Os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19.

De que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020-Março 2021?

Versão final após defesa

Paula Filipa Trilho Gonçalves

Dissertação para obtenção do Grau de Mestre em
Relações Internacionais
(2º ciclo de estudos)

Orientador: Prof. Doutora Liliana Domingues Ferreira Reis

Abril de 2022

Folha em branco

Dedicatória

Aos meus pais e à minha irmã.

Folha em branco

Agradecimentos

Em primeiro lugar, gostaria de agradecer à minha orientadora Prof. Doutora Liliana Domingues Ferreira Reis por ter acreditado nas minhas capacidades e me ter orientado com a excelência no objetivo.

Seguidamente, em especial, quero demonstrar a minha eterna gratidão aos meus pais, que sempre me apoiaram e fizeram com que esta dissertação fosse possível de acontecer.

Quero agradecer também aos meus avós e às minhas tias, Bela e Ilda, por todo o carinho manifestado.

À minha amiga e companheira de mestrado Hilma Lopes, que tanto me ajudou neste projeto com toda a discussão de ideias e afeto, bem como, igualmente, às minhas amigas por todos os bons momentos de distração e companheirismo.

Por fim, mas não menos importante, agradecer à minha irmã pela sua constante boa-disposição e carinho, que tanta motivação ofereceram.

A todos, o meu muito obrigada.

Folha em branco

Resumo

A segurança internacional tornou-se numa das principais áreas de discussão no âmbito das Relações Internacionais. Com efeito, observou-se nos últimos anos o alargamento do conceito de modo a incluir novos atores, mas também novas dimensões no âmbito da segurança. Esta investigação propôs-se a analisar não apenas a dimensão conceptual-normativa sobre os estudos sobre a segurança, mas procurou refletir sobre a agenda internacional do ciberterrorismo e onde elabora, em particular sobre a dimensão da cibersegurança na União Europeia.

Tendo a pandemia provocada pelo Covid19 modificado os padrões de utilização dos meios digitais, quer a nível público, quer a nível privado, esta investigação procurou, também avaliar o aumento do risco da cibersegurança durante este período, analisando quais foram as principais ciberameaças que surgiram em comparação com os ataques de 2017-2018 e quais os novos desafios.

A dissertação conclui com uma análise à política de cibersegurança da União Europeia durante o período de março 2020 a março 2021 e a resposta que foi dada para mitigar as principais ameaças.

Palavras-chave:

Cibersegurança;União Europeia;Resiliência;Ameaças;Cibercrime.

Folha em branco

Abstract

International security has become one of the main areas of discussion in International Relations. In fact, in recent years, the concept has been expanded to include new members, but also new dimensions in the field of security. The propose of this research, was to analyze not only the conceptual-normative dimension of security studies, but also to reflect on the international cyberterrorism agenda and where it elaborates, in particular on the cybersecurity dimension in the European Union.

The pandemic caused by Covid19 had changed the patterns of use of digital media, both at a public and private level, this investigation also sought to assess the increase in cybersecurity risk during this period, analyzing the main cyber threats that emerged, compared to the 2017-2018 attacks and what the new challenges are.

The dissertation concludes with an analysis of the European Union's cybersecurity policy during the period from March 2020 to March 2021 and the response that was given to mitigate the main threats.

Keywords:

Cybersecurity;European Union;Resilience;Threats;Cibercrime.

Folha em branco

Índice

Folha em branco

Lista de Figuras

Folha em branco

Lista de tabelas

Folha em branco

Lista de Acrónimos e Siglas

BEC	Business email compromisse
CEO	Chief Executive Officer
CERT	Community Emergency Response Team
CNCS	Centro Nacional de Cibersegurança
CSIRT	Computer Security Incident Response Team
CUREX	Secure and Private Health Data Exchange
CyCLONe	Cyber Crises Liaison Organization Network
DEFeND	Data Governance for Supporting GDPR
DDos	Distributed denial-of-service
DNS	Domain Name System
EM	Estados-Membros
ENISA	Agência Europeia para a Segurança das Redes e da Informação
ESI	Estudos Segurança Internacional
FBI	Federal Bureau of Investigation
FFP	*filtering facepiece*
GDPR	General Data Protection Regulation
GWOT	Global War on Terrorism
IA	Inteligência Artificial
ICE	Infra-estruturas Críticas Europeias
IdC	Internet das Coisas
INTCEN	Intelligence Analysis Centre
INTERPOL	International Criminal Police Organization
NATO	North Atlantic Treaty Organization
OCDE	Organização de Cooperação e Desenvolvimento Económico
OMS	Organização Mundial de Saúde
ONU	Organização das Nações Unidas
PANCEA	Protection and Privacy of Hospital and Health Infrastructures with Smart Cyber Security and Cyber Threat Toolkit for Data and People
PAPAYA	PlAtform for PrivAcY preserving data Analytics
PESC	Política Externa e de Segurança Comum
PIB	Produto Interno Bruto
PMEs	Pequenas e Médias Empresas
PNUD	Programa das Nações Unidas para o Desenvolvimento
RI	Relações Internacionais
SPHINX	A Universal Cyber Security Toolkit for Health-Care Industry
SRI	Segurança das Redes de Informação
TI	Tecnologias da Informação
TIC	Tecnologias de informação e comunicação
UBI	Universidade da Beira Interior
UE	União Europeia
URSS	União das Repúblicas Socialistas Soviéticas

Folha em branco

Introdução

A presente investigação tem como tema "Os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19" e o seu principal objetivo é entender de que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020-Março 2021.

Esta investigação teve como objectivo promover um melhor conhecimento no âmbito da avaliação das ameaças e dos riscos que se inserem no domínio da cibersegurança, os quais se revestem, hoje, de uma importância fulcral nos Estudos de Segurança no domínio da área epistémica das Relações Internacionais.

Esta temática reveste-se de importância não apenas pelas aparentes consequências causadas, mas também pelo aumento exponencial de ataques informáticos reportados a entidades particulares e estatais, durante a crise epidemiológica, colocando novos desafios à segurança. Ademais, podemos considerar que a Cibersegurança se tem revelado um dos principais domínios de preocupação por vários atores políticos e públicos, dada a ameaça que constitui quer a nível de ameaça interna como ameaça externa. Cumpre-nos ainda sublinhar que o tema de cibersegurança tem dominado as agendas internacionais nos últimos tempos, havendo a tentativa de perceber se se terá acentuado durante o último ano.

Ora, para a condução da investigação optou-se pela adoção de uma metodologia qualitativa, sobretudo recorrendo ao método hipotético-dedutivo. A metodologia utilizada socorreu-se do uso de fontes primárias, recorrendo à legislação nacional e da União Europeia face à cibersegurança. Recorre-se também a relatórios do Centro Nacional de Cibersegurança.

Utiliza ainda fontes secundárias uma vez que, se debruça em investigações e artigos científicos de autores reconhecidos na área da segurança, da cibersegurança e da União Europeia como Barry Buzan, Nelson Lourenço, André Barrinha, Helena Carrapiço ou investigações nacionais, do Instituto de Defesa Nacional, Instituto Português de Relações Internacionais, entre outros. Conta também, como ferramenta, atentar aos impactos da Covid19 segundo alguns especialistas. Ainda nas fontes secundárias acrescentam-se a revisão de literatura, monografias.

Para uma melhor avaliação da nossa problemática foram projetadas a seguintes perguntas derivadas: Será que a pandemia veio alterar a perceção da ameaça digital? Os Estados estavam preparados para o aumento do tráfego comercial informativo a nível

digital? Como foi a adequação dos Estados em Março 2020 – Março 2021 do ponto de vista estratégico da cibersegurança?

Na orientação desta investigação foi necessária a elaboração das seguintes hipóteses, estabelecidas como possíveis respostas para as perguntas derivadas acima mencionadas:

H1: A pandemia não veio alterar os desafios à cibersegurança. Estes já existiam e a pandemia apenas veio confirmá-los.

H2: A pandemia veio colocar a cibersegurança e a saúde pública no topo da agenda internacional e defesa da União Europeia.

H3: Apesar da cibersegurança estar desde a apresentação da estratégia de segurança, em 2003, como um dos eixos estratégicos da União Europeia a pandemia veio revelar as vulnerabilidades da União Europeia face a esta ameaça.

No âmbito de uma melhor organização, esta investigação será dividida em capítulos como: (C1) Enquadramento conceptual-normativo - que tentará aferir o debate epistemológico em torno da cibersegurança e simultaneamente tentar analisar os artigos da União Europeia face à mesma conceptualização. Neste seguimento, surgirá o capítulo (C2) A pandemia Covid19 e a cibersegurança - de modo a avaliar o risco ao nível da cibersegurança e da pandemia, qual o aumento tráfego e quais as principais ameaças que se subordinará à pandemia Covid19 em segurança. Por fim, no último capítulo (C3) A política de cibersegurança para a União Europeia depois da pandemia, onde será avaliada a política de cibersegurança da União Europeia compreendida no periodo de Março 2020 a Março 2021.

1ºCapítulo – Enquadramento conceptual-normativo

1.1. Estudos sobre a segurança

Os Estudos de Segurança Internacional começaram como área de estudo independente e foram-se consolidando ao longo século XX. A questão da segurança nas Relações Internacionais esteve ao longo do desenvolvimento da área epistemológica relacionada com a segurança dos Estados. A este propósito foi-se consolidando através dos Estudos da Guerra[1] ou estratégia militar, e no desenvolvimento conceptual do poder ou da sobrevivência, onde incluíam autores como Clausewitz , Kenneth Waltz (1924), Hans Morgenthau (1904) (Alencar, 2015; p.188; Esteves, 2015; p.52). Mas a Segunda Guerra Mundial, a Guerra Fria e o pós- Guerra Fria marcariam uma viragem histórica neste paradigma, ao mesmo tempo que contribuiriam para o desenvolvimento dos Estudos de Segurança (Duque, 2009).

Após a Segunda Guerra Mundial, o Estado, a defesa e a guerra deixam de ser os principais domínios e começa a aparecer literatura específica sobre a Segurança, centrada nas ameaças e proteção dos Estados (Esteves, 2015 ; p.53). Segundo (Alencar, 2015; p.186) o facto de a teoria realista, dominante após a Segunda Guerra Mundial, se ter demonstrado insuficiente por não ter previsto o início da Guerra Fria, levou a novos debates teóricos e à reformulação do conceito de segurança.

O mesmo se sucedeu após a Guerra Fria. Como explica (Duque, 2009;p.464), através de (Freedman, 1998), "o colapso da URSS gerou perda de credibilidade na utilidade de previsão dos estudos estratégicos, uma vez que o evento não poderia ser explicado dentro do paradigma do (neo)realismo". Assim, os estudos estratégicos, apoiados pela teoria realista, deixaram de fazer sentido, e adotou-se o campo dos Estudos de Segurança (Duque, 2009;p.464). Para Esteves (2015;p.52) o facto da URSS representar, para o Ocidente, uma ameaça militar e ideológica, fez com que o campo militar continuasse como prioridade nas agendas internacionais, ainda depois da Guerra Fria. Tal como, Rodrigues & Mèrcher (2017;p.3) que consideram que o debate precisou de ser renovado por se refletir na política de manutenção da Guerra Fria a quantidade de literatura centrada em aspetos militares e estratégicos. Contudo, Buzan, Waever e Wilde

[1] Polemologia- "Termo criado por Gaston Bouthoul, para designar o estudo sociológico dos conflitos e da guerra" (Sousa, 2005, p. 144).

(Buzan, Waever, & Wilde, 1998;P.2), refletem que essa concentração dos estudos de segurança em questões militares e nucleares da Guerra Fria, despoletou o debate de alargamento e acrescentam como estímulo o surgimento das agendas económica e ambiental, bem como as questões de identidade e o crime transnacional.

Em 1985, é fundado o Centre for Peace and Conflict Research, atualizado para Copenhagen Peace Research Institute (COPRI)[2], que deu origem à Escola de Copenhaga. Na Escola de Copenhaga, Ole Waeve, Barry Buzan e Jaap de Wilde demonstram o seu importante contributo, desde o início, com a formulação de conceitos e a sua revisão, tais como o conceito de securitização, os níveis de análise, e a análise multisetorial, que se empenharam por, ao longo dos anos, manter os conceitos atualizados às características das sociedades. Tanno (2003; p.53) explica que, a Escola de Copenhaga formou-se com o objetivo de "desenvolver um conjunto de conceitos e quadros analíticos para viabilizar a analise de segurança internacional sob uma perspetiva abrangente"

A Escola de Copenhaga viu surgir três vertentes teóricas da Segurança Internacional, fruto da já referida insatisfação e dos debates teóricos discutidos, ao longo dos anos. Assim, nasceu a perspetiva tradicionalista, a perspetiva abrangente e a perspetiva crítica. De uma forma geral, a perspetiva tradicionalista, assente no realismo, centra a segurança em torno do Estado e das questões militares. A perspetiva abrangente, defendida pelos teóricos de Copenhaga, considera que o conceito de segurança deve incorporar tanto as questões militares como acrescentar questões referentes aos setores político, económico, ambiental de modo a garantir o bem-estar do Estado (Buzan, 1991 apud Tanno,2003; p.50). Por último, a perspetiva crítica, apoiada pela Escola de Frankfurt, propõe que a segurança humana seja inserida no conceito de segurança, tal como, a igualdade e a liberdade (Booth, 1991 apud Tanno,2003; p.50).

No desenvolvimento da perspetiva abrangente, Buzan, Waever e Wilde, em "A New Framework of Analysis" (1998), explicam que a segurança pode ser analisada por diferentes níveis, setores e regiões. No que se referem aos níveis, dividem-nos numa escala que vai do Sistema Internacional até ao indivíduo; por setores, agrupam-nos como político, económico, societal e ambiental e por regiões entendem as relações

[2] A sua atualização deve-se à mudança do conceito de segurança. Os estudos militares e o Estado como ator principal foram substituídos por uma abordagem multidisciplinar da segurança, com aproximação aos estudos da paz e da segurança internacional.

regionalizadas fruto do pós-guerra fria. Para além desta análise da segurança, um dos principais contributos desta escola é o processo de securitização, onde apresentam os critérios necessários para uma ameaça se tornar um problema de segurança, alvo de intervenção urgente: a ameaça pode ser existencial, fazendo uso de meios emergenciais para a resolução do problema, permitindo aos Estados a quebra de regras. Assim, é necessário que o problema seja aceite pela sociedade, ou seja, quem pretende securitizar algum tema precisa, como refere Mercher e Rodrigues (2017; p.4), que seja socialmente reconhecido como uma ameaça. Neste sentido, tem de passar pelo ato da fala/speech act que é, segundo Duque (2009; p.479) baseada em Buzan et al., (1998; p.25) onde os indivíduos manifestam quais as suas prioridades e se consideram que um determinado problema deve ou não ser securitizado. Para esta autora, é neste conceito que se verifica a maior influência do construtivismo pois, para além de os problemas serem decididos pela sociedade se representam ou não uma ameaça para a segurança, o Estado não é o único objeto de referência. Acrescendo que esta corrente é definida por ter o sujeito como um participante ativo, fazendo interpretações das suas experiências, levando-o a tomar a decisão de quais situação deverão ser alvo de securitização, selecionando e desenvolvendo as suas próprias estratégias. Seabra (2016; p.51), acrescenta que a securitização é um conceito inclusivo, na medida em que, introduz para o debate "ameaças intersubjetivas previamente ignoradas".

A nível do alargamento setorial Esteves (2015, p.52) explica que, a partir de 1990, vários teóricos de diversas áreas entraram em debates sobre os Estudos de Segurança Internacional, pelo que, a segurança pode "percorrer tanto a teoria das RI e da Economia Política internacional como a análise política e a Teoria Política", pois não está claramente definida.

À luz do que considera Lourenço (2015;p.29), este alargamento deve-se não só a uma aproximação ao construtivismo, mas também à alteração do quadro de ameaças internacional e acrescenta que, no que diz respeito à segurança política esta é a "estabilidade institucional do Estado do seu regime político", a segurança económica refere-se à "prosperidade Estado e bem-estar dos seus cidadãos"; a segurança ambiental preocupa-se com "a relação entre a sociedade e a biosfera à escala planetária" e a segurança societal que se refere "aos elementos identitário de uma entidade política, isto é, de um determinado Estado com a língua e a cultura". A revisão de literatura tem referido que estes elementos estão interligados e são interdependentes, pelo que, a falha de um destes setores, para além da possibilidade de condicionar os outros, significa a insegurança do indivíduo e do Estado. A Escola de Copenhaga defende que a ameaça é

variável não só de Estado para Estado, mas também entre os próprios setores e níveis. Ao que Alencar (2015; p.192), confere um caráter transnacional à ameaça, afirmando que "podem acontecer tanto a partir de outros Estados, de atores não-estatais ou de relações de poder" e que não é necessária a existência de uma fronteira física para que o indivíduo se possa sentir ameaçado.

Contudo, A Escola de Copenhaga atribui à segurança o significado de "sobrevivência", ainda que, para Tanno (2003,p.52-53) a segurança não possua qualquer significado intrínseco, ou mesmo para Santos (2016; p.109) para quem "a segurança é um conceito amplo e sem significado único". Para Esteves (2015; p.54), a segurança é um "conceito hifenizado", isto é, estruturado em torno de alguma questão. Paulo (2016; p.107) trata a segurança como uma necessidade básica que "requer paz e passa pela ausência de obstáculos e ameaças à realização das necessidades e fins das pessoas e dos grupos em que se integram". Duque (2009; p.486), vai mais além e considera que segurança é um "processo dinâmico, uma construção social que depende da ação de agentes e estruturas". A literatura ressalva que, o significado de segurança também varia consoante o contexto histórico ou a localização geográfica, pois existem diferenças da perceção de segurança entre o hemisfério sul e o hemisfério norte e até mesmo "diferentes modos de construção de segurança de acordo com as culturas locais", como explica Alencar (2015; p.189).

Cinco anos após a criação da Escola de Copenhaga e do surgimento do pós-colonialismo, os estudos de Segurança Internacional começam a debater as grandes dificuldades não-ocidentais. As estruturas políticas, económicas, ambientais e sociais dos países descolonizados, que enfrentavam períodos de instabilidade e pouco desenvolvimento, levaram a que os debates chegassem até ao conceito de Segurança Humana. O conceito foi formulado pelo Programa das Nações Unidas para o Desenvolvimento (PNUD), através do Relatório de Desenvolvimento Humano, em 1994, para acentuar as questões da pobreza e da saúde, na agenda global (Esteves, 2015; p.75). Deste modo, o PNUD definiu o conceito como "segurança contra ameaças crónicas como a fome, doença e repressão, bem como proteção contra interrupções súbitas e prejudiciais nos padrões de vida quotidianos, sejam estas verificadas a nível individual ou comunitário" (PNUD, 1994: 23 apud Reis, 2017; p.2). O indivíduo passou a ser o objeto de referência, e não o Estado. A perspetiva crítica, da qual a escola de Frankfurt é adepta, propõe a emancipação humana e reflete que os objetos são socialmente construídos (Mèrcher e Rodrigues, 2017; p.3).

Marcos Farias Ferreira (2016; p.108) menciona Kofi Annan para referir que, a segurança humana vai para além da ausência de violência e que engloba o cumprimento de outras necessidades, essenciais ao bem-estar e prosperidade da vida humana. Deste modo, Ferreira (2016; p.108) escreve que "(...)Kofi Annan fez questão de salientar que se trata de muito mais do que a ausência de conflito ou de violência: diz respeito à proteção de direitos humanos, à boa governação, ao acesso à educação e aos cuidados de saúde, constituindo uma nova agenda internacional que estabelece um nexo ou vínculo entre paz, segurança e desenvolvimento". Neste contexto, Alkire (2003; p.14) cita também Kofi Annan no relatório das Nações Unidas "We the People", em 2000, para demonstrar que a segurança, para além do cumprimento de outras necessidades, é a construção de um percurso: *"Every step in this direction is also a step towards reducing poverty, achieving economic growth and preventing conflict"*.

1.2. Segurança Internacional e CiberTerrorismo

O 11 de setembro de 2001, segundo Alencar (2015; p.188) foi um marco histórico sobre o debate de Segurança Internacional e, na perspetiva de Santos (2016; p.113), *"mostra a falência explicativa dos estudos tradicionais e a necessidade de se pensar a segurança num quadro amplo e profundo de análise com capacidade de se empenhar no mundo social"*. Segundo Barrinha e Carrapiço (2016; p.250) a cibersegurança esteve separada da segurança até inícios de 1990. O terrorismo deixou de ser visto como um tema periférico e ganhou lugar no topo das agendas internacionais. Segundo Alencar (2015; p.188), este marco "demonstrou que os conflitos internacionais haviam estacionado temporariamente durante a década de 90" e que o uso da força voltou a ter lugar, tal como no Afeganistão, em 2002, ou no Iraque, em 2003 (Rudzit, 2005; p.298). Este novo quadro de ameaças passou a "reconhecer ameaças não convencionais", como ameaças ambientais e digitais (Aparício, 2017; p.7). As agendas internacionais reformulam as suas prioridades, voltaram-se para conflitos que ameaçassem os Direitos Humanos e passaram a incluir questões como segurança regional, tecnologia ou conflitos no Médio Oriente (Esteves, 2015; p.84). Aqui, e com a generalização das redes de informação nos novos pilares da segurança humana (âmbito económico, político, e militar), a cibersegurança alcançou um lugar de destaque e deixou de ser pensada apenas como termos técnicos e falhas informáticas para se tornar uma das principais

preocupações das Organizações Internacionais e potencias mundiais, até porque, muitas das atividades governamentais, empresariais e quotidianas passaram a ser on-line (Aparício, 2017; p.51 ; Brown & Veale, 2020).

A este respeito, Barrinha e Carrapiço(2016; p.250) acrescentam que, ao passo que a Cibersegurança utilizada em termos técnicos, também salientava as falhas e a necessidade de as proteger. Para estes o termo em si surge após o 11 de setembro, a par das ameaças não convencionais. Como Bayuk et al. (2012; p.245), acrescenta-se à segurança o ciberespaço e esse passa a ser "a coisa a ser protegida". Os ataques de 11 de Setembro e a GWOT (Global War On Terrorism) demonstram que a tecnologia e a identificação das ameaças e dos inimigos estão intimamente ligadas e que a listagem das tecnologias mais centrais dos ESI muda com o passar do tempo(Esteves, 2015; p.64) . Mesmo considerando que a tecnologia não seja o principal condutor no desenvolvimento dos ESI (Estudos de Segurança Internacional), ela é, sem dúvida, determinante.

Ainda que, o conceito de cibersegurança derive do conceito de segurança, não há um conceito único e universal para a descrever nenhum dos dois. Seja pela complexidade do tema, seja por estar em constante mudança (consoante o tempo e o espaço, como acima mencionado), a definição mais usada por diversos autores, durante a revisão de literatura, é a definição da União Internacional das Telecomunicações – agência especializada das Nações Unidas. A definição ultrapassa a ideia clássica de 1970, os chamados *"the early days"*, onde o foco era proteger o computador de softwares maliciosos (Comissão Europeia, 2020b), e pormenoriza que:

> 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 (ITU-T, 2008; p.2).

Hansen & Nissenbaum (2009; p.1155), deixam de lado a conceção de que a cibersegurança diz respeito apenas às inseguranças técnicas de computadores em redes e esclarecem que as ameaças consequentes do ciberespaço podem manifestar efeitos devastadores na sociedade.

Para a agência russa especializada em cibersegurança (kaspersky, 2021b), a cibersegurança pode vir subdividida em diversas categorias, entre as quais: segurança de rede, de informação, de software, operacional, entre outras. Acima de tudo, esta agência explica que o sucesso da cibersegurança está dependente dos primeiros passos, da "fase de projeto", isto é, de um forte programa a ser implantado, que lhe permitirá mais segurança no uso do ciberespaço (Kaspersky,2021).

O Parlamento Europeu e o Conselho, numa diretiva de 2016 (Parlamento Europeu & Conselho, 2016)[3], definiram a cibersegurança como a proteção dos sistemas de informação, que é "alvo de ações danosas deliberadas destinadas a danificar ou a interromper a opção dos sistemas" (Parlamento Europeu & Conselho, 2016; p.1). Como consequência, podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, destruir a confiança dos utilizadores e causar graves prejuízos à economia da União. Também, da parte da UE, Juhan Lepassaar (2018), diretor executivo da agência da União Europeia para a cibersegurança considera que a cibersegurança representa tanto a obrigação como o direito à proteção de dados: "Cybersecurity techniques are an integral part to meet data protection obligations, and allow users to enjoy fully their fundamental rights to personal data protection and privacy".

A cibersegurança, considerada "a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrónicos, redes e dados contra-ataques maliciosos", protege não só a tecnologia de informação, mas também todas as ligações tecnológicas como carros, semáforos e veículos aéreos não tripulados (Kaspersky,2020; Comissão Europeia, 2020a). Protege também de ameaças cibernéticas a "dispositivos de monitoramento cardíaco em hospitais ou sistemas de aviação em que, em ambos os casos, a falta de cibersegurança pode levar à perda de vidas humanas" (Poel,2020; p.52) o que, paradoxalmente, faz da conectividade o maior problema da segurança (Caldas & Freire, 2013; p.2). Esta é também a componente moral atribuída à cibersegurança, embora, alguns se refiram a esta como um mero valor instrumental de proteção humana. A cibersegurança pode ser uma condição necessária para defender a segurança pessoal e da saúde, revelando-se que é um meio em determinado contexto, e um fim em outros (Poel, 2020;p.52 baseado em Dewey, 1922).

[3] Parlamento Europeu, & Conselho. (2016). Diretiva (EU) 2016. Jornal Oficial Da União Europeia. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L2102

Para Custódio et al., (2015; p.143), a cibersegurança é a "capacidade operacional de uma organização recolher, processar e disseminar um fluxo ininterrupto de informação, enquanto se explora ou nega a capacidade de um adversário fazer o mesmo", o que implica a identificação e análise das ameaças. Esta análise pode representar também uma vulnerabilidade quando explorada pelo invasor (ITU-T 2008; p.8). Posto isto, é importante o envolvimento de agentes estatais para evitar "uma série de ações, como atividades criminosas, espionagem industrial, guerra económica, entre outras", uma vez que, quem pratica estas ações tem conhecimento técnico para não deixar rasto, mas para causar danos de grandes dimensões (Artigo19, 2016; p.9).

Além da capacidade operacional descrita, a cibersegurança é também um "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado"(CNCS, 2019; p.16), apresentando três grandes objetivos, contemplados em toda a literatura, quer internacional quer nacional: Confidencialidade, Integridade e Disponibilidade. Não importa se os termos se referem ao usurário, à informação, a redes digitais ou aos sistemas de informação, o que importa é garantir os mesmos, em cada ponto da cibersegurança (CNCS, 2019; p.16). Assim, esta ação de fiscalização do ciberespaço tem como propósito o combate ao crime (Nunes,2013 apud Leite, 2016; p.5) como a garantia de que "terceiros não consigam ler, ou modificar mensagens destinadas a outros recetores"(Sousa Teles, 2015; p.14). É objetivo da cibersegurança evitar o acesso a serviços a que não estão autorizados e verificar a fiabilidade das fontes de mensagem (Sousa Teles, 2015; p.14). Através do cumprimento destes objetivos tenta-se, da melhor e mais eficaz maneira, proteger a sociedade e as suas organizações, uma vez que, o risco se torna reduzido sem a exploração não autorizada (Haapamäki & Sihvonen, 2019; p. 812).

Os três objetivos mencionados alcançam-se através de meios como a intervenção política, domínio de meios técnicos e a intervenção educacional, para que o utilizador obtenha segurança, quer esteja online quer esteja offline (ITU-2018; p.1) e se adquira a confiança do usuário, seja ele uma entidade pública, privada, coletiva ou individual, de modo a evitar o repúdio do uso do ciberespaço (ITU,2008; p.6). O ciberespaço pretende-se, assim, uma infraestrutura digital confiável e resiliente (Bayuk et.al,2012; p.1).

Barrinha e Carrapiço explicam que, a importância da cibersegurança é cada vez maior. As principais potências olham para o conceito como "prioridade estratégica" e

como "questão fundamental" e exemplificam que, para a China, "a cibersegurança é uma questão fundamental no que diz respeito à sua segurança, mas também no seu desenvolvimento económico e tecnológico." E acrescentam as palavras do presidente chinês Xi Jinping "sem cibersegurança não há segurança nacional, sem tecnologias de informação não há modernização" (2016; p.245). Para estes autores, a exagerada abrangência do conceito traz como consequência a dificuldade de criação e aplicação de políticas públicas, como também a dificuldade de atribuição de responsabilidades diretas a atores estatais. Consideram também, que a natureza do ciberespaço pode ser preocupante no que toca à questão do privado e do público e consequente lógica de responsabilização política, quer nacional quer internacional, e por isso se tem vindo a tornar uma área prioritária nas Relações Internacionais (Barrinha e Carrapiço,2016; p.256). Hermenegildo (2020; p.5) vai de encontro com a perspetiva da abertura da cibersegurança, o que, para si, representa uma resposta alicerçada em diversos setores, desde o geral ao particular.

Ora, este alargamento da cibersegurança surge na sequência dos enormes desafios e alterações que se têm colocado não apenas ao sistema internacional, mas em particular aos Estados. Na verdade, a redução dos riscos emergentes é um desafio para os Estados devido ao rápido desenvolvimento e permanente evolução e modificação do ciberespaço, que tornam os instrumentos de regulação difíceis de implementar (Nunes, 2012; p.118). Nunes (2012, p.117) sublinha que, a natureza virtual do ciberespaço faz com que este não seja gerido ou propriedade de algum Estado ou Organização. É um espaço comum, sem dono e, por isso, pertence a quem uso faz do mesmo. Garantir a segurança do ciberespaço (cibersegurança) constitui hoje um imperativo nacional, essencial para garantir a soberania e a sobrevivência do país (Nunes, 2012; p.116).

Militão (2014, p. 25), destaca que para além de um conjunto de medidas que procuram garantir o bem-estar do Estado e da sua população, a cibersegurança distingue-se da ciberdefesa, mesmo que ambas comportem ações específicas no ciberespaço. A primeira contém a ação das forças policiais e ainda dos serviços informáticos, e a segunda ocorre, exclusivamente, das forças armadas. Além disso, a cibersegurança contempla os seguintes pilares de ação: cibercrime, hacktivismo, ciberespionagem e ciberterrorismo. Também Barrinha e Carrapiço (2016; p.250), partilham da mesma opinião, considerando que cibersegurança não tem uma definição específica o que, por consequência, "não permite uma classificação específica dos fenómenos que pretende cobrir". Acrescentam que, corresponde a diversos fenómenos tendo estes efeitos políticos, económicos e sociais. Contudo, a sugestão dos mesmos é

seguir a tipologia de Dunn Cavelty citado em Barrinha e Carrapiço, 2016; p.249), "por ser popular entre as estratégias nacionais europeias". Posto isto, Cavelty (2010), decompõe a cibersegurança em três tipos de ameaças: cibercrime, ciberterrorismo e ciberguerra. A distinção contextual destas três ameaças faz-se por: autoria, os meios, intenções e consequências. Assim, Cavelty (citado em Barrinha e Carrapiço, 2016; p.250) assume que o cibercrime faz uso de computadores e redes eletrónicas e está relacionado com lavagem de dinheiro, prostituição infantil, "DDoS, pharming, phishing e botnets". Dado o seu elevado número de vítimas e impacto económico, "não é, portanto, de todo, surpreendente que o cibercrime seja considerado uma ameaça à democracia, aos direitos humanos e ao Estado de direito" (Cavelty citado em Barrinha e Carrapiço, 2016; p.250). Não tem contornos políticos ao contrário do ciberterrorismo.

De uma forma particular, o ciberterrorismo é caracterizado como premeditado e sofre de motivações políticas contra informação com o objetivo de causar violência (Cavelty citado em Barrinha e Carrapiço, 2016; p.251). A intenção do ciberterrorismo é atacar as infraestruturas críticas como "as bases militares, os hospitais, o setor energético, bancário e governamental, mas também os sistemas de informação que liga os hospitais em rede, os serviços de e-Government, o sistema bancário digital e o setor das telecomunicações" (Cavelty citado em Barrinha e Carrapiço,2016; p.251), de modo a afetar o bom funcionamento do Estado e bem-estar das sociedades (Cavelty citado em Barrinha e Carrapiço, 2016; pp.245-262).

Por fim, a ciberguerra "refere-se às ações levadas a cabo por um estado nação para aceder ao computador de outra nação com o intuito de danificar ou causar disrupção". No sentido de completar este conceito proposto por Cavelty, os autores Barrinha e Carrapiço (2016; p.252) mencionam Arquilla e Ronfeldft (1993) referindo que, a ciberguerra é uma "guerra focada no conhecimento sobre quem sabe o quê, quando, onde, porquê e sobre o grau de certeza que uma sociedade ao exército que tem relativamente à informação que dispõe sobre si mesmos e sobre o adversário", portanto, "passa por uma reorientação da doutrina militar para uma perspetiva de informação" (Barrinha e Carrapiço, 2016; p.252).

Podemos, pois, concluir que a cibersegurança é um termo multidisciplinar, abordado nas mais diversas áreas, uma vez que, estamos perante "Crescente digitalização da vida e necessidade de utilização segura de toda a informação que transita na dimensão

virtual" Hermenegildo (2020), porque grande parte de todos os assuntos do quotidiano têm, hoje, o ciberespaço presente. Por sua vez, quanto mais se amplia a conectividade, surgem novos riscos e novas ameaças, resultando em novos desafios. Este aumento de novos desafios representam "uma preocupação com as consequências de incidentes a nível nacional, europeu e até mesmo mundial" (Hermenegildo, 2020; p.1) uma vez que, os riscos e as ameaças são transfronteiriços e daí uma maior complexidade (Hermenegildo, 2020; p.2).

Para o mesmo autor, a cibersegurança, para além da proteção das tecnologias em equipamento, preocupa-se com a criação de políticas e estratégias que sejam capazes de prevenir ataques e lidar com danos. Contudo, dá ainda importância ao processo de recuperação dos sistemas afetados, fazendo da cibersegurança um processo completo desde a prevenção, combate e recuperação de sistemas afetados, na procura de uma resposta eficaz.

Se para Esteves (2015, p.54), a segurança é um termo "hifenizado", para Hermenegildo a cibersegurança é um termo guarda-chuva porque "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 este respeito, cumpre-nos sublinhar que Hermenegildo (2020; p.9), destaca que "fornecimento de água, energia, serviços financeiros, hospitalares, transportes, comunicação, redes e sistemas de informação", são infraestruturas essenciais para o funcionamento da sociedade, onde uma falha da sua segurança no ciberespaço pode significar consequências graves, como visto anteriormente. E dado que, a "ciberdependência é um caminho sem volta" (Hermenegildo, 2020; p.9), procura-se combater as ciberameaças quer por meios técnicos, quer legislativos, de modo a garantir que a sociedade e os seus valores não sejam ameaçados. A autora reflete que foi atribuída uma maior importância ao combate às ameaças híbridas ("ações hostis com o objetivo de destabilizar uma região ou um Estado, elas visam explorar as vulnerabilidades e, muitas vezes, pretendem minar os valores democráticos e liberdades fundamentais") (Hermenegildo, 2020; p.25). Esta priorização leva ao aparecimento do regulamento da cibersegurança 2019 (ARTº2, n2) que corresponde à perspetiva atual da UE, como "todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação e os seus utilizadores e outras pessoas afetadas".

1.3. Enquadramento Legal da Cibersegurança

Em matéria de legislação, o relatório "Cibersegurança em Portugal- Ética e Direito", de 2020[4](CNCS, 2020b), menciona que, devido às recorrentes transformações tecnológicas, há dificuldades, por parte do legislador, em acompanhar essas transformações tão rápidas. Inicialmente, a proteção em termos de legislação, acompanhava o significado do conceito, isto é, legislação ligada à proteção dos meios técnicos, do sistema económico e do Mercado Único. Ainda assim, o relatório data que, foi a partir do Plano de Ação para a Sociedade de Informação, de 1994, que se verificou a maior produção de legislação relacionada com o ciberespaço (CNCS, 2020; p.42). Logo a seguir, em 1995, surge a preocupação com o tratamento de dados pessoais e em 1996, a primeira iniciativa colaborativa dos Estados-Membros da União Europeia, no quadro a OCDE, para a formulação de uma Carta para a Cooperação Internacional na Internet.

Bélaz (2019; p.19), considera que, os primeiros passos foram dados em 1985, com o *Single Market* (Mercado Único) onde as TIC (Tecnologias da Informação e Comunicação), graças à livre circulação de bens, serviços e pessoas, foram vistas como oportunidade de desenvolvimento social e económico.

Em 2001, com o objetivo de "alargar a conectividade à Internet na Europa, abrir o conjunto das redes de comunicação à concorrência e promover a utilização da Internet colocando a tónica na formação e proteção dos consumidores", é lançado o comunicado eEurope 2002, que principalmente visava "uma Internet mais barata, mais rápida e segura; investir nas pessoas e nas qualificações e estimular a utilização da Internet" (Conselho Europeu, 2001).

Após o 11 de setembro, surge de imediato uma tentativa da União Europeia, de combater o terrorismo nas suas diversas formas. Neste seguimento, é apresentada pela Comissão a 19 de Setembro de 2001, a Proposta de decisão-quadro do Conselho relativa à luta contra o terrorismo, onde considera que:

> Cada Estado-Membro tomará as medidas necessárias para assegurar que as seguintes infrações, definidas em conformidade com o seu direito nacional, cometidas intencionalmente por um indivíduo ou por um grupo contra um ou mais países, as suas instituições ou a sua população, com o objectivo de os intimidar e afectar gravemente ou

[4]CNCS. (2020b). Ética & Direito. Observatório de Cibersegurança. 1-138. Retirado de https://www.cncs.gov.pt/docs/relatorio-eticadireito2020-observatoriociberseguranca-cncs.pdf. Acesso em março 2021.

> destruir as suas estruturas políticas, económicas ou sociais, sejam puníveis como infracções terroristas: a) O homicídio; b) As ofensas corporais; c) O rapto ou a tomada de reféns; d) A extorsão; e) O roubo ou o furto; f) A ocupação ilícita ou os danos causados aos edifícios públicos ou do governo, aos meios de transporte públicos, às infra-estruturas e locais públicos e outra propriedade; g) O fabrico, posse, aquisição, transporte ou fornecimento de armas ou explosivos; h) A libertação de substâncias contaminadoras ou a provocação de incêndios, explosões ou inundações, pondo em perigo pessoas, bens, animais ou o ambiente; i) A perturbação ou a interrupção da distribuição de água, energia ou qualquer outro recurso fundamental; j) Os ataques através da interferência num sistema de informação; k) A ameaça de cometer qualquer uma das infrações enumeradas supra; l) Dirigir um grupo terrorista; m) Promover, apoiar ou participar num grupo terrorista (Comissão Europeia, 2001).

A 23 de novembro do mesmo ano, realizou-se a Convenção de Budapeste, sobre o cibercrime

> Para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a deteção, a investigação e o procedimento criminal relativamente às referidas infrações, tanto a nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável (Conselho Europeu, 2014, p. 1).

O período compreendido de 2002 a 2006 assume, para Beláz, "o papel de facilitador", uma vez que, "os Estados-Membros, em vez de serem instruídos a fazer algo, nos novos documentos foram encorajados ou convidados a tomar certas medidas", o que se evidenciou na Estratégia para uma Sociedade da Informação Segura, de 2006 (Beláz, 2019; p.20).

Em 2004, nasce a ENISA (Agência Europeia para a Segurança das Redes e da Informação), com o propósito de

> ser um centro especializado a nível europeu, competente para orientar, dar pareceres e prestar assistência às instituições da União e aos Estados Membros, e para cooperar com a comunidade empresarial, a fim de garantir um nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas (CNCS, 2020; p.42).

O seu sucesso é valorizado com a renovação sucessiva de mandatos e o reforço de atribuições da agência (CNCS, 2020; p.42).

Os ataques cibernéticos à Estónia, em 2007, influenciaram a União Europeia, nomeadamente a que esta repensasse a prioridade que atribuía ao ciberespaço. Posto isto, como Fernandes afirma p. 5), a cibersegurança ganha mais autonomia iniciando o "despertar da política de cibersegurança" (citado em Hermengildo,2020; p.21). E destaca o seu papel importante para a recuperação económica da crise financeira, de 2008.

Em 2009, entraria em vigor o Tratado de Lisboa que reforça o status político da UE e evidencia que a cibercriminalidade está ao abrigo da cooperação judiciária, o que impulsionou à criação da Europol EC3.

No ano de 2013, foi proposta a Estratégia da União Europeia para a Cibersegurança de: um ciberespaço aberto, seguro e protegido[5] (Parlamento Europeu, 2013). Esta proposta, passou por medidas de sensibilização e educação, pela criação de equipas de resposta (CERT), assim como, pelo desenvolvimento de um mercado interno de produtos e serviços relacionados com a cibersegurança e pela promoção de investimentos na sua investigação, desenvolvimento e inovação (Parlamento Europeu, 2013; p.4). A acrescentar ao apelo da UE para que os seus EM adotassem estratégias de cibersegurança nacionais que abordem a parte técnica, de recursos humanos e financeiros, a mesma revelava que apenas com a cooperação dos Estados-Membros se atingirá um elevado nível de segurança em toda a União, para a "(…)manutenção de serviços que são essenciais para o bom funcionamento da sociedade e da economia, mas também para salvaguardar a integridade física dos cidadãos através do reforço da eficiência, da eficácia e da segurança do funcionamento das infraestruturas críticas(…)" (Parlamento Europeu, 2013; p.4). Salienta que, qualquer política da União, relativa à cibersegurança, deve assegurar o cumprimento da proteção das liberdades e do respeito pelos direitos fundamentais. O mesmo documento apela à prestação de cuidados a nível técnico, de informação jurídica, e à prudência na ótica do utilizador, não negligenciando a necessidade da cooperação a nível operacional entre autoridades públicas e o setor privado, para que, no intercâmbio de conhecimentos, se desenvolva um sentido de confiança e seja mais eficaz no combate às ciberameaças (Parlamento Europeu, 2013, p. 6). Esta primeira Estratégia que menciona "cibersegurança" no seu título, sublinhou, segundo o Relatório Ética e Direito, "as responsabilidades partilhadas por Governos, indústria e cidadãos e mapeou as ações necessárias por parte das instituições europeias, dos Estados e da indústria para "tornar o ambiente em linha na UE o mais seguro do

[5] Parlamento Europeu. (2013). Estratégia da UE para a cibersegurança : um ciberespaço aberto , seguro e protegido. Retirado de: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52013JC0001. Acesso em março de 2021.

mundo", incluindo medidas legislativas em matéria de cibercriminalidade (sobretudo por referência à Convenção de Budapeste) e de segurança das redes e da informação". Desta Estratégia de Cibersegurança, resulta a Diretiva SRI e o Regulamento (UE) 2019/881 sobre a cibersegurança da UE, aprovado em 2016 e 2019 respetivamente.

Em 2016, a Diretiva SRI (segurança das redes e da informação), considerou que, as capacidades existentes não são suficientes para garantir o nível de segurança pretendido, devido à diferente preparação que os Estados-Membros revelam. Assim, atenta à necessidade da prestação de requisitos mínimos comuns que os operadores de serviços essenciais e os prestadores de serviços digitais devem respeitar, não os impedindo de prestar um maior nível de exigência, se assim o pretenderem (Parlamento Europeu & Conselho, 2016, p. 1). A Diretiva SRI entende como operador de serviços essenciais, serviços relacionados com: energia, transportes, setor bancário, infraestruturas do mercado financeiro, setor da saúde, fornecimento e distribuição de água potável e infraestruturas digitais. Por prestadores de serviços digitais entende-se: mercados em linha, motores de pesquisa em linha e serviços de computação em nuvem. A estes, compete-lhes garantir a segurança das redes e dos sistemas de informação que utilizam.

À luz da Estratégia de Cibersegurança sublinha-se, novamente, o elevado grau de pertinência da cooperação dos Estados-Membros, quer entre si, quer com as instituições da União relevantes ao tema, bem como a adoção de uma equipa de resposta. Se a Estratégia de Cibersegurança de 2013 apelava aos Estados-Membros para a criação de Equipas de Resposta a Emergências Informáticas (CERT), a Diretiva SRI veio fazer um "upgrade", invocando para a criação de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT). Apesar de serem tecnicamente distintas, o objetivo mantém-se o mesmo: resposta a incidentes no ciberespaço.

A Estratégia de Cibersegurança de 2013 salienta o valor da educação do cidadão quanto aos incidentes que possam ocorrer a nível particular ou empresarial, tendo em conta o aumento dos serviços prestados no ciberespaço e o aumento de serviços transfronteiriços prestados por parte das empresas. Por isso torna-se importante, "promover e desenvolver uma cultura de gestão de riscos que passe pela avaliação dos riscos e pela aplicação de medidas de segurança adequadas aos riscos enfrentados, estabelecendo para tal requisitos regulamentares adequados e adotando práticas setoriais de cárter voluntário"(Parlamento Europeu & Conselho, 2016, p. 7).

Esta Diretiva SRI foi o primeiro ato legislativo no domínio de cibersegurança e um ponto de destaque da integração direta da cibersegurança nas políticas da União Europeia.

Hermenegildo, (2020; p.34) resume que, no seu essencial a Diretiva é um mecanismo de resposta completo porque

> 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 serem cumpridos), na preparação (origem) para a ocorrência de incidentes graves nas infraestruturas críticas (2020; p.34).

Para o autor, a partir de 2016, a União Europeia mudou a sua postura para um papel de liderança, onde atribuiu maior importância à cibersegurança (e ao combate às ameaças híbridas), que sai de um patamar de subcategoria e alcança um patamar de priorização.

Em 2017, é proposto a criação de um Quadro de Certificação de Cibersegurança, concretizado com o Regulamento (EU) 2019/881. Para além desta proposta, foi publicada a Estratégia "Resiliência, dissuasão e defesa: reforçar a cibersegurança na EU", uma atualização da Estratégia de 2013. Esta Estratégia surgiu da incapacidade de proteger os dispositivos controladores de redes de energia, de redes de transportes, de fábricas, de finanças, de hospitais e restantes infraestruturas prestadoras de cuidados de saúde, onde as consequências poderiam derivar quebras de confiança dos consumidores nas tecnologias emergentes (Parlamento Europeu e Conselho da União Europeia, 2019, p. 3). De acordo com a presente Estratégia, ataques de natureza política tendem a agravar a quebra de confiança (Parlamento Europeu e Conselho da União Europeia, 2019, p.3). Posto isto, são providenciadas medidas baseadas nas abordagens do Mercado Único Digital, com a finalidade de melhorar o acesso a bens e serviços digitais, potencializando o crescimento da economia digital; da Estratégia Global; da Agenda Europeia para a Segurança, onde apostou na melhoria da aplicação da lei e na renovação de políticas; do Quadro Comum em matéria de luta contra ameaças híbridas e na comunicação "Lançar o Fundo Europeu de Defesa". Ainda parte, inclui um mandato permanente para a ENISA. Apoia a criação de um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança.

Nesta Estratégia, assume-se a falta de capacidade da União Europeia no que respeita à cripto-análise, quer de produtos quer de serviços, no âmbito do Mercado Único

Digital, pelo que, reforçar esta capacidade é melhorar a eficácia da cibersegurança (Comissão Europeia, 2017, p. 11). Esta melhoria conta com o reforço da educação em matéria de cibersegurança, assim como da ciber-higiene, tal como refere o documento (Comissão Europeia, 2017, p. 12). A educação, não só se refere a profissionais de informática, mas também em outras áreas profissionais. Acresce que, também deve existir um esforço de sensibilização do cibercrime e da cibersegurança em todos os escalões de ensino. Deste modo, o cidadão deve obter as competências necessárias para identificar a ameaça e fazer uso das ferramentas competentes para se proteger, considerando que "(...)cerca de 95 % dos incidentes são alegadamente possibilitados por «algum tipo de erro humano, intencional ou não»"(Comissão Europeia, 2017, p. 12). Na concordância de que a cibersegurança é essencial quer para os cidadãos, quer para os negócios, Barrinha e Carrapiço explicam que o mesmo se aplica a empresas e organizações, fazendo uso da sua atualização, conscientes da evolução do cenário de risco (Carrapiço & Barrinha, 2018, p. 1).

A presente proposta assume que "enquanto os autores de ciberataques, estatais ou não estatais, nada tiverem a recear, além do insucesso, terão pouco incentivo para pararem de tentar" (Comissão Europeia, 2017, p. 2) e acrescenta que só com o aumento da deteção e com a aplicação de sanções se consegue combater o aumento de ciberataques. Na medida de aplicar uma resposta adequada, entende-se que deve ser reforçada a aplicação da lei, com foco na deteção, identificação e ação penal contra os cibercriminosos, ou seja, com uma aplicação coerciva da lei (Comissão Europeia, 2017, p. 6). Por último, e ainda com a intenção de oferecer uma melhor resposta ao combate ao cibercrime, salientou-se que deve continuar a existir e a aprofundar-se a cooperação entre os setores público e privado, tal como se aprofundou a cooperação entre a União Europeia com a NATO, em matéria de investigação, inovação, desenvolvimento técnico e partilha de informação em cibersegurança, ameaças híbridas e defesa (Comissão Europeia, 2017, p. 9).

O ano de 2018, caracterizou-se pela aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD). Este regulamento permitiu aos cidadãos da UE, controlarem os seus dados pessoais. Quanto aos direitos dos cidadãos, também introduziu o direito à portabilidade dos dados entre pessoas e os prestadores de serviços e de saber se os dados pessoais foram alvo de pirataria informática, devendo a empresa prestadora do serviço informar o utilizador lesado (Parlamento Europeu, 2016, p. 13). Acrescenta-se a

clarificação do direito ao apagamento de dados, sempre que o utilizador considerar não haver razão legítima para a conservação dos mesmos (Parlamento Europeu, 2016, p. 7). No que concerne às empresas, este regulamente permitiu um mecanismo de balcão único e um conjunto único de regras à escala da União Europeia, permitindo a poupança de, em estimativa, 2,3 mil milhões de euros por ano e facilitando a comunicação entre as mesmas. As empresas externas à União Europeia devem aplicar as mesmas regras quando comercializam no interior da EU. Além disso, o RGPD permite salvaguardar a privacidade e a cifragem com campos de identificação substituídos por identificadores artificiais ou codificados de forma a serem lidos apenas por quem tem autorização, respetivamente (Parlamento Europeu, 2016, p. 16).

No ano seguinte, em 2019, é publicado o Regulamento (UE) 2019/881 sobre a Cibersegurança da UE, que resulta da Estratégia de Cibersegurança de 2013. O presente regulamento está diretamente relacionado com "os objetivos, as atribuições e os aspetos organizativos da ENISA" (Parlamento Europeu e Conselho da União Europeia, 2019, p. 9) e com

> Um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível de vida adequado de cibersegurança para os produtos, os serviços e os processos TIC na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União (Parlamento Europeu e Conselho da União Europeia, 2019, p. 32).

Quanto à ENISA, que é referida como "ponto de referência em matéria de aconselhamento e conhecimentos especializados e como facilitadora da cooperação e do desenvolvimento de capacidades, assim como no âmbito da nova política de cibersegurança da União(...)"(Parlamento Europeu e Conselho da União Europeia, 2019, p. 18), foi reformulada para continuar a contribuir eficazmente, mas com mais capacidade de resposta e mais rápido. Refere-se o aumento de cooperação operacional, com o setor público e privado; aumento das capacidades técnicas e humanas e também os seus conhecimentos especializados e as suas capacidades. A esta, compete-lhe promover a aplicação do regime jurídico, nomeadamente da Diretiva SRI, referida anteriormente. Presta assistência a Estados-Membros e a organizações. Resumidamente, o novo Regulamento define as atribuições da ENISA, a sua estrutura organizacional, as regras de funcionamento, o regime orçamental, o quadro pessoal e as formas de desenvolvimento e acompanhamento dos trabalhos da agência (Hermenegildo 2020, p. 36).

Quanto à certificação da cibersegurança, esta desencadeou o crescimento da confiança e segurança dos produtos, serviços e processos de TIC, pelo que ao União relata:

> "O mercado único digital e, em especial, a economia dos dados e a IdC, apenas pode prosperar se houver uma confiança pública generalizada em que esses produtos, serviços e processos forneçam um determinado nível de cibersegurança. Os automóveis conectados e automatizados, os dispositivos médicos eletrónicos, os sistemas de controlo da automação industrial ou as redes inteligentes são apenas alguns exemplos de setores nos quais a certificação é já amplamente utilizada ou suscetível de o vir a ser no futuro próximo" (Parlamento Europeu e Conselho da União Europeia, 2019, p. 24).

Assim sendo, a abordagem para a certificação deve ser comum, com a adoção dos mesmos requisitos em todos os Estados-Membros. Estabeleceu o procedimento para a criação de sistemas de certificação, com a abrangência de produtos, serviços e sistemas, que adaptem o nível de garantia à sua utilização. Reduz custos às empresas, uma vez que, deixam de ter de passar por vários processos de certificação. O quadro constitui um passo importante para o desenvolvimento de capacidades de sinalização e de reação a nível da UE e dos Estados-Membros.

A cronologia da União Europeia para a cibersegurança, complementa que foi estabelecido um quadro que permite sancionar pessoas ou entidades responsáveis por tentativa ou ataque cibernéticos, pelo suporte financeiro, técnico ou material, ou que de certa forma mostram o seu envolvimento, constituindo uma ameaça externa para a União Europeia, os seus Estados-Membros ou países terceiros ou organizações internacionais necessárias para atingir os objetivos da PESC (Conselho da União Europeia & Conselho Europeu, 2021). Por último, o Conselho adotou conclusões sobre o 5G e o seu impacto económico, sendo que este tipo de rede fará parte da manutenção de funções sociais e económicas vitais (Conselho da União Europeia & Conselho Europeu, 2021).

Mais recentemente, em 2020, foi apresentada a proposta para a Estratégia de cibersegurança da União Europeia para a Década Digital (Comissão Europeia; 2020c). Neste documento , foi proposto um regulamento que iniciasse o projeto de criação do Centro Europeu de Competência para a Cibersegurança de Coordenação, com destaque para a transformação digital no combate à pandemia e o seu papel na recuperação após Covid-19. A União Europeia pretende com a criação deste Centro melhorar a capacidade de resposta e salvaguardar os pontos chaves "integridade, segurança e resiliência da infraestrutura digital, redes e serviços de comunicação" (Conselho da União Europeia &

Conselho Europeu, 2021). No último ano de 2021 foram impostas as primeiras sanções contra ciberataques, proibindo os cibercriminosos de viajar, com a prática do congelamento de bens, e proibição de receberem fundos de pessoas ou entidades da EU ou outras incluídas[6]. Foi ainda estabelecido um acordo provisório sobre a criação Centro Europeu de Competências em Cibersegurança (competências industriais, tecnológicas e de investigação em cibersegurança) e de uma Rede de Centros Nacionais de Coordenação, que em conjunto estabelecerão segurança e autonomia da EU (Conselho da União Europeia & Conselho Europeu, 2021).

Portugal tem acompanhado as diretrizes da União Europeia no que respeita a políticas e desenvolvimentos legislativos no âmbito da cibersegurança. De acordo com o relatório de ética e direito, a cibersegurança, em Portugal, é apoiada pelo Gabinete Cibercrime do Ministério Público, pela Polícia Judiciária, pela Comissão Nacional de Proteção de Dados e pelo Centro Nacional de Cibersegurança (formado em 2014) (CNCS, 2020b, p. 43). Mas, seria apenas em 2015, que Portugal adotaria a primeira estratégia nacional de cibersegurança[7](Presidência do Conselho de Ministros, 2015), com o objetivo de manter a mesma linha de trabalho da União Europeia, cooperando como Estado-Membro e com vista para um maior auxílio em gestão de crises. Sob o princípio da subsidiariedade, da complementaridade, cooperação, proporcionalidade e sensibilização prontificou-se a "promover uma utilização consciente, livre, segura e eficiente do ciberespaço", a "proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos"), pretendia "fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais" e por fim, "afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação" (Andrade et al., 2020, p. 44). Mais especificamente, o objetivo passava por reforçar a estrutura de segurança do ciberespaço, assim como protegê-lo e às suas infraestruturas; combater o cibercrime; educar, sensibilizar e prevenir e por fim, investigar, cooperar e apoiar o desenvolvimento do ciberespaço. Neste sentido, Portugal reuniu esforços para aplicar as medidas em linha com a União Europeia.

[6]Comissão Europeia. (2020c). Estratégia de cibersegurança da UE para a década digital. 2014, 1–32. Retirado de: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0605. Acesso em maio de 2021.

[7] Presidência do Conselho de Ministros. (2015). Estratégia Nacional de Segurança do Ciberespaço. Diário Da República, 3738–3742. Retirado de: www.dre.pt. Acedido em: maio de 2021.

Figura 1: Cronologia legal da cibersegurança na União Europeia (Parte I)

Figura 2: Cronologia legal da cibersegurança na União Europeia (Parte II)

Fonte: Cronologia adaptada de Ética e Direito (CNCS, 2020a, pp. 42, 43).

2ºCapítulo- A pandemia Covid19 e a cibersegurança

A pandemia Covid-19 veio alterar o contexto internacional. De modo mais ou menos intenso, acabou por afetar todos os Estados e cidadãos. Não só ao nível da saúde, mas pelas mudanças que provocou na vida em sociedade. A mais significativa pode assumir-se que foi a digitalização da vida pública e privada. Se por um lado se observou o distanciamento físico social, por outro, Santos e Marques (2020; p.3) consideram que a tecnologia foi utilizada como "instrumento de mitigação" deste distanciamento físico. Além do maior uso da tecnologia para interações sociais, teletrabalho, escola, Lallie et al (2020; p.2) acrescenta que, as compras, os negócios, a indústria e o crime, também reforçaram a sua presença no mundo online que, tal como Nunes (2020; p.7) indica, a sociedade passou a estar mais interligada do que nunca.

Ora, o tipo de combate à pandemia ficou ao encargo de cada Estado, contudo, foram obrigados a mudar o panorama da vida em sociedade e a implementar medidas para que fosse cumprido o distanciamento social e, para que se evitasse a propagação do vírus. Para que o distanciamento social fosse cumprido, muitos dos Estados optaram por períodos de confinamento, que significou, segundo a KPMG (2020; p.1), uma rápida transição da vida presencial para online, à exceção dos serviços mínimos e de urgência que, apesar do seu trabalho continuasse presencial, sofreram alterações e adaptações.
Esta transição da vida remota para online, levou a KPMG (2020; p.1) a considerar que cibersegurança das organizações poderia estar comprometida. Isto porque, a transição efetuada foi de caráter instantâneo, não sobrando tempo para definir estratégias de segurança. Ceballos (2020; p.1) é da opinião que esta transição seria para demorar anos, de maneira a ser realizada com mínimo de fragilidades possível. Tal como Castro (2021), em declarações ao Jornal Económico, que de encontro a esta opinião pormenoriza que o teletrabalho estava pensado só para daqui a 10 anos, pelo que não foi possível garantir a cibersegurança nesta transição (J. V. Rodrigues, 2021).

É consensual entre vários autores que a transformação digital se iniciou em março de 2020, data que marca também o aumento de ciberincidentes, quer pela rápida e desordenada transição (Gouveia,2020; p.7), quer pelo aumento de dispositivos ligados à rede.

Ainda que em teletrabalho, as empresas puderam continuar a trabalhar, no entanto, autores como Ceballos (2020; p.135) realçam que as empresas facilitaram em pontos essenciais à sua cibersegurança, colocando as informações confidenciais mais expostas a ataques. Neste sentido, a Delloite mencionou a utilização do computador pessoal para fins laborais, ou vice-versa. Isto acontece porque com a utilização do computador laboral para fins privados, pode haver o facilitismo de aceder a sites menos seguros de interesse pessoal, e como consequência infetar o computador com vírus. No uso do computador pessoal para fins laborais, torna-se mais fácil de aceder e obter informações confidenciais pois, normalmente, os computadores pessoais encontram-se desprotegidos face a ataques maliciosos. O uso de uma rede gratuita/pública é para o cibercriminosos uma porta de entrada pelo fácil acesso que proporciona ao dispositivo que faz uso da rede, pois é uma rede menos protegida e torna o seu uso um facilitismo por parte das empresas em não garantir maior proteção de rede. Ainda a "imaturidade tecnológica" que Castro (2021) explicou a J. V. Rodrigues (2021), pela falta de investimento em dispositivos tecnológicos devidamente protegidos e constantes atualizações de proteção e de formação do utilizador.

O risco ao nível da cibersegurança e da pandemia também se fez sentir pelo novo paradigma espaço-tempo que a FAL (2020) explica ser mais breve devido à rapidez tecnológica. Isto é, o confinamento e o aumento do uso de tecnologias espoletaram novos ciberataques mais sofisticados, que adaptam novos meios e fazem uso de novas estratégias para explorar vulnerabilidades que, consequentemente, proporciona cada vez novos riscos num curto espaço de tempo. No seguimento desta explicação, Castro (2021) denota que, o tempo entre adoção do teletrabalho e a adaptação da sociedade e empresas ao digital com segurança foi demasiado, o que permitiu tempo para os cibercriminosos realizarem ataques com sucesso. Assim como, a adaptação ao ciberespaço com segurança por "tentativa e erro" (Ceballos,2021), que deixa, novamente, abertura para que ataques cibernéticos ocorram. O que, na ótica de Gouveia (2020; p.7) representa uma situação desafiante e de constante monitorização. A Delloite relembra ainda que o atraso na deteção da atividade maliciosa torna a sua resolução mais complexa.

Cumpre ainda sublinhar que o stress financeiro dos funcionários e as incertezas causadas pela pandemia representam fatores de vulnerabilidade que os cibercriminosos poderiam também aproveitar. Muitos negócios foram obrigados a despedir funcionários ou a colocá-los em lay-off, como aconteceu em Portugal. Esta situação de vulnerabilidade e incerteza económica é, por isso, um risco como ameaça interna, sendo que, é explorada por cibercriminosos que procuram roubar dados corporativos importantes (Kpmg, 2020,

p. 1). A "confidencialidade em casa" é, para a KPMG (2020; p.2), de extrema importância, pois determinadas informações não devem ser partilhadas mas podem ser ouvidas ou vistas por outros membros da casa que não estão cientes da confidencialidade das informações.

O medo, a ansiedade, a pressão de tempo e de trabalho e o cansaço são fatores de vulnerabilidade que a pandemia intensificou. Essencialmente, porque a solução para algumas empresas, passou por despedimentos ou pela colocação dos funcionários em regime de lay-off. Como publicado no boletim de maio de 2021 do Observatório de Cibersegurança, do Centro Nacional de Cibersegurança (CNCS), entre fevereiro e março de 2020, o número de incidentes registados pelo CERT.PT aumentou 84% e, em comparação com o número de incidentes registados em março de 2019, o aumento foi de 176%. Os meses de abril e maio confirmaram esta tendência, com aumentos de 142% e 134%, respetivamente, relativamente ao período homólogo de 2019 (CNCS, 2020a).[8]

Com isto, a redução de salários, a instabilidade financeira e o medo do despedimento, representaram uma vulnerabilidade de tal forma para a sociedade, que o cibercrime foi, para alguns, uma oportunidade de sobrevivência, uma vez que é uma atividade lucrativa e com a possibilidade de ser realizada a partir de qualquer lugar (Delloite, 2020). Este "terreno fértil para criminosos" (Geraldes, 2020, p. 9) também resultou num aumento no número e espectro de cibercrimes, com estretégias de venda de bens com alta procura como medicamentos e testes de coronavírus, segundo Lallie et al (2020; p.1). Pelo que, Santos e Marques (2020; p.3) acreditam na igual importância quer "do investimento nas pessoas e na tecnologia" quer na "rigorosa avaliação de risco", para evitar situações de risco. Sob a mesma perspetiva, a EY (2020) considera que empresas também têm no seu papel no que se refere à cibersegurança e à pandemia pois, para além de treinar os seus funcionários ao nível da cibersegurança, as empresas podem identificar, avaliar e responder com eficácia aos riscos relacionados com a pandemia. Deste modo, devem concentrar-se nos "aspetos operacionais, tecnológicos, de segurança cibernéticos, financeiros, de força de trabalho e fiscais para fornecer recomendações e estabelecer um plano para lidar com os riscos e impactos".

[8] CNCS. (2020a). Cibersegurança em Portugal -Riscos e conflitos. 1–104. Retirado de: https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf. Acedido em julho de 2021.

Todavia, Castro (in J. V. Rodrigues, 2021) critica a atitude das empresas face à cibersegurança. Não considera que a "ignorância" das empresas face à cibersegurança seja uma justificação nos dias de hoje, mas uma opção, dada a importância revelada aos longo dos anos. Esta visão é partilhada por Ceballos (2021; p.1), à qual acrescenta os exemplos da Estónia em 2007, notPeteya e WannaCry em 2017. O autor considera que os exemplos evidenciaram os riscos do ciberespaço, as falhas de segurança e as vulnerabilidades dos Estados e empresas, o que não deixa margem para desconhecer a importância da cibersegurança e daí não se aceitar a "ignorância" como justificação. Quer para Castro (2021), quer para Ceballos (2021, p. 1) o aumento de ciberataques é fruto da impreparação tecnológica, pois, na mesma medida que a empresa não avalia o seu próprio risco de segurança nem se prepara tecnologicamente, os seus trabalhadores também não estão protegidos pela empresa e, consequentemente, vulneráveis às consequências do teletrabalho.

No que concerne ao aumento dos ataques informáticos, Barrinha e Carrapiço (2020; p.2), mencionam que "em abril de 2020, o FBI deu conta de um crescimento de 300% no número de queixas relativas a ataques informáticos", sendo hospitais e instituições de investigação médica os alvos preferenciais, por conta do Covid19. A Forbes Staff (2020) vai mais longe e, através de uma comunicação da ONU, escreve que "O cibercrime disparou durante a pandemia do coronavírus, com um aumento de 600% em número de correios eletrónicos maliciosos e com repetidos ataques contra organizações sanitárias e de investigação médica(...)" e acresce a informação de que, em estimativa, há um ataque informático a cada 39 segundos, no mundo. Esses ataques explicam-se pelo crescimento do uso das tecnologias como exemplificam Marques e Santos (2020, p. 3) "crescimento superior a 40% dos volumes de tráfego de voz e dados em Portugal. Aumento de 90% do comércio eletrónico em Itália o um acréscimo de cerca de 75% da utilização das redes sociais em Espanha".

Na generalidade dos ataques e do aumento destes por tipo ou taxionomia de acordo com o boletim de segurança 2020-2021 que a Kaspersky elaborou em relação às estatísticas da União Europeia, "70% dos computadores dos utilizadores da Internet na União Europeia sofreram pelo menos um ataque do tipo malware"(kaspersky, 2021a). E adicionam "As tentativas de infeção por malware projetado para roubar dinheiro por meio de acesso online a contas bancárias foram registadas nos dispositivos de 79.315 usuários"(kaspersky, 2021a), "56.877 usuários únicos na UE foram atacados por ransomware" e "132.656 usuários únicos na UE foram atacados por miners"(kaspersky, 2021a). Ordenam também os 10 principais países da União Europeia onde os usuários

enfrentam o maior risco de infeção local de malware, sendo eles: Grécia, Bulgária, Letónia, Estónia, Hungria, Lituânia, Portugal, Chipre, Itália e Espanha. Por ataques de phishing, Portugal ocupa o primeiro lugar seguindo-se da França, Bélgica, Grécia, Hungria, Itália, Eslováquia, Espanha, Polónia e Letónia (kaspersky, 2021a)[9].

De acordo com o Global Cybersecurity Index de 2020, com uma avaliação a partir de medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidades e medidas cooperativas, o país da União Europeia que se encontrava com melhor preparação para responder às ciberameaças, reflexo do covid-19, é a Estónia. Portugal ocupa o 8º lugar e em último, sendo o país menos preparado, está a Bulgária (International Telecommunication Union, 2020). Contudo, Portugal é o país de toda a União Europeia mais atacado por phishing e, à exceção das ameaças à Internet das Coisas, consta no top 10 de todas as ameaças elaboradas no Boletim estatístico de segurança da União Europeia de 2020-2021 (kaspersky, 2021a).

No top de ameaças em 2017/2018, já estava o malware, seguido de ataques na web, ataques de aplicações na web e o phishing, que continuaram a ocupar os primeiros 4 lugares, pela ordem referida. Assim como a ameaça interna, manipulação física ou dano, perda de identidade e ciberespionagem que continuaram no mesmo lugar face a 2017. Contudo, houve um aumento de negação de serviço, botnets, fuga de informação e kits de de 2017 para 2018. Surgiu ainda como ameaça a Crytojacking (ENISA, 2018; p.9)[10].

Em 2018, a ENISA faz um balanço das ameaças desse mesmo ano, pelo que aqui importa mencionar que "a Europol comunicou que 73% das violações foram cometidas por agentes externos mal intencionados e 50% atribuídos a grupos de crime organizado" (ENISA, 2018, p. 65). Além disso, a indústria acredita que atores patrocinados pelo Estado estiveram envolvidos em 12% das violações de dados" (ENISA, 2018, p. 65); quanto aos media "está no topo do número de registos violados (56%) devido aos dados de clientes de alto perfil comprometidos do Facebook e Twitter, envolvendo 2,2 bilhões e 336 milhões, respetivamente" (ENISA, 2018, p. 65) e em questões da área da saúde que

[9] kaspersky. (2021a). Kaspersky Security Bulletin 2020-2021. EU statistics. Retirado de: https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/. Acedido em agosto 2021.

[10] ENISA. (2018). Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends. In European Union Agency For Network and Information Security. https://doi.org/10.2824/622757. Retirado de: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. Acedido em agosto de 2021.

"continua a liderar em número de incidentes (27%) (...)" (ENISA, 2018, p. 65). No sentido de familiarizar a sociedade das maiores ciberameaças a nível da União Europeia, a ENISA apresentou as ameaças, as quais se podem observar nas tabelas 1 e 2.

Tabela 1: Principais ameaças 2017-2018 (ENISA,2018; p.9)

Principais ameaças 2017	Tendências 2017	Principais ameaças 2018	Tendências 2018	Mudança na classificação
1.Malware	–––	1.Malware	–––	–––
2.Ataques na web	↗	2.Ataques na web	↗	–––
3.Ataques de aplicações da web	↗	3.Ataques de aplicações da web	–––	–––
4.Phishing	↗	4.Phishing	↗	–––
5.Spam	↗	5.Negação de serviço	↗	↗
6.Negação de serviço	↗	6.Spam	–––	↙
7.Ransomware	↗	7.Botnets	↗	↗
8.Botnets	↗	8.Violação de dados	↗	↗
9.Ameaça interna	–––	9.Ameaça interna	↙	–––
10.Manipulação física, dano, roubo, perda	–––	10.Manipulação física, dano, roubo, perda	–––	–––
11.Manipulação de dados	↗	11.Fuga de informação	↗	↗
12.Roubo de identidade	↗	12.Roubo de identidade	↗	–––
13.Fuga de informação	↗	13.Cryptojacking	↗	NEW
14.Kits de exploração	↙	14.Ransomware	↙	↙
15.Cyber espionagem	↗	15.Cyber espionagem	↙	–––
Legenda:	Tendências: ↙ Declíneo, ––– Estável, ↗ Subida Classificação: ↗ Subir, ––– Mantém, ↙ Descer			

Fonte: Adaptado de Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends (ENISA, 2018; p.9).

No que toca ao top de ameaças 2019/2020, o malware continou a ocupar o primeiro lugar, assim como, os ataques na web e o phishing em que a sua tendência continua a ser em aumentar. A acompanhar este aumento, mas em outros patamares deste top15, está o spam e o roubo de identidade, ransomware e ciberespionagem. Em

declínio estão a negação de serviço, aplicações da web, botnets, manipulação física/ danos, fuga de informações e cryptojacking, que foi ocupar o último lugar da tabela.

Acerca do phishing e da sua relação com a pandemia, a Kaspersky (2020) tem a acrescentar que o alvo preferido do phishing passou a ser as páginas de venda online (comércio online) como isca para se passar por marcas, enganando assim funcionários e clientes, onde atingiram valores de 7,57% de ataques em 2019 e quase triplicaram em 2020 com valores de 18,12%. Junto a este crime está o ataque contra usuários PayPal que aumentaram de 26,8% em 2019 para 28,7%, em 2020. Daniela Santos (2020; p.4) evidencia o phishing como um simulador de serviços digitais "com maior consumo e fidelização, como os serviços de homebanking, conteúdos digitais em streaming e lojas online" e soma o facto de explorarem "os receios das pessoas com o intuito de induzir certos comportamentos como, por exemplo, instalar uma aplicação que prometia ver o número de casos e a sua evolução no concelho de residência ou de trabalho, quando na realidade era uma APP maliciosa, COVID-19 Tracker, que instalava ransomware nos telemóveis" (Santos, 2020; p.4).

As ameaças à cibersegurança que a pandemia Covid-19 proporcionou bem como as consequências durante 2020 e 2021 ainda estão a ser alvo de estudo pormenorizado, pelo que, as conclusões e os dados que as organizações alcançam são ainda poucos e insuficientemente detalhados. A ENISA (2021; p.3) concentra alguns pontos essenciais, divididos em grupos, como: 50% dos ataques foram pertencentes ao grupo de ameaça persistente avançada, "42% dos ataques analisados ainda não foram atribuídos a um determinado grupo" e "em 62% dos ataques a clientes tiraram partido da confiança no fornecedor". O malware como mostrado acima, foi o maior tipo de ataque cibernético, aparecendo em 65% dos casos.

Tabela 2: Principais ameaças 2019-2020 (ENISA, 2020; P.5)

Principais ameaças 2019-2020	**Tendências avaliadas**	**Mudança no ranking**
1.Malware	–––	–––
2.Ataques na web	–––	↗
3.Phishing	↗	↗
4.Ataques de aplicações na web	–––	↙
5.Spam	↙	↗

6.Negação de serviço	↙	↙
7.Roubo de identidade	↗	↗
8.Violação de dados	---	---
9.Ameaça interna	↗	---
10.Botnets	↙	↙
11. Manipulação física, dano, roubo, perda	---	↙
12.Fuga de informação	↗	↙
13.Ransomware	↗	↗
14.Cyberespionagem	↙	↗
15.Crytojacking	↙	↙
Legenda:	Tendência:↙(descer), ---(estável), ↗(subir). Ranking:↙(desceu), ---(mesmo), ↗(subiu).	

Fonte: Adaptado de The year in review- ENISA Threat Landscape (ENISA, 2020; P.7).

Os ciberataques direcionados à pandemia covid19, iniciados por volta de março 2020, assumiram diversas formas e feitios. Assim, neste período a KPMG reuniu alguns dos ataques mais importantes: "Fraude do CEO", ou também conhecida por "Business Email Compromise" (BEC), que passa pelo roubo de identidade do CEO ou de outro membro relevante na empresa, e através de emails ou telefonemas tenta que o destinatário (normalmente, com acesso às contas bancárias da empresa) efetue transferências bancárias, sob pretexto da pressão de tempo do CEO para a realização de um pagamento importante (KPMG,2020; p.1), ou apenas para o roubo das credenciais de acesso (Smartfense, s.d). A ameaça é detetada através da comunicação entre colegas. Houve, pois, um aumento de spear-phishing. Spear-phishing, ao contrário do phishing que envia emails em massa, envia emails a um indivíduo, empresa ou organização em específico, seja para roubar dados ou instalar um malware num computador específico (Kaspersky, s.d). KPMG (2020, p.2), mencionou alguns exemplos: emails com o tema Covid19, com documentos maliciosos da Microsoft, para executar códigos intrusivos ou ainda, com o mesmo tema, mas com documentos com "informações de saúde", que acionam um malware quando descarregados no computador. O cibercriminoso leva a que o utilizador insira as suas credenciais de acesso em cópias falsas de sites relacionados com a saúde. Ainda, emails relacionados com recomendações e precauções da OMS, ou e-books com a origem do corona e recomendações de proteção pessoal e dos que o rodeiam convencendo o utilizador com frases como "Está agora a receber este email porque a sua vida conta como todas as outas contam" e ainda curas, vacinas e conselhos sobre tratamentos eficazes para o vírus (Lallie et al., 2020).

Não faltaram fraudes alusivas à redução de impostos em contexto de pandemia (KPMG,2020; p.2), para que o utilizador partilhasse as suas informações financeiras e fiscais através de apelos como "saiba como reduzir os seus impostos durante o período de confinamento" ou "saiba como receber apoios em períodos de pandemia". Lallie et.al (2020) remetem para um caso notável destes ataques com a menção de um e-mail cujo objetivo centrava a obtenção de Bitcoin. Os cibercriminosos mostravam conhecimento do nome da vítima e de uma das suas senhas e ameaçavam infetar o destinatário com Covid-19, bem como a sua família caso não realizassem o pagamento. A revisão de literatura aponta ainda que a Microsoft e o Google falharam quanto ao serviço de cibersegurança oferecido aos seus utilizadores. Sendo que, com o confinamento, as aulas online e o teletrabalho passaram pelo uso destas plataformas em massa, seja para reuniões de trabalho por Teams, Skype, etc, seja para a elaboração de documentos confidenciais, ou por partilhas do foro privado pessoal.

No quadro Internacional, Miller (2020) escreve a partir das declarações de Tonya Ugoretz, subdiretora assistente da Divisão Cibernética do FBI, que o Internet Crime Complaint Center estava a receber por dia cerca de 3000 a 4000 reclamações de cibersegurança, quando em 2019 rondava cerca de 1000 reclamações diárias. Como alvo preferido dos cibercriminosos em tempo de pandemia Covid-19, em qualquer parte do mundo, encontram-se os hospitais. Os hospitais sobrelotados com pacientes e com carência de equipamentos para dar uma resposta ao problema em mãos, tornaram-se alvos fáceis e de sucessivos ataques. O objetivo era a obtenção de uma elevada quantia de dinheiro em troca do desbloqueio da rede, que os mesmos cibercriminosos bloquearam para poder chantagear. O senador Mark Warner transmitiu ao The Hill que mesmo antes da pandemia começar, já tinha observado grandes sistemas hospitalares mal equipados no que toca a cibersegurança e afirmou "O COVID-19 só piorou a situação, com o aumento de ataques e recursos hospitalares perigosamente escassos" (Beavers & Miller, 2020). Confraria (2020, p. 6) em concordância à falta de preparação dos hospitais reflete ainda que "as decisões dos últimos anos estiveram tão alheias a isto que um dos objetivos do confinamento (em todo o lado) foi arranjar tempo para construir capacidade de resposta que não existia" e coloca duas questões em relação ao investimento de cibersegurança na saúde: "há três ou quatro anos a sociedade aceitaria os custos adicionais na saúde e na segurança social para construir capacidade de resposta a riscos deste tipo? E sabendo o que se passou, aceitamos agora custos adicionais para nos protegermos de riscos futuros?" (Confraria,2020; p.6). Mais se acrescenta que, os

cibercriminosos pedem valores extremamente elevados, como o senador exemplifica com o hospital do Illanois que pagou cerca de 350,000 dólares (Beavers & Miller, 2020). A Europol acrescenta o Hospital Universitário de Brno, na República Checa, também sofreu interrupções e foi obrigado a adiar cirurgias urgentes e redirecionar pacientes, além do facto de pode trazer consequências fatais (Europol, 2020; p.5). Ainda na área da saúde, Tonya Ugoretz, esclareceu ao The Hill (2020) "que muitos dos hackers são de países que têm um "desejo de obter insights" sobre pesquisas relacionadas ao COVID-19", sobretudo informações sobre vacinas. Miller (2020) acresce o testemunho de Marc Rogers sobre o facto de se ter pronunciado que estamos a vivenciar uma Ciber Guerra Mundial, "Não estávamos prevendo World War Cyber, que é basicamente o que estamos enfrentando" (Miller, 2020).

O material de abuso infantil onde "devido ao isolamento, menos supervisão e maior exposição online" sejam mais vulneráveis foi também uma das áreas onde os cibercriminosos mais atacaram (Europol, 2020, p. 4). Assim como, a venda de produtos falsificados relacionados com a Covid-19, desde máscaras (apreendidas 34 mil máscaras falsificadas) a medicamentos (13 milhões de euros apreendidos). Constatado pela Europol "a investigação de um Estado-Membro centrou-se na transferência de 6,6 milhões de euros de uma empresa para outra empresa em Singapura para comprar álcool gel e máscaras FFP2 e FFP3. As mercadorias nunca foram recebidas" ou então, outro exemplo de uma empresa que perdeu 300000€ quando as 3,85 milhões de máscaras que nunca chegaram ao destino (Europol, 2020; p.7). A Operação Pangea, coordenada pela INTERPOL, contou com 90 países de todo o mundo para combater o tráfico de medicamentos falsificados (Europol, 2020; p.9).

Fruto do maior tempo despendido no ciberespaço, nomeadamente nas redes sociais, a desinformação também se revelou uma ameaça com a tentativa de manipulação de grupos e o incentivo a conflitos sociais noutros países (Nunes, 2020, p. 8) . Geraldes (2020, p. 9) complementa a perspetiva com o exemplo das campanhas de desinformação elaboradas por Estados sobre as "(...) origens e a propagação do vírus, o que provoca situações de tensão". A desinformação é de tal forma impactante na sociedade que Geraldes (2020; p.9) sublinha o facto de o Diretor-Geral da Organização Mundial da Saúde ter considerado como "infodemic" a "explosão de informação, que acompanha a pandemia (...)". O seu impacto é notório em exemplos que a autora revela, como a ingestão de álcool ou cloroquina para o tratamento do vírus, que pode levar à morte e com "a infraestrutura 5G, a qual se diz ser responsável pela propagação do vírus,

contribuindo para que no Reino Unido mais de 70 postes de telecomunicações tenham sido vandalizados e levando mesmo à perseguição de alguns engenheiros" (Geraldes, 2020; p.10). Esta desinformação gera cada vez mais um ambiente propício ao aumento do cibercrime, pelo que, Daniela Santos (2020; p.4), destaca que o Covid-19 enalteceu a urgência de se educar e formar quanto à cibersegurança, com foco à necessidade de informação.

No caso de Portugal, os ataques aumentaram 88% em 2020, o que representa 1418 incidentes – 689 incidentes no primeiro semestre e 729 no 2º semestre (CNCS,2021; p.19). Destes, 43% são phishing, sendo a ciberameaça mais relevante de 2020 (aumento de 160% face a 2019), com incidência no primeiro período de 2020 e no Natal devido ao aumento do tráfego comercial. Ainda relativamente ao phishing, foi a ameaça com maior aumento no período de pandemia com aumento de 217% apenas de fevereiro 2020 para março 2020 (D. Santos, 2020, p. 4). Contudo, verifica-se que em 99% dos casos não utilizaram os temas ligados à pandemia nas suas ações, mas afetaram "principalmente setores que ganharam relevância para os seus clientes com a maior necessidade de utilização do digital, como a banca, os serviços postais ou as plataformas de streaming" (CNCS,2021; p.13). Posto isso, os ataques à banca mais do que triplicaram com 229 incidentes, representando o segundo setor mais atacado. As principais vítimas dos cibercriminosos, em Portugal, são os cidadãos em geral, as pequenas e médias empresas, os Órgãos de Soberania, a Administração Pública e os setores da Banca e da Educação e Ciência, Tecnologia e Ensino Superior (CNCS,2020; p.23). Todavia, o CNCS (2021; p11) os principais agentes de ameaças a afetar o ciberespaço foram os cibercriminosos e os agentes estatais pelo uso do aparelho de Estados com intuitos estratégicos e políticos.

Da análise efetuada aos ataques cibernéticos, observou-se que 12% são infeções por malware, mas o smishing, ransomware, sextortion (6%) e desinformação digital representam também ciberameaças relevantes em 2020, resultado do isolamento e da crescente utilização tecnológica. Em Portugal, a CNCS relata que 167 pessoas foram condenadas por burla informática e 123 condenados por falsidade informática, mais 21% de arguidos e mais 80% de condenados face ao ano transato (CNCS, 2021; p. 21).

Existe uma grande dependência do ciberespaço que a sociedade manifesta, seja pela fraqueza de redes e servidores domésticos, que colocou em situação de maior vulnerabilidade aqueles que usufruíram do teletrabalho, seja pela importância que a pandemia veio salientar do funcionamento da cibersegurança. E, por isso, a grande

quantidade de ataques relatados por diversas entidades, desde governos, organizações de segurança, empresas e a nível pessoal revela a necessidade de desenvolver medidas de proteção urgentes (Lallie et al,2020; p.1) e de fortalecer as capacidades de cibersegurança na União Europeia, de modo a impedir que o número e impacto dos ciberataques continue a aumentar. Neste sentido, Nunes (2020; p.8) considera que este aumento pode comprometer as infraestruturas críticas e a resiliência dos Estados, dado que, a pandemia expôs as fragilidades da cibersegurança às quais os cibercriminosos souberam utilizar como fonte de rendimento (Ceballos, 2021). Mesmo que se tenha em atenção o paradoxo que a ENISA (2020; p.8) se esforça em explicar:

> A cibersegurança depara-se com um paradoxo: tem sido o desafio e a oportunidade dessa transformação. As mudanças impostas no panorama da tecnologia da informação (TI) enfraqueceram as medidas de segurança cibernética existentes, tornando a sua rápida adaptação um desafio. Ao mesmo tempo, a segurança cibernética é o facilitador da confiança em casos de uso emergentes para serviços digitais e, portanto, tem a oportunidade de facilitar a transformação (ENISA, 2020; p.8).

É ainda urgente criar uma orientação mais específica e não esquecer que "os mesmos tipos de furtos por engano encontrados durante a crise do COVID-19 já existiam, mas os criminosos adaptaram seus *modus operandi* à situação atual" (Europol,2020; p.11).

Por fim, ainda que não tenha se tenha chegado ao fim da pandemia, a revisão de literatura prevê, tanto quanto possível, que a tendência será o contínuo aumento de ciberataques mas com a diversificação e adaptação dos mesmos, de modo a explorar a situação pós-pandemia, com a plena noção de que "na atual sociedade em rede, de sistemas de informação e comunicação digital, a posse de dados sensíveis sobre qualquer cidadão é cada vez mais uma fonte de poder" (CNCS, 2020; p.30).

3ºCapítulo - Avaliação da política de cibersegurança para a União Europeia entre Março 2020 a Março 2021.

A evolução da Internet é uma constante e tem conhecido, ao longo dos últimos anos, uma expansão ao nível dos domínios e utilizadores. Esta evolução, conduziu ao debate sobre o tipo de Internet que queremos para o futuro, compreendendo, primeiramente, que a resiliência e a gestão de crise se tornaram uma prioridade com a pandemia Covid-19, no que toca à cibersegurança. Ora, de acordo com a infografia da União Europeia (Conselho Europeu & Conselho da União Europeia, n.d.) elaborada para explicar como é que a UE combate as ciberameaças, a pandemia Covid-19 expôs não só a sociedade como a própria economia a ciberameaças. A perda de confiança dos utilizadores, sejam eles empresas, governos ou o utilizador individual apenas pode ser colmatada com o aumento da regulamentação objetiva e capaz de acompanhar os avanços tecnológicos e com a capacidade de responder a futuras crises. Não obstante, a cibersegurança aumenta a partir do momento em que o utilizador compreende como a mesma funciona, devendo haver uma aposta na prévia na educação do ciberespaço e das suas ameaças. Assim, o trabalho da União Europeia no período compreendido de Março 2020 a Março 2021, foi no desígnio de "aumentar a ciber-resiliência, combater a cibercriminalidade, fomentar a ciberdiplomacia, reforçar a ciberdefesa, impulsionar a investigação e a inovação, proteger infraestruturas críticas" (Conselho Europeu & Conselho da União Europeia). [11]

Em março de 2020, a Comissão Europeia elaborou uma comunicação intitulada "Política para a Parceria Oriental para o pós-2020 - Reforçar a resiliência - Uma Parceria Oriental em benefício de todos", com o objetivo de apoiar os países parceiros no domínio da saúde pública, da cibersegurança e na transformação digital (Comissão Europeia, 2020b;p.13)[12]. Este documento é sustentado pela visão de que uma maior resiliência, bem como um crescimento sustentável da cibersegurança nos países parceiros que conduzirá a uma maior segurança da União Europeia, reduzindo as hipóteses de os seus

[11]Conselho Europeu, & Conselho da União Europeia. (n.d.). Cibersegurança: como combate a UE as ciberameaças.Retirado de: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acedido em agosto de 2021.

[12] Comissão Europeia. (2020b). Cybersecurity - our digital anchor - A European perspective. https://publications.jrc.ec.europa.eu/repository/handle/JRC121051. Acedido em agosto de 2021.

parceiros se tornarem vulneráveis e futuros atacantes cibernéticos da União. De uma forma operacional, o apoio prevê a elaboração de "quadros jurídicos, políticos e operacionais sólidos em matéria de cibersegurança com base na legislação e nas melhores práticas da UE, incluindo o quadro de certificação da cibersegurança da UE" e pelo alargamento aos benefícios do Mercado Único Digital (Comissão Europeia, 2020b; p.17).

No mesmo mês, a Comissão Europeia comunicou, também, a "Estratégia para as PME com vista a uma Europa Sustentável e Digital", onde logo na primeira página esclarece que "os 25 milhões de pequenas e médias empresas da europa, constituem a espinha dorsal da economia da UE", dado que, "empregam mais de 100 milhões de pessoas, representam mais de metade do PIB da europa" (Comissão Europeia, 2020h, p. 1) . A Comissão Europeia sustenta que as PME motivam a competitividade que, por sua vez, levará à prosperidade tecnológica. Para tal, a estratégia para uma Europa digital e segura passa pela modernização e inovação digital, bem como pela formação dos trabalhadores das PME através do desenvolvimento de Cursos Digitais Intensivos (Comissão Europeia, 2020h, p. 7). Pois, como já mencionado anteriormente, a falta de formação digital representou uma porta aberta para ataques cibernéticos durante o período de confinamento provocado pela pandemia.

Ora, uma vez que, a pandemia levantou problemas de elevada emergência também necessitou de respostas com o mesmo grau de rapidez. Neste sentido, a União Europeia trabalhou no desenvolvimento de um instrumento temporário e capaz de recuperar a Europa, chamado *Next Generation EU,* o qual será também acompanhado de um quadro financeiro plurianual reforçado para 2021-2027. Cabe-lhe coordenar a capacidade orçamental da União Europeia para 2021-2027 consoante os desafios prioritários, como a recuperação da economia, cooperação na saúde e na gestão de crises, e as transições ecológica e digital dos EM, como o investimento e reformas que, através do orçamento, canalizará aos Estados-Membros os seus fundos (Comissão Europeia, 2020g, p. 3). Este instrumento de recuperação surge para que a União, além de responder aos problemas emergentes, consiga obter uma capacidade de resiliência consistente para que, mais tarde, consiga estar dotada de uma maior segurança e rápida capacidade de resposta em caso de novas ameaças. Mais, é sublinhada a necessidade do instrumento de recuperação e de criação de legislação com a urgência de restaurar a confiança de todos os utilizadores da internet no ciberespaço, para que possam trabalhar, comprar e socializar com confiança e segurança (Comissão Europeia, 2020a, p. 1).

Cumpre referir que esta capacidade de ação pontual não compromete os orçamentos a longo prazo, mas é-lhes adicional (Comissão Europeia, 2020g, p. 4).

O *Next Generation EU* apoia os Estados-membros através da criação de um Mecanismo de Recuperação e Resiliência, o qual é o elemento central deste instrumento (Comissão Europeia, 2020g, p. 5). Esse Mecanismo de Recuperação e Resiliência, surge com o propósito de "contrariar as disparidades crescentes entre Estados-membros" (Comissão Europeia, 2020g, p. 1) e apoia investimentos e reformas, centrados na recuperação económica e transição ecológica e digital, no sentido de a recuperação ser duradoura (Comissão Europeia, 2020g, p. 5).

A iniciativa REACT-EU também nasce do *Next Generation EU* e surge para "colmatar o fosso entre as primeiras medidas de resposta e a recuperação a longo prazo" (Comissão Europeia, 2020g, p. 5) com a aposta em economias resilientes e sustentáveis e numa política de coesão ao serviço da recuperação económica, como nos sistemas de saúde, por exemplo (Comissão Europeia, 2020g, p. 6).

Um caminho importante que o *Next Generation EU* percorre é a recolha de ensinamentos da crise COVID-19 com a lição de que "União deve urgentemente reforçar a sua capacidade de resposta a situações de crise e aumentar a resiliência a futuros choques" (Comissão Europeia, 2020g, p. 10). Daqui nasce então outros programas como "Programa EU pela Saúde", para dotar a União e os seus EM de rápida capacidade de resposta. Esta capacidade de resposta requer investimento na transformação digital na saúde a curto e longo prazo com frequentes atualizações, na formação do pessoal médico e na implementação de infraestruturas digitais interoperáveis (Comissão Europeia, 2020g, p. 11). Ainda assim, a União está ciente que os planos elaborados até à data não são suficientes para tornar a União Europeia resiliente no ciberespaço (Comissão Europeia, 2020g, p. 13).

Contudo, o Centro de Estudos de Política Europeia acrescenta passos importantes dados em matéria da cibersegurança como o facto de a Europa ser "a primeira e única região do mundo onde a identificação digital e a verificação são fornecidas com segurança e de maneira legalmente aplicável" onde existe uma maior aproximação cidadão-governo em simultâneo com a garantia da privacidade (Echikson, 2020), confirmando primeiros passos de crescimento na cibersegurança.

Durante o período de março 2020 a março de 2021 a União Europeia esforçou-se por elaborar uma Nova Estratégia de Cibersegurança. Os principais esforços foram

visíveis no planeamento e adoção de uma nova Diretiva, a Diretiva SRI2, na formulação da Diretiva relativa à resiliência das entidades críticas e de uma nova estratégia de cibersegurança. Apesar de não ter sido adotada nesse período de tempo, a proposta anexa em si outras duas propostas: a Diretiva relativa a medidas destinadas a assegurar um elevado nível comum em cibersegurança em toda a União (Diretiva SRI2)[13] e a Diretiva relativa à resiliência das entidades críticas[14] (Cocco, Barros, & Kindylidi, 2020).

A Nova Estratégia de Cibersegurança visa uma abordagem de proteção para as empresas, instituições e cidadãos, para que possa ser alcançada uma liderança tecnológica resiliente assente na cooperação internacional, com o reconhecimento da importância da ligação quer interna e quer externa (Comissão Europeia, 2020c, p. 5). No sentido de estimular o crescimento industrial da cibersegurança na União Europeia a "cibersegurança deve ser integrada em todos estes investimentos no domínio digital, particularmente em tecnologias fulcrais, como a inteligência artificial (IA), a cifragem e a computação quântica(...)" (Comissão Europeia, 2020c, p. 5).

Em resposta aos atuais desafios e de modo a evitar futuras ameaças esta Nova Estratégia para a década digital assenta em três pilares fundamentais ao seu bom funcionamento.

O primeiro pilar é a "Resiliência, soberania tecnológica e liderança", que denota que as regras da segurança de informação são essenciais para o funcionamento do mercado único da UE e, portanto, se deve proceder à revisão da Diretiva SRI, no sentido de aumentar a resiliência das infraestruturas e dos serviços críticos cibersegurança (Comissão Europeia, 2020c, p. 6). Neste pilar, a União Europeia deverá implementar medidas regulamentares ao uso seguro da Internet e financiar programas que intervenham eficazmente na resolução de problemas e atuem como mecanismos de recuperação. As PME são incluídas neste pilar, para que possam proceder à adoção de tecnologias de cibersegurança como mão de obra qualificada, e ainda acrescenta o desenvolvimento de DNS (Sistema de Nomes de Domínio) "como alternativa segura e aberta para o acesso dos cidadãos, empresas e administrações públicas da UE à Internet" (Comissão Europeia, 2020c, p. 14). Para finalizar este pilar, a estratégia aborda que faz parte da sua iniciativa a criação de uma rede de centros de operações de segurança de IA (Inteligência Artificial) e uma infraestrutura de comunicação ultrassegura que potencie

[13] Comissão Europeia. (2020e). Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148. 12. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020PC0823&from=FR. Acedido em setembro de 2021.

[14] Comissão Europeia. (2020f). Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à resiliência das entidades críticas. 1–59. Acedido em setembro de 2021.

as tecnologias quânticas, sem esquecer que deverão ser tomadas conclusões sobre instrumentos 5G (Comissão Europeia, 2020c, p. 14).

O segundo pilar da Nova Estratégia é a "Criação da capacidade operacional para prevenir, dissuadir e responder" (Comissão Europeia, 2020c, p. 14). O combate ao cibercrime e a promoção da ciberdiplomacia são os principais temas deste pilar. Aqui, não só o objetivo passa por desencorajar a ações de cibercriminalidade, mas também por criar uma ciberunidade conjunta, com metas calendarizadas, para combater lacunas que sublinhou, isto é, a falta de um espaço comum para agir com uma cooperação estruturada e a falta de exploração do potencial da cooperação internacional (Comissão Europeia, 2020c, p. 15). A partilha de informação é incentivada, assim como a criação de grupo de trabalho sobre ciberinformação dos EM da União, em vista a melhorar a ciberdiplomacia (INTCEN UE) e a partilhar a sua visão daquilo que é um mundo ciberseguro e simultaneamente aberto mundialmente (Comissão Europeia, 2020c, p. 21).

A "Promoção de um ciberespaço mundial e aberto" (Comissão Europeia, 2020c, p. 22) é o terceiro pilar, que fomentará o comportamento responsável no ciberespaço através da cooperação da União com os seus parceiros internacionais, como a ONU, na condição da existência de regras e do respeito dos direitos humanos e liberdades da União e dos seus EM (Comissão Europeia, 2020c, p. 23). Por sua iniciativa, formula orientações práticas sobre a aplicação dos direitos humanos e das liberdades fundamentais no ciberespaço (Comissão Europeia, 2020c, p. 26). A elaboração de normas no espaço internacional com os seus parceiros, é segundo a nova estratégia, uma maneira de expandir a sua visão sobre um espaço aberto e seguro, bem como o consecutivo apoio da UE à adesão de países terceiros à adesão da Convenção de Budapeste (Comissão Europeia, 2020c, p. 23,24). Ainda neste ponto, compromete-se à melhor proteção infantil contra o abuso e exploração sexual de menores e à apresentação de uma estratégia sobre os direitos da criança (Comissão Europeia, 2020c, p. 26).

No âmbito da Nova Estratégia de Cibersegurança e para preparar a Europa para a era digital, como mencionado anteriormente, a Diretiva SRI de 2016 foi revista e revogada pela Diretiva SRI2[15], que engloba medidas destinadas a garantir um elevado nível comum de cibersegurança na União. Também como mencionado anteriormente, e

[15] Comissão Europeia. (2020e). Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nÍvel comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148. Retirado de: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0008.02/DOC_1&format=PDF. Acedido em: outubro de 2021.

a par desta nova Diretiva SRI2, foi proposta do Parlamento Europeu e do Conselho outra diretiva relativa à resiliência das entidades críticas. Quanto ao Regulamento de Cibersegurança da União Europeia de 2019, adotou um quadro de certificação de cibersegurança para produtos, serviços e processos, com reforço ao mandato da ENISA (Agência Europeia para a Segurança das Redes e da Informação).

Embora a Diretiva SRI 2016 tivesse contribuído para a cooperação da cibersegurança e ter revelado progressos significativos, revelou também "deficiências intrínsecas que a impedem de responder de forma eficaz a desafios contemporâneos e emergentes no domínio da cibersegurança" (Comissão Europeia, 2020e, p. 2), como por exemplo, as diferentes aplicações da própria Diretiva SRI a nível nacional nos EM (Comissão Europeia, 2020e, p. 2). Em sua substituição, a SRI2 visa eliminar divergências profundas entre EM, em especial:

> [...] estabelecendo regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações (Comissão Europeia, 2020e, pp. 2–3).

Ainda assim, a presente Diretiva SRI2 permite que os EM tomem as medidas que considerem necessárias, em conformidade com o direito da União, para assegurar a proteção dos seus interesses e da sua segurança (Comissão Europeia, 2020e, p. 3).

No seu objeto, a presente Diretiva "Estabelece a obrigação de os Estados-Membros adotarem estratégias nacionais de cibersegurança e de designarem autoridades nacionais competentes, pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (CSIRT)"(Comissão Europeia, 2020e, p. 20). As obrigações são também ao nível da gestão do risco e de notificação às entidades importantes, bem como à partilha de informações sobre cibersegurança (Comissão Europeia, 2020e, p. 20). Ora, tem-se em atenção que esta obrigatoriedade de partilha de informações faz com que o processo de diagnóstico e correção seja mais eficaz na resolução das vulnerabilidades. Não só é feita uma gestão de risco mais eficaz, como também são retirados ensinamentos para melhorar a resiliência das empresas (Comissão Europeia, 2020e, p. 13).

Neste seguimento, os EM devem designar uma CSIRT, para fazer a ponte de informação entre as entidades competentes, e a ENISA deve criar um registo de vulnerabilidades que permitam aos utilizadores tomarem as devidas precauções (Comissão Europeia, 2020e, p. 10)

Na Diretiva SRI2 passa a estar presente a distinção entre entidades essenciais e entidades importantes. Isto porque, o regime de supervisão é distinto, sendo completo e simplificado, respetivamente. Na prática, a diferença resume-se a que:

> [...] as entidades importantes não são obrigadas a documentar sistematicamente o cumprimento dos requisitos em matéria de gestão dos riscos de cibersegurança e que as autoridades competentes devem adotar uma abordagem ex post reativa à supervisão, pelo que não estão sujeitas a uma obrigação geral de supervisionar essas entidades (Comissão Europeia, 2020e, p. 12,13).

A coima foi introduzida nesta Diretiva, conferindo esse poder a cada autoridade competente, contudo, ressalva que

> [...] sempre que a presente diretiva não harmonize sanções administrativas, ou se necessário noutros casos (por exemplo, incumprimento grave das obrigações estabelecidas na presente diretiva), os Estados-Membros devem criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deve ser determinada pelo direito do Estado-Membro (Comissão Europeia, 2020e, p. 18).

O mais relevante nesta alteração normativa é que a Diretiva SRI2 traz consigo os critérios necessários para que os EM possam recorrer à adoção de uma estratégia nacional de cibersegurança, que deve ser notificada à Comissão, e avaliada de em menos de quatro em quatro anos (Comissão Europeia, 2020e, p. 27). De acordo com o seu processo de fiscalização (Comissão Europeia, 2020e, p. 25), a fiscalização é um mecanismo trabalhado nesta Diretiva, até para a mesma, que é avaliada pela Comissão, pois, o processo de fiscalização permite que a Diretiva e as estratégias nacionais de cibersegurança se adaptem às necessidades políticas, sociais, económica e de mercado.

A criação de uma nova rede de CSRIT nacionais de forma a garantir o desenvolvimento de confiança e de cooperação entre os EM, com o intercâmbio de informações e a aplicação de respostas coordenadas (Comissão Europeia, 2020e, p. 10). É ainda mencionada a criação da Rede Europeia de organizações de Coordenação de Cibercrises (CyCLONe) que, no seu essencial, prepara e ajuda a desenvolver o nível de gestão de incidentes em grande escala (Comissão Europeia, 2020e, p. 10).

A Diretiva SRI2 estabelece, ainda, que os trabalhos coordenados com a de Diretiva do Conselho e do Parlamento Europeu para a Resiliência das Entidades Críticas, no sentido de reduzir vulnerabilidades e de aumentar a resiliência das infraestruturas críticas no âmbito da cibersegurança. Pois, as infraestruturas críticas são essenciais ao normal funcionamento da sociedade, como já referido. Para tal, proposta de Diretiva para a resiliência das entidades críticas aumentou o seu âmbito de atuação para 10 setores, nomeadamente os da energia, dos transportes, dos serviços bancários, das infraestruturas do mercado financeiro, da saúde, da água potável, das águas residuais, das infraestruturas digitais, da administração pública e do espaço (Comissão Europeia, 2020f, p. 16). Esta veio substituir a Diretiva ICE, que apenas se focava nos setores da energia e dos transportes (Comissão Europeia, 2020f, p. 3).

Valoriza, tal como a Diretiva SRI2, o processo de avaliação de riscos e a supervisão, pelo que prevê um mecanismo adequado para que os EM possam identificar as entidades críticas bom base em critérios comuns para proceder à sua avaliação nacional, bem como, a supervisão específica dos EM e das entidades críticas (Comissão Europeia, 2020f, p. 8). Seguidamente, de encontro à linha de cooperação internacional que a União pretende reforçar, esta Diretiva visa também a cooperação com os países parceiros no domínio das avaliações de risco(Comissão Europeia, 2020f, p. 13). Junto da avaliação e da cooperação, segue-se também a obrigatoriedade de os EM tomarem medidas de manutenção de atividades essenciais, bem como obrigações para as entidades críticas reforçarem a sua capacidade e resiliência e regras de supervisão por estas mesmas entidades, assim como estipulado no seu primeiro artigo (Comissão Europeia, 2020f, p. 24).

A proposta pretende “reforçar a prestação, no mercado interno, de serviços essenciais para a manutenção de funções sociais ou atividades económicas vitais, aumentando a resiliência das entidades críticas que prestam tais serviços” (Comissão Europeia, 2020f, p. 1), uma vez que, a pandemia Covid-19, despertou ainda mais a importância da segurança destes serviços. Para tal, estima-se que a proposta recorra a 42,9 milhões de euros entre 2021-2027 (Comissão Europeia, 2020f, p. 10).

A União Europeia, para além da parte legislativa acrescenta outros instrumentos que as infraestruturas devem percorrer para estarem protegidas no que toca à cibersegurança. Nomeadamente, no setor da saúde que foi fortemente afetado pela Covid-19.

No que toca às soluções elaboradas para a diminuição das vulnerabilidades ou combate às ciberameaças, a ENISA refere que, as soluções Cloud são o que tem permitido "elasticidade e acesso rápido para a implementação de novos serviços incluindo saúde «virtual» e telemedicina" (ENISA, 2021a, p. 7). O que, de uma maneira ou de outra, leva-nos ao encontro da elaboração de legislação na cibersegurança no sentido de que, a segurança em Cloud para o setor da saúde ainda está numa fase inicial de desenvolvimento, segundo a ENISA (2021a, p. 11) e que, segundo o GDPR, os dados da saúde requerem um padrão de proteção mais elevado para o seu processamento, que deve ser trabalhado também em matéria da legislação da União Europeia.

Através do programa Horizonte2020, a União Europeia preocupa-se em elaborar programas que desenvolvam soluções eficazes, a curto e longo prazo, ao nível da cibersegurança na saúde, como DEFeND, PANCEA, PAPAYA, CUREX E SPHINX. Veja-se que, o programa DEFeND é uma plataforma para proteção e gestão de dados e privacidade, em conformidade com GDPR (Cyberwatching.eu, n.d.). O PANCEA foi projetado para melhorar a proteção e privacidade das infraestruturas hospitalares com fornecimento da avaliação do fluxo de trabalho e monitoramento do sistema (Cyberwatching.eu, n.d.).
Seguidamente, PAPAYA, está relacionado com o desenvolvimento de soluções de privacidade e trabalhar dados não confiáveis (Cyberwatching.eu, n.d.). O CUREX deteta ativos e vulnerabilidades, deteta em tempo real comportamentos anormais de usuários, dispositivos e dados, produz pontuações de risco, entre outras funções (Cyberwatching.eu, n.d.). Por fim, o SPHINX fornece um "dispositivo automatizado sem toque e um conjunto de ferramentas de verificação de serviço que será facilmente adaptado ou incorporado em infraestruturas médicas, clínicas ou de saúde existente" (Cyberwatching.eu, n.d.), ou seja, foi elaborado para aumentar a cibersegurança das tecnologias de informação da saúde com a proteção dos dados do paciente. Este projeto contribuirá com um relatório de "quais vulnerabilidades podem existir" para as solucionar e aumentar a confiança e segurança do paciente (Cyberwatching.eu, n.d.).

Já em março de 2021, a Comissão publicou as "Orientações para a Digitalização até 2030: a via europeia para a Década Digital" (Comissão Europeia, 2021). Neste domínio, é possível verificar a aproximação do documento publicado pela UE com a acima mencionada hipótese 3 - (H3) Apesar da cibersegurança estar desde a apresentação da estratégia de segurança, em 2003, como um dos eixos estratégicos da União Europeia a pandemia veio revelar as vulnerabilidades da União Europeia face a esta ameaça.
E, para responder a estas vulnerabilidades elabora um plano com quatro objetivos que

considera fundamentais serem atingidos como resposta a essas vulnerabilidades . São eles a qualificação da população no que concerne às competências digitais, a criação de infraestruturas digitais seguras e sustentáveis, a transformação digital das empresas e a digitalização dos serviços públicos. Estes objetivos são acompanhados de recomendações e metas concretas para cada uma deles ser acompanhados detalhadamente(Comissão Europeia, 2021, p. 20).

Ora, uma sociedade com maiores competências digitais e o investimento em profissionais qualificados (nomeadamente, através da convergência entre homens e mulheres) para que, para além de aumentar a confiança nas ações digitais e nos produtos e serviços fornecidos, a sociedade consiga identificar tentativas de ciberameaças, seja qual for a forma em que se manifestam (Comissão Europeia, 2021, p. 5).

Refere, novamente, o empenhamento na cooperação internacional para uma melhor conectividade (mais rápida e mais segura) que é importante na resolução de problemas "(...)para resolver, em horas, aquilo que atualmente demora centenas de dias, se não anos" (Comissão Europeia, 2021, p. 9) e para garantir que, ao haver cooperação se diminua a quantidade de possíveis inimigos.

Quanto às PMEs, uma vez que são o grande motor de funcionamento da própria União, esta melhorará o acesso ao seu financiamento para que as PME consigam melhorar os seus serviços digitais e fazer uso do serviço de nuvem e de inteligência artificial, e fazer uso de profissionais e empresas competentes em cibersegurança (Comissão Europeia, 2021, p. 11).

No que se refere à digitalização dos serviços públicos o objetivo passa por disponibilizar a 100% a utilização destes serviços por via digital, como registos médicos e soluções de identificação pessoal com segurança (Comissão Europeia, 2021, p. 13).

O cumprimento destas metas faz com que o documento refira que este método é caminho que levará a Europa à soberania digital que pretende. Assim,

> Esta é a forma de a Europa ter soberania digital num mundo interligado, construindo e implantando capacidades tecnológicas de uma forma que capacite as pessoas e as empresas para aproveitarem o potencial da transformação digital e contribua para a construção de uma sociedade mais saudável e mais ecológica (Comissão Europeia, 2021, p. 1).

Ainda, segundo o Parlamento da União Europeia (2021; p.2), procura-se estabelecer padrões de segurança na Internet e monitorizar sinais de ataques a redes, bem como indicar ferramentas de ciberdiplomacia. A União ressalva ainda que, estas vulnerabilidades reveladas só conseguem ser resolvidas com o empenho de todos, da sociedade, das PME, dos Estados e dos seus parceiros (Comissão Europeia, 2021, p. 23) e que deverão ser acompanhadas com regularidade.

Após o período de março de 2021, o Parlamento em plenário de junho de 2021, publicou o documento "Ataques cibernéticos recentes e a segurança cibernética da UE"[16], que consagra a sua disposição para ouvir o Conselho e a Comissão sobre ciberataques recentes na procura de novas soluções (Parlamento Europeu, 2021a, p. 2). Ou seja, uma constante atualização de ciberameaças torna-se importante para a adaptação dos meios de combate e assim melhorar o nível de resiliência.

Por último, a última Resolução do Parlamento Europeu sobre a Estratégia de Cibersegurança, teve por base não só a Estratégia de Cibersegurança da UE para a década digital (de 2020) e a Diretiva SRI2, mas como um conjunto de propostas elaboradas ao longo do tempo em matéria de cibersegurança (Parlamento Europeu, 2021b, pp. 2–3). Também teve em consideração o facto de que a "transformação digital é uma prioridade estratégica fundamental da União que está inevitavelmente associada a uma maior exposição de ciberameaças" (Parlamento Europeu, 2021b, p. 4). Esta resolução, à luz do documento publicado em março de 2021 "Orientações para a Digitalização até 2030: a via europeia para a Década Digital", continua a sublinhar uma aproximação com a hipótese 3 (H3) Apesar da cibersegurança estar desde a apresentação da estratégia de segurança, em 2003, como um dos eixos estratégicos da União Europeia a pandemia veio revelar as vulnerabilidades da União Europeia face a esta ameaça. Ora, veja-se o mencionado pela Resolução

> a crise covid-19 veio expor ainda mais as vulnerabilidades cibernéticas em alguns setores críticos, em particular nos cuidados de saúde, e que as medidas associadas no domínio do teletrabalho e distanciamento social aumentaram a nossa dependência das tecnologias digitais e da conectividade, enquanto toda a Europa, estão a aumentar, em número e nível de sofisticação, os ciberataques e a cibercriminalidade, incluindo a espionagem e a sabotagem, bem como o acesso a sistemas,

[16] Parlamento Europeu. (2021a). *Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade*. Retirado de https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_EN.pdf. Acedido em: outubro de 2021.

> estruturas e redes TIC e a respetiva manipulação através de aplicações maliciosas e ilegais" (Parlamento Europeu, 2021b, p. 4).

Na verdade, a União Europeia sabe que a crise covid-19 expôs ainda mais as suas fragilidades cibernéticas, onde a resposta a esta investigação é dada pela terceira hipótese (H3) elaborada para esta investigação: apesar da cibersegurança estar desde a apresentação da estratégia de segurança, em 2003, como um dos eixos estratégicos da União Europeia a pandemia veio revelar as vulnerabilidades da União Europeia face a esta ameaça. O percurso de trabalho da União focou-se em, de imediato, criar mecanismos e instrumentos de apoio a curto e longo prazo, como o *Next Generation EU*. As PME que estavam pouco preparadas ao nível tecnológico receberam investimento para se munir de equipamentos tecnológicos e de formações para os funcionários. A educação básica da cibersegurança e a redução da disparidade entre homens e mulheres também foi uma aposta de trabalho da União Europeia nos seus EM. Mas, não só nos EM a União investiu. Investiu em países parceiros com parcerias orientais (Balcãs, ASEAN…) quer em matérias de transformação digital quer em matérias de apoio à saúde (e auxílio de cibersegurança na saúde). Sublinhou a importância de os EM, empresas e cidadãos partilharem entre si conhecimentos e ciberameaças e de se reduzir a dependência tecnológica estrangeira, no sentido de promover a sua liderança e competitividade digital (Parlamento Europeu, 2021b, pp. 7–8). No que toca à responsabilização do ciberatacante, a União introduziu pela primeira vez a coima, como consequência, contudo, não descarta a noção das dificuldades encontradas no processo de deteção do cibercriminosos.

Por fim, sublinhar que "resiliência" é uma palavra-chave para o período pós crise covid-19 no que toca à cibersegurança por ter de se adaptar instantaneamente a bruscas mudanças, ao passo que, resolvia vários problemas ao mesmo tempo, e com a consciência de que "a digitalização da nossa sociedade significa que todos os setores estão interligados e que as fragilidades de um setor podem prejudicar outros setores(…)" tentou não só resolver os problemas, mas alcançar a soberania digital da União Europeia.

Conclusão

No final da investigação que foi conduzida sobre os Novos Desafios à cibersegurança na União Europeia em tempos de pandemia Covid19 cumpre destacar cumprimento dos objetivos e as conclusões retiradas.

Começámos pela elaboração do enquadramento conceptual-normativo, nomeadamente o enquadramento do conceito de segurança e do conceito de cibersegurança. Observa-se que o conceito de segurança nas Relações Internacionais esteve ao longo do desenvolvimento da área epistemológica relacionada com a segurança dos Estados e que se foi consolidando através dos Estudos da Guerra e da estratégia militar. Contudo, a Segunda Guerra Mundial, a Guerra Fria e o pós-Guerra Fria foram marcos históricos para este conceito. Após a Guerra fria a segurança deixou de se centrar na defesa e na guerra e é elaborada literatura específica sobre a segurança cenradas nas ameaças e proteção dos Estados (Esteves, 2015; p.53). Nesta fase, surgiram novos debates teóricos e o conceito de segurança foi reformulado, uma vez que, a teoria realista não conseguiu prever o início da Guerra Fria. Foi após a Guerra Fria, pela imprevisibilidade do colapso da URSS, que o debate de alargamento do conceito de segurança espoletou, ainda que, para alguns autores a URSS representava para o Ocidente uma ameaça militar, este campo continuasse como prioridades das agendas internacionais, após Guerra-Fria.

Após 1985, data de criação do Conflict and Peace Reasearch Institute, que deu origem à Escola de Copenhaga, os teóricos desta mesma escola consideram que, pela perspetiva abrangente, o conceito de segurança deve incorporar tanto as questões militares como acrescentar questões do setor político, económico, ambiental e social de modo a garantir o bem-estar do Estado (Buzan, 1991 apud Tanno,2003; p.50). Nesta mesma perspetiva abrangente, a segurança pode ser analisada por níveis, numa escala que vai do Sistema Internacional até ao indivíduo; por setores, agrupados em setor militar, setor político, setor económico, setor social e setor ambiental e por regiões, que compreendem as relações regionalizadas no pós-Guerra Fria. Compreende ainda que, estes elementos estão interligados e são interdependentes, pelo que, a falha de um destes setores, para além da possibilidade de condicionar os outros, pode comprometer a segurança do indivíduo e do Estado. A Escola de Copenhaga defende que a ameaça é variável não só de Estado para Estado, mas também entre os próprios setores e níveis.

Um dos principais contributos da Escola de Copenhaga foi o processo de securitização, processo pelo qual uma ameaça se torna um problema de segurança. Aqui, a existência da ameaça faz uso de meios emergenciais para resolução de problemas e permite aos Estados a quebra de regras. Este processo conta com a aceitação da sociedade para securitizar algum tema, onde manifestam as suas prioridades pelo ato da fala. A securitização é caracterizada como inclusiva pois, permite que ameaças outrora ignoradas sejam, assim, trazidas para o debate. O alargamento do conceito de segurança dá-se, então, pela proximidade ao construtivismo, mas também pela alteração do quadro de ameaças internacional. Contudo, ainda que para alguns autores o conceito de segurança não apresente uma definição única e universal ou com significado intrínseco, a Escola de Copenhaga atribui o significado de "sobrevivência". A revisão de literatura explica que a segurança pode ser definida como um conceito "hifenizado" pois, adapta-se a temas que se pretendam securitizar, tal como a cibersegurança. Cabe, ainda, mencionar que a segurança ganha diferentes perceções consoante o contexto histórico ou localização geográfica.

Em resultado da alteração do quadro de ameaças internacional, após o 11 de setembro de 2001, passaram a ser reconhecidas ameaças não convencionais, como as ameaças ambientais e digitais. As agendas internacionais reformularam as suas prioridades e a cibersegurança deixou de ser pensada como um termo técnico que visava apenas responder a falhas informáticas. Ainda que tenha abandonado essa visão clássica, tal como a segurança, a revisão de literatura também não aponta nenhum conceito único e universal, mas definições utilizadas por vários autores. O conceito é definido como a proteção dos sistemas de informação e de todas as ligações tecnológicas. O conceito mais utilizado é elaborado pela União Internacional das Telecomunicações que, no seu essencial, faz uso de ferramentas, políticas, diretrizes, entre outros conjuntos, para garantir a proteção do ciberespaço e do utilizador. A cibersegurança não só é vista como uma ferramenta de solução, mas também como prevenção de ciberameaças e do regular funcionamento do ciberespaço. O conceito de cibersegurança aborda também que é tanto como um direito como uma obrigação manter a segurança do ciberespaço.

À semelhança com o conceito de segurança, a cibersegurança também é um termo multidisciplinar, uma vez que, nos encontramos em crescente digitalização das ações quotidianas, e também se encontra em constante mudança e pode variar entre o tempo e o espaço utilizado. Em contrapartida, se para alguns autores a segurança é um termo "hifenizado", para outros a cibersegurança é um termo guarda-chuva porque "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" (Hermenegildo, 2020; p.9).

Quanto ao enquadramento legal da cibersegurança, cabe mencionar que são apresentadas dificuldades, por parte do legislador, em acompanhar as transformações tecnológicas pela sua rápida e constante evolução. Inicialmente, a legislação acompanhava a proteção dos meios técnicos, em meado de 1985, mas, em 2001, a Europa já tinha como objetivo alargar a sua conectividade e formulou o eEurope 2002. Em poucos anos, a União Europeia reuniu esforços para que essa conectividade fosse segura. Realizou a Convenção de Budapeste, criou a Agência Europeia para a Segurança das Redes e da Informação, incluiu como forma de terrorismo os ataques a sistemas de informação, o Tratado de Lisboa reforçou que a cibercriminalidade se encontra ao abrigo da polícia judiciária e impulsionou à criação da Europol EC3. Assim, em 2013, a União Europeia apresenta a primeira Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido. Esta estratégia contemplava medidas educacionais, investimentos, investigação e a criação de quipas de resposta emergenciais a ataques informáticos. Esta Estratégia de 2013, resultou na Diretiva SRI e no Regulamento (UE) 2019/881 sobre a cibersegurança da UE.

Na Diretiva SRI pode-se concluir que as capacidades existentes não eram suficientes para garantir o nível de segurança pretendido, devido à diferente preparação que os Estados-Membros revelam. Criou ainda outro mecanismo de resposta, o CSIRT, para continuar a responder a incidentes no ciberespaço. Assim, a Diretiva SRI insiste no continuo trabalho de promover uma cultura de gestão de riscos e de se continuar a investir em requisitos regulamentares à cibersegurança.

Em 2018, aplicou-se o Regulamento Geral sobre a Proteção de Dados, que permitiu aos cidadãos controlarem os seus dados pessoais e salvaguardar a sua privacidade. No ano seguinte, em 2019, é publicado o Regulamento (UE) 2019/881 sobre a Cibersegurança da UE, que resulta da Estratégia de Cibersegurança de 2013 e que visava a criação de sistemas europeus de certificação da cibersegurança para os produtos, serviços e processos para aumentar a confiança do utilizador no ciberespaço.

Mais recentemente, em 2020, foi apresentada a proposta para a Estratégia de cibersegurança da União Europeia para a Década Digital, que tinha como objetivo

aumentar a sua capacidade de resposta e salvaguardar os três pontos-chave. No último ano de 2021 foram impostas as primeiras sanções contra ciberataques, proibindo os cibercriminosos de viajar, com a prática do congelamento de bens, e proibição de receberem fundos de pessoas ou entidades da EU ou outras incluídas.

Nesta investigação, foi escrutinada a relação da pandemia Covid19 com a cibersegurança. Neste capítulo, podemos observar que o confinamento aumentou o uso da Internet e de meios tecnológicos, seja para trabalho, escola, lazer, mitigação do distanciamento físico e até mesmo para o crime. O risco ao nível da cibersegurança foi analisado pelo que, através do paradigma espaço-tempo, surgiram novos ciberataques mais sofisticados, com novas ferramentas e estratégias de exploração de vulnerabilidades, que representam novos riscos num curto espaço-tempo. Diversos autores mencionam que a tendência será aumentar o número de ciberataques, mas com a adaptação de pós-pandemia, uma vez que, a posse de dados sobre qualquer cidadão se torna, com o passar do tempo, uma fonte de poder cada vez maior.

O medo, a ansiedade, a pressão de tempo e de trabalho e o cansaço foram os fatores de maior vulnerabilidade detetados que a pandemia e o confinamento intensificaram. Assim, o trabalho da União Europeia no período compreendido de Março 2020 a Março 2021, foi no desígnio de aumentar a ciberesiliência dos Estados, empresas, organizações e do próprio cidadão. Expandiu as suas parcerias e realizou parceiras Orientais, com a noção de que uma maior resiliência, bem como um crescimento sustentável da cibersegurança nos países parceiros que conduzirá a uma maior segurança da União Europeia, reduzindo as hipóteses de os seus parceiros se tornarem vulneráveis e futuros atacantes cibernéticos da União.

Os esforços da União Europeia passaram pela transformação digital, modernização e inovação digital das pequenas e médias empresas, hospitais (e infraestruturas relacionadas com a saúde), entre outras infraestruturas; pela formação dos trabalhadores, nomeadamente ligados ao setor da saúde, com cursos digitais intensivos. Estes esforços contaram ainda com a elaboração de mecanismos temporários de recuperação como o *Next Generation,* com a capacidade de coordenar a capacidade orçamental de 2021-2027. O maior objetivo da União Europeia incidiu sobre a capacidade de resiliência e do restauro de emergência da confiança no ciberespaço de todos os utilizadores, para que possam trabalhar, comprar e socializar em segurança.

Com efeito, de março 2020 a março de 2021 a União Europeia empenhou-se por elaborar uma Nova Estratégia de Cibersegurança. Apesar de não ter sido adotada nesse período de tempo, a proposta anexa em si outras duas propostas complementares: a Diretiva relativa a medidas destinadas a assegurar um elevado nível comum em cibersegurança em toda a União (Diretiva SRI2, que revoga a Diretiva SRI) e a Diretiva relativa à resiliência das entidades críticas.

A Nova Estratégia de Cibersegurança aborda a necessidade de proteção das empresas, instituições e cidadãos e, na mesma medida, a importância da cooperação internacional interna e externa. Assenta em três pilares: "Resiliência, soberania tecnológica e liderança", "Criação da capacidade operacional para prevenir, dissuadir e responder" e "Promoção de um ciberespaço mundial e aberto". A Diretiva SRI2 introduz a coima, e confere o poder a cada autoridade competente e o mais relevante nesta alteração normativa é que a Diretiva SRI2 traz consigo os critérios necessários para que os EM possam recorrer à adoção de uma estratégia nacional de cibersegurança. Das últimas soluções emergenciais conferidas pela União Europeia, de março 2020 a março 2021, para diminuição das vulnerabilidades na cibersegurança foram as soluções Cloud, mas que requerem ainda trabalhos de elaboração legislativa, pois exigem um padrão de proteção mais elevado.

Na verdade, em resposta à pergunta de partida "De que forma a pandemia Covid19 veio alterar a cibersegurança na União Europeia, no período compreendido entre Março 2020-Março 2021?", a pandemia Covid19 trouxe novos desafios à cibersegurança, nomeadamente com o confinamento e o maior uso e desprotegido das TIC, com a intensificação de vulnerabilidades como o medo, a ansiedade, a pressão de tempo e de trabalho e o cansaço. Assim, com as medidas elaboradas pela União Europeia, o cidadão deve agora conseguir identificar uma ciberameaça, seja qual for o formato em que este se apresente. Deste modo, podemos também observar esta adaptação à cibersegurança foi por "tentativa e erro", em que o aumento de regulamentação objetiva e capaz de acompanhar os avanços tecnológicos e com a capacidade de responder a futuras crises é a única via para colmatar a perde de confiança dos utilizadores.

Conclui-se, pois, que a pandemia provocada pelo COVID19 veio alterar a perceção da ameaça digital; os Estados não estavam preparados para o aumento do tráfego comercial informativo a nível digital e foi através da qualificação da população no que concerne às competências digitais, a criação de infraestruturas digitais seguras e sustentáveis, a transformação digital das empresas e a digitalização dos serviços

públicos, acompanhados da cooperação internacional que os Estados-membros da União Europeia se adequaram, de março 2020 a março 2021, do ponto de vista estratégico da cibersegurança.

Em relação às hipóteses dispostas, esta investigação conclui que, existe uma maior aproximação à H3: Apesar da cibersegurança estar desde a apresentação da estratégia de segurança, em 2003, como um dos eixos estratégicos da União Europeia a pandemia veio revelar as vulnerabilidades da União Europeia face a esta ameaça. Para confirmar esta aproximação, documentos elaborados pela União Europeia, nomeadamente, a "Resolução do Parlamento Europeu sobre a Estratégia de Cibersegurança", tal como, "A via Europeia para a Década Digital" sublinham esta aproximação.

Concluindo, esta investigação abre ainda caminhos no âmbito de investigações futuras, nomeadamente o acompanhamento dos ciberataques e ciberterrorismo na União Europeia antes e após pandemia Covid19, para verificar se a regulamentação produzida pela UE e escrutinada no âmbito desta investigação será ou não eficaz.

Bibliografia

Alencar, M. N. (2015). Debates dos Estudos de Segurança Internacional e Segurança Humana: uma breve análise sobre a evolução dos Estudos de Segurança. *Conjutura Global*, *4*(2), 185–195.

Alkire, S. (2003). *A conceptural framework for Human security*.

Aparício, M. (2017a). *O Ciberespaço como Dimensão de Segurança*. Academia da Força Aérea.

Aparício, M. (2017b). *O CIberespaço como Dimensão de Segurança*. Sintra.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming. *Comparative Strategy*, 141–165.

Artigo19. (n.d.). *Da cibersegurança à ciberguerra*. 1–80.

Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., & Weiss, J. (2012). *Cyber Security - Policy Guidebook*.

Beavers, O., & Miller, M. (2020). Hospitals brace for increase in cyberattacks. *The Hill*. Retrieved from https://thehill.com/policy/cybersecurity/493410-hospitals-brace-for-increase-in-cyberattacks

Beláz, A. (2019). the Changing Role of the Eu in Cybersecurity. *Biztonságtudományi Szemle*, *1*(1-2.), 17–30.

Booth, K. (1991). Security and Emancipation. *Review of International Studies*, *17*.

Brown, I., & Veale, M. (2020). Cybersecurity. *Internet Policy Review*, *9*(4).

Buzan, B. (1991). *People, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era*.

Buzan, B., Waever, O., & Wilde, J. de. (1998). *Security- A New Framework For Analysis*.

Caldas, A., & Freire, V. (2013). Cibersegurança : das Preocupações à Ação Alexandre Caldas. *Instituto de Defesa Nacional*.

Carrapico, H., & Barrinha, A. (2018). *European Politics and Society European Union cyber security as an emerging research and policy field*. https://doi.org/10.1080/23745118.2018.1430712

Cavelty, M. (2010). Cyber-threats. In *The Routledge Handbook of Scurity Sctudies* (pp. 180–189). Londres.

Ceballho, G. (2021). *O mundo não está preparado para uma Ciberpandemia*. 133–138.

CNCS. (2019). *Quadro nacional de referência para a cibersegurança*.

CNCS. (2020a). *Cibersegurança em Portugal -Riscos e conflitos*. 1–104.

CNCS. (2020b). Ética & Direito. *Observatório de Cibersegurança*, 1–138.

CNCS. (2021). *Cibersegurança em portugal, Riscos & Conflitos*. 1–128.

Cocco, M., Barros, I. A., & Kindylidi, I. (2020). A nova estratégia da UE para cibersegurança e as novas regras de ciber-resiliência para entidades críticas. Retrieved from https://www.vda.pt/pt/publicacoes/insights/a-nova-estrategia-da-ue-para-ciberseguranca-e-as-novas-regras-de-ciber-resiliencia-para-entidades/22888/

Comissão Europeia. (2001). Proposta deDecisão-Quadro do Conselho relativa à luta contra o terrorismo. *Eur-Lex*.

Comissão Europeia. (2017). *Comunicação conjunta ao Parlamento Europeu e ao Conselho: Risiliência, dissuasão e defesa: reforçar a cibersegurança na UE*.

Comissão Europeia. (2020a). *A Hora da Europa: Reparar os Danos e Preparar o Futuro para a Próxima Geração*.

Comissão Europeia. (2020b). *Cybersecurity - our digital anchor - A European perspective*. https://doi.org/10.2760/352218

Comissão Europeia. (2020c). *Estratégia da UE para a União da Segurança*. *2014*, 1–31.

Comissão Europeia. (2020d). *Política para a Parceria Oriental para o pós-2020-Reforçar a resiliência - Uma Parceria Oriental em benefício de todos*. Bruxelas.

Comissão Europeia. (2020e). *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nivel comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148*. 12.

Comissão Europeia. (2020f). *Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à resiliência das entidades críticas*. 1–59.

Comissão Europeia. (2020g). *Um orçamento da UE que potencia o plano de recuperação da Europa*.

Comissão Europeia. (2020h). *Uma Estratégia para as PME com vista a uma Europa Sustentável e Digital*. 1–21. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0103&from=EN

Comissão Europeia. (2021). *Orientações para a Digitalização até 2030: a via europeia para a Década Digital*.

Confraria, J. (2020). Covid-19 e cibersegurança: o que ficámos a saber sobre as nossas decisões? *IDN - Especial Pandemia*.

Conselho da União Europeia, & Conselho Europeu. (2021). Cronologia – cibersegurança.

Conselho Europeu. (2001). eEurope 2002. https://doi.org/10.2807/esw.10.26.02738-

en

Conselho Europeu. (2014). *Convenção sobre o Cibercrime*.

Conselho Europeu, & Conselho da União Europeia. (n.d.). Cibersegurança: como combate a UE as ciberameaças. Retrieved from https://www.consilium.europa.eu/pt/policies/cybersecurity/

Custódio, M., Galindro, A., Martins, J., Pimentel, C., Rocha, J., & Silva, J. (2015). Sensibilização e Treino em Cibersegurança - exercício de recolha de informação -. *Proelium*, *7*(8), 163–178.

Cyberwatching.eu. (n.d.). Cybersecurity and Privacy Project Clusters - Health. Retrieved from https://www.cyberwatching.eu/cybersecurity-and-privacy-project-clusters/health

Delloite. (2020). COVID-19's Impact on Cybersecurity. *Deloitte*, (March). Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html

Dewey, J. (1922). *Human nature and conduct; an introduction to social psychology*. New York.

Duque, M. (2009). O Papel de Síntese da Escola de Copenhague nos Estudos de Segurança Internacional. *Contexto Internacional*, *31*(3), 459–501.

Echikson, W. (2020). Europe's Digital Verification Opportunity. *CEPS*. Retrieved from https://www.ceps.eu/ceps-publications/europes-digital-verification-opportunity/

ENISA. (2018). Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends. In *European Union Agency For Network and Information Security*. https://doi.org/10.2824/622757

ENISA. (2021a). *Cloud security for healthcare services*.

ENISA. (2021b). *Enisa Landscape for Supply Chain Attacks*. https://doi.org/10.2824/168593

Ernst & Young. *Cyber Security Resilience and Response throughout COVID-19 pandemic.* , (2020).

Esteves, J. A. (2015). Estudos de direito internacional: Formação e evolução do conceito de segurança. *Revista Direito Lusíada*, *XV*(2014), 51–98.

Europol. (2020). Pandemic profiteering: how criminals exploit the COVID-19 crisis. *European Union Agency for Law Enforcement Cooperation.*, (March), 2–13. Retrieved from https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Fernandes, A. (2014). *A dimensão política da Segurança para o Ciberespaço na União Europeia: A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE-*

OTAN. Universidade dos Açores.

Ferreira, M. (2016). A segurança humana. In *Segurança Contemporânea* (pp. 99–112).

Forbes Staff. (2020). Se calcula que hay un ataque informático en el mundo cada 39 segundos: ONU. *Forbes*. Retrieved from https://forbes.co/2020/05/22/actualidad/se-calcula-que-hay-un-ataque-informatico-en-el-mundo-cada-39-segundos-onu/

Freedman. (1998). International Security : Changing Targets. *Foreign Policy*, *Special Ed*(110), 48–63.

Geraldes, S. (2020). Covid-19 e cibersegurança: a mente humana como infraestrutura crítica. *IDN - Especial Pandemia*.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hermenegildo, G. (2020). *Cibersegurança na União Europeia e os seus desafios para a sua eficácia*. Universidade do Porto.

International Telecommunication Union. (2020). Global Cybersecurity Index (GCI). In *ITU Publications*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

ITU-T. (2008). *Series X: data networks, open system communications and security*. *1205*.

kaspersky. (2021a). Kaspersky Security Bulletin 2020-2021. EU statistics.

kaspersky. (2021b). O que é cibersegurança?

Kpmg. (2020). *Coronavirus and Cyber Security*. (March), 1–2.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the paandemic.* , (2020).

Leite, A. (2016). *A problemática da cibersegurança e os seus desafios*.

Lepassar, J. (2021). Cybersecurity to the Rescue: Pseudonymisation for Personal Data Protection. Retrieved from ENISA website: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-to-the-rescue-pseudonymisation-for-personal-data-protection

Lourenço, N. (2015). *As novas Fronteiras da Segurança- Segurança Nacional, Globalização e Modernidade* (pp. 26–37). pp. 26–37. Segurança e Defesa.

Marques, António Santos, L. (2020). Resiliência física versus resiliência digital. *IDN-*

Especial Pandemia.

Militão, O. P. (2014). *Guerra da Informação : a cibersegurança , a ciberdefesa e os novos desafios colocados ao sistema internacional*. Universidade Nova de Lisboa.

Miller, M. (2020). FBI sees spike in cyber crime reports during coronavirus pandemic. *The Hill*.

Nunes, P. F. V. (2020). A face digital da pandemia Covid-19: cibersegurança, ciberdefesa e resiliência nacional. *IDN - Especial Pandemia*.

Parlamento Europeu. (2013). *Estratégia da UE para a cibersegurança : um ciberespaço aberto , seguro e protegido*.

Parlamento Europeu. (2016). Regulamento (UE) 2016/679 - RGPD. *Jornal Oficial Da União Europeia*, *2014*(3), 1–119.

Parlamento Europeu. (2021a). *Recent cyber-attacks and the EU's cybersecurity strategy for the digital decade*.

Parlamento Europeu. (2021b). *Resolução do Parlamento Europeu sobre a Estratégia de Cibersegurança da UE para a década digital* (Vol. 2129).

Parlamento Europeu, & Conselho. (2016). Diretiva (EU) 2016. *Jornal Oficial Da União Europeia*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L2102

Parlamento Europeu e Conselho da União Europeia. (2019). REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEU E DO CONSELHO. *Jornal Oficial Da União Europeia*, *2019*(3).

Paulo, J. (2016). *Economia e Segurança: Públicas e Privadas* (Vol. 143).

Presidência do Conselho de Ministros. (2015). Estratégia Nacional de Segurança do Ciberespaço. *Diário Da República*, 3738–3742. Retrieved from www.dre.pt

Reis, F. (2017). *Segurança Humana e Responsabilidade de Proteger: A consolidação de um regime internacional de proteção em contexto de intervenção humanitária?* Universidade de Coimbra.

Rodrigues, J., & Mèrcher, L. (2017). *A Cibersegurança Americana e a Escola de Copenhague: Do paradigma da securitização ao caso de Edward Snowden*.

Rodrigues, J. V. (2021). Covid-19 abriu porta a uma "pandemia cibernauta." *Jornal Económico*.

Rudzit, G. (2005). O debate teórico em segurança internacional: mudanças frente ao terrorismo? *Civitas - Revista de Ciências Sociais*, *5*(2), 297–323. https://doi.org/10.15448/1984-7289.2005.2.5

Santos, Á. (2016). Segurança e Globalização: A Perspetiva dos Estudos Críticos de Segurança. *Proelium*, *7*(10), 107–114.

Santos, D. (2014). *A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança*. Instituto Universitário de Lisboa.

Seabra, P. (2016). Construtivismo e segurança. In *Segurança Contemporânea* (pp. 41–53).

Sousa, F. (2005). *Dicionário das Relações Internacionais*.

Sousa Teles, T. (2015). *Cibersegurança - Deteção de outliers*. Escola Naval.

Tanno, G. (2003). A Contribuição da Escola de Copenhague aos Estudos de Segurança Internacional. *Contexto Internacional*, *25*(1), 47–80.