético). "Cibercrime" é um termo muito amplo, com vários significados, e as definições podem incluir desde crimes cometidos por meio de tecnologias até crimes cometidos contra computadores individuais. Os principais atores são os agentes da lei. As principais ameaças são atos de criminalidade informática, mas também "ciberterrorismo".
4. **A cibersegurança é uma questão de segurança nacional:** a sociedade como um todo e seus valores tutelados constitucionalmente são vistos como ameaçados, devido à sua dependência das TIC. A ação contra a ameaça tem como objetivo vários níveis (técnico, legislativo, organizacional

¹² SANTOS, Lino, BRAVO, Rogério e NUNES, Paulo Viegas - **Proteção do Ciberespaço**. Visão Analítica: Riscos, Segurança e Sustentabilidade, C. Guedes Soares, A. P. Teixeira, C. Jacinto (Eds), Edições Salamandra, Lisboa, 2012, (ISBN 978-972-689-247-2), pp.163 a 176. Tabela na p. 164.

ou internacional). Os principais atores são especialistas em segurança. As principais ameaças são terroristas, mas também ameaças de guerra de informação de outros estados.¹³

Dunn (2005, p. 20) faz uma análise comparada das iniciativas de cibersegurança ao redor do mundo e explica que, apesar de a maioria dos países adotarem todas as tipologias mencionadas, a ênfase dada a uma ou outra perspectiva varia consideravelmente e a predominância de uma ou outra tipologia tem implicações na formação das políticas de cibersegurança e, conseqüentemente, na determinação de esforços, metas, estratégias e instrumentos de proteção para a solução do problema. Neste estudo, Dunn observou que a maioria dos Estados envidou maiores esforços nas políticas de combate à cibercriminalidade e na defesa nacional.

Isto pode ser explicado pelo fato de a elaboração de políticas estratégicas ainda ter uma perspectiva muito centrada no Estado o que impacta nas decisões relacionadas à segurança do ciberespaço, ainda que seja uma matéria de natureza transfronteiriça. Beláz (2019, p. 17) explica que em geral *“legal discussions about cyberspace governance often focus on international cybercrime arrangements, international standards and national sovereignty”*. Porém, ele frisa que devido ao fenômeno da globalização, a partir desta perspectiva torna-se muito difícil *“to manage cyberspace and cyber threats without an adequate level of cooperation with various partners and allies”*.

Por exemplo, Santos, Bravo e Nunes (2012, p. 167) colocam que Estados com grande preocupação com o combate ao terrorismo, como os Estados Unidos, incluem a cibersegurança com maior foco nas questões de defesa nacional através do “desenvolvimento de meios técnicos para a monitorização do uso da Internet e para a construção de capacidades militares destinadas a fazer face a ataques de larga escala”.

Por isso, a depender da forma com que a temática da cibersegurança é desenvolvida no âmbito das políticas estaduais, muitas vezes pode ser confundida com a **ciberdefesa**, que se refere exclusivamente a questões de defesa nacional ou comunitária (no caso da UE), para proteger informações de interesse nacional e estratégicos militares contra ataques por meio de sistemas informáticos. No contexto da UE, a ciberdefesa também é contemplada pela Estratégia para a Cibersegurança, embora seja considerada uma “subdivisão da cibersegurança que visa defender o ciberespaço através de meios militares e outras formas adequadas a fim de alcançar objetivos estratégico-militares” (TCE, 2019, p. 65).

¹³ Dunn, M. 2005, Op. Cit. p.20.

Por outro lado, é crescente a preocupação dos Estados com o impacto das ciberameaças na economia, cujo maior enfoque e peso são mais compatíveis com perspectiva da UE sobre as ciberameaças e com a estratégia adotada centralizada no mercado interno, o que será tratado mais adiante. Santos, Bravo e Nunes explicam que:

Pelo fato de a Internet ser gerida e operada maioritariamente por entidade privadas colocaram o enfoque da cibersegurança no plano do combate à cibercriminalidade e da regulação e do robustecimento da resiliência das infra-estruturas de comunicação, independentemente do tipo de ameaça. Neste ponto de vista, a cibersegurança é vista como factor de geração de confiança no comércio electrónico e como parte integrante das políticas de desenvolvimento da designada sociedade da informação ou, mais recentemente, sociedade do conhecimento. Neste contexto, a cibersegurança é igualmente vista como um instrumento necessário à garantia da protecção da privacidade dos cidadãos. (SANTOS, BRAVO e NUNES, 2012, p. 167)

Sob esta ótica, a cibersegurança é alçada a um elemento fundamental na construção de confiança da sociedade nas transformações digitais, uma vez que a ciberdependência é um caminho sem volta, e por isso, as demandas de combate às ciberameaças passam a fazer parte das prioridades nas agendas políticas. A partir desta perspectiva, os ativos que carregam maior grau de importância na política de cibersegurança são as infraestruturas essenciais para o funcionamento da sociedade (como fornecimento de água e energia, serviços financeiros, hospitais, transportes, comunicação, redes e sistemas de informação etc.) onde a ocorrência de um ciberincidente na continuidade dos serviços teria consequências graves. Como o foco deste trabalho compreende a estratégia da UE nesta matéria e os desafios para a eficácia das medidas, a seguir será feita uma breve explicação sobre as ciberameaças e uma noção geral dos impactos relativos aos riscos associados a cibersegurança para a UE.

2.1 As Ciberameaças

As políticas de cibersegurança desenvolvidas no âmbito da UE partem de uma prévia avaliação das ameaças e, para isso, é necessário compreender o que significa uma ciberameaça. Assim como não existe um consenso sobre o conceito de cibersegurança – que pode ter significados diferentes para partes com interesses divergentes – e considerando a diversidade de atores (vítima/alvos ou de autores/agentes de ameaças), inexistente um entendimento universal do que constitui uma ciberameaça. Para Van der Meulen, A Jo e Soesanto (2015, p. 26) “*this absence prevents the establishment of a universally accepted categorisation system for threats and leads to variability in what is included in threat assessments*”.

Apesar disso, com vistas a estabelecer uma compreensão sobre o que são as ciberameaças, Van der Meulen, A Jo e Soesanto (2015, p. 25) propõem a síntese de dois conceitos: o da ISO (International Standards Organisation) e o do NIST (National Institute of Standards and Technology dos Estados Unidos). O primeiro define ameaça como um potencial

evento, que, ao se tornar um evento de fato, pode causar um incidente indesejado, pois danoso a uma organização ou sistema. Já o segundo conceito define a ameaça como sendo qualquer circunstância ou evento com potencial de afetar adversamente operações ou ativos de uma organização ou de indivíduos (incluindo missão, funções, imagem ou reputação), através de um sistema informático via acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço.

Com base nisso, Van der Meulen, A Jo e Soesanto (2015, p. 25) propõem a utilização do conceito da ISO que limita as ameaças a um evento potencial (não às circunstâncias que possam facilitar a ocorrência, que não o compõe) e complementa com a categorização do NIST que menciona **os meios** de afetar as operações e os ativos, de forma a estabelecer um *core* do que constitui uma ciberameaça. Além disso, considerando os domínios de atuação supracitados – proteção simples, prossecução criminal e defesa de Estado – na avaliação das potenciais ameaças, Santos, Bravo e Nunes (2012, p. 10) atentam para a necessidade de estabelecer uma adequada noção e articulação entre esses domínios a depender da estrutura ameaçada:

No plano tático e operacional, a resposta a ciberataques contra infraestruturas da informação críticas pressupõe sempre uma intervenção no domínio da protecção simples, podendo ainda, considerando a sua motivação e a extensão do seu impacto, implicar a acção nos domínios da prossecução criminal e da defesa do Estado.

Isso implica na necessidade de identificação dos atores responsáveis pela cibersegurança e do seu papel, em conformidade com o risco social e com o potencial efeito dos diversos tipos de agressões cibernéticas. Além disso, pressupõe um tratamento diferenciado de acordo com a motivação, o alvo e o impacto (por exemplo um crime de divulgação de pornografia infantil de uma rede internacional deve ter um tratamento diferente de um ataque a uma rede de energia elétrica). Neste contexto, alguns autores propõem uma distinção entre as atividades ilícitas realizadas no ciberespaço de maneira a categorizá-las e a organizar os meios de respostas. Por exemplo, é comum a utilização dos termos cibercrime e ciberataque como sinônimos, porém alguns autores frisam uma distinção entre eles.

Alexander (2014, p. 2) define **cibercrime** como sendo um crime “*enabled by or that targets computers*”. Já Godwin (2014, p. 29) define cibercrime como “*the use of cyberspace for criminal purposes as defined by national or international law*”, o que o limita a ações puníveis em instrumentos legais pré-existent. Por sua vez, Godwin (2014, p. 44) define um **ciberataque** como “*an offensive use of a cyber weapon intended to harm a designated target*”. Já de acordo com a definição do NIST, ciberataque se refere a:

*An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.*¹⁴

A partir disso, Gonçalves (2016, p.24) levanta um questionamento (pois os conceitos aparentam ser sinônimos) se uma ação com objetivo de lesar algo ou alguém também não seria um crime. O autor mesmo explica que a distinção entre um ciberataque e um cibercrime se assenta na dimensão e no foco do ataque, pois para o mesmo “um ataque cibernético tem em vista o comprometimento do funcionamento ou a lesão de um Estado, pondo em risco o seu funcionamento sustentável e a sua independência e soberania”. No mesmo sentido, Alexander (2014, p. 2) complementa dizendo que frequentemente os ciberataques miram nas infraestruturas críticas (serviços financeiros, telecomunicações, água, energia, indústrias, etc), mas acrescenta que “*they increasingly inflict damage on government targets, including the military, intelligence, and law enforcement*”. Dessa forma, de acordo com essas noções, se referir a um ciberataque traz a ideia de que a abrangência do incidente seja mais ampla e/ou de que o alvo carregue um grau de importância maior, cujo impacto tenha consequências mais graves para o funcionamento do Estado, da sociedade, da economia, etc. O que não deixa de constituir um cibercrime, porém de natureza complexa, a ser instrumentalizado por meios de coordenação e de resposta diferenciados.

Entretanto, embora um ciberataque possa partir potencialmente de uma diversidade de agentes e de motivações (política, religiosa, financeira, de inteligência/espionagem, etc.), e possa gerar cibercrises, ciberconflitos e até mesmo ciber guerras, Tikk, Kaska e Vihul (2010, p. 101), alertam para o que ocorreu na Estônia em seu estudo sobre os ciberconflitos ocorridos em 2007¹⁵. Apesar do alerta internacional e das ousadas declarações de que a Rússia estava envolvida (que alegou não ter envolvimento, mas cooperou de forma insatisfatória), de acordo com os autores, até a realização do estudo pelos autores, a única pessoa condenada por participar dos ataques foi um estudante (ativista pró-Kremlin) que, por descuido, assumiu a autoria em um fórum da internet. O incidente foi realizado por meio de um bombardeamento de pedidos eletrônicos aos sites do governo da Estônia causando colisão temporária, e foi motivado pela derrubada de uma estátua da era soviética¹⁶. Neste caso, o enquadramento como

¹⁴ National Institute of Standards and Technology (NIST). *Glossary of Key Information Security Terms*. July.2019. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>>. Acesso em Jun.2020.

¹⁵ Tikk, Kaska e Vihul. *International Cyber Incidents: Legal Considerations*. 2010, p. 101. Uma série de ataques realizados em abril de 2007 deixou sites do governo da Estônia fora do ar e indisponíveis por algumas horas.

¹⁶ REUTERS. *Kremlin loyalist says launched Estonia cyber-attack*. Disponível em: <https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313>. Acesso em: Jun.2020.

ciberataque associado a um ato de ciberguerra torna-se um tanto nebuloso (apesar motivação política do agente), pois as acusações de que a Rússia era responsável pelo incidente fez a tensão política entre os países escalonar, o que poderia levar a consequências catastróficas.

Neste contexto, Tikk, Kaska e Vihul (2010, p. 101) revelam a necessidade de estabelecer uma padronização em termos de estruturas legais e de cooperação para lidar com ciberataques e cibercrimes, bem como a urgência de uma revisão terminológica ao expor que:

Much confusion is currently created by the fact that virtually all cyber attacks are referred to as cyber war and cyber terrorism, which in legal terms may be misleading unless the facts are filtered through the relevant legal frameworks. Not every deviation from, or a violation of everyday IT-security can be regarded as a manifestation of “cyber warfare”, terrorists or ordinary criminal act. In some cases, we deal only with breaches of IT security regulations. The point is that it is important to develop a full léxicon that speaks to all legal frameworks, not just terrorism or warfare, and to not assume that every incident is an attack or onset of war.

Além disso, a inconsistência terminológica dificulta a qualificação legal de um ciberincidente e a efetividade de uma resposta em termos de autoridades, meios e procedimentos envolvidos, o que pode criar incertezas jurídicas e dificultar o exercício das atribuições dos entes responsáveis por tomar medidas contra as atividades maliciosas. A problemática desta questão vai ao encontro do que Van der Meulen, A Jo e Soesanto (2015, p. 21) colocam em termos análise de ciberameaças e de políticas de cibersegurança: “*the more countries focus on their cybersecurity from cyberwar, the more they do that at the expense of cooperation on cybercrime*”. Pois, nessa perspectiva, a tendência é a de que os países se alinhem e se fechem entre seus aliados internacionais tradicionais em detrimento a tratados e acordos internacionais que tentam promover novas formas de cooperação no combate ao cibercrime.

Com vistas a facilitar o entendimento dos conceitos mencionados neste trabalho, propõe-se a utilizar a subdivisão de Muggah, Glen e Diniz (2015, p. 78), que classifica os cibercrimes e ciberameaças que envolvem utilização de meios informáticos como instrumentos ou como alvo em três subconjuntos: 1. cibercrime convencional, 2. cibercrime complexo e 3. ameaças emergentes:

1. Atividades criminosas tradicionais mais difundidas, já categorizadas em instrumentos legais nacionais ou internacionais, como por exemplo: interceptação de dados, pornografia infantil, fraude bancária, furto de identidade, infração contra direitos autorais, etc. Os mais comuns são os de motivação económica e os relativos ao conteúdo ilícito. Os órgãos responsáveis normalmente são associados à segurança pública (domínio da proteção simples e prossecução criminal).

2. Atividades criminosas complexas ou combinadas são as que se enquadram em mais de uma categoria do cibercrime convencional, ou crime organizado, ou aquelas com maior potencial ofensivo/disruptivo como: ciberterrorismo, ciberspionagem, ataques contra infraestruturas críticas, ciberguerra, ciberbranqueamento de capitais, etc. Neste tipo é necessária a combinação de inteligência, segurança pública, e até mesmo ação militar (articulação entre os três domínios de ação) visto que há fontes múltiplas de ameaças assim como alvos.

3. Novas ameaças provenientes da expansão do ciberespaço, do surgimento de novas tecnologias, do reconhecimento da dimensão política do ciberespaço e do aumento da superfície de ataque (*Internet of things*, Mercado Único Digital, Cryptomoedas, técnicas de inteligência artificial, *machine learning*, autômatos, *Internet of Everything*, etc.) que não se enquadram nos crimes previstos ou que ainda não existam instrumentos adequados de resposta dos Estados. Por exemplo as ameaças híbridas, ciber-mercenários, hackativismo, monitoramento da internet, controle da internet, utilização de dados (para fins de manipulação de mercados, perfis de consumo, eleitorais, *fakenews*, propaganda enganosa, etc.).

Nesta classificação, um ciberataque se enquadra em um tipo de cibercrime complexo, embora também possa se enquadrar nas ameaças emergentes não instrumentalizadas. Por outro lado, associada a esta noção de ameaças, também se mostra adequado o mapeamento de Van der Meulen, A Jo e Soesanto (2015, p. 43) (Figura 1) de **avaliação das ameaças** que leva em consideração o agente da ameaça, as ferramentas utilizadas, o tipo de dano causado e os alvos.



Figura 1 – Sistema simplificado de avaliação de ameaças

Van der Meulen, A Jo e Soesanto (2015, p. 43) explicam que o mapa partiu de classificações retiradas de estudos pré-existentes e se propõe a servir como uma base para um sistema de avaliação das ameaças, no entanto, não tentou avaliar o importância relativa de cada ator, ferramenta ou ameaça, o que é crucial para qualquer decisão política¹⁷, e tampouco considerou quais componentes de ameaça estão se a tornar mais ou menos pertinentes ao longo do tempo. Além da necessidade de pesar a gravidade das ameaças, Van der Meulen, A Jo e Soesanto (2015, p. 43) frisam que um sistema de avaliação das ameaças não pode somente se basear nas ameaças existentes, mas também deve considerar as tendências atuais e o que denominou de “*threat vectors*”, ou seja, tal sistema deve incluir análises e previsões para o futuro e as ameaças inovadoras potenciais, em consonância com a subdivisão de Muggah, Glen e Diniz (2015, p. 78) de ameaças emergentes.

Devido a incompatibilidades de definições, métricas e abordagens, foi observada a necessidade de uma revisão sistemática do que constitui uma ameaça no contexto da cibersegurança, de forma a delinear os componentes que devam estar incluídos em um sistema de avaliação de ameaças e para fornecer aspetos relativos a gravidade e a como ser operacionalizado. Essas classificações são importantes para o que este trabalho se propõe ao analisar a eficácia das medidas de Cibersegurança na UE; porém, na ausência de um padrão universalmente aceite, serão utilizadas como base as sistematizações já mencionadas.

Além disso, tal como consta na Figura 1 (acima), a título exemplificativo, cabe mencionar algumas ferramentas de ciberameaças utilizadas no lançamento de ciberataques. De acordo com o TCE (2019, p. 10), as ferramentas mais comuns são:

- Malware (software malicioso): provocam danos em dispositivos ou redes, tais como: vírus, cavalos de Troia, worms (vermes), adware (software de publicidade não solicitada) e spyware (software espião).
- Ransomware (software de sequestro): encripta os dados, impedindo que os utilizadores acedam aos ficheiros/sistema até que seja pago um resgate.
- DDoS (ataques distribuídos de negação de serviço): tornam os serviços ou recursos indisponíveis para os seus utilizadores através do envio em massa de mais pedidos do que conseguem tratar causando sobrecarga.
- Phishing: método comum em que mensagens eletrónicas que aparentemente provêm de uma fonte fidedigna enganam os utilizadores e levam-nos a revelar informações ou clicar em ligações que infetam os dispositivos mediante o descarregamento de malware.
- Ameaças persistentes avançadas: agressores se envolvem a longo prazo na vigilância e roubo de dados, por vezes com intuítos destrutivos (¼ dos Ciberincidentes), muito associada à ciberespionagem.

2.2 Impacto das Ciberameaças na UE

Os ciberincidentes¹⁸ contra o sistema elétrico da Ucrânia ocorridos em 2015 e 2016, e os ciberataques de impacto global do ransomware ‘WannaCry’ e do malware ‘NotPetya’,

¹⁷ Van der Meulen, A Jo e Soesanto (2015, p. 43).

¹⁸ Registo dos Ciberincidentes mais significativos desde 2006 – considera ataques cibernéticos a agências governamentais, empresas de segurança e tecnologia ou crimes económicos com perdas de mais de um milhão de

ocorridos em 2017 (que atingiram mais de 320 000 vítimas em cerca de 150 países) causaram um impulsionamento no sentido de priorizar e reforçar as políticas de Cibersegurança na UE (TCE, 2019, p. 11). Isso fez com que a UE instituísse, em 2017, um conjunto de instrumentos de ciberdiplomacia¹⁹ que incluem a imposição de sanções, se necessário, para responder a ciberatividades maliciosas dirigidas contra a UE e seus Estados-Membros. Apesar disso, a ameaça que os ciberataques representam ainda são um desafio de difícil superação e o impacto da falta de preparação para um ciberataque é difícil de ser mensurado devido à ausência de dados fiáveis, conforme veremos a seguir.

Apesar do esforço da UE em reforçar sua estratégia em matéria de cibersegurança para combater as ciberameaças e tirar proveito do desenvolvimento trazido pela era digital, de acordo com o Conselho Europeu²⁰, o impacto económico da cibercriminalidade quintuplicou entre 2013 e 2017, atingindo tanto governos como empresas de diversas dimensões. Segundo o Conselho, calcula-se que o prejuízo proveniente de ciberataques tenha um custo de cerca de 400 milhões de euros por ano. Além disso, segundo o TCE²¹ o crescimento previsto para os prémios de seguro de riscos cibernéticos, passou do patamar de 3 milhões de euros em 2018 para 8,9 milhões de euros em 2020, o que espelha esta tendência ascendente.

O Banco Mundial e Nações Unidas produziram um relatório²², voltado ao combate ao cibercrime nas economias emergentes (2017, p. 16,17), que, expõe que, em 2014, mais de 348 milhões de identidades foram expostas pela ação de *hackers* e estimam que cerca de 594 milhões de pessoas foram vítimas de cibercrime globalmente. Além disso, Karake, Shalhoub e Ayas (2019, p. 3) informam que “*it is estimated that in 2016 cybercrime cost the global economy US\$0.5 trillion and it is expected the cost will rise to US\$7 trillion by 2021*”.

A partir de 2020, estima-se que o incremento dos dispositivos conectados com a ‘*internet of things*’ (IoT) ultrapassará o número de pessoas no mundo em seis para um, aumentando exponencialmente a superfície de ataque, porém a cibersegurança ainda não se tornou uma realidade a partir da sua conceção. Neste passo, num futuro próximo, a interconectividade não será limitada à rede de dispositivos, mas também se estenderá a

dólares. Disponível em: <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>. Acesso em Jun. 2020.

¹⁹ Em 30 de junho de 2020 a UE impôs as primeiras sanções contra pessoas e organizações da China, Rússia e Coreia do Norte, envolvidas nos ataques NotPetya e WannaCry. DECISÃO (PESC) 2020/1127 DO CONSELHO EUROPEU.

²⁰ Disponível em: <https://www.consilium.europa.eu/pt/policies/cybersecurity/>. Acesso em Jan. 2020.

²¹ TCE (2019). Op. Cit. p.2.

²² World Bank and United Nations. 2017. **Combating Cybercrime: Tools and Capacity Building for Emerging Economies**, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

humanos, tanto no nível individual quanto nível coletivo - a ‘Internet of Everything’ (IoE), o que “*it will become hard to imagine a “computer crime”, and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity*”. (WORLD BANK AND UNITED NATIONS, 2017, P. 25)

A partir desses dados, é notório perceber que o cibercrime está em ascensão e que as oportunidades e ganhos estão cada vez mais atraentes, pois a utilização do ciberespaço tornou a prática de crimes muito mais simples que os métodos considerados “tradicionais”. De acordo com a Comissão Europeia, dados de 2017²³, os cibercrimes correspondem a 50% do total de crimes cometidos em alguns países da UE. Por este motivo, “a cibercriminalidade é vista como um grande desafio para a segurança interna da UE por 87 % dos europeus”²⁴.

Para se ter uma noção da gravidade do problema, de acordo com o TCE (2019, p. 11), ao passo que o impacto financeiro dos ciberataques aumenta, “existe uma disparidade alarmante entre o custo de lançar um ataque e o custo da prevenção, investigação e reparação”. Por exemplo, segundo a Europol²⁵ em uma rede mundial de vendas de ciberataques – que foi derrubada pela agência – era possível encomendar um ciberataque de negação de serviço (DDos) por apenas 15 euros mensais, porém as perdas para a organização atingida (ativos como imagem, reputação, perdas financeiras, etc.) são consideravelmente mais elevados. Um outro exemplo desta disparidade ocorreu nos Estados Unidos, em 2010²⁶, onde um único *hacker* foi condenado a 20 anos de prisão por roubar mais de 170 milhões de números de cartão de crédito e débito, tornando-se o maior caso realizado por um indivíduo que o Departamento de Justiça dos Estados Unidos (DoJ) já processou.

Ademais, apesar de 80% das empresas da UE já terem sofrido algum tipo de incidente de cibersegurança, de acordo com dados expostos no relatório do TCE (2019, p. 11), “entre as empresas da UE, 69% não estão cientes da sua exposição a ciberameaças ou estão-no de forma limitada e 60% nunca fizeram uma estimativa das potenciais perdas financeiras”. Além disso,

²³ Comissão Europeia. Disponível em: <https://www.consilium.europa.eu/pt/infographics/cyber-security/>. Acesso em Fev.2020.

²⁴ COMISSÃO EUROPEIA. Disponível em: <https://www.consilium.europa.eu/pt/policies/cybersecurity/>. Acesso em Fev.2020.

²⁵ EUROPOL. Press release: **World’s Biggest Marketplace selling internet paralysing DDos attacks taken down**. (Retirado o maior mercado mundial de venda de ataques DDos para paralisar a Internet), comunicado de imprensa, 25 de abril de 2018. Disponível em: <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down>. Acesso em Fev.2020.

²⁶ World Bank and United Nations (2017). Op. Cit. p.17.

um inquérito global da NTT Security (2018, p. 6)²⁷, que entrevistou 1800 empresas globais, concluiu que muitas organizações ainda estão presas a uma mentalidade reativa quando o assunto é cibersegurança. Uma das estatísticas mais alarmantes deste relatório demonstra que um terço (1/3) dos entrevistados responderam que preferiam pagar um resgate a um hacker depois do que investir em cibersegurança antes e outros 16% responderam que não sabiam. Ou seja, apenas metade dos tomadores de decisão das empresas entrevistadas consideraram importante investir em cibersegurança.

Pelos motivos expostos, para uma efetiva redução dos riscos e do impacto das ciberameaças ainda existem muitos obstáculos para responder à altura dos desafios apresentados (associados a uma capacidade de constante adaptação), devido: à falta de consciencialização e de preparação das organizações e da sociedade em geral; ao aumento da sofisticação dos ciberataques; à diminuição da eficácia dos mecanismos de defesa trazidos pela evolução tecnológica; ao baixo custo (potencial) para lançar um ciberataque; entre outros. A partir do cenário apresentado, posteriormente, serão abordados o caminho da UE em matéria de cibersegurança, o panorama estratégico na UE nesta temática e os principais instrumentos jurídicos, com a finalidade de avaliar a adequação e eficácia das medidas propostas.

3 A UE EM MATÉRIA DE CIBERSEGURANÇA

Para compreender o panorama estratégico da Cibersegurança na UE, em suma, anteriormente buscou-se fornecer uma noção do significado e da dimensão da Cibersegurança, os domínios de atuação e as diferentes perspetivas que existem e que impactam na tomada de decisão ao estabelecer uma estratégia para lidar com esta temática. Além disso, também foi abordada a noção de ciberameaça, os diferentes tipos de atividades maliciosas, os diferentes autores envolvidos, as ferramentas mais comuns utilizadas e a necessidade de um sistema de avaliação de ameaças que vá ao encontro dos objetivos a que a UE se propõe. Finalmente, foi relatado o impacto das ciberameaças na Europa e no mundo, bem alguns dos obstáculos a serem enfrentados na redução dos riscos associados para responder à altura dos desafios apresentados (associados a uma capacidade de constante adaptação), devido: à assimetria entre o custo para lançar um ataque e o respetivo impacto, e à disparidade entre os meios disponíveis para

²⁷ NTT Security. *Risk:Value Report 2018*. (Relatório risco-valor 2018). Disponível em: https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_report_risk-value_2018_us_uea_v1.pdf?sfvrsn=c96bf84f_0. Acesso em Mai.2020.

realização de atividades maliciosas e os meios necessários para identificar, punir, recuperar e proteger os sistemas e ativos. A partir disto, será vista a evolução das políticas de Cibersegurança na UE e analisar os instrumentos jurídicos vigentes.

3.1 O Caminho escolhido pela UE – A Estratégia

Para entender como a UE se coloca em termos de política e instrumentos jurídicos de Cibersegurança, faz sentido avaliar o caminho percorrido e as diferentes perspectivas que a levaram à atual situação. Por este motivo, pretende-se examinar os principais marcos político-jurídicos até a estruturação atual, para posteriormente verificar a conformidade com os objetivos e aspirações da UE de se tornar uma liderança mundial em termos de cibersegurança. De acordo com Beláz (2019, p. 19), no período de 1985 a 2001 quatro eventos estabeleceram uma dinâmica importante para o desenvolvimento posterior de uma política de cibersegurança, são eles:

1. a Realização do Mercado Interno (1985)²⁸ pela livre circulação de bens, serviços e pessoas, e onde as TIC passaram a ser vistas como importantes para o desenvolvimento económico e social;
2. o relatório de Bangemann (1994)²⁹ intitulado “A Europa e a Sociedade de Informação Global” que buscava a instituição de políticas europeias para desenvolver este setor e o promissor comércio eletrónico, e que continha as sementes conceituais para todos os elementos do discurso posterior da UE e da política “cibernética”;
3. o Ato Único Europeu (1987)³⁰ com a criação de novas competências comunitárias e preparação do terreno para o reforço da integração política e para a União Económica e Monetária; e
4. o Tratado de Maastricht (1992) - depois de articular o interesse no setor das TIC - as competências da UE foram solidificadas pelos Tratados que formalizaram o papel da UE na segurança cibernética, mas restringiu suas competências aos “aspectos políticos e económicos” e limitada pelo exercício de um “*soft-power*” no setor.

A partir disto, Beláz (2019, p. 20) explica que a política de segurança cibernética adotada pela UE, devido aos limites de suas atribuições e às dificuldades de articular em conjunto com os EM as capacidades/competências “*hard*” no setor (militarizada e centralizada), adotou uma abordagem não militar, estratégica e socioeconómica. Este ponto de vista mais restritivo decorria do fato de as ações militares da UE se limitarem à pacificação e à manutenção da paz, no entanto, para a autora “essa atitude limitou a UE de desenvolver uma abordagem holística de cibersegurança, incluindo capacidades de ataque cibernético ofensivo”.

²⁸ COMISSÃO DAS COMUNIDADES EUROPEIAS. COM (85) 310 final. Bruxelas, 14.6.1985. **Realização do mercado interno** - Livro Branco da Comissão ao Conselho Europeu. No ponto 113 (p. 30), as novas tecnologias foram reconhecidas pelo seu papel na economia e no desenvolvimento de novos serviços transfronteiriços.

²⁹ Segundo Beláz (2019, p. 19) o relatório deixa claro que fatores económicos como as forças de mercado e a criação de empregos estão na base dos interesses e da visão estratégica da União nas TIC. A proteção dos direitos fundamentais, como privacidade, segurança e proteção são elementos centrais, ambos no Relatório Bangemann e posteriormente na Estratégia de Segurança Cibernética da União Europeia.

³⁰ Síntese do Ato Único Europeu [JO L 169 de 29.6.1987, p. 1-28]. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Axy0027>. Acesso em Ago.2020.

Mais adiante, em Janeiro de 2001, surge um embrião de uma política de Cibersegurança com o lançamento do comunicado³¹ intitulado ‘Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade’ - esta última apoiada no terceiro pilar³² da UE. O documento frisa que as tecnologias da informação e da comunicação têm um impacto importante na economia e na criação de um espaço de Liberdade, de Segurança e de Justiça e se compromete a apresentar “propostas legislativas para uma aproximação mais aprofundada do direito penal material em matéria de criminalidade que utiliza tecnologias avançadas”.

Posteriormente, em Junho de 2001, foi proposta a primeira estratégia europeia de segurança das redes e da informação³³ considerada um documento mais completo e identificável com uma política de cibersegurança, que fornecia uma tipologia detalhada das ameaças cibernéticas, medidas técnicas, recomendações específicas para melhorar a segurança e a necessidade de compartilhamento de informações a nível europeu (Beláz (2019, p. 20). Neste contexto, Kasper e Antonov (2019, p. 24) colocam que as políticas de cibersegurança “*in early EU regulations had two main considerations: protection of privacy and personal data, and harmonizing requirements for the sake of completing the single market*”, o que denota a ausência de uma perspetiva mais abrangente.

Foi neste ano também que realizou-se a Convenção sobre o Cibercrime em Budapeste³⁴, um tratado internacional de direito penal vinculativo e ainda vigente, que contém um quadro legislativo sobre cibercriminalidade (estabelece as tipologias de crimes praticados por meio da Internet e as formas de persecução) e contém diretrizes para a cooperação internacional entre os Estados signatários. A UE aderiu ao Comité do Conselho da Europa para a referida Convenção e atualmente é representada pela Comissão, pelo Conselho da União Europeia, pela Europol, pela ENISA e pela Eurojust (TCE, 2019, P. 11). Beláz (2019, p. 20) destaca que devido à importância das TIC para o mercado interno, as questões cibernéticas caíram no

³¹ COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2000) 890 final. Bruxelas, 26.1.2001.

³² Pilares da União Europeia: Com a entrada em vigor do Tratado de Lisboa, a expressão “*pilares da UE*” deixou de fazer sentido.(...) De 1993 a 2009 estava em vigor o sistema de três pilares: o primeiro pilar com as competências comunitárias para a realização do mercado único e criação de políticas económicas, sociais e ambientais ; o segundo pilar para uma Política Externa e de Segurança Comuns; e o terceiro pilar de cooperação (Polícia e Judiciária) em matéria penal. Disponível em: <<http://euroogle.com/dicionario.asp?definition=715>> e <<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:xy0026>>. Acesso em ago.2020.

³³ COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2001) 298 final. Bruxelas, 26.1.2001. **Segurança das redes e da informação**: Proposta de abordagem de uma política europeia.

³⁴ CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23.11.2001. Série de Tratados Europeus / 185.

primeiro pilar, o que permitiu que a UE iniciasse a tomada de decisão e elaboração de legislação no setor apoiada na natureza econômica, porém, separou-a das questões ciberdelitivas.

No período seguinte, que vai de 2002 a 2006, Beláz (2019, p. 20-21) coloca que começou a ser definido o papel da UE no ramo cibernético como um agente “facilitador”. Após o estabelecimento do viés econômico das ciberpolíticas e devido à preocupação com a cibercriminalidade, foi criada a ENISA³⁵ (2004), que visava estabelecer um quadro harmonizado para a regulamentação dos serviços de TIC e segurança das redes e da informação; e criado também um departamento no âmbito da Europol³⁶ (2002) especializado em criminalidade “*high-tech*” (HTCC - *High-Tech Crime Centre*).

Contudo, a criação da ENISA foi fundamentada em uma aproximação ao artigo 95.º CE (atual artigo 114º do TFUE)³⁷, o que levou o Reino Unido a recorrer ao Tribunal de Justiça para questionar a escolha da base jurídica³⁸. O recorrente alegou que o fundamento utilizado consistia “no poder de harmonizar as legislações nacionais e não de criar organismos comunitários e de lhes atribuir missões”. Além disso, observou também que a criação de um órgão meramente consultivo e limitado a dar pareceres não vinculativos, nem mesmo indirectamente aproxima as normas nacionais, pois poderia na prática, inclusivamente, aumentar as disparidades existentes entre as legislações nacionais conforme a discricionariedade das entidades consultantes. No entanto, foi negado provimento ao recurso com o entendimento de que a criação de um organismo comunitário poderia contribuir para o processo de harmonização e que, para facilitar a transposição e aplicação uniforme de atos, era adequada a adoção de medidas não vinculativas. Ou seja, concluiu-se que a Agência poderia servir de meio adequado para prevenir o aparecimento de disparidades susceptíveis de levantar obstáculos ao bom funcionamento do mercado interno nesta matéria e suas atribuições foram entendidas como medidas relativas à aproximação, em conformidade com o artigo 95.º CE.

Neste contexto, Kasper e Antonov (2019, p. 24-25) revelam que a criação da Agência teve mais relação com a criação de elementos para realização do mercado interno do que com o estabelecimento de medidas de segurança para combater potenciais riscos e ameaças, e sublinha que “*it can be claimed that the EU’s primary concern was data security, and the*

³⁵ REGULAMENTO (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação.

³⁶ A Europol é uma agência da UE que iniciou suas atividades em 1999 para atuar na prevenção e no combate da criminalidade grave transnacional (terrorismo, tráfico de drogas, crime organizado, etc).

³⁷ O artigo 114.º do TFUE constitui a base jurídica para medidas de harmonização que visam o estabelecimento do mercado interno.

³⁸ Processo C-217/04: Reino Unido da Grã-Bretanha e da Irlanda do Norte VS Parlamento Europeu e Conselho da União Europeia. Acórdão do Tribunal de Justiça (Grande Secção) de 2 de Maio de 2006.

broader network and information or cybersecurity aspects were rather incidental in special legal regimes". No mesmo sentido, Beláz (2019, p. 21) destaca o aspeto facilitador do papel que a UE assume neste período, ao invés de uma liderança política, ao analisar a linguagem utilizada nos documentos afirmando que *"Member States instead of being instructed to do something, in the new documents they were encouraged or invited to take certain actions"*. Segundo este autor, o papel facilitador da UE foi oficializado com a publicação de uma nova Estratégia para uma Sociedade da Informação Segura³⁹. Além disso, há de se destacar que nesta época a abordagem sobre as questões de cibersegurança ainda era muito ligada a um campo meramente complementar e técnico ligado à segurança das redes e da informação, que não comportava o conceito amplo e multifacetado que temos hoje (KASPER e ANTONOV, 2019, p. 26). Ademais, Fernandes (2014, p. ix) explica que:

Associado à problemática da segurança do crime eletrónico, estava a necessidade de incrementar a utilização da Sociedade de Informação e a consequente Economia de Conhecimento, como instrumentos de crescimento económico e luta contra a infoexclusão. Esta estratégia inseriu-se nas iniciativas eSociety e nos consequentes Planos de Ação de 2002, 2005 e de 2010⁴⁰.

Essa visão mudou completamente depois dos acontecimentos ocorridos na Estónia em 2007, que causaram um despertar para as questões de cibersegurança na UE e no mundo. De acordo com Cavelty (2013, p. 4), até este momento *"the EU's approach to cyber-security was framed mainly as sub-category and side issue of the efforts to stimulate and secure the development of an Information Society in Europe"*. Para Fernandes (2014, p. 5), a partir deste ponto, iniciou-se uma nova abordagem na UE com o fim da inclusão das políticas de cibersegurança como subcategoria das políticas relacionadas à designada sociedade de informação ou eSociety, onde àquela passou a ganhar maior autonomia.

A partir desta diferenciação, Beláz (2019, p. 21) classifica o período que vai de 2007 a meados de 2016 de "o Despertar" da política de cibersegurança, onde este tema passou a ser uma prioridade na pauta da UE e, como consequência disso, o autor verificou que, entre 2007 e 2013, *"73 of the total 143 legal documents accepted relates to cybersecurity in some extent"*. A esta altura, os ataques também foram considerados uma ameaça à estabilidade do mercado interno e impulsionou o início de uma série de medidas para o fortalecimento da segurança digital. Deward (2017, p. 171 *apud* Beláz, 2019, p. 21) destaca que:

³⁹ COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2006) 251 final. Bruxelas, 31.5.2006. **Estratégia para uma sociedade da informação segura** – "Diálogo, parcerias e maior poder de intervenção".

⁴⁰ **eEurope 2002**: Impacto e prioridades, Comunicação ao Conselho Europeu da Primavera, em Estocolmo, de 23 a 24 de Março de 2001 [COM (2001) 140 final]; **eEurope 2005**: Plano de acção eEurope 2005: Uma sociedade da informação para todos. 28 de Maio de 2002 [COM(2002) 263 final]; **Uma Agenda Digital para a Europa**: Bruxelas, 19.5.2010. COM(2010)245 final.

Economic threats are issues where the EU can act. Direct threats to national security, by contrast, are sectors where Union action is severely restricted. It needed to address or at least acknowledge, the threat of state-sponsored aggression against national communications infrastructures and the potential impact of such incidents on the EU's financial and economic viability.

Neste contexto, em 2008, o mandato da ENISA foi prorrogado até Março de 2012 e em 2009 foi lançada uma nova comunicação⁴¹ relativa à protecção das Infra-estruturas Críticas da Informação (ICI), com destaque para a necessidade de reforçar as capacidades da referida agência e de “uma abordagem multilateral e multiníveis de dimensão europeia, mas que respeite e complemente inteiramente as competências nacionais”. O documento propôs um plano de ação (Protecção das infra-estruturas críticas da informação - PICI) baseado em cinco pilares:

1. Preparação e prevenção: assegurar a preparação a todos os níveis;
2. Detecção e resposta: criar mecanismos adequados de alerta rápido;
3. Mitigação e recuperação: reforçar os mecanismos de defesa das ICI na UE;
4. Cooperação internacional: promover internacionalmente as prioridades da UE;
5. Critérios para o sector das TIC: apoiar a aplicação da directiva relativa à identificação e designação das infra-estruturas críticas europeias.

Embora o plano de ação PICI tenha sido uma tentativa mais coerente de abordagem da política de cibersegurança, a postura assumida pela UE foi a de colocar os interesses e práticas nacionais em primeiro plano (BELÁZ, 2019, p. 21). Além disso, depois da crise financeira de 2008, a necessidade de assegurar e desenvolver setor das TIC foi considerada uma estratégia importante para a recuperação económica e do mercado de trabalho. Portanto, no contexto do segundo pilar da UE (Política Externa e de Segurança Comuns) ainda em vigor a época, apesar da preocupação com a protecção das infraestruturas críticas de informação e da identificação de que a cibersegurança era também um problema de segurança a nível europeu (conforme relatório sobre a implementação da Estratégia Europeia de Segurança, 2009, p. 13)⁴², o papel assumido pela UE permaneceu em segundo plano como agente incentivador, fomentador e facilitador, buscando a conscientização e cooperação dos EM neste tema; pois, evitava o avanço da UE em questões sensíveis de segurança interna, sem atrapalhar o processo de integração.

Devido a isso, dois anos após a adoção do plano PICI, a Comissão Europeia avaliou os resultados obtidos e lançou nova comunicação⁴³, que concluiu que: “a experiência mostra que as abordagens puramente nacionais ou regionais para responder aos desafios da segurança e da

⁴¹ COMUNICAÇÃO DA COMISSÃO DAS COMUNIDADES EUROPEIAS. COM/2009/0149 final. Bruxelas, 30.3.2009. **Relativa à protecção das infra-estruturas críticas da informação** - "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência".

⁴² CONSELHO DA UNIÃO EUROPEIA. **Estratégia Europeia em Matéria de Segurança**: Uma Europa Segura num Mundo Melhor. Luxemburgo: 2009. 43 p. ISBN 978-92-824-2431-5.

⁴³ COMUNICAÇÃO DA COMISSÃO EUROPEIA. COM(2011) 163 final. Bruxelas, 31.3.2011. **Protecção das infra-estruturas críticas da informação** «Realizações e próximas etapas: para uma cibersegurança mundial».

resiliência não são suficientes”. Apesar disso, ao mesmo tempo, Beláz (2019, p. 21-22) destaca alguns pontos positivos no avanço das políticas de Cibersegurança deste período:

Two Ministerial Conferences were held (Tallinn, 2009 and Balatonfüred, 2011) which led to the adoption of the European Parliament Resolution on Critical Information Infrastructure Protection, the establishment of the European Forum for Member States and of the European Public-Private Partnership for Resilience; two pan-European exercise (Cyber Europe 2010 and 2012); policy recommendation by ENISA on a minimum set of baseline capabilities and services; and recommendations on the functioning of national CERTs (Computer Emergency Response Teams).⁴⁴

Ainda que, em 2010, a cibersegurança estivesse inserida⁴⁵ no Plano “Uma Agenda Digital para a Europa (ADE)”⁴⁶, após o “despertar”, a UE conferiu maior prioridade e autonomia à matéria e assumiu o papel de levar adiante as questões de cibersegurança, tendo em conta os resultados obtidos e a noção dos riscos associados caso uma estratégia coerente e funcional não fosse levada adiante a nível europeu. Com a entrada em vigência do Tratado de Lisboa em 2009, o *status* político da UE foi reforçado, conforme explica Beláz (2019, p. 22):

The Treaty's core was, to improve the coherence and effectiveness of the policy-making, and policy implementing structure, with the abolition of the pillar structure, and the codification of the exclusive, shared and supporting competences of the Union. In the fields of foreign affairs and security, the role of the High Representative of the Union for Foreign Affairs and Security Policy was extended. The High Representative was to be assisted in the fulfilment of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), by the new European External Action Service (EEAS) and the European Defence Agency (EDA).

Além disso, o Tratado postula em seu Artigo 83.º (TFUE), especificamente, que as questões relativas à cibercriminalidade situam-se no domínio da cooperação judiciária em matéria penal, o que, exercício pela UE de competências de interesse europeu, impulsionou a criação da Europol EC3⁴⁷ (antigo HTCC), que tornou-se um centro de referência oficial para políticas e regulação de combate ao cibercrime, devido ao seu carácter transfronteiriço (BELÁZ, 2019, p. 22). Dessa forma, Beláz (2019, p. 22) observa que, devido à extinção do sistema de

⁴⁴ Mais informações sobre os resultados e seguimentos do plano PICI em: <https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip>. Acesso em Ago.2020.

⁴⁵ COMUNICAÇÃO DA COMISSÃO EUROPEIA. COM(2010)245 final. Bruxelas, 19.5.2010. Item: “2.3. Confiança e segurança”.

⁴⁶ Resumo do ADE disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/64/una-agenda-digital-para-europa>. Acesso em Set. 2020. A ADE visa definir o papel fundamental que as TIC poderão vir a desempenhar (...) A fim de assegurar um ambiente digital equitativo, aberto e seguro (...) O objectivo geral da Agenda Digital é extrair benefícios económicos e sociais sustentáveis de um mercado único digital, com base na Internet rápida e ultra-rápida e em aplicações interoperáveis. **Fundamentos:** Embora os Tratados não contenham disposições específicas relativas às TIC, a UE pode tomar medidas pertinentes no quadro das políticas setoriais e horizontais, como: a política industrial (artigo 173.º do Tratado sobre o Funcionamento da União Europeia (TFUE)); a política da concorrência (artigos 101.º a 109.º); a política comercial (artigos 206.º e 207.º); a aproximação das legislações para melhorar o estabelecimento e o funcionamento do mercado interno (artigo 114.º); a livre circulação de mercadorias (artigos 28.º, 30.º, 34.º e 35.º); a livre circulação de pessoas, de serviços e de capitais (artigos 45.º a 66.º); etc. Todos estes elementos são essenciais para uma Europa digital.

⁴⁷ EC3 (Ato): COMUNICAÇÃO DA COMISSÃO EUROPEIA. COM(2012) 140 final de 28 de março de 2012. **Luta contra a criminalidade na era digital:** criação de um Centro Europeu da Cibercriminalidade.

pilares da UE, foi possível uma abordagem mais holística da cibersegurança, o que culminou na Estratégia da União Europeia para a Cibersegurança de 2013: Um ciberespaço aberto, seguro e protegido⁴⁸.

Assim, com base nas conclusões acima mencionadas da ADE, referindo-se à dependência das tecnologias e dos sistemas de informação que estão presentes em todos os segmentos da sociedade e economia, no sentido de reduzir as vulnerabilidades (prevenção e resposta), aumentar o grau de confiança nas TIC e realizar o mercado único digital, foi criada a primeira estratégia a utilizar a nomenclatura “cibersegurança” no título. A visão da UE apresentada nesta estratégia articula-se em cinco prioridades estratégicas:

- Garantir a resiliência do ciberespaço;
- Reduzir drasticamente a cibercriminalidade;
- Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da política comum de segurança e defesa (PCSD);
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança;
- Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da UE. (JOIN(2013) 1 final)

Esta estratégia foi publicada em duas partes. A primeira elencava as prioridades supracitadas e a segunda contemplava uma proposta para elaboração de uma Diretiva de segurança das redes e da informação (SRI) - concluída em 2016⁴⁹. Conforme explicam Kasper e Antonov (2019, p. 27), após a adoção da Estratégia de 2013, o termo ‘cibersegurança’ “*turned into a policy buzzword*” e a cibersegurança passou a ser parte integrante das políticas da UE.

Ao analisar a nova estratégia, Kasper e Antonov (2019, p. 27) revelam que o documento abordou a cibersegurança de uma forma abrangente e que as medidas propostas operariam em diferentes instrumentos normativos “*notably network and information security, law enforcement and defence, and on two levels, the national and EU level*”. Entre as principais ações e instrumentos desenvolvidos até a publicação da Diretiva SRI estavam: o reforço da ENISA, com a atribuição de criar uma rede funcional de resposta a emergências informáticas (CERT) e elaboração de requisitos mínimos de segurança das redes e da informação (SRI); aos EM coube a tarefa de estabelecer a CERT a nível nacional (até cobrir toda a Europa); aos EM também foi reforçada a necessidade de adesão à Convenção de Budapeste, assim como a criação de plataformas nacionais de alerta ou adaptá-las à plataforma para o cibercrime da Europol; a realização de operações de simulação de ataques em grande escala para testar estratégias de mitigação; o lançamento do Mês Europeu da Cibersegurança

⁴⁸ JOIN(2013) 1 final. Op.cit. (Estratégia para a Cibersegurança de 2013).

⁴⁹ DIRETIVA SRI. Op. Cit.

(European Cyber Security Month - ECSM); entre outras. Dessa forma, foi se desenvolvendo um novo modelo de governação multinível para a Cibersegurança pela UE, que teve de ser acompanhado progressivamente pelos EM na definição de suas políticas para o setor.

Assim, os processos de formulação e mudança de políticas que começaram no início de 2007 (fortalecidos pelo Tratado de Lisboa), até meados de 2016, eram o de construir uma cibersegurança resiliente, se tornar uma referência mundial e, ao mesmo tempo, adaptável a novos desafios. Apesar dos incidentes que iniciaram o período do “despertar” serem considerados ciberataques, a estratégia adotada, de acordo com Kasper e Antonov, foi:

Centered mostly on the importance of cybersecurity for economic reasons, but also mentions particular concerns, thereby implying what harms are considered: economic losses both in terms of damages and decreased productivity, decreased confidence of citizens to use e-services, physical and intangible harms to citizens, and the loss of autonomy for citizens outside the EU. (KASPER e ANTONOV, 2019, p. 27)

Embora tenha sido possível desenvolver uma estratégia abrangente e em diversas camadas neste período, conforme Beláz (2019, p. 23) destaca, o *modus operandi* continuou o mesmo: *“high-level information sharing and political cooperation platform”*. E continua, ao argumentar que *“behind this state of affairs is the lack of a truly pan-European vision of the role of the EU as an agent of cyber-security on the part of particular member states as well as the whole institution”* (SWILINSKI, 2014, p. 13 *apud* BELÁZ, 2019, p. 23).

Porém, buscando equacionar essas dificuldades e avançar para um modelo capaz de enfrentar os desafios impostos pelas ameaças, após esse longo período de despertar (de 2007 a meados de 2016) - onde a cibersegurança saiu de um patamar de subcategoria das TIC para um patamar de maior compreensão, priorização e abordagem holística – e com a publicação da Diretiva SRI, houve uma transformação da perspectiva da UE e do seu papel como agente de cibersegurança, para uma postura de liderança e a atribuição de maior grau de importância para questões relativas à ciberdefesa e ao combate às **ameaças híbridas**⁵⁰ (as ameaças híbridas incluem ações hostis com o objetivo de desestabilizar uma região ou um Estado, elas visam explorar as vulnerabilidades e, muitas vezes, pretendem minar os valores democráticos e liberdades fundamentais). Beláz (2019, p. 26) aponta que a partir deste momento começou a ser redesenhado o papel da UE e que *“this new approach is clearly a paradigm shift towards a more centralised policy-making and governance”*.

⁵⁰ COMUNICAÇÃO CONJUNTA. JOIN(2016) 18 final. Bruxelas, 6.4.2016. **Quadro comum em matéria de luta contra as ameaças híbridas**: uma resposta da União Europeia.

Esse *shift* foi evidenciado pela publicação de uma nova estratégia⁵¹, em 2017, denominada ‘Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE’, que inseriu um pacote de reformas na Cibersegurança e atualizou a Estratégia de 2013. A nova visão alterou a abordagem abrangente/holística para uma mais integrada, onde ameaças econômicas, políticas e estratégicas recebem igual atenção, e a cibersegurança passa a ser vista como uma questão de política horizontal e um desafio comum da sociedade.

Dessa forma, conforme Kasper e Antonov (2019, p. 28) descrevem, a nova abordagem vai além as áreas previamente declaradas NIS, cibercrime e ciberdefesa, e propõe medidas em responsabilidade pelo produto, proteção ao consumidor, mercado de trabalho, serviços financeiros, educação, comércio e campos de investimento. Além disso, os autores sublinham que a ênfase “*is on building resilience and deliver better EU response to cyber-attacks, signifying a shift from a reactive to a proactive approach*”. E continuam, ao avaliar que:

The threats outlined in the introduction part of the Communication imply that the EU is ready to address potential harms by different measures. The concern about negative economic impact of misuses and degradation in the functioning of computer systems is still central, however the issue has grown in magnitude and worries are expressed about potential economic destabilization, decreased political autonomy, disrespect for territorial integrity, physical harms, decrease in consumer trust and the decreased ability of states to provide order in the society by enforcing their laws. (KASPER e ANTONOV, 2019, p. 27)

Para melhor compreender o caminho percorrido pela UE até o momento atual elaborou-se um quadro resumido contendo as diferentes abordagens da UE nas questões de cibersegurança ao longo do tempo. Na próxima seção, serão abordadas as principais medidas e instrumentos que compõem o quadro geral da cibersegurança na UE vigente.

1985 – 2001 Fase Inicial	2002 – 2006 Fase Facilitadora	2007 – Jun/2016 Fase do Despertar	Jul/2016 – (...)Atual Fase Centralizadora
- Potencial das TICs para a economia; - Apoiada no 1º pilar, - Foco na privacidade e integridade das TIC; - Convenção de Budapeste para o cibercrime; - Soft power; - eSociety.	- Agente facilitador e incentivador; - Cibersec. como subcategoria das TICs; - Criação da ENISA e HTCC. - Interesses e práticas nacionais em primeiro lugar.	- Cybersec. como prioridade da UE; - Compreensão e autonomia do tema; - Ampliação da abordagem; - Assegurar TICs + diversos setores ciberdependentes; - Preocupação para a continuidade dos serviços essenciais; - Plano PICI; - Estratégia para a Cibersegurança 2013.	- UE Centraliza elaboração de medidas e políticas; - Postura de liderança; - Ações horizontais, multiníveis e de maior integração; - Legislação específica (Diretiva SRI, RGPD, Regulamento de Cibersegurança.) - Reforço da Ciberdefesa e combate a ameaças híbridas.

Tabela 2 – Fases das abordagens e perspectivas da UE para a Cibersegurança

⁵¹ COMUNICAÇÃO CONJUNTA. JOIN(2017) 450 final. Bruxelas, 13.9.2017. **Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE.** (Estratégia para a Cibersegurança de 2017).

3.2 Panorama geral da cibersegurança na UE

Como visto na seção anterior, o quadro jurídico em matéria de cibersegurança está ligado a Estratégia para a Cibersegurança de 2013, que estabeleceu como seu principal pilar a elaboração da Diretiva SRI – elemento jurídico central e a primeira legislação à escala da UE em matéria de cibersegurança. Com vistas a compreender o panorama geral e multifacetado da política de cibersegurança (que abrange ações em diversos setores e, principalmente, a segurança das redes e das informações, a proteção das infraestruturas críticas, a cibercriminalidade, a ciberdefesa e a desinformação), deve-se compreender que a estratégia supracitada está interligada às outras três adotadas posteriormente, assim como ao novo pacote para a Cibersegurança de 2017. De acordo com o TCE (2019, p. 14-15), são descritos abaixo esses elementos e como estão interligados para formar o panorama estratégico da cibersegurança na visão da UE:

- a **Agenda Europeia para a Segurança**⁵² que tem por finalidade melhorar a aplicação da lei e a resposta judicial ao fenómeno da cibercriminalidade, principalmente através da renovação das políticas e da legislação em vigor. Pretende ainda detetar os obstáculos às investigações penais sobre cibercriminalidade e estimular as iniciativas de reforço de capacidades em cibercriminalidade;
- a **Estratégia para o Mercado Único Digital**⁵³ que visa melhorar o acesso a bens e serviços digitais, criando as condições adequadas para maximizar o potencial de crescimento da economia digital. Para este efeito, é essencial reforçar a segurança, a confiança e a inclusão na Internet;
- a **Estratégia Global**⁵⁴ que tem por fim reforçar o papel da UE no mundo. A cibersegurança forma um pilar fundamental, graças a um compromisso renovado com as questões nesta matéria, à cooperação com os principais parceiros e à vontade de abordar essas questões em todos os domínios de intervenção, incluindo refutar a desinformação através de comunicação estratégica;
- e a **Estratégia para a Cibersegurança de 2017**⁵⁵, pacote de reforma que atualiza a estratégia de 2013, e contém um plano de ação para uma resposta rápida e coordenada a um ataque de grande envergadura e para a rápida aplicação da Diretiva SRI. Faz ainda parte do pacote a proposta do regulamento sobre a cibersegurança, com o fim de reforçar a ENISA e estabelecer um mecanismo de certificação à escala da UE. O pacote também propõe a adoção de legislação para a criação de um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, que deverá ser apoiado por uma rede de centros nacionais de coordenação. Estas estruturas ajudarão a reforçar a segurança do mercado único digital e a autonomia da UE no domínio da cibersegurança.

Nesse contexto, o panorama estratégico pode ser desmembrado em diversas medidas de política interna ou externa e instrumentos legais, que visam, além de assegurar o mercado único digital e a autonomia da UE em termos de cibersegurança, possibilitar o combate às

⁵² COMISSÃO EUROPEIA. **Agenda Europeia para a Segurança**. COM(2015) 185 final. 28.4.2015.

⁵³ COMISSÃO EUROPEIA. **Estratégia para o Mercado Único Digital na Europa**. COM(2015) 192 final. 6.5.2015.

⁵⁴ SERVIÇO EUROPEU PARA A AÇÃO EXTERNA (SEAE). **Estratégia Global para a Política Externa e de Segurança da União Europeia**. Visão partilhada, ação comum: uma Europa mais forte, junho de 2016.

⁵⁵ JOIN(2017) 450 final. Op.cit.

ciberameaças em diversos domínios, tais como: a luta contra a criminalidade organizada – onde a cibercriminalidade é elencada entre as prioridades para o período de 2018-2021⁵⁶; a política externa e de segurança comum – cuja prioridade é a dissuasão dos ciberataques; e a Ciberdefesa – cujo quadro foi atualizado e reforçado conforme será visto a seguir. Dessa forma, antes de abordar os instrumentos jurídicos centrais (Diretiva SRI e o Regulamento para a Cibersegurança), propõe-se a abordar o conjunto de medidas que fazem parte deste complexo panorama da Cibersegurança⁵⁷.

Devido à preocupação com a utilização do ciberespaço para fins políticos, estratégico-militares, espionagem e até mesmo guerra, e considerando os crescentes vínculos entre a cibersegurança e a ciberdefesa, foi elaborado um quadro Estratégico da UE para a Ciberdefesa⁵⁸ (atualizado em 2018), onde são definidas algumas prioridades, entre as quais, o desenvolvimento de capacidades de ciberdefesa e de proteção para a Política Comum de Segurança e Defesa (PCSD) e a cooperação entre as comunidades civis e militares de resposta a incidentes, cujo documento⁵⁹ salienta que um ciberincidente ou ciber crise grave “poderia constituir razão suficiente para um Estado-Membro invocar a cláusula de solidariedade e/ou a cláusula de assistência mútua da UE”⁶⁰.

⁵⁶ As dez prioridades da UE adotadas pelo Conselho baseiam-se nas recomendações formuladas na Avaliação da Ameaça da Criminalidade Grave e Organizada da UE (AACGO da UE), elaborada pela Europol. Disponível em: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>. Acesso em: Ago.2020.

⁵⁷ CONSELHO EUROPEU. Página de acolhimento > Políticas. **Cibersegurança na Europa:** regras mais rigorosas e uma melhor proteção. Disponível em: <https://www.consilium.europa.eu/pt/policies/cybersecurity/>. Acesso em Jul.2020.

⁵⁸ **Quadro Estratégico da UE para a Ciberdefesa** (atualizado em 2018), documento nº 14413/18, 19 de novembro de 2018. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pt/pdf>. Acesso em Ago. 2020.

⁵⁹ Ibid Idem (p. 6).

⁶⁰ **Cláusula de Assistência Mútua.** Esta cláusula está prevista no artigo 42.º n.º 7 do Tratado da União Europeia (TUE). A cláusula de assistência/defesa mútua é uma disposição em matéria de Política Comum de Segurança e Defesa (PCSD) e que estatui que “*se um Estado-Membro vier a ser alvo de agressão armada no seu território, os outros Estados-Membros devem prestar-lhe auxílio e assistência por todos os meios ao seu alcance, em conformidade com o artigo 51.º da Carta das Nações Unidas. Tal não afeta o carácter específico da política de segurança e defesa de determinados Estados-Membros*”. Numa resolução de 22 de novembro de 2012, o Parlamento Europeu contribuiu para uma interpretação mais rigorosa da cláusula, no que respeita aos tipos de ataques, referindo expressamente que o tipo de agressão a um EM pode não ser armada, mas tomar a forma de ciberataque a infraestruturas críticas, caso em que a cláusula pode ser ativada. Conteúdo disponível em: <http://euroogle.com/dicionario.asp?definicion=1788>. **Cláusula de Solidariedade.** O artigo 222.º do TFUE, estabelece que: «*A União e os seus Estados-Membros atuarão em conjunto, num espírito de solidariedade, se um Estado-Membro for alvo de um ataque terrorista ou vítima de uma catástrofe natural ou de origem humana*». No contexto da aprovação desta cláusula houve um intenso debate sobre a sua estruturação como um mecanismo de defesa comum, mas os trabalhos comprovam que este instrumento foi perspectivado com o objetivo de fazer face a ameaças de realidades não-estatais. Por outro lado, a cláusula de assistência mútua prossegue esses objetivos de intervenção em caso de agressão militar de Estado para Estado. Este debate ressurgiu em 2015, quando a França recorreu à cláusula de assistência mútua e não à de solidariedade, nos ataques de Paris de 13 de novembro. Conteúdo disponível em: <http://euroogle.com/dicionario.asp?definicion=364>. Acessos em Ago. 2020.

Ademais, o âmbito da ciberdefesa integra o quadro de Cooperação Estruturada Permanente (CEP)⁶¹ e da cooperação UE-NATO, assim como o Quadro Comum da UE em matéria de luta contra as ameaças híbridas (2016), onde consta a necessidade de: compreender melhor esse fenómeno (ameaças emergentes) e seus vetores de ameaças (que incluem campanhas de desinformação, entre outros fenómenos político-sociais que dão origem este tipo de ameaça); de aumentar as capacidades de resposta; e de intensificar a cooperação entre a UE e a NATO - que foi consubstanciada nas Declarações Conjuntas UE-NATO de 2016 e 2018⁶² (TCE, 2019, p. 15). Para complementar este panorama, em 2017, o Conselho adotou conclusões sobre um quadro com instrumentos de ciberdiplomacia⁶³ para uma resposta conjunta da UE, que estabeleceu, inclusivamente, a imposição de medidas restritivas para responder a ciberatividades maliciosas de grande impacto. Posteriormente, o Conselho publicou um quadro com medidas restritivas/sanções específicas⁶⁴ destinadas a dissuadir e responder aos ciberataques que constituam ameaça externa à União ou aos seus Estados-Membros, bem como prorrogou este regime de sanções até 18 de maio de 2021⁶⁵. Além disso, este quadro também estabelece que:

⁶¹ A **Política Externa e de Segurança Comum (PESC)** da União Europeia foi instituída em 1993, tendo desde então sido reforçada pelos Tratados subsequentes, que criou uma série de novos intervenientes no domínio da PESC, incluindo o cargo de Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, que exerce também as funções de Vice-Presidente da Comissão (VP/AR) e o novo cargo de Presidente permanente do Conselho Europeu. Além disso, criou o Serviço Europeu para a Ação Externa (SEAE) e elevou a um novo patamar a **Política Comum de Segurança e Defesa (PCSD)**, que constitui parte integrante da PESC. A base jurídica da PESC está disposta nos artigos 21.º a 46.º do Título V do TUE que estabelecem as «Disposições Gerais Relativas à Ação Externa da União e Disposições Específicas Relativas à Política Externa e de Segurança Comum (PESC)». (...) Em termos operacionais, a visão definida na Estratégia Global (supramencionada) relativamente às questões de segurança e defesa, a VP/AR apresentou ao Conselho dos Negócios Estrangeiros, em novembro de 2016, um plano de execução da PCSD que identifica três conjuntos de prioridades: dar resposta aos conflitos e crises externos, desenvolver as capacidades dos parceiros e proteger a União e os seus cidadãos, bem como cria uma **cooperação estruturada permanente (CEP)** única para os Estados-Membros que desejem assumir maiores compromissos em matéria de defesa e de segurança. Em 6 de março de 2018, o Conselho adotou um roteiro para a aplicação da CEP que conta atualmente, com a participação de 25 Estados-Membros. Este conteúdo está disponível em: <https://www.europarl.europa.eu/factsheets/pt/sheet/158/politica-externa-objetivos-instrumentos-e-realizacoes>. Acesso em Set. 2020.

⁶² COMISSÃO EUROPEIA/SEAE. **Quadro comum em matéria de luta contra as ameaças híbridas**: uma resposta da União Europeia, JOIN(2016) 18 final, de 6 de abril de 2016; e Declarações Conjuntas dos Presidentes do Conselho Europeu e da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte, 8 de julho de 2016 e 10 de julho de 2018.

⁶³ CONCLUSÕES DO CONSELHO sobre um quadro para resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia"), **DOC. Nº 9916/17**, de 7 de junho de 2017. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pt/pdf>. Acesso em Ago. 2020.

⁶⁴ DECISÃO DO CONSELHO relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros Bruxelas, 14 de maio de 2019 (OR. en) **DOC. Nº 7299/19**. Disponível em: <https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/pt/pdf>. Acesso em Ago. 2020.

⁶⁵ CONSELHO DA UE, Comunicado de imprensa de 14 de maio de 2020. Conselho prorroga regime de sanções contra os ciberataques até 18 de maio de 2021. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2020/05/14/cyber-security-council-extends-sanctions-regime-until-18-may-2021/>. Acesso em Ago. 2020.

Sempre que for considerado necessário para atingir os objetivos da PESC nas disposições pertinentes do artigo 21.º do Tratado da União Europeia, a presente decisão também possibilita que sejam aplicadas medidas restritivas em resposta aos ciberataques com um efeito significativo contra Estados terceiros ou organizações internacionais.

Para finalizar o panorama geral, consta na Estratégia de 2017⁶⁶ a necessidade de melhoria na eficácia da investigação e da ação penal contra a cibercriminalidade potenciada pelo ciberespaço e dificultada pelo problema da atribuição e da necessidade de cooperação transfronteiras. Para isso, a Comissão propôs, em abril de 2018, novas regras para facilitar e agilizar o acesso às provas eletrónicas armazenadas noutro Estado-Membro, permitindo às autoridades judiciais de um país solicitar diretamente o acesso às provas eletrónicas a um prestador de serviços noutro país da UE; esta proposta inclui duas medidas legislativas: 1. um regulamento relativo às ordens de entrega ou de conservação de provas eletrónicas; 2. e uma diretiva relativa aos representantes legais⁶⁷.

Além dessas medidas, no âmbito de investigações criminais, também consta na referida estratégia o desenvolvimento de uma plataforma eletrónica para intercâmbio de informações na UE, e a normalização dos formulários utilizados para a cooperação judiciária entre os EM. Adicionalmente, está sendo negociado o aditamento de um protocolo à Convenção de Budapeste⁶⁸, o que poderá proporcionar abordar a questão do acesso transfronteiriço a provas eletrónicas num contexto internacional. Nesse contexto, a Estratégia de 2017 frisa que ao invés de elaborar novos instrumentos jurídicos internacionais para as questões da cibercriminalidade “a UE apela para que todos os países elaborem legislação nacional adequada e prossigam a cooperação no âmbito do quadro internacional existente”⁶⁹.

Paralelamente ao panorama exposto, em maio de 2018, iniciou-se a aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD)⁷⁰ que objetiva proteger os dados

⁶⁶ JOIN(2017) 450 final. Op.cit. p. 16.

⁶⁷ O regulamento relativo às ordens de entrega ou de conservação de provas eletrónicas permitirá às autoridades aceder às provas eletrónicas armazenadas pelos prestadores de serviços independentemente do local de armazenamento. A diretiva relativa aos representantes legais obrigará todos os prestadores de serviços a designarem um representante legal na UE. Este será responsável por receber e respeitar as decisões e ordens. O objetivo é assegurar que todos os prestadores de serviços a operar na UE tenham as mesmas obrigações no que se refere às provas eletrónicas. Conteúdo disponível em: <https://www.consilium.europa.eu/pt/policies/e-evidence/>. Acesso em Set. 2020.

⁶⁸ Termos de referência para a elaboração de um projeto de 2.º Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime, T-CY (2017). E COMISSÃO EUROPEIA. Recomendação de DECISÃO DO CONSELHO que autoriza a participação nas negociações respeitantes ao Segundo Protocolo Adicional à Convenção do Conselho da Europa sobre o Cibercrime (STCE-185). Bruxelas, 5.2.2019. COM(2019) 71 final.

⁶⁹ JOIN(2017) 450 final. Op.cit. p. 17.

⁷⁰ 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). O Considerando nº 1 dispõe que: A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito

pessoais estipulando regras sobre o seu tratamento e divulgação. Neste diploma constam os requisitos de notificação à autoridade nacional de proteção de dados para os casos de violações, onde as sanções podem chegar a 20 milhões de euros ou 4% do volume de negócios anual mundial. Este dispositivo é complementar ao panorama da cibersegurança no que concerne à salvaguarda da proteção de dados pessoais e da privacidade.

A partir do panorama geral descrito, pode-se perceber o ecossistema complexo e multifacetado desenvolvido pela UE para lidar com as questões de cibersegurança. As dificuldades em avançar nas questões de segurança necessárias para lidar com este tema que extrapola as fronteiras são, sobretudo, juspolíticos, agravados pelo grau de desconfiança da UE como agente de cibersegurança para lidar com questões sensíveis aos EM, no que tange à legitimidade dos atores de regulação e à fiscalização e controlo político e judicial. Construir um quadro multinível coerente para esta matéria constitui um desafio, uma vez que envolve medidas em diversas áreas e diversos intervenientes, e a necessidade de equacionar as questões sensíveis aos EM. Assim, buscou-se elencar os principais elementos que formam a abordagem estratégica atual da UE em matéria de cibersegurança, para na próxima seção analisar os instrumentos jurídicos centrais vigentes (Diretiva SRI e o Regulamento para a Cibersegurança).

4. PRINCIPAIS INSTRUMENTOS JURÍDICOS

Após analisar o caminho escolhido pela UE em termos de estratégia e objetivos, e passar pelo panorama geral, para uma melhor compreensão da amplitude do domínio da cibersegurança, pretende-se, a partir deste ponto, expor resumidamente as principais disposições da Diretiva (UE) 2016/1148⁷¹ sobre a segurança das redes e da informação (SRI) e do o Regulamento (UE) 2019/881⁷² de Cibersegurança e tecer algumas considerações quanto a base jurídica utilizada e a aplicação dos princípios da subsidiariedade e proporcionalidade.

4.1 A Diretiva SRI

Esta diretiva constitui o pilar principal da Estratégia para a Cibersegurança de 2013, foi primeiro ato legislativo à escala da UE nesta matéria e tem como destinatários os Estados

fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.

⁷¹ DIRETIVA SRI. Op. Cit.

⁷² REGULAMENTO DA CIBERSEGURANÇA. Op.Cit.

Membros (Artigo 27º)⁷³. Dentre os 75 considerandos, pode-se destacar o nº. 3 que identifica as principais motivações e o âmbito de atuação, conforme o exposto a seguir:

(3) As redes e os sistemas de informação e, sobretudo, a Internet desempenham um papel crucial para facilitar a circulação transfronteiriça de mercadorias, de serviços e de pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas, intencionais ou não, e independentemente do local onde ocorram, podem afetar os Estados-Membros, individualmente considerados, e a União no seu conjunto. Por consequência, a segurança das redes e dos sistemas de informação é essencial para o bom funcionamento do mercado interno.

Dessa forma, a diretiva se propõe a criar um **mecanismo de resposta** aos incidentes que possam prejudicar os serviços essenciais para o funcionamento da sociedade e do mercado interno e tem como objetivo estabelecer medidas para alcançar um elevado nível comum de segurança das redes e dos sistemas de informação (SRI) na União (artigo 1º). Uma vez que este objetivo pode não ser suficientemente alcançado pelos Estados-Membros isoladamente considerados, devido aos efeitos da ação proposta, poderá ser mais bem alcançado ao nível da União, através de medidas que sejam adotadas em conformidade com o princípio da subsidiariedade e da proporcionalidade consagrados no artigo 5.º do TUE⁷⁴. Para atingir esse objetivo, a presente diretiva estabelece o seguinte⁷⁵:

- a) estabelece a obrigação de os EM adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação (Artigo 7º);
- b) cria um grupo de cooperação a fim de apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os EM e de desenvolver a confiança entre eles (Artigo 11º);
- c) cria uma rede de equipas de resposta a incidentes de segurança informática («rede de CSIRT⁷⁶») a fim de contribuir para o desenvolvimento da confiança entre os EM e de promover uma cooperação operacional célere e eficaz (Artigo 12º);
- d) estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais – OSE (Artigo 14º) e para os prestadores de serviços digitais (Artigo 16º);

⁷³ Os Artigos e Considerandos informados nesta seção estão dispostos na Diretiva SRI. Os dispositivos de outros instrumentos legais serão informados seguidos do respetivo diploma.

⁷⁴ DIRETIVA SRI. Op. Cit. Considerando nº. 74 “a presente diretiva não excede o necessário para alcançar esse objetivo”.

⁷⁵ DIRETIVA SRI. Op.cit. Nota 6. Artigo 1º, n. 2.

⁷⁶ DIRETIVA SRI. Op. Cit. ANEXO I. **Equipas de Resposta a Incidentes de Segurança Informática (CSIRT)**. Suas atribuições estão definidas no ponto 2 do Anexo I, e são elas: a) As atribuições das CSIRT devem incluir pelo menos o seguinte: “i) monitorizar os incidentes a nível nacional, ii) ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às partes interessadas relevantes sobre riscos e incidentes, iii) intervir em caso de incidentes, iv) proceder à análise dinâmica dos riscos e dos incidentes e ter uma visão geral da situação, v) participar na rede de CSIRT; b) As CSIRT devem estabelecer relações de cooperação com o setor privado; c) A fim de facilitar a cooperação, as CSIRT devem promover a adoção e a utilização de práticas comuns ou normalizadas para: i) os procedimentos de gestão de risco e de incidentes, ii) os sistemas de classificação de incidentes, de risco e de informações”.

e) e estabelece a obrigação de os EM designarem as autoridades nacionais competentes, os pontos de contacto únicos e as CSIRT com atribuições relacionadas com a segurança das redes e dos sistemas de informação (Artigo 8º, 9º, 10º e Anexo I).

Além disso, a diretiva designa para cada EM a obrigação de identificar os operadores de serviços essenciais de cada setor que estejam estabelecidos em seu território - cujos critérios de identificação estão dispostos no artigo 5º, n. 2⁷⁷ - e de revisar esta lista de operadores identificados a cada dois anos (e atualizar se for caso). Os setores considerados essenciais a serem abrangidos pelas medidas da diretiva são os seguintes:

Operador de serviços essenciais – OSE (Anexo II, Diretiva SRI):

1. Energia: a) Eletricidade, b) Petróleo, c) Gás;
2. Transportes: a) Transporte aéreo, b) Transporte ferroviário, c) Transporte marítimo e por vias navegáveis interiores, d) Transporte rodoviário;
3. Setor bancário;
4. Infraestruturas do mercado financeiro;
5. Setor da saúde: Instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas);
6. Fornecimento e distribuição de água potável;
7. Infraestruturas digitais: Pontos de troca de tráfego, Prestadores de serviços de DNS, Registos de nomes de domínio de topo.

Prestadores de Serviços digitais – PSD (Anexo III, Diretiva SRI):

1. Mercados em linha;
2. Motores de pesquisa em linha;
3. Serviços de computação em nuvem.

Adicionalmente, a Diretiva estabelece obrigações para os OSE e pelos PSD de atenderem a requisitos mínimos relativos a medidas técnicas e de segurança adequadas, e a notificar as autoridades nacionais ou as CSIRT da ocorrência de qualquer incidente grave.

Em relação aos requisitos de segurança a serem cumpridos, a diretiva não os especifica, somente estabelece que os EM devem assegurar que os operadores de serviços essenciais e digitais se adequem técnica e organizacionalmente para garantir um nível adequado de segurança das redes e sistemas utilizados em suas operações, de forma a evitar os incidentes que afetem a segurança e a continuidade dos serviços e para reduzir ao mínimo o seu impacto. Para isso, devem ter em conta os progressos técnicos mais recentes, a implementação de medidas de gestão de riscos, o tratamento dos incidentes, a realização de auditorias e testes e a conformidade com normas internacionais. Apesar disso, a União emite recomendações de

⁷⁷ DIRETIVA SRI. Op. Cit. Artigo 5º, n. 2. Os critérios para a identificação dos operadores de serviços essenciais referidos no artigo 4.o, ponto 4, são os seguintes: “a) Uma entidade presta um serviço essencial para a manutenção de atividades societárias e/ou económicas cruciais; b) A prestação desse serviço depende de redes e sistemas de informação; e c) Um incidente pode ter efeitos perturbadores importantes na prestação desse serviço”.

cibersegurança setoriais⁷⁸ com diretrizes técnicas mais específicas. Além disso, a ENISA também presta apoio aos operadores para auxiliá-los quanto ao cumprimento desses requisitos.

Relativamente à obrigação de notificação, os OSE devem notificar à autoridade competente os incidentes graves. Para determinar a gravidade do impacto de um incidente, devem ser considerados os seguintes parâmetros: a) o número de utilizadores afetados pela perturbação do serviço essencial; b) a duração do incidente; c) a distribuição geográfica, no que se refere à zona afetada pelo incidente. Por sua vez, em relação aos PSD, além dos parâmetros mencionados, para determinar a gravidade do incidente também deve ser considerado o seguinte: d) o nível de gravidade da perturbação do funcionamento do serviço; e) a extensão do impacto nas atividades económicas e societárias. Adicionalmente, quando o incidente der origem à violação de dados pessoais, as autoridades competentes devem trabalhar em colaboração com as autoridades encarregadas da proteção de dados.

Caso os operadores e prestadores não cumpram com as obrigações supracitadas, a diretiva estabelece que os EM devem impor sanções que sejam efetivas, proporcionadas e dissuasivas. Além disso, as entidades que não forem identificadas pelos EM podem notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados. Contudo, neste caso, não pode dar origem à imposição de obrigações a que não estariam sujeitas por força da diretiva (Artigo 20º).

Finalmente, a diretiva propõe medidas para uma harmonização mínima no âmbito da UE relativa à SRI, mas estabelece que os EM podem adotar disposições destinadas a atingir um nível mais elevado de SRI em seu território (Artigo 3º). A referida diretiva foi publicada em julho de 2016 e estabeleceu o prazo de transposição até maio de 2018. Em suma, a Diretiva SRI introduz requisitos de segurança e de notificação como obrigações jurídicas para os principais agentes económicos responsáveis pela operação de serviços essenciais (OSE) e prestação de serviços digitais (PSD), bem como a adoção de estratégias de cibersegurança e de equipes de resposta com ponto de contacto único para os EM para tratamento e resposta a incidentes de cibersegurança, e cria uma rede de resposta e cooperação a nível da UE, onde a ENISA desempenha um papel fundamental na implementação dessas medidas. Ou seja, basicamente a diretiva corresponde a um mecanismo de **resposta**, pois trabalha no sentido da redução do impacto dos incidentes (consequências) através de uma resposta coordenada, e também, em menor grau (já que não especifica em pormenor quais são os requisitos de cibersegurança a

⁷⁸ Como, por exemplo, a RECOMENDAÇÃO (UE) 2019/553 DA COMISSÃO de 3 de abril de 2019 sobre a cibersegurança no setor da energia.

serem cumpridos), na preparação (origem) para a ocorrência de incidentes graves nas infraestruturas críticas.

4.2 O Regulamento da Cibersegurança da UE

O Regulamento (UE) 2019/881 sobre a cibersegurança da UE⁷⁹, aprovado em 17 de abril de 2019 pelo Parlamento Europeu e Conselho, é relativo ao um novo mandato para a Agência da União Europeia para a Cibersegurança (ENISA) e a criação de um quadro de certificação à escala da UE, cujo objeto e âmbito de aplicação enunciado é o seguinte:

Com vista a assegurar o bom funcionamento do mercado interno e, simultaneamente, a alcançar um nível elevado de cibersegurança, de ciber-resiliência e de confiança no seio da União, o presente regulamento estabelece:

- a) Os objetivos, as atribuições e os aspetos organizativos da ENISA («Agência da União Europeia para a Cibersegurança»); e
- b) Um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de TIC na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União.

A ENISA criada pelo presente regulamento, sucede à ENISA criada pelo Regulamento (UE) n.º 526/2013. Este, foi revogado por força do novo instrumento devido ao entendimento que: o contexto geral de ação política da UE em matéria de cibersegurança foi alterado significativamente; o ambiente mundial se tornou mais incerto e menos seguro; foram atribuídas à ENISA novas funções por força da Diretiva SRI; a agência também deverá exercer as atribuições conferidas pelo presente regulamento e pelos outros atos jurídicos da União no domínio da cibersegurança; e o mandato previsto no Regulamento (UE) n.º 526/2013 (até junho de 2020) não era suficiente. Portanto, o novo Regulamento transforma a ENISA em uma agência de Cibersegurança de caráter permanente, define suas atribuições⁸⁰, sua estrutura

⁷⁹ REGULAMENTO DA CIBERSEGURANÇA. Op. Cit. Os Artigos e Considerandos informados nesta seção estão dispostos no Regulamento da Cibersegurança de 2019. Os dispositivos de outros instrumentos legais serão informados seguidos do respetivo diploma.

⁸⁰ REGULAMENTO DA CIBERSEGURANÇA. Op. Cit. A ENISA possui atribuições relativas: à elaboração e execução da política e do direito da União (Artigo 5º); ao reforço das capacidades na União para melhorar a prevenção, a deteção e a análise de ciberameaças e incidentes e a capacidade de resposta (Artigo 6º); à cooperação operacional a nível da União, apoiando os EM, as instituições, os órgãos e os organismos da União e as partes interessadas, incluindo a CERT-UE, Rede CSIRT, os serviços que se ocupam da cibercriminalidade e autoridades competentes pela Diretiva SRI e RGPD (Artigo 7º); ao Mercado, certificação da cibersegurança e normalização, onde apoia e promove a elaboração e a execução da política da União em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC, conforme dispõe o título III do presente regulamento (Artigo 8º); à cooperação internacional, no âmbito dos quadros de cooperação internacional com países terceiros e organizações internacionais no acompanhamento de exercícios, intercâmbio de informações e melhores práticas e apoio a acordos de reconhecimento mútuo; e à investigação, inovação, sensibilização, educação e conhecimento.

organizacional⁸¹, as regras de funcionamento, o regime orçamental, o quadro pessoal e as formas de desenvolvimento e acompanhamento dos trabalhos agência.

Além disso, o regulamento cria o Grupo das partes interessadas para a certificação da cibersegurança (Artigo 22º), copresidido pela ENISA e cujo secretariado é garantido pela agência, que é constituído por peritos a serem selecionados por concurso transparente e aberto, que terão a função de aconselhar a Comissão sobre questões estratégicas relacionadas com o enquadramento europeu para a certificação da cibersegurança e na elaboração do Programa de trabalho evolutivo da União para a certificação europeia da cibersegurança⁸² (Artigo 47º). A Comissão, com o apoio do Grupo Europeu para a Certificação da Cibersegurança (GECC – Artigo 62º)⁸³ e o grupo das partes interessadas para a certificação da cibersegurança supracitado, após a realização de uma consulta aberta e alargada, devem preparar e publicar o referido programa, na forma de instrumento não vinculativo. O programa compreende, designadamente, uma lista dos produtos, serviços e processos de TIC ou das respetivas categorias, que podem beneficiar da inclusão no âmbito de aplicação de um sistema europeu de certificação da cibersegurança e deverá ser atualizado, pelo menos de três em três anos, ou com maior regularidade.

Nos termos do regulamento, o recurso à certificação europeia da cibersegurança e a declarações UE de conformidade deverá ser voluntário, salvo disposição em contrário. No entanto, os EM podem adotar regulamentação que preveja a certificação obrigatória (Considerando 91). Além disso, para algumas áreas, poderá vir a ser necessária a imposição de

⁸¹ REGULAMENTO DA CIBERSEGURANÇA. Op.cit. A estrutura da ENISA será composta por: (a) um conselho de administração composto por um membro nomeado por cada EM e dois membros nomeados pela Comissão, com mandato de quatro em quatro anos renovável; b) uma comissão executiva que assiste ao conselho de administração e prepara as decisões a serem deliberadas; c) um diretor executivo que deve gerir a ENISA e desempenhar as suas funções com independência, responder perante o conselho de administração e apresentar ao Parlamento Europeu relatórios sobre o desempenho das suas funções; d) um grupo consultivo da ENISA para aconselhamento quanto ao exercício das suas atribuições (exceto quanto à aplicação do título III do regulamento); e) uma rede dos agentes nacionais de ligação que servem de ponto de contacto a nível nacional para facilitar a cooperação entre a ENISA e os peritos nacionais de intercâmbio de informações entre a ENISA e os EM e apoia a ENISA na divulgação das suas atividades, conclusões e recomendações às partes interessadas em toda a União.

⁸² REGULAMENTO DA CIBERSEGURANÇA. Op.cit. O Programa de trabalho evolutivo da União para a certificação europeia da cibersegurança é um documento estratégico que deve permitir que a indústria, as autoridades nacionais e os organismos de normalização, em particular, se preparem com antecedência para os futuros sistemas europeus de certificação da cibersegurança.

⁸³ REGULAMENTO DA CIBERSEGURANÇA. Op.cit. Artigo 62º, n. 1. É criado o grupo europeu para a certificação da cibersegurança (a seguir designado «GECC»). 2. O grupo é composto por representantes das autoridades nacionais de certificação da cibersegurança (...) O GECC tem as seguintes atribuições: aconselhar e assistir a Comissão no seu trabalho de assegurar a execução e aplicação coerentes do presente título, nomeadamente no que se refere ao programa de trabalho evolutivo da União, às questões da política de certificação da cibersegurança, à coordenação das abordagens políticas e à elaboração de sistemas europeus de certificação da cibersegurança; entre outras.(...) 5. Com a assistência da ENISA, a Comissão preside ao GECC e assegura a prestação dos seus serviços de secretariado ao GECC.

determinados requisitos de segurança e tornar obrigatória a certificação, a fim de elevar o nível de cibersegurança na União (Artigo 56º).

O sistema de certificação deverá especificar um conjunto mínimo de elementos que deverão incluir: o âmbito de aplicação e o objeto da certificação da cibersegurança, designadamente as categorias de produtos, serviços e processos de TIC abrangidos; a especificação pormenorizada dos requisitos de cibersegurança; os critérios e métodos de avaliação; o nível previsto de garantia; entre outros (Artigo 54º). Além disso, devem levar em conta domínios setoriais nos quais é aplicada a certificação. Dessa forma, o sistema de certificação a ser criado deverá conter especificações para um enquadramento coerente dos produtos, serviços e processos a serem certificados correspondente ao nível de garantia do certificado emitido, que poderá ser: básico, substancial ou elevado. Já a declaração UE de conformidade, poderá ser emitida a partir do nível de garantia básico (Artigo 52º).

Portanto, o enquadramento europeu para a certificação da cibersegurança tem a finalidade de evitar a fragmentação do mercado interno de produtos, serviços e processos de TIC, a fim de melhorar as condições de funcionamento elevando o nível de cibersegurança na UE e permitindo uma abordagem harmonizada. A partir do nível de garantida certificado, é possível atestar⁸⁴ o cumprimento de requisitos de segurança, aumentar a resiliência da UE como um todo para resistir e responder às ciberameaças e elevar o grau de confiança da sociedade e do mercado. Ou seja, o regulamento corresponde a uma medida que trabalha na **origem** do problema, pois busca aumentar a resiliência a nível da UE, inclusive, no caso de novos produtos de TIC, a partir da conceção (*by design*).

4.3 Base Jurídica, Subsidiariedade e Proporcionalidade

Primeiramente, antes de abordar os critérios de enquadramento dos instrumentos jurídicos vigentes que tratam da cibersegurança, cabe mencionar que, por força do princípio da atribuição (art. 5.º, n.º 1 e 2, TUE), a União exerce as competências que lhe foram atribuídas pelos Tratados para alcançar os objetivos por estes fixados, onde as demais atribuições ficam reservadas aos EM. Porém, conforme coloca Campos e Campos (2010, p. 277), “o Tratado não delimita com absoluto rigor, por âmbitos materiais ou de funções, as competências conferidas

⁸⁴ Artigo 46º. “Atestar que os produtos, serviços e processos de TIC que tenham sido avaliados de acordo com esses sistemas de certificação cumprem os requisitos de segurança especificados, para efeitos da proteção da disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, ou as funções ou serviços oferecidos por esses produtos, serviços e processos ou acessíveis por seu intermédio ao longo do respetivo ciclo de vida”.

à União e as reservadas para os EM”, e isto não obstante o art. 2 do TFUE⁸⁵. Por isso, de acordo com os autores (2010, p. 278), existe um fenómeno de retração no domínio das competências reservadas aos EM que acelerou fortemente por força do TUE, e, particularmente, como resultado da União Económica e Monetária. Assim, associado ao princípio da atribuição, para evitar o esvaziamento das competências dos EM, contrabalancear o poder de intervenção e ingerência da UE, e, entretanto, permitir o alcance dos objetivos a que UE se propõe, a fórmula encontrada foi a adoção do princípio da subsidiariedade, consagrado no art. 5.º, n.º 3⁸⁶, do TUE, que rege, em conjunto com o princípio da proporcionalidade, o exercício das competências da União, nos domínios de competência concorrente entre a UE e EM.

Cabe ressaltar, que a ideia moderna do princípio da subsidiariedade deveu-se a doutrina social da Igreja Católica⁸⁷, que expõe que, a subsidiariedade serve como critério de limitação do grau de ingerência dos poderes, mas também como exigência de atuação sempre que as necessidades do corpo social ou a dimensão da função a prosseguir tornem insuficiente a ação das instâncias menores. Ou seja, a subsidiariedade funciona como uma matriz ordenadora entre os vários níveis de decisão, que, por um lado, estimula a existência de competências comunitárias, ao impor que a UE deve agir quando os objetivos pretendidos possam ser melhor alcançados ao nível da União, e, por outro lado, impõe uma limitação, que implica que a UE não deve atuar quando a ação dos EM for suficiente para alcançar os objetivos pretendidos. (DUARTE, 2000, p. 108)

Além disso, a aplicação do princípio da subsidiariedade acompanha o processo de integração da UE, o que, de acordo com Vidal (2017, p. 50) “*ha permitido organizar la división*

⁸⁵ Artigo 2.º, n.º 2 (TFUE): “Quando os Tratados atribuam à União competência partilhada com os Estados-Membros em determinado domínio, a União e os Estados-Membros podem legislar e adotar atos juridicamente vinculativos nesse domínio. Os Estados-Membros exercem a sua competência na medida em que a União não tenha exercido a sua. Os Estados-Membros voltam a exercer a sua competência na medida em que a União tenha decidido deixar de exercer a sua”.

⁸⁶ Artigo 5.º n.º 3 (TUE): “Em virtude do princípio da subsidiariedade, nos domínios que não sejam da sua competência exclusiva, a União intervém apenas se e na medida em que os objetivos da ação considerada não possam ser suficientemente alcançados pelos Estados-Membros, tanto ao nível central como ao nível regional e local, podendo contudo, devido às dimensões ou aos efeitos da ação considerada, ser mais bem alcançados ao nível da União. As instituições da União aplicam o princípio da subsidiariedade em conformidade com o Protocolo relativo à aplicação dos princípios da subsidiariedade e da proporcionalidade. Os Parlamentos nacionais velam pela observância do princípio da subsidiariedade de acordo com o processo previsto no referido Protocolo”.

⁸⁷ GORJÃO-HENRIQUES, Miguel. **Direito da União** (2014, p. 334). O princípio da subsidiariedade é por esta formulado da seguinte forma: “uma sociedade de ordem superior não deve interferir na vida interna duma sociedade de ordem inferior, privando-a das suas competências, mas deve antes apoiá-la em caso de necessidade e ajudá-la a coordenar a sua acção com a das outras componentes sociais, com vista ao bem comum” (cfr. SS. Pio XI, Carta Enclítica Quadragesimo Anno, I, 1931, pp. 184-186; vide ainda SS. João XXIII, Mater et Magistra, 1961, n.º 55). O princípio opõe-se assim a todas as formas de coletivismo e traça os limites da intervenção do Estado, tendendo a instaurar uma verdadeira ordem internacional (Catecismo da igreja Católica, 1993, p.1885, pág. 411).

del creciente número de competencias compartidas entre la UE, los Estados miembros y los niveles de gobierno subestatales". Segundo o autor, este princípio encontra-se ligado a Governação Multinível (MLG sigla em inglês) que na prática funciona como um sistema de ingerência das relações entre os diversos níveis de governação entre a UE e os EM, incluso, todo o sistema de atores, valores e ações que influenciam direta ou indiretamente no processo de tomada de decisão tanto dentro de um nível de governo, como nas relações entre os vários níveis. Ademais, conforme explica Vidal:

*Ambos conceptos están relacionados con un tercero, el del principio de atribución de competencias. Tanto la subsidiariedad como la MLG reposan sobre la cuestión crucial de determinar cuál es la atribución adecuada de competencias entre la UE y los niveles nacional o subnacionales. Como ya se aclaró en el art. 4, TFUE, la mayoría de los ámbitos de la política públicas son ahora competencia compartida entre la UE y los otros niveles de gobierno. Dicho de otro modo, si bien la UE debe actuar dentro del marco de sus competencias atribuidas, el art. 4, TFUE indica que la mayoría de las competencias de la UE gozan de una competencia de atribución compartidas con otros niveles, nacionales o subnacionales de gobierno. Decidir en todos esos casos cómo se articula esta competencia de atribución es, en el plano jurídico, responsabilidad del principio de subsidiariedad, por cuanto que la **MLG se ocupa más de la praxis política y la de políticas públicas en el sentido de cómo se ejercen esas competencias compartidas** (VIDAL, 2017, P. 51)*

Contudo, conforme explica o autor, o reconhecimento da MLG tem ocorrido de uma maneira mais implícita *"fundamentalmente en la legislación derivada de la UE y, sobre todo, en la aplicación práctica de las políticas de la UE"* (VIDAL, 2017, P. 51). A partir deste entendimento, pode-se observar que o quadro estratégico e legislativo estabelecido para a cibersegurança se insere no carácter prático da MLG, e ao mesmo tempo, não foge de uma interpretação mais expansiva das competências da UE. Isso decorre, tanto do enquadramento da cibersegurança no âmbito das competências compartilhadas, ou seja, nos domínios em que uma intervenção da UE tenha uma vantagem acrescida face a uma intervenção dos EM, quanto da fundamentação dos dois instrumentos jurídicos vigentes (Diretiva SRI e Regulamento da Cibersegurança) com base no artigo 114º do TFUE⁸⁸, relativo à adoção de medidas legislativas de aproximação, em conformidade com a realização dos objetivos enunciados no artigo 26º do mesmo tratado, que visa a estabelecer o mercado interno ou a assegurar o seu funcionamento. Mas também, decorre da quadro alargado da governação da cibersegurança e da necessidade de avanço nas questões que envolvem a segurança interna, o que seria reservada aos EM.

Ambos os instrumentos possuem graus de incidência diferentes, nos termos do artigo 288º do TFUE⁸⁹, onde a sua escolha deve levar em conta o binômio: ‘capacidade de harmonizar

⁸⁸ DIRETIVA SRI. Op.cit. e REGULAMENTO DA CIBERSEGURANÇA. Op.cit. Ambos citam: “Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º”.

⁸⁹ A diretiva vincula o EM quanto aos resultados, mas cabe ao mesmo a competência quanto à forma e aos meios, ou seja, o objetivo não é a unificação do direito, mas uma aproximação das diversas legislações e a diminuição das diferenças, de modo a criar condições mais harmônicas em toda UE. Por outro lado, o regulamento constitui

e cumprir com os objetivos de forma eficaz’ versus ‘interferir nas ordens jurídicas na medida necessária’, pois, como a Diretiva e o Regulamento são atos legislativos que decorrem do exercício das competências derivadas da UE, consequentemente, são subordinados ao princípio da subsidiariedade e proporcionalidade. Por este motivo, para avaliar efetivamente a possibilidade e necessidade de uma regulamentação ao nível da UE deve-se avaliar as facetas habilitadoras e limitadoras da subsidiariedade para determinar se a ação da UE pode melhor alcançar os objetivos pretendidos dentro das competências que lhe foram atribuídas, bem como a questão da intensidade e do tipo da medida a adotar, que decorre do princípio da proporcionalidade, ou seja, a partir da verificação em pormenor se o instrumento jurídico é necessário e/ou adequado, ou se outro meio de ação não seria suficiente em termos de eficácia.

Tendo em conta essas duas facetas, foi introduzido um mecanismo⁹⁰ que permite aos Parlamentos dos EM verificarem o respeito aos princípios da subsidiariedade e proporcionalidade. Caso julgue que determinado ato legislativo da União não esteja em consonância com estes princípios, o Parlamento de um EM pode contestá-lo mediante a emissão de um parecer fundamentado. Após isso, se a Comissão decidir pela manutenção, modificação ou retirada do projeto, deverá realizar um parecer fundamentado para ser apreciado pelo Conselho ou pelo Parlamento Europeu, que decidirá pela sua manutenção. Tal mecanismo foi acionado pelo Senado francês na apreciação da Proposta do Regulamento da Cibersegurança, onde pode-se destacar os seguintes pontos do parecer⁹¹: que o mandato da ENISA e o quadro da certificação deveriam estar em diplomas distintos; que a competência em matéria de segurança é atribuída aos EM e não à ENISA; que, a partir da criação de um sistema de certificação europeu, os certificados nacionais serão suprimidos o que impede a criação de sistemas futuros ainda que estabelecessem um nível mais elevado de segurança; que a cibersegurança é também questão de soberania nacional e que a capacidade de criar normas dos EM deveria ser mantida e o novo sistema a nível deveria ser com base na participação voluntária; que a base jurídica da proposta não é fundamentada somente no mercado interno, mas deve incluir os desafios de segurança (artigo 4.º do TUE); e que a ENISA não possui

ato jurídico que interfere mais profundamente nos ordenamentos nacionais, pois vincula em todas as suas partes os EM e destinatários ao direito da União e possui aplicabilidade direta. Ou seja, tem um caráter comunitário, que consiste na particularidade de impor um direito unificado, válido para toda a União.

⁹⁰ TFUE - PROTOCOLO Nº 2 RELATIVO À APLICAÇÃO DOS PRINCÍPIOS DA SUBSIDIARIEDADE E DA PROPORCIONALIDADE, Artigo 6º.

⁹¹ Parecer fundamentado do Senado francês sobre a Proposta de 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)0477 – C8-0310/2017 – 2017/0225(COD))

qualquer experiência no domínio da certificação, portanto o papel central previsto para a agência neste domínio poderia conduzir ao enfraquecimento da cibersegurança na UE.

No entanto, foi decidido pela manutenção do Regulamento após apreciação do parecer apresentado pela Comissão⁹², que avaliou escolha do instrumento e da base jurídica eram acertadas, assim como os princípios da subsidiariedade e proporcionalidade foram respeitados, conforme a seguinte exposição de motivos:

BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE: A base jurídica do mercado interno para criar a ENISA foi validada pelo Tribunal de Justiça (no processo C-217/04 Reino Unido da Grã-Bretanha e da Irlanda do Norte contra Parlamento Europeu e Conselho da União Europeia) (...). Além disso, as atividades que refletiriam os objetivos de aumentar a cooperação e a coordenação entre EM e aquelas que aditariam capacidades a nível da UE para complementar a ação dos EM enquadrar-se-iam na categoria de «cooperação operacional». Tal é especificamente identificado pela Diretiva SRI (cuja base jurídica é o artigo 114.º do TFUE) como um objetivo a perseguir no contexto da rede de CSIRT, à qual a «ENISA assegura os serviços de secretariado e apoia ativamente a cooperação» (artigo 12.º, n.º 2). Em especial, o artigo 12.º, n.º 3, alínea f), acrescenta que a identificação de outras formas de cooperação operacional é uma tarefa da rede CSIRT, nomeadamente no que se refere: i) às categorias de riscos e de incidentes, ii) aos alertas rápidos, iii) à assistência mútua, iv) aos princípios e às formas de coordenação na resposta dos EM a riscos e incidentes de dimensão transfronteiriça. A atual fragmentação dos sistemas de certificação de produtos e serviços de TIC é também uma consequência da inexistência de um processo-quadro comum eficaz e juridicamente vinculativo aplicável aos Estados-Membros. Tal dificulta a criação de um mercado interno para os produtos e serviços de TIC e afeta a competitividade da indústria europeia neste setor. A presente proposta visa resolver a fragmentação existente e os obstáculos conexos ao mercado interno mediante a disponibilização de um quadro comum para a criação de sistemas de certificação da cibersegurança válidos em toda a UE. (...)

Escolha do instrumento: Tendo em conta o papel importante da ENISA na criação e gestão de um quadro de certificação da cibersegurança a nível da UE, o novo mandato da ENISA e o referido Quadro são mais adequadamente criados ao abrigo de um instrumento jurídico único, utilizando-se para tal um regulamento. (...)

Subsidiariedade: (no caso de competência não exclusiva) O princípio da subsidiariedade requer a avaliação da necessidade e do valor acrescentado da ação da UE. (...) A cibersegurança é uma questão de interesse comum da União. As interdependências entre redes e sistemas de informação são de tal ordem que os intervenientes (...) muitas vezes não podem enfrentar ameaças, gerir os riscos e os eventuais impactos de ciberincidentes isoladamente. Por um lado, as interdependências entre EM, nomeadamente no tocante ao funcionamento de infraestruturas críticas (energia, transportes, água, apenas para referir algumas), tornam a intervenção pública a nível europeu não só benéfica, mas também necessária. Por outro lado, a intervenção da UE pode criar um efeito indireto positivo devido à partilha de boas práticas entre os EM, que poderá conduzir ao reforço da cibersegurança na União. Resumindo, no contexto atual e ponderando os futuros cenários, afigura-se que, para aumentar a ciber-resiliência coletiva da União, a ação individual dos EM da UE e uma abordagem fragmentada à cibersegurança não serão suficientes. A ação da UE é também considerada necessária para resolver a fragmentação dos atuais sistemas de certificação da cibersegurança. Permitirá que os fabricantes beneficiem plenamente de um mercado interno, com economias consideráveis no atinente a custos de ensaios e de reformulação. (...)

Proporcionalidade: As medidas propostas não excedem o necessário para atingir os seus objetivos políticos. Ademais, o âmbito da intervenção da UE não impede outras ações nacionais no domínio das questões de segurança nacional. A ação da UE está, por conseguinte, justificada com base na subsidiariedade e proporcionalidade.

Embora seja reconhecível a consonância dos instrumentos com o princípio da subsidiariedade pelo valor acrescentado da UE nesta matéria nos dois diplomas, podem ser

⁹² COM(2017) 477 final 2017/0225 (COD). Bruxelas, 4.10.2017. EXPOSIÇÃO DE MOTIVOS.

levantadas algumas questões quanto ao princípio da proporcionalidade e da escolha da base jurídica. O primeiro, decorre do fato de a Diretiva SRI não estabelecer objetivos mensuráveis e não ser específica quanto aos requisitos de segurança para proteção das infra-estruturas críticas, tampouco, quanto às sanções aplicáveis, além de como não ter em conta os efeitos negativos que as diferenças na transposição possam acarretar para a eficácia da sua aplicação (o que será visto no próximo capítulo). Já no caso do Regulamento a utilização deste instrumento no que se refere à relação da cibersegurança com as questões de segurança nacional não ficaram claras no parecer da Comissão (uma vez que suprime os sistemas de certificação nacionais e impede a criação de novos sistemas) e, além disso, se baseia, à partida, na voluntariedade dos pedidos de certificação para atingir a ciber-resiliência. Portanto, em relação à proporcionalidade das medidas cabe uma melhor avaliação para determinar se as medidas excedem, ou se ficam aquém do necessário para atingir os respetivos objetivos.

Já em relação à base jurídica escolhida relacionada exclusivamente com o mercado interno, caberia uma melhor justificação nos dois instrumentos, pois é evidente a importância das infraestruturas críticas para a soberania dos países, bem como dos sistemas de certificação aplicados a essas infraestruturas. Além disso, também é evidente a relação com as questões de segurança nacional no caso de eventuais ataques decorrentes de ameaças híbridas, o que, apesar do impacto económico, podem desestabilizar países inteiros e/ou causar danos graves. Por este motivo, o desenvolvimento e o funcionamento desses diplomas na prática que irá determinar se o equilíbrio na ‘capacidade de harmonizar e cumprir com os objetivos de forma eficaz’ versus a ‘interferência nas ordens jurídicas na medida necessária’ foi encontrado.

A partir desta noção do conteúdo dos instrumentos jurídicos vigentes, da base jurídica utilizada e de como foram aplicados e justificados os princípios da subsidiariedade e proporcionalidade, este trabalho se propõe, em seguida, a analisar os desafios à eficácia das medidas da UE, tendo por base o quadro estabelecido pela UE para a cibersegurança, bem como as considerações introduzidas nos capítulos anteriores.

5 DESAFIOS PARA EFICÁCIA DA CIBERSEGURANÇA NA UE

Após analisar os caminhos estratégicos escolhidos pela UE e as mudanças em sua perspectiva para lidar com a Cibersegurança, foi avaliado o panorama geral da política da UE vigente, e um resumo dos dois principais instrumentos jurídicos que tratam desta temática. A partir disso, nesta seção, propõe-se a elencar alguns dos principais desafios para a eficácia do

panorama estratégico e das medidas propostas para lidar com a temática da Cibersegurança, com base no relatório do TCE (2019) – que é um documento informativo baseado em informações disponíveis ao público – em outros estudos, bem como relembrar alguns pontos abordados anteriormente neste trabalho que impactam na eficácia, de forma a destacar alguns fatores que impõem dificuldades para a construção de uma UE cibersegura.

Sobre o quadro estratégico e legislativo, o principal desafio é o de dar coerência ao domínio da cibersegurança por conta das dificuldades em reunir todas as partes do ecossistema cibernético multifacetado e com muitos intervenientes⁹³, como é o da UE. Carrapico e Barrinha (2017, p. 1266-1268) abordam a problemática da coerência da UE como ator de cibersegurança, e fazem os seguintes apontamentos:

Focusing on the specific case of cybersecurity, it was possible to conclude in this preliminary study, that the EU has an explicit ambition to be a coherent security actor. However, both the architecture put in place under the 2013 strategy and the resistance from Member States to allow the EU to have a more stringent control over their cyber activities, limit the EU's coherence in the field. That said, both the rising political importance given to cybersecurity and the progressive consolidation of what is still a rather recent field of activity, means there are signs the EU might move towards a more coherent actorness in the field. (...) Particularly in the field of cybersecurity, where decision-making 'is characterised by a lack of transparency and accountability' (Bendiek, 2012, p. 24), it is fundamental that we understand that a coherent actor must also be coherent with the values it defends.

Além disso, Carrapico e Barrinha (2017, p. 1267) argumentam que “*there is also the notion that a more coherent Union is, in the security field, a more integrated union where different policy areas coincide to offer the best possible toolkit of action*”, ou seja uma maior coerência no quadro estratégico e legislativo, é essencial para que a UE desempenhe um papel coerente na Cibersegurança, tanto em termos internos (maior integração, cooperação e harmonia) quanto externos (dada à natureza transfronteiriça do ciberespaço e da posição da UE

⁹³ TCE (2019, p. 12) **Quem intervém?** A **Comissão Europeia** pretende melhorar as capacidades e a cooperação em matéria de cibersegurança e integrar a cibersegurança noutras políticas da UE. As principais Direções-Gerais (DG) com competências na política de cibersegurança são as DG **CNECT**(cibersegurança) e **HOME** (cibercriminalidade), responsáveis respetivamente pelo Mercado Único Digital e pela União da Segurança. A DG **DIGIT** é responsável pela segurança informática dos sistemas próprios da Comissão. Várias agências da UE, designadamente a **ENISA** que é a agência da UE para a cibersegurança. O Centro Europeu da Cibercriminalidade da Europol (**EC3**) para reforçar a resposta das autoridades policiais da UE à cibercriminalidade. A Comissão acolhe ainda uma Equipa de Resposta a Emergências Informáticas (**CERT-UE**), que dá apoio a todas as instituições, organismos e órgãos da União. O **Serviço Europeu para a Ação Externa** (SEAE) conduz a ciberdefesa, a ciberdiplomacia e a comunicação estratégica, albergando centros de recolha e análise de informações. A **Agência Europeia de Defesa** (AED) tem por finalidade desenvolver as capacidades de ciberdefesa. Os **Estados-Membros** são os principais responsáveis pela sua própria cibersegurança e, a nível da UE, intervêm através do **Conselho**, que tem uma série de organismos de coordenação e partilha de informações (entre os quais o Grupo Horizontal das Questões do Ciberespaço). O **Parlamento Europeu** intervém enquanto colegislador. As **organizações do setor privado**, nomeadamente através de uma **parceria público-privada contratualizada**. Entre outros, como as CSIRTs e autoridades nacionais (Diretiva SRI), Operadores de Serviços Essenciais, Prestadores de serviços Digitais, autoridades e organismos para a realização do sistema de certificação europeu, etc.

no contexto internacional). Dessa forma, de acordo com o TCE (2019, p. 19), para enfrentar o desafio de construir um quadro coerente, deve-se: a) proceder a uma verdadeira avaliação e prestação de contas; e b) colmatar as lacunas na legislação da UE e na sua desigual transposição.

Sobre o ponto ‘a’, o TCE (2019, p. 19-20) coloca que os objetivos estratégicos “foram formulados de forma muito geral, exprimindo uma visão e não uma meta quantificável”, e que “não foram estabelecidos objetivos que definam o nível desejado de resiliência para a UE como um todo”. Portanto, constitui um desafio a criação de métodos de avaliação a partir de objetivos mensuráveis e dados fiáveis que possam medir o progresso das medidas adotadas, incluindo a recolha de dados oficiais dos EM e da UE sobre as questões relacionadas com a cibersegurança, e com isso, “garantir uma verdadeira prestação de contas e avaliação, através de uma transição para uma cultura de desempenho com práticas de avaliação integradas” TCE (2019, p. 5).

Já sobre ponto ‘b’, o TCE (2019, p. 5) destaca que o “quadro legislativo permanece incompleto⁹⁴, além de que as lacunas e as diferenças na transposição da legislação da UE podem dificultar a concretização de todo o seu potencial”. Isso decorre, por um lado, das dificuldades em regular uma matéria incipiente que é ultrapassada pelo surgimento de novas tecnologias e novas ameaças. Dessa forma, o quadro legislativo deve ser flexível o suficiente para se moldar ao futuro e se antecipar às transformações, pois à medida que o ciberespaço evolui, continuarão a surgir lacunas. Por outro lado, segundo o TCE (2019, p. 23), “as diferenças na transposição do direito da União entre os EM podem resultar em incoerência jurídica e operacional” e impedir que a legislação atinja os objetivos pretendidos.

Dadas as grandes diferenças entre os EM em termos de estágio de desenvolvimento, capacidade, empenho e estratégias de cibersegurança, a transposição da Diretiva SRI abre margem para uma série de abordagens diferentes no que se refere à proteção das infraestruturas críticas – elemento prioritário para a estratégia da UE. No relatório elaborado pelo grupo TwoBirds⁹⁵ (2020), consta um levantamento do regime jurídico adotado pelos EM na

⁹⁴ Fatores que revelam esta incompletude. O TCE (2019, p. 10) aponta que as ameaças mais nefastas são, possivelmente, as **ameaças persistentes avançadas (referidas no capítulo 2)** “em que agressores sofisticados se envolvem a longo prazo na vigilância e roubo de dados, por vezes também com intuítos destrutivos”. A ciberespionagem representa, de acordo com o TCE pelo menos um quarto de todos os ciberincidentes e a maioria das despesas. Além disso, o TCE (2019, p. 21) revela que “**algumas partes interessadas consideram que é gritante a ausência de uma abordagem comum à ciberespionagem e de uma política industrial claramente definida no domínio da cibersegurança**”. Já sobre a cibercriminalidade, o TCE (2019, p. 20) frisa que “devido à ausência de uma definição de cibercriminalidade consignada num código, é praticamente impossível encontrar indicadores europeus pertinentes que contribuam para o seu acompanhamento e avaliação”.

⁹⁵ Bird&Bird& (Janeiro, 2020). *Developments on NIS Directive in EU Member States*. Disponível em: <https://www.twobirds.com/~media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf>. Acesso em Fev.2020. **Exemplos de Sanções aplicadas: Bélgica** - *Articles 51 and 52 of the Draft Act provide for criminal and administrative sanctions respectively. Criminal sanctions include both prison sentences (ranging from 8 days*

transposição da Diretiva SRI que demonstra essas diferenças. Por exemplo, nos casos mais graves de infrações, existem disparidades enormes no que se refere ao regime sancionatório, que podem chegar a: “*up to EUR 5.000.000, or in specific cases up to 10% of the total worldwide annual turnover of the preceding financial year*” na Alemanha; ou no Reino Unido “*from a limit of £1 million for any contravention which could not cause a NIS incident; to £17 million for the most severe breaches*”; em contrapartida, outros EM estipularam sanções máximas em patamares muito inferiores, também para os casos mais graves, como de, no máximo, 50.000 EUR em Portugal, e 20.000 EUR no caso da Estónia. Também existem diferenças quanto à autoridade responsável por aplicar as sanções, como por exemplo, na Dinamarca cada Ministério estipula o regime sancionatório do setor que é responsável. Ou ainda, há casos onde as sanções podem ser administrativas e penais, como no caso da Bélgica que estipulou que: “*criminal sanctions include both prison sentences (ranging from 8 days to 2 years) and fines (ranging from EUR 26 to EUR 75.000)*”. Ou seja, um mesmo incidente com graves repercussões (sanção máxima) pode ser penalizado como um crime em um EM, custar 5.000.000 EUR em outro, ou ainda 20.000 EUR em outro.

Há de se notar que o artigo 21.º da Diretiva SRI estabelece que as sanções adotadas pelos EM devem ser efetivas, proporcionadas e dissuasivas e que a obrigação de notificação de incidentes se refere à incidentes graves. As disparidades verificadas nos regimes sancionatórios

*to 2 years) and fines (ranging from EUR 26 to EUR 75.000). It should be noted however that in Belgium, criminal fines as indicated in the law must always be multiplied with a multiplication factor. The current factor is 8, consequently, the range is between EUR 208 and EUR 600.000. The administrative sanctions range between EUR 500 and EUR 200.000. **Austria** § 26 NISG provides for the following administrative fines: up to EUR 50.000 and, for repeating offenders, up to EUR 100.000. **Dinamarca:** Each act sets out its own reporting scheme: Ministry of Transport, Building and Housing; Ministry of Defense; Ministry of Health and Elderly; Ministry of Commerce; Ministry of Environment and Food; Ministry of Energy, Supply and Climate. **Estónia:** Fines in misdemeanour procedure of up to EUR 20.000, in case of not following requirements imposed on implementing security measures. **Alemanha:** - up to EUR 50.000 under the Atomic Energy Act; - up to EUR 5.000.000, or in specific cases up to 10% of the total worldwide annual turnover of the preceding financial year, under the Energy Industry Act; - up to EUR 50.000 under the Social Insurance Code V; and - up to EUR 500.000 under the Telecommunication Act. **Netherlands:** The Act provides for the following administrative fines: - a maximum of EUR 5 million for any breach of the draft implementation act by essential service operators or DSPs; - a maximum of EUR 1 million for failing to cooperate with a request for further information from the National Cyber Security Centre; and - a maximum of EUR 1 million for failure to adequately cooperate with supervisory authorities exercising their competencies. **Espanha:** The following penalties will apply: (i) fines of EUR 500.001 to EUR 1.000.000 in case of very serious infringements; (ii) fines of EUR 100.001 to EUR 500.000 in case of serious infringements and a reprimand or fines to EUR 100.000 in case of minor infringements. **Portugal:** Very serious infractions (Art. 23) are punished with a fine of EUR 5,000 to EUR 25,000 in the case of a natural person, and of EUR 10,000 to EUR 50,000 in the case of a person collective. Serious administrative offenses are punished by a fine of EUR 1,000 to EUR 3,000, in the case of a natural person, and of EUR 3,000 to EUR 9,000, in the case of a legal person. **UK:** The NIS Regulations set out caps on the penalties which can be imposed reflective of the breach; from a limit of £1 million for any contravention which could not cause a NIS incident; to £17 million for the most severe breaches, being a material contravention which has the potential to cause an incident resulting in an immediate threat to life or significant adverse impact on the UK economy.*

adotados levam a questionar: em qual medida as sanções aplicadas são dissuasoras, proporcionadas e efetivas? Tal problema poderia ter sido evitado se a diretiva estipulasse uma margem do que seria adequado (como, por exemplo, uma margem de x% a y% sobre o percentual do volume de negócios, conforme a infração cometida). Ademais, como a gravidade do incidente é relativa e incidentes menos graves não precisam ser notificados, muitos incidentes podem deixar de ser contabilizados, avaliados e tratados.

Além disso, cada EM elabora a lista dos operadores de serviços essenciais (OSE) conforme o que considerar importante no contexto interno (desde que inclua todos os setores indicados da diretiva), e também a lista dos prestadores de serviços digitais (PSD). Por exemplo, no caso dos OSE, o setor de alimentos ou de determinada indústria pode estar abrangido por um EM e não estar por outro. No caso dos PSD, a jurisdição é definida conforme a sede/estabelecimento principal, e se estiver sediado fora da UE, deve escolher um representante na União dentre os EM que presta serviço (artigo 18º, DSRI), onde valerá a regra da jurisdição designada. Assim, essas disparidades de regimes sancionatórios e de setores abrangidos conforme cada EM estabelece, além das potenciais dificuldades e incoerências jurídicas e operacionais a nível da UE, também podem servir de estímulo ou desestímulo para migração de jurisdição (se possível) das OSE ou PSD para EM com regimes sancionatórios mais brandos, ou para a escolha da jurisdição, no caso de novas empresas que pretendem se instalar na Europa – principalmente no caso das PSD. Por estes motivos, devido às diversas interpretações e abordagens, a eficácia das medidas da UE como um todo podem ficar comprometidas.

Apesar de a Diretiva SRI ser um diploma central para a política de cibersegurança da UE, por si só não garante resiliência, uma vez que para atingir um elevado nível de cibersegurança, centra-se em alcançar uma harmonização mínima e não máxima para proteger as infraestruturas críticas (TCE, 2019, p. 23). Ademais, alguns aspetos da legislação da UE continuam a ser voluntários, tais como: a disponibilização de informações sensíveis (de segurança nacional), a notificação de incidentes graves para setores não listados na Diretiva SRI, e o pedido de certificação de produtos, serviços e processos TIC. Como visto, a maior responsabilidade pela aplicação dessas medidas de cibersegurança recai sobre os EM e setores abrangidos, e devido as diferentes abordagens já adotadas, corre-se o risco de a fragmentação gerar desarmonia e dificuldades na cooperação, bem como dificultar o processo de reforço conjunto das capacidades dos EM.

A respeito do financiamento e despesas, o TCE (2019, p. 5-6) destaca também alguns desafios. O principal é dispor de uma visão geral clara das despesas, pois “uma vez que não

existe um orçamento específico da UE para financiar a estratégia de cibersegurança, não se dispõe de uma ideia precisa sobre que fundos vão para que destinos”. Também constitui um desafio, segundo o TCE (2019, p. 25) “adaptar os níveis de investimento aos objetivos”. Além disso, esta falta de definição, gera muita confusão nos diversos intervenientes “que resulta da natureza transversal da cibersegurança e da impossibilidade de distinguir as suas despesas das despesas informáticas gerais”, tanto no setor público quanto privado. No âmbito da UE e dos EM, para cada objetivo estratégico (e categorias associadas), caberia uma visão clara dos investimentos necessários e das despesas de cibersegurança, bem como a possibilidade de rastreabilidade destes recursos para aferir sua adequação ou ajuste ao longo do tempo.

Outro desafio para eficácia da Cibersegurança está no quesito ‘criação de ciber-resiliência’, que consiste em um dos principais objetivos do panorama estratégico atual, e envolve: a variedade de modelos de governação de cibersegurança, a falta de um sistema padronizado para avaliação de ameaças e gestão de riscos, o reforço das capacidades de cibersegurança em diversos níveis, a falta de consciencialização sobre o tema, as dificuldades na coordenação e no intercâmbio de informações construídos sob uma base sólida de confiança, entre outros (TCE, 2019, p. 33). Sobre a necessidade de melhorar a governação da cibersegurança, pode-se destacar as seguintes considerações:

Os modelos de governação da cibersegurança variam consoante os EM e, dentro de cada um, a responsabilidade nesta matéria está frequentemente repartida entre muitas entidades. Estas diferenças podem entravar a cooperação que é necessária para dar resposta a incidentes transfronteiriços em grande escala e para o intercâmbio de informações sobre ameaças a nível nacional e – ainda mais – a nível da UE. (...) A governação da segurança da informação implica instituir estruturas e políticas que garantam a confidencialidade, integridade e disponibilidade dos dados. (...) A falta de um quadro de governação da cibersegurança coerente a nível mundial prejudica a capacidade de a comunidade internacional limitar os ciberataques e dar-lhes resposta. As tentativas de estabelecer normas internacionais vinculativas para o ciberespaço estão a tornar-se cada vez mais problemáticas (...) pela falta de consenso sobre o modo de aplicação do direito internacional às respostas dos Estados a incidentes. (...) É importante, por conseguinte, **construir um consenso sobre esse quadro de governação de modo a que esteja em consonância com os interesses e valores da UE.** (TCE, 2019, p. 33-34)

Um dos elementos básicos para a governação da cibersegurança, tanto para o setor público como privado, abrange a necessidade de **ferramentas de avaliação das ameaças e riscos standardizados** (referido no capítulo 2 deste trabalho), o que constituiria **a base** para determinar as estratégias, investimentos, modelos de governação e de avaliação contínua nos diversos níveis de atuação. Porém, conforme destaca o TCE (2019, p. 37) não existe uma abordagem normalizada para a classificação e o levantamento das ciberameaças e dos riscos “fazendo com que o conteúdo dessas avaliações varie consideravelmente e dificultando, assim, uma abordagem coerente a nível da UE em matéria de cibersegurança”.

Isso remonta ao disposto nos capítulos 1 e 2 deste trabalho no que se refere à padronização de terminologias, de estruturas legais e de cooperação para lidar com ciberataques e cibercrimes e de ferramentas de avaliação das ameaças e riscos standardizados. A começar pela ‘cibersegurança’, Kasper e Antonov (2019, p. 1-2) colocam que:

The European Union has a wide spectrum of legal instruments addressing various aspects of cybersecurity all this without having a commonly accepted definition of cybersecurity. The proposed Cybersecurity Act purports to define cybersecurity as it “comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats”, (...) however the definition is not explained in available preparatory documents (...) and also refer to cybersecurity as it was an attribute or a desired state to be achieved. The lack of clarity about this core concept raises questions about coherence and consistency of already adopted and newly proposed legislative acts in the field of cybersecurity. Precisely what harms EU cybersecurity-related laws seek to prevent?

Apesar disso, Kasper e Antonov (2019, p. 14) pontuam que a ENISA já se manifestou sobre esta falta de definição ao colocar que “[c]ybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers” e que definições contextuais já estão em uso. Essa abordagem pode ser conveniente, uma vez que o termo já virou uma *buzzword*, contudo também implica em dificuldades em determinar outros conceitos como de ‘cibercrime’ e ‘ciberameaça’. Além disso, Tikik, Kaska e Vihul (2010, p. 101) explicam a necessidade de estabelecer uma padronização em termos de estruturas legais e de cooperação para lidar com ciberataques e cibercrimes, bem como a urgência de uma revisão terminológica, pois a inconsistência terminológica dificulta a qualificação legal de um ciberincidente e a efetividade de uma resposta em termos de autoridades, meios e procedimentos envolvidos, o que pode criar incertezas jurídicas e dificultar o exercício das atribuições dos entes responsáveis por tomar medidas contra atividades maliciosas.

Como explicado nos capítulos 1 e 2, a cibersegurança entrou na pauta política da UE e se modificou pelo fenómeno das *threat politics*, onde foram estabelecidos domínios de atuação (proteção simples, prossecução criminal e defesa de Estado), sem que para isso houvesse, de partida, um entendimento universal comum do que constitui uma ciberameaça. Para Van der Meulen, A Jo e Soesanto (2015, p. 26) “*this absence prevents the establishment of a universally accepted categorisation system for threats and leads to variability in what is included in threat assessments*”, que poderiam ser aplicados a diversos níveis e setores. Como visto no decorrer deste trabalho, as abordagens (tomadas de decisão), perspetivas (questão de TI, criminal, económica ou soberania/defesa) e o peso atribuído a cada uma delas em matéria de cibersegurança, foram sofrendo mutações e se moldando muito em função da perspetiva da UE em relação às ameaças (reação), na medida que aumentou a preocupação e a gravidade das

ameaças no tempo, até o ponto da situação com a Estratégia de 2017 - Resiliência, dissuasão e defesa: reforçar a cibersegurança na EU – com medidas mais duras e preocupação maior com as ameaças híbridas, com o reforço das capacidades (resiliência) e com a ciberdefesa.

Portanto, a modelização das ciberameaças⁹⁶ favoreceria a melhor fundamentação da análise estratégica para lidar com o problema e incrementaria a compreensão global sobre o assunto. Ademais o TCE (2019, p. 37) destaca que “as avaliações das ameaças poderiam abranger não só as de natureza tecnológica, mas também as de cariz sociopolítico e económico, bem como os elementos condutores das ameaças e as motivações dos intervenientes” e seriam um elemento fundamental na construção de ciber-resiliência. Por este motivo, foram abordadas neste trabalho algumas categorizações de cibercrime e ciberameaças (convencional, complexo e ameaças emergentes) e um modelo simplificado de avaliação de ciberameaças, muito embora sem ter a pretensão de indicar quais modelos, definições e métricas fosse mais adequado. Isso porque, durante a elaboração deste trabalho, esbarrou-se na falta de definições e padrões, e o mesmo problema foi evidenciado em diversas pesquisas. Dessa forma, buscou-se exemplificar e frisar a importância dessas definições e sistemas padronizados, o que poderia servir para proporcionar uma **base** para abordagens estratégicas mais claras, precisas, funcionais e efetivas a serem usadas, não só a nível da UE, mas também no contexto internacional, o que também favoreceria a cooperação nesta matéria.

Outro desafio importante para a construção de ciber-resiliência é o reforço das capacidades, das competências e da consciencialização em todos os setores e níveis da sociedade face à escassez de competências em matéria de cibersegurança. Além disso, outro fator que influencia nesta construção (também mencionado no capítulo 2 deste trabalho), é a crescente assimetria entre os conhecimentos necessários para cometer um cibercrime ou lançar um ciberataque e as competências necessárias para se defender dele. Adicionalmente, conforme destaca o TCE (2019, p. 37) “ainda não existem suficientes incentivos legais e económicos para que as organizações comuniquem e partilhem informações sobre incidentes”. Ademais, conforme consta no capítulo 2, muitas organizações preferem lidar diretamente com os incidentes e pagarem resgates para evitar danos à sua reputação. Portanto, na ausência de dados fiáveis e acessíveis, de sistemas padronizados de avaliação de ciberameaças e de pessoal

⁹⁶ Sugere-se a criação de uma Framework colaborativa de avaliação das ciberameaças com ferramentas estatísticas disponíveis baseada em dados públicos (por exemplo, com tipos de ameaças, riscos, histórico de ocorrência, impacto/afetação dos ativos, tendências e filtros – por tipo de alvos, de ataque, de motivação, de método aplicado, etc.). Ou seja, uma revisão sistemática (melhores práticas) para fornecer um sistema de avaliação de ameaças, inclusive com aspetos relativos a gravidade e a como ser operacionalizado pelos diversos agentes.

capacitado, ao avaliar o custo-benefício, muitas organizações preferem ‘assumir o risco’ do que investir em cibersegurança, o que compensa ainda mais se as sanções forem brandas.

Cabe considerar que, o setor privado, principalmente os responsáveis pela continuidade dos serviços essenciais para a sociedade, acabam por projetar a imagem da resiliência da UE para o mundo. Portanto, para além da introdução de requisitos técnicos de cibersegurança, de mecanismos de notificação e resposta a incidentes e da busca pela redução de vulnerabilidades pela certificação (voluntária), trazidas pelos diplomas jurídicos (cuja eficácia permanece por averiguar), ainda há um longo caminho a trilhar, bem como lacunas a colmatar, na construção de uma cultura de cibersegurança através da educação, capacitação e da consciencialização, bem como de criação de incentivos, para se chegar a uma sociedade ciber-resiliente.

Outro desafio apontado pelo TCE é o da ‘resposta eficaz a ciberincidentes’. Um fator importante neste quesito é o “fato de a UE ser grande importadora de produtos e serviços de cibersegurança, o que aumenta dependência tecnológica e de vulnerabilidade” onde esta realidade pode ameaçar a proteção das infraestruturas críticas da UE. Para colmatar esse déficit os investimentos no setor da indústria digital e na cibersegurança da UE são essenciais para se alcançar e reforçar a autonomia. Além disso, os níveis de cooperação para incidentes de cibersegurança são complexos e com muitos intervenientes, o que dificulta uma resposta coordenada na ocorrência de grandes incidentes. Dessa forma, constitui um grande desafio assegurar que o roteiro é prático e que todos os intervenientes sabem qual o seu papel, o que necessitará de testes alargados nos próximos anos. (TCE, 2019, p. 54)

Todos estes desafios para a eficácia do panorama estratégico e das medidas legislativas para a cibersegurança estão interligados e, em certa medida, influenciam uns aos outros. Entretanto, cabe o apontamento de algumas tendências. Como, por exemplo, do aumento da cibercriminalidade, que tem sido impulsionado pelo fenómeno da ‘cibercriminalidade como serviço’ onde pessoas sem conhecimentos técnicos podem contratar *hackers* e *bots* para as mais diversas atividades maliciosas (TCE, 2019, p.38). Este fenómeno tende a crescer e cabe lembrar o mencionado na seção sobre os impactos das ciberameaças, em que uma rede de cibercriminosos chegava a cobrar irrisórios 15 EUR por mês pelos seus serviços. Além disso, outra tendência chama atenção. Após a declaração da NATO em 2016⁹⁷, que passou a

⁹⁷ “Cyberattacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO’s core task of collective defence. Now, in Warsaw, we reaffirm NATO’s defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea”. (NATO, 2016, item 70). North Atlantic Treaty Organization (NATO). (2016). Warsaw Summit. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Acesso em Mai. 2020.

oficialmente considerar o ciberespaço como uma dimensão operacional de guerra, muitos estudos^{98,99} apontam que os países tem intensificado as capacidades defensivas e ofensivas e levado à militarização do ciberespaço, ao aumento da ciberespionagem, e à utilização de cibermercenários e *hackers* contratados como *proxies* para executar certas ações de *warfare* em nome de Estados que preferem manter suas ações no anonimato. Sobre essa tendência, Faesen, Torossian, Mayhew e Zensus (2020)¹⁰⁰ avaliam que:

*This paper has examined trends relevant to conflict in cyberspace by delving into the intentions, capabilities and activities of states in this critical domain. The primary takeaway is that **conflict in cyberspace is intensifying, and is likely to continue to do so**. The rise in reported cyber espionage, and Computer Network Attacks, as well as the indication that disinformation campaigns are proliferating, is leading states to regard threats emanating from cyberspace as a crucial security concern, which in turn contributes to an escalation of tensions between states and an increase in cyber military spending.*

Conforme visto na análise do panorama estratégico atual da UE, a preocupação com ameaças complexas tem sido preponderante, onde a sociedade como um todo e seus valores centrais são vistos como ameaçados. Inclusive, a UE reconhece que não está preparada, como pode ser verificado no discurso de Jean-Luc Junker sobre o estado da União de 2017:

Ainda não estamos suficientemente preparados para fazer face a ciberataques. **Mais do que as armas ou os tanques de guerra, os ciberataques podem representar uma maior ameaça à estabilidade das democracias e das economias.**¹⁰¹

Isso justifica o recrudescimento das políticas de cibersegurança UE e o aumento das medidas relacionadas à ciberdefesa, e demonstra também a transformação da perspectiva da UE para este sentido, em conjunto com a assunção de um papel mais centralizador neste domínio. Conforme aponta Beláz, (2019, p. 26): “*this new approach is clearly a paradigm shift towards a more centralised policy-making and governance*”. Porém, esse avanço em matéria de ciberdefesa vem carregado de objeções, uma vez que a questão da segurança é resguardada aos EM. Como visto, na perspectiva da UE a cibersegurança passou de sub-ramo de TIC e cibercrime para uma abordagem mais holística e, mais recentemente, com grande foco em ciberdefesa. No entanto, essa mudança não foi acompanhada da autonomia tecnológica e do desenvolvimento de capacidades para construir a ciber-resiliência almejada, pois esses elementos ainda constituem um objetivo a perseguir. Ou seja, a mudança da perspectiva não foi baseada na

⁹⁸ BUCHANAN, Ben. ***The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics***. Harvard University Press, 2020.

⁹⁹ **Review:** ‘Cyber Mercenaries: The State, Hackers, and Power’ by Tim Maurer’. Disponível em: <https://www.consilium.europa.eu/pt/documents-publications/library/library-blog/posts/cyber-mercenaries-the-state-hackers-and-power-by-tim-maurer/>. Acesso em Set. 2020.

¹⁰⁰ FAESEN, Louk; TOROSSIAN, Bianca; MAYHEW, Elliot; e ZENSUS, Carlo. ***Conflict in Cyberspace: Parsing the threats and the state of international order in cyberspace***. Disponível em: <https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/>. Acesso em Set. 2020.

¹⁰¹ Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/SPEECH_17_3165. Acesso: Set. 2020.

superação dos diversos desafios relacionados a cibersegurança, e sim baseada em uma espécie de reação às ameaças (*threat politics*) que foram surgindo e sendo priorizadas na tomada de decisão, conforme a gravidade apresentada. Além disso, embora a elaboração de políticas de segurança ter uma perspectiva muito centrada no Estado, devido à preocupação com militarização e uso político do ciberespaço com propósitos de *ciberwarfare*, e também devido ao foco estratégico da Cibersegurança e do discurso da UE sobre esta temática a avançar sobre a ciberdefesa, o fundamento das medidas de cibersegurança somente no mercado interno tem demonstrado inconsistências, o que ficou evidenciado no Parecer fundamentado do Senado francês sobre a Proposta do Regulamento de Cibersegurança (no capítulo 4 deste trabalho).

Neste sentido, a centralização das políticas de cibersegurança da UE e o foco cada vez maior nas questões de ciberdefesa podem provocar tanto um movimento centrípeto (para o centro) como centrífugo (para fora). Ou seja, o papel centralizador das políticas no domínio da cibersegurança pode tanto servir para reforçar o papel da UE, para maior integração e cooperação em relação aos EM, como pode causar o efeito contrário. Dessa forma, as questões relativas à governação da cibersegurança na UE devem ser aprofundadas e aprimoradas no sentido de oferecer diretrizes com ações que devam ser tomadas em todos os níveis de forma eficaz. Para isso, no desenvolvimento constante do quadro multinível da cibersegurança, com responsabilidades partilhadas entre os vários intervenientes da UE, deve-se considerar que atribuições são necessárias para a sua governação eficaz e qual a forma mais adequada para lidar com as questões de ciberdefesa (e não só, mas esse é um tema mais sensível e merece maior atenção), sem que isto provoque o movimento indesejado (centrípeto). Além disso, deve-se reconhecer o caráter global da cibersegurança, e que, nem os EM, nem a UE, terão capacidade de resistir aos ciberataques sem que a questão da governação da cibersegurança seja tratada e reforçada a nível global adequadamente. De acordo com Pernice (2017, p. 27):

As a means of effectively containing cyberrisks, recourse to digital sovereignty is not the solution. The internet is global, and so must be the framework providing protection for its security and functioning. As — and as long as — the attribution of cyberattacks and threats is technically impossible, deterrence and hack-back are not an option.

Pernice (2017, p. 27) explica que, na constelação digital, uma governação efetiva, requer uma regulação global. Para isso, devem ser incluídos todos os atores em todos níveis de ação, o que acarretaria na construção de “Multi-Stakeholder Governance Mechanisms”. Por este motivo, o autor propõe uma abordagem baseada no constitucionalismo multinível para construir “a legal framework for global cybersecurity governance”, com as seguintes características:

first of all, that globally recognised human rights must be the foundation and a leading point of reference in the respective normative processes (human dignity and personal freedoms, privacy (...))

the constitutional right to security —or better: a fundamental principle of security — is an incentive and guideline for action taken to effectively protect cybersecurity at all levels; responsible risk assessment, of the kind that would be a precondition for any insurance scheme; digital competence and specialised expertise in all disciplines is required; awareness of the risks is also increasing, but raising awareness of the shared responsibility of all actors for cybersecurity seems to be a priority; Furthermore, business, user organisations and general political processes should quickly focus on appropriate technical standards and certification on cybersecurity, and legislation not only regarding information and alert systems but also on private and product liability and adequate insurance. Such normative processes should be undertaken at all levels, including the global level, for the democratic organisation of which, through a constitutional framework of global cybersecurity governance, the internet itself can play a crucial role. (PERNICE, 2017, p. 27-28)

Em suma, os desafios para a eficácia das políticas de cibersegurança da UE são muitos e na medida que o ciberespaço evolui, também evoluem a sofisticação das ameaças e aumentam as vulnerabilidades. Este é um caminho sem volta e, por este motivo, as medidas de cibersegurança devem ser continuamente avaliadas e adaptadas, de forma a apresentar melhor coerência e consistência em relação aos objetivos traçados e buscando sempre o equilíbrio necessário entre a defesa dos direitos fundamentais e o cumprimento das medidas de segurança da UE. Cabe à UE desempenhar um papel coerente na governação da cibersegurança, considerando as atribuições que lhe foram conferidas constitucionalmente, e no quadro internacional, para preservar uma perspectiva multifacetada capaz de lidar com as múltiplas dimensões das ameaças advindas do ciberespaço. Para finalizar, Giantas (2019, p. 31)¹⁰² avalia o contexto das políticas de cibersegurança da UE e as perspectivas futuras, e conclui que:

*Clearly, the EU has the ambition to play a leading role, both in Europe and internationally. It invests in tools, introduces frameworks, wants to exercise power in the cyberspace, **advance EU interests and at the same time stand by its values**. However, the EU faces the serious challenges of skills gap and different levels of digital literacy and development across its members, the euro-skepticism towards EU's competences in security and defense issues, the lack of trust and cooperation of its member states, the mix of issues such as Brexit, refugee crisis and economic hardships of some EU countries and the operational and strategic superiority of organization such as NATO, regarding defense and security. All of these create a complex, volatile and unpredictable environment for the EU and baffle EU's effort to have a strong presence in the cyber-related issues. For now, the EU's role in this territory is more formative compared to the dominant powers such as the United States or China, and EU's responses are often diverse, lack coherence and could create conflicts inside the EU.*

6 CONCLUSÃO

Os desafios para a construção de um espaço digital seguro a nível da UE demandam uma complexidade de ações para garantir a eficácia das medidas de cibersegurança adotadas, dada a transversalidade desta matéria. Devido as novas ameaças advindas do ciberespaço e ao aumento da preocupação com a ocorrência de ciberincidentes, a cibersegurança foi alçada a um

¹⁰² Giantas, Dominika H. *Cybersecurity in the EU: Threats, frameworks and future perspectives* (2019) Disponível em: <https://www.researchgate.net/publication/335909463>. Acesso em Set. 2020.

elemento fundamental para construção de confiança da sociedade e para os benefícios trazidos para economia pelas transformações digitais. Uma vez que a ciberdependência é um caminho sem volta, o combate as ciberameaças passaram a fazer parte das prioridades da agenda política da UE, onde os ativos que carregam maior grau de importância são as infraestruturas críticas essenciais para o funcionamento da sociedade (como fornecimento de água e energia, hospitais, transportes, redes e sistemas de informação etc.) onde a ocorrência de um ciberincidente na continuidade dos serviços pode ter consequências graves.

Neste trabalho, buscou-se, primeiramente, abordar as questões terminológicas relativas a cibersegurança, as definições sobre a sua dimensão e os correspondentes domínios de atuação (proteção simples, prossecução criminal e defesa de Estado), onde se introduziu uma noção do fenómeno das *threat politics* e foram abordadas as diferentes perspetivas sobre a cibersegurança que impactam na tomada de decisão ao estabelecer uma estratégia. Após isso, foi vista a noção de ciberameaça, os diferentes tipos de atividades maliciosas, os diferentes atores envolvidos, as ferramentas mais comuns, e a necessidade de um sistema de avaliação de ameaças que vá ao encontro dos objetivos a que a UE se propõe. Neste ponto, foi observada a necessidade de uma revisão sistemática do que constitui uma ameaça no contexto da cibersegurança, de forma a estabelecer uma padronização para um sistema de avaliação de ameaças, devido as incompatibilidades de definições, métricas e abordagens.

Posteriormente, foi analisado o caminho percorrido pela UE até o momento atual, onde elaborou-se um quadro resumido contendo as diferentes perspetivas da UE nas questões de cibersegurança ao longo do tempo (passou de sub-ramo de TIC e cibercrime para uma abordagem mais holística, e atualmente com grande foco em ciberdefesa). Em seguida, foi descrito o panorama estratégico da UE na atualidade em matéria de cibersegurança, onde pode-se perceber o ecossistema complexo e multifacetado desenvolvido, que envolve medidas em diversas áreas (ações em diversos setores e, principalmente, a segurança das redes e das informações, a proteção das infraestruturas críticas, a cibercriminalidade, a ciberdefesa, ciberdiplomacia, etc.) e com diversos intervenientes, para na seção seguinte analisar os instrumentos jurídicos centrais vigentes (Diretiva SRI e o Regulamento da Cibersegurança).

Foi visto que a Diretiva SRI é um instrumento de resposta coordenada e de recuperação de incidentes que estabelece uma série de medidas (tais como a obrigação de notificação de incidentes graves e de atender aos requisitos de segurança) para a prevenção e tratamento de ciberincidentes nas infraestruturas críticas, essenciais para o funcionamento da sociedade. Ou seja, é mais focada na preparação e na capacidade de responder a grandes incidentes. Já o

regulamento da Cibersegurança é relativo ao um novo mandato para (ENISA), onde estabelece seu reforço e reestruturação, bem como a criação de um quadro de certificação à escala da UE. Ou seja, é instrumento que trabalha na origem, que objetiva reduzir as vulnerabilidades e aumentar a resiliência através da certificação de produtos, serviços e processos de TIC.

Na última parte, foi feito levantamento dos principais desafios para a eficácia da política de cibersegurança da UE com base na perspectiva e abordagem atual para lidar com esta temática, onde pode-se elencar os seguintes desafios: dar coerência ao quadro estratégico e legislativo multifacetado e com muitos intervenientes; proceder a uma avaliação e prestação de contas das medidas adotadas; colmatar as lacunas na legislação da UE e na sua desigual transposição; disparidades verificadas nos regimes sancionatórios adotados na transposição da diretiva SRI; voluntariedade de certas disposições; falta de visão clara das despesas; adaptação dos níveis de investimento aos objetivos estratégicos; melhorar a governação da cibersegurança; falta de ferramentas de avaliação das ameaças e riscos standardizados como a base para determinar as estratégias; reforçar as competências e a consciencialização; buscar autonomia; alcançar rapidez de deteção e resposta na proteção das de importância crítica em graves incidentes; construir uma cultura de cibersegurança, entre outros.

Finalmente, foram pontuados os esforços na condução das políticas de cibersegurança pela UE, cujo foco tem sido caracterizado pela ciberdefesa. Esse avanço em matéria de ciberdefesa vem carregado de objeções, pois a segurança é assunto sensível aos EM, e pode comprometer a eficácia das medidas de cibersegurança com um todo. Além disso, foi abordada importância de uma regulação da governação da cibersegurança a nível global com base no constitucionalismo multinível, o que beneficiaria a todos na construção de um ciberespaço mais seguro. Enfim, a redução dos riscos e do impacto das ciberameaças ainda requer a superação de muitos obstáculos para responder à altura dos desafios apresentados, o que carece de constante avaliação e adequação, buscando manter a coerência e consistência para perseguir os interesses da UE nesta matéria e ao mesmo tempo proteger os valores em que se funda.

REFERÊNCIAS

ALEXANDER, Dean. **Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses**. Istambul: İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi. 2014.

BIRD&BIRD&. **Developments on NIS Directive in EU Member States**. [Em linha]. Alemanha, 2020. [Consult. Fev. 2020]. Disponível em WWW:

<URL:<https://www.twobirds.com/~media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf>>.

BELÁZ, Annamaria. **The changing role of the EU in cybersecurity**. Biztonságtudományi Szemle Safety and Security Sciences Review. Hungria. Vol. 1 (2019), pp. 17-30.

BUCHANAN, Ben. **The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics**. Massachusetts: Harvard University Press. 2020.

CAMPOS, J.M.; E CAMPOS, J. L. M. **Manual de Direito Europeu**. 6ª Edição. Ed. Wolters Kluwer-Coimbra. 2010. ISBN 9789723218121.

CARRAPICO, Helena; BARRINHA, André. **The EU as a Coherent (Cyber)Security Actor?** JCMS 2017. Nova Iorque. Vol. 55, nº 6 (2017), pp. 1254-72.

CONSELHO DA UNIÃO EUROPEIA. **Estratégia Europeia em Matéria de Segurança: Uma Europa Segura num Mundo Melhor**. Luxemburgo: Serviço das Publicações da União Europeia 2009, 43 p. ISBN 9789282424315. doi: 10.2860/16255 QC-78-09-568-PT-C.

DUARTE, Maria Luísa. **Estudos de Direito da União e das Comunidades Europeias**. 2000. Editora Coimbra. ISBN: 9789723209952.

DUNN, Myriam. **A Resilient Europe for an Open, Safe and Secure Cyberspace**. UI Occasional Papers. Suécia. Nº 23. 2013.

DUNN, Myriam. **A Comparative Analysis of Cybersecurity Initiatives Worldwide**. ITU - WSIS Thematic Meeting on Cybersecurity. Tunísia. 2005. [Em linha]. [Consult. Fev. 2020]. Disponível em WWW: <URL:http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf>.

E SILVA, Karine. **Europe's fragmented approach towards cyber security**. . [Em linha]. Internet Policy Review 2 (4). 2013. [Consult. Jul. 2020]. Disponível em WWW: <URL:<https://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cyber-security/>>. DOI: 10.14763/2013.4.202.

EUROPOL. **Avaliação da Ameaça da Criminalidade Grave e Organizada da UE (AACGO da UE)**. [Consult. Ago. 2020]. Disponível em WWW:<URL:<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>>.

FAESEN, Louk; TOROSSIAN, Bianca; MAYHEW, Elliot; ZENSUS, Carlo. **Conflict in Cyberspace - Parsing the threats and the state of international order in cyberspace**. [Em linha]. Holanda. 2019. [Consult. Fev. 2020]. Disponível em WWW: <URL:<https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/>>.

FERNANDES, Aníbal M. C. **A dimensão política da segurança para o ciberespaço na União Europeia: a agenda digital, a estratégia de cibersegurança e a cooperação UE-OTAN**. Ponta Delgada: Universidade dos Açores. Vols. 1, 2. 2014.

GEHEM et al. **Assessing cyber security: A meta-analysis of threats, trends, and responses to cyber attacks**. [Em linha]. Holanda. 2015. [Consult. Fev. 2020]. Disponível em WWW: <URL: <http://www.hcss.nl/reports/download/164/2938/>>.

GIANTAS, Dominika H. **Cybersecurity in the EU: Threats, frameworks and future perspectives**. [Em linha]. Grécia. 2019. [Consult. Fev. 2020]. Disponível em WWW: <URL: <https://www.researchgate.net/publication/335909463>>.

GODWIN III et al. **Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity**. The EastWest Institute & Information Security Institute Moscow State University. Nova Iorque. 2014.

GONÇALVES, João A. P. **Enquadramento legal da cibersegurança em Portugal e no Mundo**. [Em linha]. Escola Naval: Lisboa. 2016. [Consult. Jul. 2020]. Disponível em WWW: <URL: <https://comum.rcaap.pt/bitstream/10400.26/15040/1/ASPOF%20EN-M%20Pinto%20Gon%c3%a7alves%202016.pdf>>.

GORJÃO-HENRIQUES, Miguel. **Direito da União: História, Direito, Cidadania, Mercado Interno e Concorrência**. 2014. 7ª Ed. Editora Almedina. ISBN: 9789724055541.

KARAKE-SHALHOUB et al. **Enforcing Cybersecurity in Developing and Emerging Economies: institutions, laws and policies**. Edward Elgar Publishing: Cheltenham. 2019.

KASPER, Agnes; ANTONOV, Alexander. **Towards Conceptualizing EU Cybersecurity Law. ZEI Discussion Paper C253 2019**. Universidade de Bonn: Bonn. 2019. [Consult. Jul. 2020]. Disponível em WWW: <URL: <http://aei.pitt.edu/100365/>>.

KOVÁCS, László. **Cyber security policy and strategy in the European Union and NATO**. National University of Public Service: Hungria. Land Forces Academy Review. Vol. 23, nº 1 (89) (2018).

MUGGAH et al. **Securitização da cibersegurança no Brasil. Cadernos Adenauer**. Fundação Konrad Adenauer: Rio de Janeiro. Vol. 15, nº4 (2014).

PERNICE, Ingolf. **Cybersecurity Governance: Making Cyberspace a Safer Place**. July 20, 2017. HIIG Discussion Paper Series No. 2017-05. [Em linha] [Consult. Out. 2020] Disponível em: SSRN: <https://ssrn.com/abstract=3012136> or <http://dx.doi.org/10.2139/ssrn.3012136>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Glossary of Key Information Security Terms**. Updated on July 2019. [Consult. Jul. 2020]. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>>.

NTT SECURITY. **2018 Risk:Value Report**. [Em linha] [Consult. Jul. 2020]. Disponível em WWW: <URL: https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_report_risk-value_2018_us_uea_v1.pdf?sfvrsn=c96bf84f_0>.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Global Cybersecurity Index 2017: in Strengthening Trust**. OECD Publishing. Paris. 2019. ISBN: 978-92-61-25071-3.

SANTOS, L., BRAVO, R. e NUNES, P. V. **Proteção do Ciberespaço: Visão Analítica. Riscos, Segurança e Sustentabilidade**, C. Guedes Soares, A. P. Teixeira, C. Jacinto (Eds), Edições Salamandra, Lisboa, 2012, pp.163 a 176. ISBN 978-972-689-247-2.

TIKK, E., KASKA, K. e VIHUL, L. **International Cyber Incidents: Legal Considerations**. Tallinn, Estonia: Cooperative Cyber Defence Center of Excellence. 2010. ISBN: 9789949904006.

TRIBUNAL DE CONTAS EUROPEU (TCE). **Documento de análise n.º 02/2019: Desafios à eficácia da política de cibersegurança da UE**. [Em linha] [Consult. Jan. 2020]. Disponível em WWW: <URL: <https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=49416>>.

VAN DER MEULEN, N.; A JO, E.; e SOESANTO, S. **Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses**, European Parliament, RR-1354-EP, 2015. July 06, 2020.

VIDAL, Serafín Pazos. **Subsidiariedad y Gobernanza Multinivel en la Praxis del Sistema Institucional de la UE**. Tese Doutoral - Resumen. UNED. Universidad Nacional de Educación a Distancia. Espanha. 2017. [Em linha] [Consult. Out. 2020]. Disponível em: <<http://e-spacio.uned.es/fez/view/tesisuned:ED-Pg-UniEuro-Spazos>>.

WORLD BANK AND UNITED NATIONS. **Combatting Cybercrime: Tools and Capacity Building for Emerging Economies**. 2017. Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Legislação e Documentos Oficiais

COMISSÃO DAS COMUNIDADES EUROPEIAS. COM (85) 310 final. Bruxelas, 14.6.1985.

COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2000) 890 final. Bruxelas, 26.1.2001.

COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2001) 298 final. Bruxelas, 26.1.2001.

COMISSÃO DAS COMUNIDADES EUROPEIAS. COM(2006) 251 final. Bruxelas, 31.5.2006.

COMISSÃO EUROPEIA. COM(2010)245 final. Bruxelas, 19.5.2010.

COMISSÃO EUROPEIA. COM(2011) 163 final. Bruxelas, 31.3.2011.

COMISSÃO EUROPEIA. COM(2015) 185 final. 28.4.2015.

COMISSÃO EUROPEIA. COM(2015) 192 final. 6.5.2015.

COMISSÃO EUROPEIA/SERVIÇO EUROPEU PARA A AÇÃO EXTERNA (SEAE). JOIN(2016) 18 final, de 6 de abril de 2016.

COMUNICAÇÃO CONJUNTA JOIN(2013) 1 final. Bruxelas, 7.2.2013.

COMUNICAÇÃO CONJUNTA JOIN(2017) 450 final. Bruxelas, 13.9.2017.

COMUNICAÇÃO DA COMISSÃO DAS COMUNIDADES EUROPEIAS. COM/2009/0149 final. Bruxelas, 30.3.2009.

CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23.11.2001. Série de Tratados Europeus / 185.

CONCLUSÕES DO CONSELHO sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia"), doc. 9916/17, de 7 de junho de 2017. [Consult. Ago. 2020]. Disponível em WWW:<[URL: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pt/pdf](https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pt/pdf)>.

DECISÃO DO CONSELHO relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros Bruxelas, 14 de maio de 2019 (OR. en) 7299/19. [Consult. Ago. 2020]. Disponível em WWW:<[URL: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/pt/pdf](http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/pt/pdf)>.

DECISÃO (PESC) 2020/1127 DO CONSELHO EUROPEU. [Consult. Ago. 2020]. Disponível em WWW:<[URL: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020D1127&from=ES](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32020D1127&from=ES)> .

DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 - relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). Warsaw Summit. 2016. Issued by the Heads of State and Government participating in the meeting.

PARECER FUNDAMENTADO DO SENADO FRANCÊS sobre a Proposta de 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)0477 – C8-0310/2017 – 2017/0225(COD))

PARECER DA COMISSÃO EUROPEIA COM(2017) 477 final 2017/0225 (COD). Bruxelas, 4.10.2017. Proposta de 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»).

REGULAMENTO (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação.

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).

REGULAMENTO (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019 - relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança).

SEAE, Visão partilhada, ação comum: uma Europa mais forte). Estratégia Global para a Política Externa e de Segurança da União Europeia, junho de 2016.

Jurisprudência

Processo C-217/04: Reino Unido da Grã-Bretanha e da Irlanda do Norte VS Parlamento Europeu e Conselho da União Europeia. Acórdão do Tribunal de Justiça (Grande Secção) de 2 de Maio de 2006.