Universidade de Lisboa

Faculdade de Direito

O CONTRIBUTO DA UNIÃO EUROPEIA PARA A SEGURANÇA DA INFORMAÇÃO: A PROTEÇÃO DA IDENTIDADE DIGITAL DOS CIDADÃOS E A POSIÇÃO SOBERANA DOS ESTADOS APLICADA AOS CONFLITOS NO CIBERESPAÇO

MÁRCIO JORGE FERREIRA GUIMARÃES
Nº 59041

CURSO DE MESTRADO EM DIREITO E CIÊNCIA JURÍDICA – ESPECIALIDADE DE CIÊNCIAS JURÍDICO-INTERNACIONAIS (2.º CICLO)

ORIENTADORA: PROFESSORA DOUTORA ANA MARIA GUERRA MARTINS

2020

Sê progressivo;
vê a sciencia porque ela te conduzirá á verdade
que tens por dever procurar

Autor desconhecido

Nada é falso que seja verdadeiro;
nada é verdadeiro que seja falso.
Tudo é o contrário de sonho, de mentira.

Isidore Ducasse
Poesias II

Agradecimentos

Neste longo e constante processo de aquisição de conhecimentos, onde tantas vezes somos levados a questionar a nossa própria capacidade de vingar nas análises e propostas científicas, cabe fazer um justo reconhecimento àqueles que nos iluminaram e souberam orientar o caminho no momento certo.

Em primeiro aos meus pais, Virgílio Guimarães e Emília Ferreira, onde não cabem palavras para descrever o agradecimento;

À memória do meu Avô,

Àqueles que nos momentos de felicidade, angústia, frustração me suportaram, entre eles família e amigos;

Aos professores, em especial, àqueles que contribuíram com o seu conhecimento e reflexões para aquilo que sou hoje, enquanto Ser, são a prova viva da emancipação do indivíduo;

À ProtectData, na pessoa da Ana Fazendeiro, que me ensinou e guiou no início de carreira.

Por último, uma palavra de agradecimento à Professora Doutora Ana Maria Guerra Martins pelo conhecimento transmitido durante o 1º ano do mestrado e pela orientação da tese de mestrado.

Ad vitam aeternam

Advertências e declarações

No presente trabalho o autor utiliza o novo acordo ortográfico, sem prejuízo das citações e/ou referências que podem ser evocadas no corpo de texto citado ou conjugações terminológicas que o autor de forma propositada considere necessário não utilizar o novo acordo ortográfico.

O autor recorre à norma APA, sem prejuízo de alterações introduzidas pelo guia da norma da revista eletrónica de Direito Público da Universidade de Lisboa, sendo estas visadas na rúbrica das "abreviaturas e siglas". Nesta última rúbrica o autor decidiu não incluir as abreviaturas ou siglas que vão sendo explanadas ao longo do corpo de texto ou em notas de rodapé, e cuja informação conste no mesmo local.

Tendo em conta o quadro temporal necessário para a realização deste estudo, a pesquisa para ulterior análise investigatória teve o seu término a 17 de outubro de 2019, sem prejuízo do autor invocar ou expressar orientações, jurisprudência ou entendimentos doutrinários considerados essenciais posteriores a essa data.

Esta dissertação de mestrado foi elaborada como requisito para obtenção do título de mestre em Direito e Ciência Jurídica na especialidade Ciências Jurídico-Internacionais pela Faculdade de Direito da Universidade de Lisboa.

É autorizada a citação mediante correta referência ao autor, visto que representa uma peça original e única como assim exige o requisito de avaliação curricular para obtenção do grau de mestre em Direito e Ciência Jurídica na especialidade Ciências Jurídico-Internacionais.

O autor, e exclusivamente o próprio, admite que o presente estudo ou parte deste possa ser submetido a concursos ou publicações científicas, com a devida identificação à finalidade primeira que se destinou.

Resumo

O estudo elenca o extenso quadro jurídico vigente sobre a segurança da informação no quadro da União Europeia. Sustentamos a ligação necessária entre a segurança da informação e a proteção de dados e, a cada vez maior dependência digital dos Estados, de onde se destacam as ameaças às infraestruturas críticas nacionais e a relevância das estratégias de cibersegurança dos Estados-membros da União. Identificamos o quadro dos direitos fundamentais aplicado à privacidade e segurança da informação, percorrendo ainda os instrumentos multinível de proteção jurídica que asseguram a proteção efetiva dos indivíduos no espaço europeu.

Ao nível dos conflitos no ciberespaço, analisamos os autores, níveis de intensidade, princípios, normas e conceções políticas que se impõe na Comunidade Internacional. Estudamos o papel da União Europeia e os dividendos cooperativos retirados da articulação com a NATO para o ciberespaço, defendendo a posição mediadora, mas autónoma na cena internacional, sob pena de não acompanhar os desafios tecnológicos emergentes.

Por último, identificámos as interações digitais diplomáticas dos Estados e analisamos o papel crucial da influência das informações nas relações internacionais, em especial o caso da Federação Russa.

Palavras-Chave: Segurança da Informação; Estados; União Europeia; Direito Internacional; Ciberespaço

Abstract

The study lists the extensive legal framework in force on information security in the framework of the European Union. We support the necessary link between information security and data protection and the increasing digital dependence of the States, from which the threats to national critical infrastructures stand out and the relevance of the cybersecurity strategies of the Member States of the Union. We identify the legal framework of fundamental rights applied to privacy and information security, also covering the multilevel instruments of legal protection that ensure the effective protection of individuals in European space.

At the level of conflicts in cyberspace, we study the authors, levels of intensity, principles, norms and political conceptions that prevail in the International Community. We study the role of the European Union and the cooperative dividends taken from the articulation with NATO for cyberspace, arguing the mediating but autonomous position on the international scene, under penalty of not following the emerging technological challenges.

Finally, we identified the diplomatic digital interactions of States and reviewed the crucial role of the influence of information in international relations, in particular the case of the Russian Federation.

***Keywords*:** Security of Information; States; European Union; International Law; Cyberspace

Abreviaturas e siglas

a.C- Antes de Cristo
AED- Agência Europeia de Defesa
AEPD- Agencia Española de Protección de Datos
AGNU- Assembleia Geral das Nações Unidas
AR/VP- Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança/Vice Presidente da Comissão Europeia
ASEAN- Associação de Nações do Sudeste Asiático
BDVA- Big Data Value Association
CDFUE- Carta dos Direitos Fundamentais da União Europeia
CEDH- Convenção Europeia dos Direitos do Homem
CEP- Cooperação Estruturada Permanente
CERT- Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores
Cfr.- Confira
CNCS- Centro Nacional de Cibsersegurança
CNU- Carta das Nações Unidas
COM- Comunicação
CSIRT- Computer Security Incident Response Team
CSNU- Conselho de Segurança das Nações Unidas
DDoS- Ataque de negação de serviço
DSP- Digital Signal Processin
DUE- Direito da União Europeia
ed./eds. – Editor/es
***EIXM*-** European Information Exchange Model
ENISA- European Union Agency for Cybersecurity
ERCC- Emergency Response Coordination Centre
ESLJ- Espaço de Segurança Liberdade e Justiça
***et alli*. –** E outros
EU- European Union
EUA- Estados Unidos da América
EU-LISA- Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça
EUMS- European Union Military Staff
EUROJUST- Agência da União Europeia para a Cooperação Judiciária Penal
EUROPOL- European Union Agency for Law Enforcement Cooperation
EUROSTAT- Serviço de Estatística da União Europeia
Ex:- Exemplo
FSB- Federal Security Service of the Russian Federation
GEG- Grupo de peritos governamentais
GSA- Global Navigation Satellite Systems Agency
HPCR- Humanitarian Policy and Conflict Research
IA- Inteligência Artifical
INTCEN- European Union Intelligence and Situation Centre
IoT- Internet of Things
IP- Endereço de Protocolo da Internet
ITU - International Telecommunication Union
JAI- Justiça e Assuntos Internos
MP- Ministério Público

N. – Número
NATO- North Atlantic Treaty Organization
NIS- Network and Information Systems
NU- Nações Unidas
OAS- Organização dos Estados Americanos
ONG´s- Organizações não Governamentais
ONU- Organização das Nações Unidas
op. cit- Referência supracitada
OPCW- Organisation for the Prohibition of Chemical Weapons
ORECE- Organismo de Reguladores Europeus das Comunicações Eletrónicas
OSCE- Organização para a Segurança e Cooperação na Europa
OSINT- Open-source intelligence
PCSD- Política Comum de Segurança e Defesa
PESC- Política Externa e de Segurança Comum
PME- Pequenas e Médias Empresas
PNR- Registos de Identificação dos Passageiros
PRISM- Program under which the United States National Security Agency
PUC-CPI- Ponto Único de Contacto para a Cooperação Policial Internacional
RGPD- Regulamento Geral sobre a Proteção de Dados
RpT- Responsável pelo Tratamento
SCADA- Supervisory Control and Data Acquisition
SEAE- Serviço Europeu de Ação Externa
SI- Segurança da Informação
SQL- Structured Query Language
SRI- Segurança das Redes e da Informação
TCP- Transmission Control Protocol
TEDH- Tribunal Europeu dos Direitos do Homem
TFUE- Tratado de Funcionamento da União Europeia
TI- Tecnologias de Informação
TICs- Tecnologias de Informação e Comunicação
TIJ- Tribunal Internacional de Justiça
TJUE- Tribunal de Justiça da União Europeia
TUE- Tratado da União Europeia
U.S- United States
UN- United Nations
v.- Ver

Introdução

O presente estudo desbrava o quadro jurídico vigente sobre a segurança da informação no quadro da União Europeia tentando interpretar de que forma o ator União protege a identidade digital dos cidadãos e, em caso de conflito no ciberespaço quais as normas e princípios para a adotar. Sustentamos de raiz a ligação necessária entre a segurança da informação e a proteção de dados e, a cada vez maior dependência digital dos Estados, bem como a importância das suas infraestruturas críticas nacionais e as estratégias de cibersegurança dos Estados-membros da União para o bem-estar e segurança dos cidadãos.

Verificamos o quadro dos direitos fundamentais aplicado à cibersegurança percorrendo os instrumentos multinível de proteção dos direitos que asseguram a proteção efetiva dos direitos dos indivíduos no espaço europeu. A União Europeia e os seus Estados-membros apresentam um amplo quadro cooperativo ao nível transatlântico, mas por força de decisões políticas e jurisdicionais estes acordos são alvo de crítica no sentido em que não asseguram a efetiva defesa dos direitos dos cidadãos da União. Verifica-se a preponderância do intercâmbio de informações entre os dois lados do atlântico e, nesse sentido, existe uma necessidade de prever e regular melhor por parte dos órgãos da União Europeia.

Definimos o ciberespaço como domínio onde a Comunidade Internacional pode entrar em conflito e, em particular, analisamos os autores e os níveis de intensidade, onde jaz a relevância interpretativa de termos clássicos do direito internacional adaptada ao ciberespaço de onde destacamos o princípio da devida diligência para a manutenção da paz e segurança internacional. Nesta senda, identificamos os instrumentos jurídico-políticos com os quais a União Europeia poderá atuar no ciberespaço e os dividendos cooperativos retirados da articulação com a NATO, defendendo a posição mediadora, mas autónoma da União na cena internacional, sob pena de não acompanhar os desafios tecnológicos emergentes.

Por último, debruçamo-nos sobre as alterações que se operam na vertente diplomática dos Estados por força da maior relevância da tomada de decisões baseadas na informação e na capacidade dos Estados, sendo que particularizamos a estratégia de influência da Federação Russa nas relações internacionais.

I- Segurança da Informação e Ciberespaço

1- Enquadramento introdutório

O desenvolvimento tecnológico evolui a um ritmo vertiginoso, os setores público e privado encetam todos os dias uma autêntica corrida *premium* pela informação, onde paralelamente são elencadas um conjunto de ameaças[1] multinível à segurança da informação e à proteção de dados. A União Europeia, através dos seus decisores políticos apresentou um quadro legislativo extenso nestas duas rúbricas, uma vez que a evolução tecnológica experienciada assim o impôs, regulando múltiplas áreas da sociedade e aspetos fundamentais da vida privada dos cidadãos[2].

A natureza amplamente multidimensional, interconectada e interdependente[3] das interações em rede no ciberespaço apresenta novos riscos e ameaças, a maior de todas – o "défice" de conhecimento humano[4] em matéria de tecnologias de informação e comunicação[5][6][7]. A consciencialização, capacitação e resiliência ao nível da segurança da informação em ambiente digital apresentam-se como os principais focos estratégicos de desenvolvimento das novas gerações e das sociedades em geral[8]. A dependência da

[1] Neste contexto, entendemos ameaça como qualquer ação que possa perturbar ou criar danos graves a um ativo de uma organização. Assim, os sistemas de informação podem enfrentar as ameaças naturais (ex: um grande desastre natural, um incêndio ou um furacão) ou as ameaças humanas, causadas por seres humanos num sistema (ex: vírus informático, introdução de código malicioso ou acesso a perfis não autorizado). Estas ameaças podem ser endereçadas de três grupos diferentes: 1) Pessoas individualmente consideradas; 2) Empresas; e 3) Organizações (que não empresas, como grupos).

[2] Murat Karaboga et. alli, Is There a Right to Offline Alternartives in a Digital World?, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Law Governance and Technology Series, N.º 36, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Springer, 2016, p. 48.

[3] A interdependência tecnológica é já um cenário sedimentado na Comunidade Internacional, a própria globalização é assente nas relações e cadeias de valor agregadas, sendo assim criadas fortes dependências ao nível económico.

[4] European Security and Defence College, *Hanbook on CSDP Missions and Operations the Commons an security and Defence Policy of the European Union*, Jochen Rehrl e Galia Glume (eds), 2015, p.197.

[5] Vicente Freire e Alexandre Caldas, *O Ciberespaço: Desafios à Segurança e à Estratégia*, *Segurança Internacional: Perspetivas Analíticas*, Imprensa Nacional-Casa da Moeda e Instituto de Defesa Nacional, Lisboa, 2013, p.81.

[6] Este fator pode ser enquadrado sobre o escopo tripartido entre: formação, treino operacional e sensibilização dos utilizadores para as TICs.

[7] Toda a revisão literária, nomeadamente através de indicadores concretos, apontam para que o risco associado ao ciberespaço tenda a aumentar e agudizar. Presumindo que a gestão associada ao risco cibernético será (num futuro próximo) uma ferramenta obrigatória a todos os operadores económicos com presença digital, sob pena de não conseguirem mensurar o risco associado aos seus negócios, pondendo este este constituir-se como o próximo desafio da década. Para mais informações, *v.* Marsh e Miscrosoft, 2019 Global Cyber Risk Perception Survey, 2019, disponível para consulta em: https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html.

[8] François Delerue, Xymena Kurowska e Patryk Pawlak, Reflections on the Pre-draft of the report of the OEWG on developments in the field of ICTs in the context of international security, in: *Research in Focus, EU Cyber Direct: Supporting EU Cyber Diplomacy*, 2020.

A limitação do conhecimento em matéria das TIC pode criar fossos e dependências sociais injustificáveis, nomeadamente no acesso a serviços essenciais garantidos pelos Estados. A estigmatização em relação à

pessoa humana em relação ao Estado está cada vez mais conectada à capacidade de acesso a uma máquina e a um ambiente virtual, entenda-se no ciberespaço - meio pelo qual ocorrem as interações e trocas de informação e comunicação[9]. Mas neste espaço virtual[10] é altamente volátil tendo em conta os riscos e ameaças existentes e emergentes (ainda que remotas e sempre presentes) que franqueiam a possibilidade da ocorrência de graves violações de segurança para os cidadãos e Estados, que por sua vez, podem comprometer valores fundamentais internacionalmente consagrados, constituindo uma ameaça no dia a dia do indivíduo[11].

A informação *just in time*, conjugada com a possibilidade de interação criada pelas máquinas digitais e alavancada pelo grande circuito de dados em massa (Big Data[12]) nas suas formas mais avançadas, tal como é o exemplo da Inteligência Artificial (IA[13])

digitalização deve ser combatida de forma a que todos os cidadãos de uma sociedade se possam sentir integrados.

[9] A digitalização dos Estados tem sido associada a uma série de conceitos, tais como e-Government, e-Services ou e-democracy, que marcam a presença digital dos Estados e a possibilidade de consulta de informações e serviços por parte dos cidadãos de acordo com as suas interações com a máquina estatal. Ott Velsber, Ulrika Westergren e Katrin Jonsson, *Exploring smartness in public sector innovation – creating smart public services with the Internet of Things*, in: European Journal of Information Systems, 2020.

[10] Hannes Ebert, Contested Cyberspace and Rising Powers, in: *Third World Quarterly*, Routledge, Vol. 34, N.º 6, 2013, p. 1054.

[11] Em 2019, um estudo levado a cabo pelo Eurostat revelou que 44% dos cidadãos da União Europeia obtiveram informações públicas consultando sites das autoridades públicas do seu Estado. Esta percentagem foi substancialmente superior aos 33% registados em igual período no ano de 2008. Existem já disparidades em termos de uso entre os vários Estados-membros da UE, este modelo de interação exige repensar as instituições, processos e mudanças comportamentais para que os serviços públicos sejam endereçados de forma mais eficiente aos cidadãos, por meio do uso de soluções em linha adequadas. No mesmo ano, a média Europeia de pessoas que utilizaram os serviços online dos governos nacionais foi de 44%, Portugal situa-se um pouco abaixo, ficando pelos 35%. Eurostat, *e-Government – more citizens consult information online*, 2020, disponível para consulta em: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20200307-1.

[12] Para um leitura aprofundada sobre a tecnologia *v*., Arvind Narayanan, Joanna Huey e Edward Felten, A Precautionary Approach to Big Data Privacy, In: *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Law Governance and Technology Series, N.º 34, Serge Gutwirth, Ronald Leenes e Paul De Hert (eds), Springer, pp. 357-381.

A maior parte dos negócios ou alguns órgãos dos Estados possuem métodos para recolha de dados como imagens, identificadores de radiofrequências ou impressões digitais de forma rápida. O vídeo e a voz são os maiores contribuintes para o crescimento da Big Data, já existem departamentos de polícia equipados com software contendo informações sobre infrações criminais, por área geográfica que conseguem prever a probabilidade de ocorrência de futuros crimes (*v*. Predpol, disponível para consulta em https://www.predpol.com/). Nesse sentido, *v*., Marco Mendola, One Step Further in the 'Surveillance Society': The Case of Predictive Policing, *Tech and Law Center*, 2016, pp. 2 e ss.

[13] O uso de IA, em particular as técnicas usadas em prol da cibersegurança e segurança da informação podem ser bastante úteis, veja-se o caso da utilização de algoritmos para resolução de problemas do dia-a-dia nos transportes ou hospitais, processos decisórios, regulação logística, regressão linear, filtros *spam*, deteção de fraudes no comércio online, registos de autenticações seguros, deteção e prevenção de entradas não autorizadas na Rede, entre outras aplicações que contribuiram para o be mestar e segurança dos cidadãos. Ramjee Prasad e Vandana Rohokale, Artificial Intelligence and Machine Learning in Cyber Security, In: *Ciber Security: The Lifeline of Information and Communication Technology*, Springer Series in Wireless Technology, Springer, 2020, p. 234-242.

proporcionou novas formas de viver em sociedade. A informação acedida via Internet tornou-se um recurso económico e uma fonte de dados necessária e valiosa para Estados, organizações e indivíduos, constituindo uma vantagem competitiva para aqueles que rentabilizarem a sua conceção à Rede[14].

O indivíduo deixou de ter capacidade de assimilação de todo o complexo tecnológico, por exemplo, veja-se a quantidade de novas aplicações diárias lançadas no mercado[15], a tipologia de tecnologia utilizada nos veículos, ou até mesmo a forma de projetar uma casa. Assistimos a uma despersonalização, no sentido me que deixamos de ter contacto imediato com uma pessoa física, para a digitalização ou se quisermos robotização, onde o processo decisório está associado a um algoritmo capaz de responder de acordo com as solicitações do requerente/ utilizador de forma a organizar o seu dia a dia[16]. Se, por um lado existe a possibilidade de controlar um imóvel através de um *smartphone*, por outro lado, também existe a possibilita de sofrermos um ciberataque que exfiltre os dados do nosso aparelho (ou qualquer outra máquina), constituindo-se então novas ameaças, às quais os prevaricadores (*hackers*[17]) do ciberespaço encontram-se atentos.

A União Europeia afirmou da aplicação integral da CDFUE à IA, "*Digital technologies, including AI, are essential for European digital sovereignty, security, innovations and economic development and can contribute significantly to the protection and promotion of fundamental rights and democracy and the rule of law* (...) no entanto "(...) *while digital technologies, including AI, present increasing opportunities and benefits, their design, development, deployment, and misuse may also entail risks to fundamental rights, democracy and the rule of law. Therefore, efforts are necessary to ensure that the respect for fundamental rights as enshrined in the Charter remains guaranteed*". O documento discorre sobre a aplicação dos direitos fundamentais aplicados aos valores enunciados no artigo 2.º do TUE. Conselho da União Europeia, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 2020, disponível para consulta em: https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.

Deste modo, a IA poderá ser uma dor de cabeça para os juristas. A IA é veiculada como uma potencial ameaça pela sua capacidade decidir à luz de determinadas funções algoritmicas, o que por si só gera controversia e um risco (pela sua conceção humana), por exemplo, na aplicação de IA à deteção e dissuasão de potenciais indivíduos que tenham como intenção perpetrar um ataque terrorista. Ora, se a aplicação de um determinado algoritmo falhar, em último caso podemos estar a criar máquinas de guerra, que podem matar humanos baseadas num algoritmo que não foi capaz de entender e calcular um padrão incalculável - a da dimensão humana, que não é percecionada por uma máquina. Nesse sentido, *v*. Global Challenges Foundation elenca a Inteligência Artificial como um dos riscos para 2020, para mais informações *v*., https://globalchallenges.org/wp-content/uploads/Global-Catastrophic-Risks-2020-Annual-Report-WEB-V2.pdf.

[14] Iguehi Ikenwe, Osahon Igbinovia e Ademakhe Elogie, Information Security in the Digital Age: The Case of Developing Countries, in: *Chinese Librarianship: an Internacional Eletronic Journal*, N.º 42, disponível para consulta em: http://www.white-clouds.com/iclc/cliej/cl42IIE.pdf.

[15] Entre o 3.º trimestre de 2016 e o 1.º trimestre de 2018, em média, foram lançadas 4828 aplicações diárias para o sistema Android. *v.* https://www.statista.com/statistics/276703/android-app-releases-worldwide/.

[16] No caso da administração pública existem projetos digitais com capacidade responsiva automática, encaminhando e respondendo às solicitações dos cidadãos, por exemplo, os balcões virtuais.

[17] O nome dado ao perpetrador individual do ciberataque é de *hacker*, por sua vez o fenómeno associado à personagem é de *hacking*.

À luz de outros desafios assumidamente internacionais, que ocupam as agendas internas dos governos, como por exemplo, os fluxos migratórios internacionais, as alterações climáticas, ou ainda os fenómenos extremos da natureza e perda biodiversidade, também os ciberataques, a conectividade e a gestão tecnológica[18] no curto - médio prazo inscrevem-se nas maiores preocupações dos líderes da comunidade internacional[19].

A informação é assumidamente o ativo mais importante no contexto da globalização e pós-globalização[20], sendo que os EUA percecionaram isso rapidamente ao integraram e criarem e desenvolverem a Internet, vindo mais tarde a liderar a sua *governance*[21]. A informação dispõe da capacidade de gerar poder, constituindo-se como fundamental para a sobrevivência das organizações e dos Estados, extravasa o domínio público e privado e é assente na competitividade e complexidade da Era digital[22]. Deste modo, as tecnologias[23] de informação e comunicação assumem um papel preponderante na concretização da aquisição e transferência de conhecimento que, concomitantemente geram uma cadeia de valor associada à modernização do espaço digital, em particular no que respeita aos modelos de negócio das organizações[24]. Devido à sua dimensão virtual, o ciberespaço não é da propriedade de nenhuma pessoa humana singular ou coletiva, e muito menos a sua gestão e governação, característica essa partilhada pelos utilizadores de Internet e, de um modo geral, pelos cibernautas a sociedade de informação global, sem prejuízo das disposições normativas dos Estados.

[18] European Strategy and Policy Analysis System e European Union Institute for Security Studies, *Global Trends to 2030: Challenges and Choices for Europe*, 2020, disponível para consulta em: https://www.iss.europa.eu/sites/default/files/EUISSFiles/ESPAS_Report.pdf.

[19]World Economic Forum, *The Global Risks Report 2020*, 2020, disponível para consulta em: https://www.weforum.org/reports/the-global-risks-report-2020.

[20] Como em qualquer área de negócio, a informação é considerada com um ativo com valor para a organização e para o mercado, pelo que deverá ser convenientemente protegida por medidas técnicas e organizativas.

[21] Hannes Ebert, *op. cit.* p.1054.

[22] Alastair Black e Rodney Brunt, Information Management in MI5 Before the Age of the Computer, *Journal Intelligence and National Security*, Vol. 16, Issue 2, 2010, pp.158-165.

[23] Neste sentido Christian Reus-Smit sustenta que "*(...) technology is usually listed among the material sources of state power. Yet technology itself reveals how problematic narrowly material conceptions of power are*". Christian Reus-Smit, Culture, Diversity and Technology, in: *Technologies of International Relations Continuity and Change*, Carolin Kaltofen, Madeline Carr e Michele Acuto (eds), Plagrave Macmillanm, 2019, p.72.

[24] Tridas Mukhopadhyay, Sunder Kekre e Suresh Kalathur, Business Value of Information Technology: A Study of Electronic Data Interchange, in: *MIS Quarterly*, Vol.19, N.º 2, 1995, pp.137-156.

2 Conceção preliminares

A Internet é uma rede descentralizada, multidireccionada e distribuída. Assenta em pontos dispersos de comunicação e uma multiplicidade de trajetos de informação enviados e recebidos para cada comunicação. Segundo a ITU, definimos Internet como "*A collection of interconnected networks using the Internet Protocol which allows them to function as a single, large virtual network*"[25][26].

O fluxo informacional associado a um determinado trajeto na Internet pode estar obstruído num determinado ponto, mas a comunicação de um utilizador pode escolher um trajeto alternativo ou redundante que não se encontre obstruído em nenhum ponto conservando desta forma o normal e corretamente funcionamento da comunicação na Internet[27].

O ciberespaço, apesar da sua associação ao digital, necessita de máquinas físicas (servidores, computadores, cabos, *routers*, entre outros) para operar, essas máquinas são consideradas a infraestrutura na composição das redes de comunicações eletrónicas, permitindo o armazenamento de informação, fornecendo os recursos computacionais sobre os quais os sistemas operam e permitem o tráfego de pacotes de dados na Internet[28].

2.1 Internet e ciberespaço

A ligação à rede (Internet) é uma realidade para mais de 2 biliões de utilizadores em todo o mundo, agregando uma utilização conjunta de atores tais como governos, sociedades, organizações e indivíduos. Não nos alongaremos sobre a história da Internet e do ciberespaço, pois este estudo não o permite, todavia não era justo ignorar alguns marcos históricos, por isso faremos algumas referências sumaríssimas. Neste seguimento, destacamos o surgimento da Internet, inicialmente em contexto militar, no auge da guerra

[25] International Telecommunication Union, Global Information Infrastructure terminology: Terms and definitions, *Y.101*, 2000, p. 37.

[26] De forma complementar, o dicionário tecnológico da universidade de Oxford dá-nos uma perspetiva holística da Internet: "*It is deliberately nonpolitical and tends to deal with nongovernmental levels within a country. The structure is informal, with a minimal level of governing bodies and with an emphasis in these bodies on technical rather than on administration or revenue generation."*. Oxford University, *A Dictionary of Comupting*, 2004, p. 269.

[27] David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, Lisboa, 2017, p.51.

[28] *Ibidem*.

fria, sendo depois desenvolvida no meio académico e, em meados dos anos 90, foi assumida mundialmente com a sua utilização em massa, sendo que o objetivo inicial não se desvirtuou até aos dias de hoje: comunicar através de uma máquina.

A rápida expensão da Internet na primeira década do séc. XXI proporcionou uma mudança no paradigma do *governance* da Internet, até então dominado pelos EUA, transitando para um sistema internacional uni-multipolar[29]. Estados como a República Popular da China ou a Federação Russa são agora atores com poder normativo no ciberespaço, com capacidades tecnológicas equivalentes aos EUA, que não procuram contestar as regras básicas ou princípios da ordem liberal, porém, tentam obter autoridade e liderança na ordem internacional[30].

Relativamente ao ciberespaço, ponto de vista epistemológico, foi William Gibson que utilizou pela primeira vez o termo em 1982, no conto *Burning chrome*, repercutindo-se mais tarde na comunidade matemática e em setores da psiquiatria, gerando termos associados, como "cibernética" e, por seu turno deram origem a termos comummente associados com o prefixo "ciber" associados à interação virtual e digital na esfera das TIC[31]. Se é certo que o ciberespaço aproximou continentes e pessoas, também é certo que a forma como os Estados atuam nele pode gerar grandes controvérsias e assimetrias nas relações internacionais, podendo mesmo ser um espaço que visa minar a verdade e semear a desconfiança nas democracias e nos sistemas constitucionais, por exemplo, através das técnicas de desinformação em ambiente digital[32][33].

Além das características supramencionadas do ciberespaço, importa ainda reconhecer que não existem fronteiras "digitalmente" definidas, sendo este domínio definindo como aterritorial. Por consequência, não existe uma jurisdição internacional para o ciberespaço, nem um tribunal internacional para os crimes perpetrados pela Internet, ao contrário do

---

[29] Samuel Huntington, Culture, Power and Democracy, in: *Globalization, Power, and Democracy*, Marc Plattner e Aleksander Smolar (ed), John Hopkins University Press, Baltimore, 2000, p.6.

[30] John Ikenberry, The Future of the Liberal World Order: Internationalism After America, in: *Foreign Affairs*, Vol. 90, N.º. 3, 2011, p. 56.

[31] Lino Santos, *op. cit.*, pp.60-63.

[32] Como introduz a ENISA, "*A key factor in the dissemination of online disinformation is human behaviour*", centrando o foco no comportamento da pessoa humana no ciberespaço. Adiante, atira "*In the digital era, where information is spreading around the globe in a few seconds, manual fact checking is not an effective and efficient way to address the problem of online disinformation*.". ENISA, *Strengthening Network & Information Security & Protection Against People Online Disinformation ("Fake News")*, 2018, disponível para consulta em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news/.

[33] O relatório informativo do Tribunal de Contas Europeu afirma que a desinformação "(…) *tem crescido em escala, rapidez e abrangência e constitui uma verdadeira ameaça de segurança para a União.".* Tribunal de Contas Europeu, *op. cit.*, p. 53-54.

que acontece nos domínios clássicos (terra, mar e ar). A capacidade de exercer coerção inter-estatal sobre este domínio é ainda um tema de debate entre académicos como se verificará nos próximos capítulos. O fluxo informacional, concretamente, dos dados, pode observar um complexo trajeto de comunicação na Rede, isto é, desde as coordenadas dos pacotes de dados enviados e recebidos entre um emissor inicial e o destinatário final. Com efeito, existe um desafio contemporâneo de averiguar em pormenor o trajeto informacional dos dados que tende a cruzar diferentes jurisdições[34].

2.2 Relações internacionais e segurança da informação no ciberespaço

Nas últimas décadas o desenvolvimento tecnológico tem sido notório e significativo para os Estados, num contexto altamente dinâmico, de elevada concorrência e competitividade para os decisores políticos. A União e os seus Estados-membros não foram exceção e, nesse sentido tentam formular estratégias à medida que as preocupações ao nível da SI vão surgindo[3536].

As preocupações com a recolha de dados pelas sociedades modernas são reconhecidas por todos, esta atitude veio mudar o paradigma do controlo dos dados e da informação, uma mudança que conduziu a uma maior preocupação coletiva com a privacidade e segurança da informação, ao mesmo tempo que se tenta conciliar e potenciar a economia digital e manter a segurança e bem-estar das populações[37]. Verificamos assim que Estados e organizações internacionais emitiram sinais de preocupação para com o ciberespaço, em especial, direcionando a segurança da informação, sem prejuízo das suas diferentes posições ao nível técnico e doutrinário[38].

---

[34] David Silva Ramalho, *op. cit.*, p.58.

[35] Parlamento Europeu, *Parlamento trabalha em prol da cibersegurança europeia (infografia)*, 2019, disponível para consulta em mais informações: https://www.europarl.europa.eu/news/pt/headlines/security/20190307STO30713/parlamento-trabalha-em-prol-da-ciberseguranca-europeia-infografia.

[36] Nesta senda, Lino Santos afirma que "*(...) informação atempada e de qualidade é fundamental para a tomada de decisão dos mais variados domínios* (…)". Lino Santos, *op. cit.*, pp. 65.

[37] Comissão Europeia, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme*, COM/2010/0171 final, disponível para consulta em: https://ipexl.europarl.europa.eu/IPEXL-WEB/dossier/document.do?code=COM&year=2010&number=171&extension=FIN&appLng=PT.

[38] Ao nível das Relações Internacionais os Estados adotam diferentes posições e terminologias em relação à segurança da informação em face da sua cultura histórica e daquelas que são as suas próprias perceções. A China entende que a segurança da informação "(…) *involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military,*

O complexo informacional vivido pode ser experimentado através dos equipamentos digitais que usamos no quotidiano, cada vez mais pequenos, mas cada vez com mais capacidades como a recolha, armazenamento, tratamento e partilha de informações, conjuntamente com a utilização de redes de comunicação que servem os mais diversos fins, entre os quais, os económicos, científicos, sociais e políticos[39].

2.3 A importância do TCP/IP

A forma de comunicação entre as máquinas na Internet operacionalizasse através do *Internet Protocol* (IP), baseando-se este numa lista de regras e métodos de comunicação, que assegura a transferência de dados entre redes e permite a conversão de dados de qualquer sistema informático ligado à Rede de forma a comunicar com sistemas diferentes de forma fluida e uniforme[40]. De forma prática, o *IP "*(...) *consiste num esquema de comunicação que define o modo como dados são enviados através da rede, o que faz essencialmente por duas vias: em primeiro lugar, fragmenta, quando necessário, os dados em pacotes de dados ou datagramas, nos quais se incluem, não só os dados da comunicação, mas também a origem e o destino da comunicação, entre outras informações; em segundo lugar, atribui um endereço numérico a cada sistema*

social, cultural and numerous other types of problems created by the misuse of information technology. Both of these factors are worthy of concern when studying the issue of information security". Paralelamente, a Federação Russa sustenta que a SI se relaciona com a "*Protection of the basic interests of the individual, society and the State in the information area, including the information and telecommunications infrastructure and information per se with respect to its characteristics, such as integrity, objectivity, accessibility and confidentiality*". Por sua vez, os EUA, através do National Institute of Standards and Technology, define a SI como "*The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability"*. No quadro europeu, o Reino Unido entende que a SI como "(…) *is also associated with the need to enforce international agreements on intellectual property (such as video and audio material, as well as computer software), so as to protect it from unauthorized copying and sale. Protection of privacy is yet another aspect of information security, that is, ensuring the security of personal and commercial information transmitted via the public international network or over private data links."*. De forma convergente, verifica-se um entendimento sobre os três objetivos ou princípios basilares da SI - a obtenção da confidencialidade, integridade e disponibilidade.
ONU, Submission to the United Nations General Assembly, Resolution A/62/98, p.7.; Russia, Submission to the United Nations General Assembly Resolution A/5 5/140, p. 3-4; United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 94.; United Kingdom, Submission to the United Nations General Assembly Resolution A/54/213, p. 12.

[39] Dário Moura Vicente e Sofia de Vasconcelos Casimiro, Data Protection in the Internet: General Report, in: *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law, Springer., Vol. 38, 2020, p.1.

[40] *Ibidem*, p.52.

informático ligado à internet (o Internet Protocol address ou IP adress), que poderá ser estático ou dinâmico[41]. Todavia, é necessária uma máquina intermediária que direcione o melhor caminho possível para transferir a mensagem (pacotes de dados), sendo o router[42] o responsável por essa função. Este redireccionamento pode transpor várias fronteiras de Estados – jurisdições para enviar a mensagem (pacote de dados, em forma de 0 e 1) ao recetor final.

Houve necessidade de robustecer a segurança da informação através de um novo protocolo, o protocolo de transporte - *Transmission Control Protocol* (TCP). Quando combinamos, *IP* e *TCP*, é concebido o TCP/IP, configurando a *arquitetura protocolar básica da Internet*, que garante o envio e receção de comunicações operacionalizando assim o tráfego de dados em rede[4344]. Estes protocolos configuram rotas virtuais que enviam e recebem dados, toleram perdas, duplicação, trancuras de datagramas *IP* através do descarte de datagramas inúteis e da retransmissão dos perdidos[45]. O problema prático do *TCP*/*IP* reside no facto dos dados serem legíveis dentro de cada pacote *IP* por via de um software disponível para qualquer pessoa (ex: Wireshark). Esta legibilidade de dados é conhecida pelo texto não criptografado (medida de segurança da informação).

Sob os princípios da segurança da informação, mesmo ao nível da ENISA, toda esta informação deverá ser ocultada ou criptografada, de modo a que os dados enviados dentro de um pacote *TCP*/ *IP* tornem o tráfego mais seguro, protegendo o nosso estilo de vida em ambiente virtual[4647].

---

[41] *Ibidem*, p.51.

[42] Como bem define o CNCS é um "*Equipamento de interconexão, instalado num nó de uma rede de computadores, que se destina a otimizar a transmissão de dados, determinando qual o melhor caminho que eles devem seguir*". Centro Nacional de Cibersegurança, Recursos, disponível para consulta em: https://www.cncs.gov.pt/recursos/glossario/.

[43] Sérgio Ferreira, *Sistemas de informação em Segurança*, Editora e Distribuidora Educacional S.A.,2017, p.51-52.

[44] As redes são categorizadas em função do seu alcance em: PAN (Personal Area network); LAN (Local Area Network), MAN (Metropolitan Area Network) e WAN (Wide Area Network).

[45] David Silva Ramalho, op. cit., pp.52 e ss.

[46] David Kim e Michael Solomon, *Fundamentals of Information Systems Security*, Information Systems Security, 3rd Edition, 2018, p. 51.

[47] As comunicações entre dois sistemas informáticos na rede funcionam segundo a regra do aperto de mão (*handsake*). Para mais desenvolvimentos nesta matéria, *v.* David Silva Ramalho, p. 55.

3 Princípios básicos da segurança da informação

A segurança da informação está intimamente relacionada com a capacidade de assegurar a tríade da *confidencialidade*, *integridade* e *disponibilidade* da informação de forma permanente e ininterrupta[48].

A confidencialidade assegura que apenas quem deve aceder o consegue fazer segundo uma escala de privilégios[49]. A integridade relaciona-se com a proteção da informação contra acessos não autorizados que possibilitem a modificação, tanto por conduta mal-intencionada ou negligente, portanto trata da validação da informação e da precisão da mesma[50]. A disponibilidade garante que a informação é usada e acedida apenas quando é necessária e de forma contínua[51].

A segurança da informação no contexto europeu também alterou o seu paradigma em termos legais e políticos, assim, o quadro regulatório contemporâneo teve em atenção os desenvolvimentos e capacidades tecnologias criadas, nomeadamente no que toca a boas práticas internacionais. As organizações ao longo dos anos tem adotado, sob uma perspetiva voluntarista, modelos de segurança da informação, pese embora não houvesse uma previsão obrigacionista neste sentido, o paradigma informacional alterou esta perspetiva. Passou a vigorar a imposição de medidas técnicas e organizativas (Secção 2 - Segurança dos dados pessoais - artigo 32.º do RGPD) para proteção e segurança da informação das organizações. Desta forma, uma organização é obrigada, à priori, a procurar de forma ativa e voluntária proteger a sua informação e os dados que se encontram sob a sua tutela, sob pena do quadro legal em vigor poder sancionar por omissão ou falta de evidências de medidas destinadas à promoção da SI[52].

---

[48] ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*, 2012, p. 4.
[49] David Kim e Michael Solomon, *op. cit*., p. 16-17.
[50] *Ibidem*, p.17.
[51] *Ibidem*, p.17-19.
[52] As evidências podem ser de vários tipos, entre os quais os próprios projetos de privacidade das empresas, códigos de conduta, implementação e verificação contínua dos controlos de segurança da informação através de normas implementadas (ex. ISO 27001 ou 27701), demonstração de investimento de equipamento que visa proteger a informação e os dados pessoais, entre outros exemplos que face a uma auditoria ou inspeção de uma autoridade de controlo pode ser demostrado como prova da ação da organização.

2.4 Política de Segurança da Informação

O impacto organizacional que uma quebra na segurança da informação pode ter no negócio é uma tarefa de análise complexa, mas que deve ser assegurada de forma preventiva. A existência de uma política de segurança da informação ou uma política de proteção de dados representa uma falha grave num dos controles de segurança mais importantes em qualquer organização, sendo a base da segurança da informação no planeamento das operações de uma organização[53][54]. O processo de elaboração e implementação de uma política de segurança da informação pode ser bastante complexo pela forma holística que deve ser estruturado, tendo em conta as especificidades das organizações, nomeadamente, deve ter em conta todos os ativos e agentes da organização de forma a que o resultado final seja a fotografia mais próxima da realidade da organização de modo a poder mitigar corretamente os riscos e gerir todo o ambiente digital[55]. A gestão da segurança dos dados associados aos processos de negócio é imprescindível, transformar a informação em conhecimento é altamente útil na Era dos dados, pois é este que gera a tomada de decisões estratégicas no seio das organizações[56][57]. No quadro internacional em geral observamos a normalidade acerca da produção de *guidelines* e orientações, como por exemplo, as boas práticas para a segurança da informação, para os sistemas de informação, ou ainda e as acreditações mais referenciadas, entre as quais se enquadram a National Institute of Standards and Technology (NIST), a International Organization for Standardization (ISO) ou a International Electrotechnical Commision (IEC). Ora, estas últimas enquadram os requisitos para sistemas de gestão da segurança da informação, nomeadamente, a norma

[53] Podemos afirmar que a falta de uma política de segurança da informação é um pecado capital nas organizações e tende a convidar os prevaricadores a penetrar nas suas informações, o que por sua vez, poderá levar à perda de valor e competitividade das organizações.
[54] David Kim e Michael Solomon, *op. cit*., p. 40-42.
[55] Por norma este tipo de implementação e revisão deve afetar todos os colaboradores das organizações, mas em especial, deve passar pelo cunho do gestor executivo da organização, departamento de *Compliance*, ou pessoa delegada da organização encarregue por esta matéria de forma a que também estes se sintam consciencientes da necessidade de alocar recursos e realizar investimentos nesta área.
[56] Luísa Santos e Mário Marques, Gestão de Risco Aplicada à Segurança da Informação, in: *CyberLaw by CIJIC*, Edição N.º VII, 2019,
[57] David Kim e Michael Solomon, *op. cit*., p. 40-44.

(ISO/IEC) 27.000[58] e, mais recentemente a norma (ISO/IEC) 27701[5960], que ligam a temática da segurança da informação conjugada à privacidade. Ambas são reconhecidas a nível europeu, tendo todas elas um objetivo comum que se prende com a proteção dos ativos de uma organização, mitigando as agressões, físicas ou lógicas, independentemente da sua origem (natural, acidental ou intencional)[61].

Quanto às estruturas e modelos de políticas de segurança da informação é necessário observar a estratégia de segurança da informação adequada em função do negócio ou missão da organização e os seus objetivos. A formulação e implementação de um processo ou modelo de SI pode diferir, dependentemente da doutrina associada a cada uma, todavia é transversal a todas elas as seguintes características abaixo descritas:

1) Identificar e avaliar os riscos dos ativos da organização;
2) Implementar os controlos das classes correspondentes (ex. tecnológicos e administrativos);
3) Elaboração de planos de contingência.

[58] Destacamos nesta família duas normas:

I. ISO/IEC 27001, define um modelo de gestão da segurança da informação para qualquer organização. Nesta norma são discriminados os requisitos necessários para estabelecer, desenvolver, operar, monitorizar, rever e melhorar o sistema de segurança da informação com enfoque na perspetiva do risco associado aos ativos das organizações. Cfr. Abhishek Chopra e Mukund Chaudhary, *Implementing an Information Security Management System Security Management Based on ISO 27001 Guidelines*, Apress.

II. ISO/IEC 27002, define um conjunto de práticas de segurança da informação (controlos) em diversas áreas tais como a definição de políticas de segurança, gestão de ativos, segurança física, ambiental e de pessoal, gestão de operações e comunicações, controlo de acessos, aquisição, desenvolvimento e manutenção de sistemas de informação, gestão de incidentes, continuidade de negócio e conformidade.

[59] A norma ISSO/IEC 27701 veio complementar o Regulamento Geral de Proteção de Dados (RGPD), pois veio assumir a gestão do sistema de informação relativo à privacidade. Na prática, são adicionados e alterados controlos à ISO/IEC 27001, para centrar o foco na privacidade e proteção dos dados e informação. Uma das inovações da ISSO/IEC 27701 refere-se à aplicação dos princípios enunciados no RGPD de *privacy by design* and *privacy by default*, adotando-se à nova realidade cibernética, criando estruturas complementares ao RGPD que elevam o nível de maturidade das estruturas de segurança e privacidade das organizações. Seguindo o exemplo de Lino Santos, uma inundação é classificada como uma agressão física de origem natural, por seu turno um ciberataque é classificado como uma agressão lógica de origem intencional. Lino Santos, *Enciclopédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (Cord), Almedina, 2015, pp. 65.

[60] A autoridade de proteção de dados da República Francesa (CNIL - *Commission Nationale de l'Informatique et des Libertés*), sustenta que a certificação das empresas com esta norma pode aumentar o nível de maturidade das organizações, contribuindo para a proteção de dados e privacidade, *v*. https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection.

[61] Lino Santos, *op. cit.*, p.423.

Os controlos de segurança da informação serão implementados após o conhecimento organizacional[62] e serão distribuídos de entre as seguintes áreas: a) física e ambiental; b) humana; c) tecnológica; e d) organizacional[63].

Um modelo de segurança da informação assume riscos reais em ambiente digital, tal como no domínio físico. Neste caso, o ambiente digital assume novas responsabilidades para os RpT pois são estes que detêm os dados sob a sua tutela, e nesse sentido devem assegurar as medidas técnicas e organizativas para cumprir as obrigações de segurança da informação atribuídas. Ainda assim, existe sempre, ainda que residual, uma probabilidade de violação da privacidade ou segurança da informação, pois em SI nenhum sistema é infalível.

Destacamos uma das metodologias mais avançadas no que concerne à gestão dos controlos em ambiente digital, que deriva do guia do *National Cyber Security Center* (NCSC) do Reino Unido[64], que apresenta um modelo (anexo A)[65] onde é possível percecionar o nível de maturidade da organização em termos de segurança cibernética e obter um valor de risco associado a cada controlo, de modo a poder priorizar investimentos nas organizações ao nível da segurança da informação e proteção de dados.

Em termos europeus houve um esfoço por parte dos órgãos e instituições para acompanhar a temática ao nível legislativo com a publicação de *hard law* ao nível da segurança da informação, segurança das redes, interoperabilidade digital, dados pessoais e privacidade.

Constatamos, por último, que caso um RpT ou mesmo um subcontratante não tome as devidas diligências para assegurar a confidencialidade, integridade e disponibilidade da informação (ou dados), poderá incorrer em sérias violações violação dos direitos fundamentais, estes últimos consagrados pelo Direito da União Europeia e pela Convenção Europeia dos Direitos do Homem.

---

[62] Envolve o conhecimento do ambiente e cultura organizacional, o modelo de gestão implementado (ex. ISSO/IEC 9001), a análise ao processo de negócios, a arquitetura dos SI, o volume e as categorias de dados tratados.

[63] José Martins et. alli, Modelo Integrado de atividades para a Gestão de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais, in: *CyberLaw by CIJIC*, Edição N.º V – 2018, p. 34-59.

[64] Para mais informações *v.*, https://www.ncsc.gov.uk/ e https://www.cpni.gov.uk/.

[65] O modelo de avaliação final de teste à resiliência pode ser consultado em: https://www.ncsc.gov.uk/blog-post/the-cyber-assessment-framework-3-0.

2.4.1 Risco

Nesta senda, não será menos importante a abordagem que terá de ser endereçada ao risco[6667]. A quantificação que resulta da avaliação do risco faz parte do *output* da segurança da informação, pois será este valor que irá definir quais os ativos que merecem maior atenção, tendo em conta o quadro de ameaças[68]. Os atores mal-intencionados no ciberespaço comportam uma série de riscos, por isso é necessário entender que a gestão de risco de uma organização ou de determinada sociedade, dependente cada vez mais da sua dependência em relação à conecção à Rede.

2.4.1.1 Das organizações

No quadro organizacional, é necessário observar que a segurança da informação é referente por um lado à proteção da informação e, por outro à proteção dos sistemas e infraestruturas.

Por norma, as organizações adotam modelos de certificação baseados em normas internacionais, como as normas *standard* ISO (ex: ISO/IEC 31000:2009 – "*Risk Managment – Principles and Guidelines*"[69]). A necessidade de avaliar o risco deriva da ponderação de tipos de ativos (internos e externos) da organização e da sua importância para o negócio, que carecem de uma análise de implementação, ou seja, de um *Processo de Gestão de Risco aplicado à Segurança da Informação* (PGRSI)[7071]. Este processo é

[66] Entendemos risco como a probabilidade de violação de segurança de um ativo. Pode ser entendido como o nível de exposição a algum evento que afeta o ativo (ex. um computador, uma folha de dados do excel). Entre outros exemplos de risco temos a perda de dados, uma trovoada que parou os sistemas da organização ou ainda o não cumprimento das leis e regulamentos. David Kim e Michael Solomon, *op. cit.*, p.11.

[67] Numa perspetiva matemática, o risco pode ser calculado através multiplicação entre as ameaças e as vulnerabilidades.

[68] David Kim e Michael Solomon, *op. cit*., pp. 60 e ss.

[69] O sistema cinco fases no processo: a) comunicação e consulta; b) âmbito; c) apreciação do risco; d) tratamento do risco; e e) monitorização e revisão.

[70] Luísa Santos e Mário Marques, *op. cit.*, p. 40-44.

[71] O Processo de Gestão do Risco de Segurança é " (1) Todo o processo de identificação, controlo e minimização de eventos incertos que tenham a potencialidade de afetar os recursos do sistema; (2) Processos de gestão de riscos de segurança aplicados para monitorizar, reduzir, eliminar, evitar ou aceitar riscos; (3) Todo o processo de identificação, controlo e minimização de acontecimentos indeterminados que possam afetar a segurança de determinada organização ou qualquer dos sistemas por ela utilizados. Este processo abarca todas as atividades relacionadas com o risco, designadamente avaliação, tratamento, aceitação e comunicação. Diretiva INFOSEC da OTAN sobre a gestão de sistemas de comunicação e informação, n.º AC/35-D/2005-REV2, de 10 de outubro de 2010; Diretiva Primária da OTAN sobre a segurança de sistemas de comunicação e informação n.º AC/35-D/2004-REV3, de 15 de novembro de 2013;

aplicado de forma transversal à organização, sendo que o objetivo último visa a minimização do impacto de uma determinada ameaça sobre a organização tendo em conta as vulnerabilidades e potenciais ameaças associadas[72].

A gestão do risco para além da sua natural mitigação, prioriza esforços no sentido de poder distribuir de forma correta os recursos organizacionais. Após uma adequada avaliação de risco, o decisor organizacional com a competência na tomada de decisões nesta matéria, deverá optar por um de três caminhos:

1) Mitigar o risco[73];
2) Transferir[74] o risco ou;
3) Assumir[75] o risco, ou um valor de risco para uma determinado ameaça.

Quando existe uma falha na gestão do risco pode afetar gravemente o negócio e impedir o normal funcionamento da organização, ou mesmo interromper por completo a atividade, sendo, para isso necessário recorrer aos controlos prévios implementadas na organização para proteger a própria atividade e recursos – Avaliação de Impacto[76]; Plano de continuidade de negócios[77] e Plano de recuperação de desastres[78].

Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE e Decisão (UE, Euratom) n.º 2015/444 da Comissão de 13 de março de 2015 relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE.

[72] No decorrer do processo podem ser apresentadas Matrizes de impacto de forma a calcular se o nível de risco é alto, médio ou baixo.

[73] A mitigação do risco passa pela implementação de um conjunto de medidas tendo em vista a ameaça, tendo como principal objetivo a diminuição da probabilidade desta se concretizar numa violação de segurança. Existe um extenso leque de medidas de mitigação que englobam as políticas aceitáveis de uso de recursos informacionais da organização, avaliações de impacto a sistemas e programas de software e sistemas de videovigilância, de forma geral segurança perimétrica física e lógica, ou um ainda mecanismo de redundância ativa e passiva de sistemas.

[74] A transferência do risco pode ser assegurada por salvaguarda dos dados ou, por via contratual, como por exemplo, entre uma organização e uma seguradora, de forma a transferir o risco dos ativos (mais importantes) da organização para a seguradora, procurando recuperar ou reduzir o prejuízo resultante de uma eventual quebra ou violação de segurança.

[75] Uma organização após o resultado do cálculo do risco pode decidir assumi-lo e optar por não adotar nenhum dos caminhos anteriormente apresentados e, naturalmente assumir que a perda poderá ser total.

[76] O primeiro passo aqui versa sobre a análise da atividade da organização e sobre o entendimento de quais as funções vitais para a atividade continua e ininterrupta da organização. Uma análise a todas as funções permite classificar entre críticas e não críticas para a continuidade das operações da organização. Se uma função crítica falhar pode comprometer o normal funcionamento da organização, deste modo é importante realizar uma avaliação de impacto na organização para entender quais as funções primárias a repor e, qual a sua ordem de importância para o plano de continuidade de negócios e plano de recuperação de desastres.

[77] O plano de continuidade de negócios é um plano de resposta estruturado para qualquer evento do qual resultem interrupções das operações ou de uma função crítica de uma determinada organização. Este plano assenta na intervenção em processos, recursos, equipamentos e dispositivos prevendo uma intervenção quando ocorra um evento que afete de forma crítica a viabilidade do negócio e, deste modo também é da máxima importância o estabelecimento de prioridades.

[78] O plano de recuperação de desastres é direcionado para as ações a tomar após um desastre. Tecnicamente, este plano é parte integrante do plano de continuidade de negócios, pois o restabelecimento dos recursos de

A promoção da educação e consciencialização generalizada na sociedade civil para a segurança da informação, sempre sob o escopo de garantia da confidencialidade, integridade e disponibilidade[7980]serve como ponto de partida importante para alertar para os perigos no ciberespaço.

2.4.1.2 Do Estado

Do ponto de vista estatal as preocupações associadas ao risco visam essencialmente as infraestruturas críticas nacionais, pois são estas que asseguram a segurança e o normal funcionamento do estilo de vida das pessoas em sociedade[81]. Pensemos nos efeitos nefastos que um ator mal-intencionado que, por hipótese, lançava um *malware* para um central elétrica e no seu código estava programado para desconfigurar vários controlos na distribuição da rede elétrica nacional que originava constantes sobrecargas energéticas, obviamente, para além dos potenciais *danos físicos*, existiriam os *danos reputacionais* (neste caso ao nível político – diplomático), quer ao nível da confiança das pessoas na instituição e no próprio ciberespaço.

O Estado pela sua competência reguladora e pelo exercício soberano sobre as infraestruturas críticas nacionais (físicas) localizadas no seu território, pode e deve ir mais além do que as organizações, utilizando as suas competências para detetar e reprimir criminosos no ciberespaço, assim como na definição do mínimo denominador comum a toda a sociedade por via de uma estratégia de cibersegurança nacional adequada à sua realidade. Convocamos ainda a função pedagógica de consciencialização digital dos cidadãos de forma a sensibilizar, educar e formar o indivíduo e as organizações para o risco[82].

---

negócios é necessário para a passagem à segunda fase suportada pelo plano de continuidade de negócios. Assim, este plano é uma extensão do anterior supramencionado, identificando pormenorizadamente os recursos necessários para apoiar cada função do negócio. A principal diferença entre estes dois últimos versam sobre o impacto causado pelos eventos na organização. Deste modo, um plano de continuidade de negócio não está programado para responder a uma grande interrupção temporal, pelo que, a afetação do negócio e os recursos a restabelecer apresentam uma previsão muito mais detalhada no plano de recuperação de desastres. David Kim e Michael Solomon, *op. cit*., USA, 2018, p. 115-122 e p. 251 e ss.

[79] Center for Digital Strategies: Tuck at Dartmouth, Cyber/information Security in the Digital Age: A Roundtable Overview European Chapter Discussion, in: *Roundtable on Digital Strategies*, p. 4 e ss.

[80] Tribunal de Contas Europeu, *Desafios à eficácia da política de cibersegurança da UE*, 2019, pp. 42-43.

[81] Paulo Moniz, Impacto do Ciberespaço na Sociedade em Rede, Contributos para uma estratégia nacional de ciberdefesa, in: *idn cadernos*, 2020, p. 21-22.

[82] *Ibidem*, p.22-23.

A proteção e defesa do ciberespaço necessitam de comportamentos atinentes à segurança da informação por todos os seus atores, desde o cidadão, às organizações e Estados, estimulando uma *cultura de segurança informacional* e, por sua vez, promovendo a maturidade e resiliência para a mitigação do risco.

2.5 Cibersegurança

A cibersegurança é entendida como um conceito fundamental na análise que levamos a cabo. Deste modo, a ENISA, qualifica a cibersegurança como "(…) *comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats*.", desdobrando-se em subconjuntos como a segurança da informação e segurança das redes[83].

Seguindo Lino Santos, o termo cibersegurança, surge em meados dos anos 90, para referir-se à segurança do ciberespaço de novos atores e ameaças, independentemente do objeto da cibersegurança visar o Estado, as organizações ou os indivíduos[84][85]. Os Estados procuram assegurar a sua competência em relação à regulação da cibersegurança a par das normas internacionais no seu espaço soberano, sendo que (e para tal) contratam meios e capacidades para aplicar em matéria de proteção e prospeção no ciberespaço, contribuindo para o bem-estar e segurança quer das infraestruturas nacionais (operações

[83] Do ponto de vista técnico temos que*: Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security)*". ENISA, *ENISA overview of cybersecurity and related terminology*, 2017, disponível para consulta em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

[84] Lino Santos, *op. cit.*, pp.63-66.

[85] Achamos pertinente apresentar alguns números apresentados pelo EUROSTAT , que nos dizem que em 2016, os *smartphones* foram os dispositivos mais utilizados, conforme relatado por 79% dos utilizadores de Internet na UE, 64% disseram utilizar um *laptop*, 54% computadores fixos e 44% usaram um *tablet*. Relativamente às empresas, o estudo retira que 7 em cada 10 empresas da UE utilizam banda larga móvel e 7 em cada 10 empresas da UE fornecem dispositivos portáteis aos seus trabalhadores. Em 2017, metade de todos os colaboradores da UE usava um computador com acesso à Internet. Essa participação foi um pouco maior nas grandes empresas (54%) do que nas PME (49%). EUROSTAT, *Digital economy and society – Overview*, disponível para consulta em: https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-1a.html.

defensivas) quer para uma eventual contra–resposta de atores mal intencionados (operações ofensivas)[86].

Paralelamente, os Estados, para além da vertente securitária na prevenção dos ativos críticos nacionais, apresentam responsabilidade no apoio e desenvolvimento às estruturas económicas e sociais, tendo para tal que agregar valor aos privados, auxiliando-os e permitindo que estes possam desenvolver as suas estratégias comerciais sem ver comprometidos os princípios básicos da SI[87].

Lino Santos elenca os grandes domínios do Estado, e de forma geral, da sociedade civil para lidar com a cibersegurança (ou falta dela), sendo eles: *a proteção simples*, a *prossecução criminal*, a *guerra* e a *diplomacia*[88].

Seguindo o autor, na *proteção simples*, devem ser observados os meios técnicos, processuais e humanos, que operacionalizam diariamente as componentes preventiva, reativa e de gestão de qualidade de segurança. Estes asseguram a linha da frente da proteção das infraestruturas, dos serviços vitais e do conteúdo da informação presente no ciberespaço, elencando assim uma co-responasibildiade da segurança no ciberespaço. Neste domínio inscrevem-se atores do setor público e privado que fornecem e gerem *software*, *hardware* e *sistemas*; a Academia; as redes CSIRT; e, no seu último desiderato o utilizador final, responsável pela boa conduta das regras de segurança em ambiente digital[89].

O ciberespaço não é um domínio alheio ao crime e aos ilícitos criminais. A perpetração de ciberataques configuram atos relevantes contra Estados, organizações e pessoas singulares, passíveis de ação penal, quer do ponto de vista dos crimes contra pessoas (ex: pornografia, *sexual arrestment*, crimes de ódio, crimes contra a honra), contra interesses patrimoniais (ex: violação de direitos de autor, burla informática) ou, contra dados e

[86] *Ibidem*.

[87] Pese embora o âmbito de aplicação (público vs. privado), temos assistido desde os finais dos anos 90´ a um quadro regulatório que vem se adaptando à luz dos acontecimentos. Por exemplo, em matéria de proteção de dados tivemos a Diretiva 95/56/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 e a Diretiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996. De forma semelhante, também os serviços eletrónicos vieram ganhando relevância, resultando num quadro legislativo europeu protecionista para o consumidor, com a Diretiva 98/84/CE do Parlamento Europeu e do Conselho de 20 de novembro de 1998, ou a Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000. Estas Diretivas viriam a relevar a sua extrema importância, mesmo até aos dias de hoje, subsistindo no quadro jurídico europeu, ainda que revogadas.

[88] Lino Santos, *op. cit.*, pp.60-63.

[89] *Ibidem*, p.65.

informação (ex. falsidade informática, dano informático, sabotagem informática, acesso ilegítimo, acesso indevido) configurando o cibercrime[90].

Relativamente à defesa do Estado, a capacidade de operação de um Estado no ciberespaço revela-se fundamental do ponto de vista da vantagem competitiva, ou pelo menos, no campo de batalha, dado que a modernização e aquisição de capacidades de defesa ao nível cibernético é já uma realidade fortemente adotada pelas grandes potencias mundiais. Neste domínio a vantagem competitiva revelasse importante no sentido em são abertas possibilidades de substituir vidas humanas por máquinas em tarefas de alto risco (ex. envio de *drones* para o reconhecimento do campo de batalha geridos por uma estrutura de comando e controlo[91]).

Por último, no domínio diplomático importa verificar do ponto de vista das relações internacionais quais as interações a decorrer entre Estados. Para tal, considera-se necessário verificar as ações dos Estados, por exemplo, ao nível da capacitação das suas infraestruturas críticas nacionais, o acompanhamento das últimas tendências tecnológicas[92] nível mundial, e as alterações de poder entre os grandes *players* tecnológicos. Reveste a máxima importância e interesse nacional entender as mensagens transmitidas nos *fora* de tecnológicos e de privacidade, verificar as cadeiras de poder (económico), os centros estratégicos e de defesa (como o desenvolvimento de armamento tecnológico), ou ainda percecionar se existem exercícios conjuntos e coordenados entre Estados, como por exemplo acontece ao nível da União[93]. O próprio Conselho da União Europeia, aquando da revisão do Quadro Estratégico da UE para a ciberdefesa afirmou que "*os instrumentos de ciberdiplomacia foram desenvolvidos tendo em vista contribuírem para lograr essa resposta mútua*.", no sentido de responder às atividades maliciosas no ciberespaço e promover a cooperação mútua entre os Estados-membros, ficando a cargo do SEAE e da AED a organização de exercícios regulares baseados nos instrumentos de ciberdiplomacia[94]. A harmonização da ciberdefesa só seria possível através de um conceito comum e agregado sobre o âmbito de aplicação da ciberdefesa,

[90] Em Portugal, o cibercrime, e por sua vez, a recolha de prova digital cabe na competência de investigação criminal atribuida à Política Judiciária. Para mais desenvolvimentos sobre a recolha de prova em ambiente digital *v*. https://www.policiajudiciaria.pt/unc3t/.

[91] Lino Santos, *op. cit.*, p.66.

[92] *V.* Anexo 4.

[93] Por exemplo, a ENISA promove regularmente este tipo de exercício entre Estados-membros, inserindo no capítulo da capacitação, *v.* https://www.cyber-europe.eu/.

[94] Resolução do Parlamento Europeu, de 13 de junho de 2018, sobre ciberdefesa (2018/2004(INI)), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IP0258&from=EN.

estabelecendo um certo grau de convergência estratégica entre os Estados-membros da União na fase do planeamento das necessidades em matéria de ciberdefesa, o que não se perspetiva como cenário futuro ao abrigo da PCSD, podendo antes passar pelas iniciativas multilaterais entre Estados ao nível da CEP, como adiante analisaremos.

3 As políticas da União Europeia para a segurança da informação

Enquanto que na época da guerra fria vigora um cenário de escassez de informação, contemporaneamente o paradigma mudou, a informação emerge de várias fontes, e obriga a um refinamento e tratamento crítico, sob pena de um *overlap* informacional. Nos últimos anos, a referência à guerra cibernética, ciberterrorismo[95], guerra da informação, ciberespionagem[96], diplomacia digital, entre outras ligadas ao léxico "ciber" tem sido uma constante experimentada em diversos *fora*, predominantemente da vertente política e militar[97].

A título meramente introdutório e para se melhor compreenda a realidade neste domínio, em 2016, o mercado de cibersegurança da UE foi avaliado em 20,1 bilhões de euros, mesmo assim, este é um número ainda baixo quando comparado com outras regiões do mundo. Enquanto que a taxa de crescimento anual composta do mercado interno da UE

[95] Numa prespetiva holística, "(…) *refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide. There is a general progression toward greater damage and disruption from the first to the third category, although that does not imply an increase of political effectiveness."*. Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Georgetown University, p.3.

[96] "*Cyber espionage should be viewed as an extension of traditional espionage. It allows a hostile actor to steal information remotely, cheaply and on an industrial scale. It can be done with relatively little risk to a hostile actor's intelligence officers or agents overseas*.". MI5, *Cyber*, Disponível para consulta em: https://www.mi5.gov.uk/cyber. A ENISA, complementa quanto às motivações, "*Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weak cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partners*". Segundo a mesma fonte, entre janeiro de 2019 e abril de 2020, 63% dos incidentes de *phishing* na UE derivaram de ciberespionagem. A tendência é contínua. ENISA, *Cyber espionage ENISA Threat Landscape*, 2020, p. 3.

[97] Em 2017, a ENISA tinha alertado para o rompimento das tradicionais ameaças e o aumento significativo das novas ameaças em ambiente digital como a espionagem cibernética ou ataques a infraestruturas críticas de segurança com *ransomware* e *malware*, dirigido a instituições democráticas e órgão políticos. ENISA, ENISA Threat Landscape Report 2017, 2017, disponível para coinsulta em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

da indústria de segurança cibernética é de 6% ao ano, as outras principais regiões que servem de referência para a União apresentam uma taxa de crescimento de 8% ao ano[98].

4. Quadro jurídico-político europeu

No que toca ao quadro legislativo europeu, os órgãos e instituições da União vem se adaptando à medida que as TIC se desenvolvem e, por sua vez, atuam no exercício da regulação comunitária, tendo em visa a melhoria continua da segurança da informação, quer no mercado único digital, quer no ESLJ e, em geral, por todas as esferas de atuação dos cidadãos europeus.

Em 2009, com as constantes preocupações elencadas por ciberataques, a Comissão Europeia emitiu uma comunicação sobre a Proteção das Infraestruturas de Comunicação e Informação, onde lançou uma proposta de plano de ação operacional que previa as ações e modelo de atuação para reforçar as estratégias e cooperação ao nível europeu, incluindo a ENISA e as redes CSIRT como preponderantes neste capítulo[99].

4.1 Abordagem da União Europeia à Cibersegurança

Os serviços de redes, sistemas de informação e comunicação em paralelo com as infraestruturas críticas nacionais consideram-se vitais para o bem-estar social, segurança física e económica na comunidade europeia. Por essa via, a cibersegurança revela uma importância de destaque para o nosso estudo, assim como as interações que ocorrem no

[98] Estima-se que cerca de 20 biliões de equipamentos IoT possam estar operacionais no corrente ano de 2020, potenciando um quadro de novos ricos e ameaças emergentes por via da introdução destes dispositivos no nosso dia a dia. Desde 2005, iniciou-se por intermédio da Comissão Europeia uma discussão multilateral com diversos intervenientes, desde Estados-membros, indústria, ONG´s, consultores, entre outros sobre os aparelhos IoT e o seu futuro. Paralelamente, alguns Estados-membros nas suas Estratégias nacionais tinham já abordado o tema. Para mais desenvolvimentos, *v.* Murat Karaboga et. alli, *op. cit.*, pp. 48 e ss.

[99] Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*", 2009, disponível para consulta em:https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

ciberespaço visto que este começa a definir-se como um domínio de perpetração de crimes de forma cada vez mais acentuado[100][101].

As preocupações políticas e regulatórias associadas à cibersegurança iniciaram-se nos anos 90, onde o paper "*Competetiveness and Employment. The challenges and Ways Forward into the 21st century* "[102] e o "*Report on Europe and the Global Information Society"*[103] mencionavam o quão essencial era a segurança no ciberespaço a par da conclusão do mercado único[104]. As preocupações à época (assim como as contemporâneas) aludiam, predominantemente ao potencial impacto económico derivado da partilha de conteúdo ilícito na Internet e à perpetração de crimes tecnológicos neste domínio[105].

A União Europeia tem publicado Regulamentos, Diretivas e outros instrumentos de *softw* law, como recomendações ou opiniões, muita matéria normativa e semi-normativa que visa contemplar a necessidade de resiliência das estratégias de cibersegurança nacionais, concertando uma ambição de alinhamento homogéneo entre todos os Estados-membros[106].

Neste campo, as estratégias nacionais de cibersegurança devem seguir uma abordagem holística *bottum-up* e acompanhar as boas práticas e as últimas orientações europeias – geralmente, trabalho elaborado pela entidade europeia independente em matéria de segurança da informação, a ENISA.

---

[100] Quanto aos crimes destacamos o ciberterrorismo e o crescimento de grupos extremistas de direita e a sua propaganda via das plataformas digitais. EUROPOL, *European Union Terrorism Situation and Trend Report 2020*, 2020, disponível para consulta em: https://www.europol.europa.eu/tesat-report.

[101] Cfr. ISS, *Yearbook of European Security*, 2019, pp. 92-93, disponível para consulta em: https://www.iss.europa.eu/content/euiss-yearbook-european-security-2019.

[102] Comissão Europeia, *Growth, competitiveness, employment: The challenges and ways forward into the 21st century*, 1994, disponível para consulta em: https://op.europa.eu/en/publication-detail/-/publication/0d563bc1-f17e-48ab-bb2a-9dd9a31d5004.

[103] Parlamento Europeu, *Report de 16 de julho de 1996*, 1996, disponível para consulta em: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1996-0244+0+DOC+XML+V0//EN.

[104] Helena Carrapico e André Barrinha, The EU as a Coherent (Cyber)Security Actor?, in: *Journal of Common Market Studies*, Vol. 55, N.º 6, 2017, p. 1259.

[105] *Ibidem*.

[106] De salientar que os instrumentos de natureza técnica e política orientam a visão de cibersegurança dos Estados–membros. Nesse sentido, a União apresenta uma abordagem comunicacional holística, fê-lo na estratégia global da EU; na agenda europeia para a cibersegurança; no quadro comum em matéria de luta contra as ameaças híbridas; na comunicação «Lançar o Fundo Europeu de Defesa»; na comunicação sobre o Estado da União em 2017 – «Cybersecurity: Commission scales up EU's response to cyber-attacks», e em subsequentes comunicações. Esta abordagem demostra a maturidade e a consciencialização estratégica deste ator. Todos estes documentos apresentam um objetivo comum para todos os Estados-membros – a mitigação do risco associada às ameaças de cibersegurança.

Com preocupações de ordem securitária, nomeadamente com fenómenos terroristas em solo europeu, alguns Estados da União lançaram as suas estratégias de cibersegurança, ou pelo menos documentos preparatórios. Em 2004, a ameaça aos sistemas de informação e comunicação, principalmente, provenientes de atores não estatais expuseram as vulnerabilidades da União. Em 2005, a Alemanha lançou o "*National Plan for Information Infrastructure Protection* (NPSI)[107]", no ano seguinte a Suécia publicou a "*Strategy to improve Internet Security in Sweden"*[108]. A União, perante tais acontecimentos decidiu alterar o a sua abordagem, alargando o quadro legal diretamente vinculativo para os Estados-membros. A coerência passou a ser ponto-chave, a UE decidiu seguir uma estratégia que aliava a autonomia de cada um dos Estados-membros às suas perceções relativamente aos riscos internos e partilhados[109][110]. Em 2007, o ataque cibernético de graves proporções às redes e infraestruturas críticas da Estónia, convocou uma tomada de decisão do governo da Estónia relativamente à cibersegurança e, consequentemente, veio a adotar uma estratégia para a segurança da informação e cibersegurança como nenhum Estado da União antes o fizera. Posteriormente, a Comissão Europeia reforçou o nível de compromisso em matéria de cibersegurança com os Estados-membros[111][112][113]. Corria o ano de 2011, e a República Checa, França, Alemanha, Lituânia, Luxemburgo, Países Baixos e Reino Unido publicaram ou reviram as suas estratégias internas[114]. Nas últimas duas décadas, todos os Estados da União lançaram

[107] Cfr. Federal Ministry of Interior, *National Plan for Information Infrastructure Protection*, 2005, disponível para consulta em: https://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf.

[108] Cfr. Government Offices of Sweden, *A national cyber security strategy*, 2016, Disponível para consulta em: https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

[109] Helena Carrapico e André Barrinha, *op. cit*., p. 1260.

[110] Por sua vez, na Diretiva NIS, um dos pontos chave é o alinhamento entre os Estados-membros para garantir uma abordagem coerente na definição de *operador de serviços essenciais*, *v*. ponto 19, artigo 4.º, n.º 4 e Anexo III da Diretiva NIS.

[111] Ministry of Defence, Cyber Security Strategy Cyber Security Strategy Committee, 2008, disponível para consulta em: http://www.sicurezzacibernetica.it/db/[Estonia]%20%20National%20Cyber%20Security%20Strategy%20-%20old%20-%202008%20-%20EN.pdf.

[112] Na lista de Estados com ciberataques no mapa europeu consta a Geórgia (2008) e a Ucrânia (2014 e 2015), também alvo de ciberataques lançados através de *proxies* alegadamente Russos. Luukas Ilves et alli, European Union and NATO Global Cybersecurity Challenges: A Way Forward, in: *PRISM*, Institute for national Strategic Security, Nacional Defense University, Vol. 6, N.º 2, p.128.

[113] George Christou a), The collective securitization of cyberspace in the European Union, in: *West European Politics*, Routledge, Vol. 42, N.º 2, 2019, pp. 285-286.

[114] Entre as quais destacamos a da Lituana, onde pode ler-se que a principal preocupação *"(…) aims towards safe and reliable ICTs and fears abuse and (large-scale) disruption – and at the same time acknowledges the need to protect the openness and freedom of the Internet*". Por seu turno, a estratégia do Reino Unido enuncia que "(…) *making the UK the major economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace. The objective is to tackle*

(alguns, inclusive já reviram) as suas estratégias de cibersegurança nacionais. Destacamos o Estado da Estónia, o qual viu o seu quadro de medidas bastante reforçado desde o primeiro incidente de cibersegurança[115].

Nesta senda, os EUA publicaram a estratégia internacional para o ciberespaço, com a sua própria visão, tentando definir e priorizar a agenda mundial dos outros governos[116][117]. Esta estratégia realça a importância de um ambiente salutar no ciberespaço, sem agressões, baseada numa política de partilha de informações de forma a assegurar um ciberespaço seguro para os cidadãos, fortalecer as democracias, as economias, promovendo a transparência e a salvaguarda dos direitos, liberdades e garantias fundamentais da pessoa humana[118].

Podemos inferir numa conclusão preparatória, que as estratégias de cibersegurança dos Estados-membros variaram de acordo com as abordagens internas em função das perceções nacionais de exposição ao risco cibernético. Contudo, é importante realçar-se alguns aspetos comuns à maior parte das estratégias nacionais dos Estados da União, entre as quais: a) definição de uma estrutura de governo para a cibersegurança, assente numa cadeia de comado; b) auscultação ao setor público e privado em relação às políticas e

the risks from cyberspace like cyber-attacks from criminals, terrorists and states in order to make it a safe space for citizens and businesses.". Por ultimo, a estratégia da França passa a concentrar o seu foco "(…) *on the enablement of information systems to resist events in cyberspace which could compromise the availability, integrity or confidentiality of data*.".

[115] Em termos estatísticos, em 2017, a Estónia ocupou o 5.º lugar no Global Ranking GCI 2018, produzido pela ITU, este ranking resulta do compromisso que cada Estado apresenta para cibersegurança. Adicionalmente, o Reino Unido, os Estados Unidos e a França ocuparam respetivamente a 1ª, 2ª e 3ª posição, para mais informações *v.*,https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[116] Note-se que no início do seu primeiro mandato presidencial como Presidente dos EUA, Barack Obama inscreveu a cibersegurança como um das principais ameaças globais, tendo em conta as suas dinâmicas e impacto, em particular, nas infraestruturas críticas nacionais, originando o documento: *US Cyberspace Policy Review: assuring a trust and resilient information and communications infrastructures*, *v.*, https://nsarchive.gwu.edu/dc.html?doc=2700108-Document-28.

Várias das preocupações latentes à época resultavam das preocupações com a SI e o ciberespaço, como: a) a clarificação da responsabilização e definição dos atores em normas; b) promoção da segurança cibernética; c) fortalecimento do diálogo entre os parceiros públicos e privados; e d) as campanhas de consciencialização digital. Para mais desenvolvimentos sobre esta matéria, *v.*, https://fas.org/irp/eprint/cyber-review.pdf.

[117] Cfr. US Department of State, *Pillars of The International Strategy for Cyberspace*, disponível para consulta em: https://2009-2017.state.gov/s/cyberissues/strategy/index.htm.

[118] Por temática, esta estratégia é subdividida por setores independentes assente num modelo colaborativo do governo, nos parceiros internacionais e no setor privado. Assim, é dada especial relevância à económia, promovendo padrões de atuação internacionais, baseados nos mercados abertos e inovadores; proteção das redes, assegurando a confiabilidade e a sua resiliência; aplicação da lei, reforçando a rede colaborativa e o Estado de direito; militar, no âmbito da ciberdefesa com estruturas capazes de enfrentar os desafios do século XXI; governança da Internet, com a promoção de estruturas capazes e eficientes; desenvolvimento internacional, fortalecendo capacidades, aumento a segurança e a prosperidade; e a liberdade na Internet, assegurando a defesa das liberdades fundamentais e proteção da privacidade em ambiente digital.

regulamentos de segurança[119][120]; c) elaboração de planos regulatórios, estruturas hierárquicas, responsabilidades dos agentes[121] e direitos dos setores público e privado[122]; d) discernimento de objetivos e meios para desenvolver capacidades nacionais e quadros legais que permitiram envolver-se no combate ao cibercrime dentro e fora de fronteiras (ainda que muito limitados); e) plano de identificação de infraestruturas críticas de segurança e informação, incluindo os seus principais ativos, serviços e interdependências estabelecidas; f) desenvolvimento e/ou melhoria dos planos e medidas de preparação, resposta e recuperação para proteger as infraestruturas críticas nacionais, através de planos nacionais de contingência, exercícios cibernéticos e de conhecimento situacional[123]; g) definição de uma abordagem sistemática e integrada à gestão dos riscos nacionais, por exemplo, intercâmbio de informações e de índices nacionais de risco; h) promoção de campanhas de consciencialização que instigavam a mudanças no comportamento por parte dos utilizadores das TIC[124]; i) estímulo às novas competências relacionadas com a cibersegurança e investimento na formação de profissionais nesta área para verter conhecimento para o ramo económico-comercial[125]; j) reforço da cooperação internacional entre Estados-membros e países terceiros na partilha de informação segmentada, ou através da assinatura e ratificação de Convenções (ex. Convenção sobre o Cibercrime); e K) desenvolvimento de programas de investigação e unidades curriculares abrangentes de pesquisa focadas nas tecnologias emergentes[126] e problemas de resiliência dos sistemas e serviços.

---

[119] ENISA a), *Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents*, v.1.0, 2018, p. 17.

[120] A este nível podemos salientar que parcerias desenvolvidas ao nível do cibercrime, como a Online Fraud Cyber Center, *v*., https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 ou a Cybercrime Support Network, *v*. https://cybercrimesupport.org/. A nível transatlântico podemos evidenciar a Internet Crime Complaiant Center, *v*. https://www.ic3.gov/default.aspx.

[121] A estes são aplicadas recomendações específicas de acordo com a posição que ocupam, visando o reforço da maturidade em cibersegurança. ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2018, pp. 26-29.

[122] Como salienta o parágrafo 35 da Diretiva NIS "(…) *a maioria das redes e dos sistemas de informação são explorados pelo setor privado, a cooperação entre o setor público e setor privado e essencial*.".

[123] George Christou a), *op. cit.*, p. 286.

[124] ENISA, *Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity*, 2018, pp.19-25.

[125] "*A UE não apela à criação de novos instrumentos jurídicos internacionais para as questões do ciberespaço"*. ENISA, *Status of Privacy and NIS course curricula in Member States*, 2015, disponível para consulta em: https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states.

[126] Nesta senda, os EUA, lançaram uma lista de 20 tecnologias que consideram críticas e emergntes e que devem elencar as suas prioridades e missões, *v*. https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

A UE, enquanto ator político na cena internacional, publicou a pedra angular que guia a sua atuação e dos Estados membros na segurança da informação no ciberespaço - a Estratégia Europeia para a Cibersegurança (2013). Alicerçada sob o lema: «*An Open, Safe and Secure Cyberspace*» pretende ser um polo agregador e um documento estratégico da ação externa da União no mundo, concentrando vários aspetos importantes, tais como a maior proximidade entre setores privado e público, num empenho e reforço das parcerias internacionais. Esta estratégia assenta em três pilares fundamentais: i) proteção das infraestruturas cítricas; ii) Cibercrime; e iii) Ciberdefesa. Mais tarde, a estratégia global da UE (2016), veio reforçar a importância da criação de uma cultura de cibersegurança comum de forma a padronizar e antever a perpetração de crimes disruptivos em ambiente digital.

Esta cultura comum de governança relaciona várias áreas, entre elas, o Espaço de Liberdade Segurança e Justiça (ELSJ), o Mercado Interno e a Política Externa de Segurança Comum (PESC), elevando o senso comum das vulnerabilidades cibernéticas dos Estado-membros de forma a que se encontre o mínimo denominador comum para alinhar um caminho de desenvolvimento e segurança em ambiente digital.

Em 2017, a Comissão publicou a comunicação conjunta ao Parlamento Europeu e ao Conselho: "*Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*"[127], elencada por uma série de preocupações, entre elas, a inscrição da tipologia de atores dos ciberataques[128], o seu *modus operandi*[129], o controlo da SI nas infraestruturas críticas[130] e a natureza dos ataques[131]. A Comissão Europeia pretendia alertar o paradigma, *"(…) de uma política reativa para uma abordagem pró-ativa, a fim de proteger a prosperidade, a sociedade e os valores europeus, bem como os direitos e liberdades fundamentais, mediante a resposta às ameaças, atuais e futuras*"[132]. Também demostrou apreensão

[127] Comissão Europeia, Comunicação conjunta ao Parlamento Europeu e ao Conselho*: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*, 2017, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

[128] "*As ciberameaças surgem de intervenientes estatais e não estatais: são frequentemente de origem criminosa, motivadas pelo lucro, mas também podem integrar uma natureza política ou estratégica*". *Ibidem.*

[129] "*As campanhas de desinformação (notícias falsas) e as ciberoperações destinadas a atingir infraestruturas críticas são cada vez mais comuns e exigem uma resposta*". *Ibidem*.

[130] "*A incapacidade de proteger os dispositivos que controlarão as nossas redes de energia, automóveis, redes de transportes, fábricas, finanças, hospitais e lares poderão ter consequências devastadoras e causar enormes danos à confiança dos consumidores nas tecnologias emergentes*. *Ibidem.*

[131] "*O risco de ataques de natureza política contra alvos civis e de falhas na ciberdefesa militar agrava ainda mais esse perigo*". *Ibidem.*

[132] Na última década as preocupações com a cibersegurança fizeram ecoar o alerta dos decisores políticos. Veja-se os ataques terroristas em Bruxelas e Berlim em 2016, lançaram o debate sobre a criptografia e a sua ligação ao foro da justiça criminal no contexto do ciberterrorismo ou, *latu sensu* cibercrime. Veja-se

relativamente aos alvos "(...) *risk of politically motivated attacks on civilian targets, and of shortcomings in military cyber defence*" incitando ao robustecimento da transformação digital[133]. Paralelamente, a ciberdefesa foi inscrita como uma preocupação "(...) *use of cyberspace as a domaine of warfare, either solely or as part of a hybrid approach, is now widely acknowledged*", tendo a Diretiva NIS contribuído para mitigar parte dessa ameaça por parte da Comissão[134].

4.1.1 Estratégia da União Europeia para a Cibersegurança

Como mencionado, em 2013, com a densificação da temática da segurança da informação e do ciberespaço com uma realidade experimentada, foi publicada a Estratégia da União Europeia para a Cibersegurança: "*Um ciberespaço aberto, seguro e protegido*"[135], apresentando diferentes níveis securitários, tendo em conta as necessidades e os desafios à época[136] (ainda atuais). A estratégia abordou o capítulo da prevenção e resposta às perturbações no espaço digital, incentivando a criação de iniciativas nesse sentido no setor privado, nas organizações não governamentais e em grupos de interesse na sociedade. Paralelamente concerta uma visão voltada para a implementação de ações concretas para proteger e promover os direitos dos cidadãos[137], nomeadamente a defesa dos direitos fundamentais. A estratégia apresentou cinco prioridades: i) alcançar a resiliência do ciberespaço; ii) reduzir drasticamente a cibercriminalidade; iii) desenvolver políticas e capacidades no domínio da ciberdefesa no quadro da PCSD; iv) desenvolver os recursos

ainda o escândalo de *hacking* a uma candidata à Casa Branca nas eleições norte-americanas de 2016. ENISA, *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps*, Presidency progress report N.º 14711/16, 2016, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf.
Cfr. Resolução da 3508ª reunião do Conselho de Justiça e Assuntos Internos, 15391/16, 2016, p. 7, disponível para consulta em: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/jha_council_en.pdf.

[133] Comissão Europeia, *op. cit.*, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

[134] *Ibidem*.

[135] Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia da União Europeia para a cibersegurança:Um ciberespaço aberto, seguro e protegido*, 2013, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT.

[136] Em 2015, com o Regulamento (UE) 2015/2120 que estabelece medidas relativas ao acesso aberto à Internet, assegurando o princípio da neutralidade da rede garantindo um tratamento equitativo, transparente e não discriminatório na gestão tráfego na Internet.

[137] A política de cibersegurança anunciada à época observou cinco princípios base: a) aplicação dos valores fundamentais da UE ao ambiente digital; b) proteção dos direitos fundamentais, da liberdade de expressão da privacidade e dos direitos pessoais; c) acesso à Internet de forma livre e segura pelo grande público; d) uma governação democrática e eficiente em todos setores da sociedade; e e) responsabilidade da segurança da informação partilhada pelos intervenientes.

industriais e tecnológicos para a cibersegurança; e v) estabelecer uma política externa em linha com as melhores orientações internacional, tendo em vista a coerência em matéria de ciberespaço na Europa de modo a promover os valores fundamentais da UE.

4.1.1.1 Estratégia de Cibersegurança da República da Estónia

Escolhemos abordar a estratégia estoniana de cibersegurança em função da sua elevada posição no Global Ranking da ITU, bem como pelo bom exemplo prático, servindo atualmente como Estado europeu a ter em conta quando se abordam as temáticas de segurança da informação e cibersegurança.

A estratégia da Estónia assenta em quatro pilares fundamentais em linha com a sua visão estratégica nacional, a saber: 1) assegurar a proteção e promoção dos direitos e liberdades fundamentais no ciberespaço como em ambiente físico; 2) Facilitar e amplificar o desenvolvimento socioeconómico do Estado[138]. A segurança deve suportar a inovação e a inovação deve apoiar a segurança; 3) garantir a segurança das soluções criptográficas de importância única para o Estado, sendo esta uma base para o ecossistema digital; e 4) considerar a transparência e a confiança pública como fundamentais para a sociedade digital aderindo ao princípio da comunicação aberta[139][140].

Complementariamente, a estratégia visa alcançar quatro grandes objetivos, divididos no espaço temporal de 2018 a 2022. Assim, quanto ao primeiro objetivo, prende-se com a meta da *sustentabilidade da sociedade digital*, de modo a contar com uma forte capacidade de resiliência e preparação tecnológica para incidentes e crises no ciberespaço.

O segundo objetivo passa pelo reforço da cibersegurança na indústria e investigação. É espectável que a Estónia consiga desenvolver um forte base industrial ao nível da

[138] A Estónia apresenta-se como um dos Estados a nível europeu e mundial com maiores indíces de desenolvimento ao nível do *e-government*, como sustentam as Nações Undias, " *The citizens in Estonia can do basically anything online except for a very few things like getting married or divorced and selling or buying real estate*.", United Nations, *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*, 2020, p.52.

[139] Republic of Estonia Ministry of Foreign Affairs, *Cybersecurity Strategy Republic of Estonia*, p.10.

[140] Por comparação a um Estado terceiro, auxiliamo-nos na Estratégia de Cibersegurança do Canadá, que apresenta como pilares: a) a segurança dos sistemas do governo central; b) as parcerias externas para proteção dos sistemas governamentais; e c) a ajuda aos cidadãos nacionais na Internet. Esta estratégia reflete ainda o compromisso com o Estado de Direito, a responsabilidade e privacidade. Repare-se que a proteção dos nacionais e das infraestruturas críticas é um aspeto comum a estas duas estratégias. Gouvernement of Canada, *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*, p.7-8.

cibersegurança e inovação através da investigação de área, nomeadamente para poder ter disponível competências-chave ao nível do conhecimento e, de forma complementar, adquirir o estatuto de *ator produtor de cibersegurança* no mercado internacional.

O terceiro objetivo é quase uma extensão do anterior, ou seja, pretende assegurar que o Estado possa ter um contributo ao nível da cibersegurança na cena internacional de modo a ter lugar nas mais altas decisões de cooperação estratégica na cibersegurança e ciberdefesa.

O quarto objetivo elenca a promoção da *literacia digital* na comunidade de modo a que os cidadãos possam assegurar a sua própria segurança digital numa tríade simbiótica entre Estado, organizações e cidadãos.

O Estado estoniano elenca ainda um conjunto de atividades prioritárias, a saber: a) desenvolver novos serviços ou produtos tendo por base o princípio *privacy by design;* b) aplicar uma cultura de segurança baseada no risco; c) aplicar as melhores práticas internacionais em matéria de segurança da informação e cibersegurança; d) cooperar numa cultura de monitorização automatizada com todos os parceiros em sede de concertação da comunidade; e) monitorizar frequentemente os sistemas dependentes e independestes, além dos testes de sustentação das bases de dados e informações mais críticas; d) desenvolver auditorias; e) implementar e programar a cibersegurança em linha com a defesa nacional, de modo a emparelhar processos e objetivos; f) enfatizar os fluxos de informações técnicas, organizar exercícios conjuntos e envolver o setor privado e a academia na elaboração legislativa e planeamento estratégico; g) desenvolver a capacidade para operações cibernéticas, defensivas e ofensivas, de modo a que as TIC se possam transformar na nova infantaria; h) aumentar o intercâmbio de informações ao nível internacional e rever o quadro legislativo para combater fortemente o crime informático; i) apoiar a inovação e desenvolvimento de novos produtos e serviços na área das TI, bem como robustecer o auxílio ao nível diplomático; j) promover a capacidade cibernética competitiva e sustentável em países parceiros e projetar a experiência estoniana ao nível internacional.

De acordo com a Europol, em alguns Estados da UE o número de crimes cometidos em ambiente digital estava em vias de exceder o número de crimes perpetrados em ambiente físico[141]. O padrão estatístico prevê o crescimento do cibercrime e a transição digital dos

[141] Europol, *Internet Organised Crime Threat Assessment (IOCTA*), 2016, disponível para consulta em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Estados, ou seja, a quantidade de pessoas ligadas à Rede irá aumentar, e consequentemente, o número de incidentes digitais seguirá o mesmo caminho. A atuação das forças judiciárias deve reforçar a coordenação e cooperação, explorando todos os canais disponíveis, mesmo ao nível do Eurojust e Europol através de mecanismos concebidos para a cooperação transfronteiriça (ex. JITS), proteção das pessoas e da economia[142]. Os esforços concentram-se na identificação e detenção dos fornecedores do cibercrime na Darknet[143] (como prestadores de serviços[144]), mesmo naqueles ataques mais simples, como por exemplo, *phishing*[145].

Quando à metodologia de ataque dos criminosos, assenta em ataques a sites cuja importância para os cidadãos seja essencial, como por exemplo, o setor da saúde, essencial para a continuidade do normal funcionamento da sociedade, procurando por essa via ganhar influência política ou ganhos financeiros através de pedidos de resgate[146]. A Estónia destaca o setor da energia, comunicações e a banca como sendo prioritários e, onde tendencialmente ocorrem a maior parte dos ataques às infraestruturas críticas.

Do ponto de vista das limitações, existe uma dependência em relação às soluções tecnológicas provenientes de países terceiros, nomeadamente na aquisição de hardware do continente asiático. Ora, esta limitação é semelhante e extensível aos Estados-membros da UE, e passível de comprometer a seguranças das infraestruturas e das redes[147]. A estratégia europeia tem seguido as recomendações da administração de Washington ao limitar a proveniência e utilização de equipamentos de *software* e *hardware* de origem Russa e Chinesa. Salientamos, que ao nível da União e dos Estados–membros a discussão em foco é centrada na nova tecnologia de redes emergente – o 5G – mais concretamente no que concerne à sua implementação em solo europeu[148].

O plano europeu passa pela produção autónoma de tecnologia de cibersegurança ao nível dos parceiros europeus, capaz de satisfazer as necessidades dos Estados-membros,

---

[142] *Ibidem*.

[143] Como descreve a ENISA, " *Darknet generally relates to an arbitrary number of unregistered computers connected to each other in a distributed way where each computer can act as a server for the others. This approach avoids the need for a central server through which all traffic would pass*". ENISA, *ENISA's Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity*, 2016, p. 11.

[144] Europol, *The EU Serious and Organised Crime Threat Assessment (SOCTA)*, 2017, p. 29.

[145] *Ibidem*.

[146] Republic of Estonia Ministry of Foreign Affairs, *op. cit.*, p. 21.

[147] *Ibidem*.

[148] Maya Guzdar e Tomas Jermalavicius, Between the Chinese Dragon and American Eagle: 5G Development in the Baltic States, in: *Internacional Center for Defense and Security*, 2020, p. 1, disponível para consulta em: https://icds.ee/en/between-the-chinese-dragon-and-american-eagle-5g-development-in-the-baltic-states/.

organizações e cidadãos. Esse trabalho tem tido evoluções significativas através do plano colaborativo na indústria de defesa da União, nomeadamente, através dos projetos ao abrigo do instrumento da cooperação estruturada permanente, sob o escopo da PCSD, previsto no artigo 42.º, n.º 6 do TUE[149].

Ao nível internacional da aplicação da lei ao ciberespaço, a Estónia tem acompanhado o cenário em conjunto com a NATO, UE e NU[150], a par das constantes atualizações face às novas ameaças internas. A Estónia é um exemplo mundial no que toca à liberdade da Internet: em 2019, segundo a Freedom House, o Estado estoniano posicionou-se entre os Estados nos quais os cidadãos mais podem confiar para navegar ma Internet sem temer restrições no acesso, limitação de conteúdos ou temer violações dos seus direitos[151].

A Estónia apostou numa estratégia integrada, ou seja, partiu dos princípios basilares de segurança e defesa do Estado e contruiu uma estratégia como múltiplos atores, entre os quais, os vários ministérios do governo[152] e arquitetou uma agenda digital. Nesta, foram integradas como prioridades: a) a *segurança da identidade eletrónica* e a capacidade de *autenticação eletrónica*; b) a implementação do princípio "*no-legacy*"; c) o desenvolvimento e adoção de uma solução de computação através de uma *nuvem governamental*; e d) realização de um ato eleitoral seguro pela Internet[153].

---

[149] Este instrumento da UE, atualmente apresenta 8 projetos ao nível da cibersegurança levados a cabo por diferentes Estados-membros da União. Para mais informações, *v*. https://pesco.europa.eu/.

[150] Através da Resolução A/RES/73/266 da AGNU, foi estabelecido, pelo Secretário Geral, um grupo de peritos ao nível governamental sobre o comportamento e as responsabilidades dos Estados no ciberespaço no contexto da segurança internacional, recorde-se que o primeiro grupo estabelecido remonta à data de 2004, estabelecido através da A/RES/58/32 originando primeiro relatório em 2005 - A/60/2002, do qual não houve consenso entre os membros.

O grupo de peritos goevrnamentais(GEG) reuniu pela primeira vez em 2019 e apresentará o seu relatório final em 2021. Quando à sua composição, conta com 25 especialistas e o seu presidente (embaixador Guilherme de Aguiar do Brasil). O mandato inclui consultas sobre o tema a serem realizadas com Estados, organizações regionais, como a União Africana, a União Europeia, a Organização dos Estados Americanos, a Organização para a Segurança e Cooperação na Europa e o Fórum Regional da Associação de Nações do Sudeste Asiático. Os pilares de trabalho incidem essencialmente em cinco grandes temas, a saber: 1) ameaças existentes e emergentes; 2) direito nternacional; 3) normas, regras e princípios; 4) medidas de fomento da confiança; e 5) cooperação internacional e assistência na capacitação. No atual mandato os membros do GEG são provenientes dos seguintes Estados: Austrália, Brasil, China, Estónia, França, Alemanha, Índia, Indonésia, Japão, Jordânia, Cazaquistão, Quénia, Maurícia, México, Marrocos, Países Baixos, Noruega, Roménia, Rússia, Singapura, África do Sul, Suíça, Reino Unido, Estados Unidos da América e Uruguai. Para mais informações consultar, https://www.un.org/disarmament/ict-security/.

[151] Freedom House, *Freedom on the NET 2019*, 2019, p. 24, disponível para consulta em: https://freedomhouse.org/issues/technology-democracy.

[152] Ministério da Economia e Comunicações, Ministério da Educação, Ministério da Justiça, Ministério da Defesa, Ministério do Interior, Centro de Tecnologia da Informação e Desenvolvimento do Ministério do Interior (SMIT), Ministério dos Negócios Estrangeiros e Ministério das Finanças. Adicionalmente, foram convocados agentes relevantes, como por exemplo, o Centro Internacional de Defesa e Segurança (RKK), o Centro de Análise Digital e Cibersegurança (TalTech) e o Centro de Excelência de Defesa Cibernética Cooperativa da OTAN (CCD COE).

[153] Republic of Estonia Ministry of Foreign Affairs, *op. cit.*, p.29.

Este documento faz ainda referência aos objetivos do Plano de Desenvolvimento de Defesa 2017-2026 e ao Plano de Desenvolvimento da Segurança da Internet (2021-2030) da Estónia.

Em termos de desafios, a limitada capacidade de especialização e investigação de área, tanto pelo setor público como setor privado é um fator a ter em atenção pela Estónia. A falta de liderança integrada dos serviços e a falta de compreensão das insuficiências (humanas e materiais), a par das dependências externas são desafios de maior nesta estratégia. As diferentes prioridades políticas e as capacidades nacionais ao nível dos recursos parecem ditar o maior ou menor grau de efetividade para conduzir operações de investigação ao nível cibernético (bem como operações atinentes à ciberdefesa) ao exigir uma estrutura institucional e recursos operacionais das autoridades nacionais. O processo da cibesegurança é complexo, por ser "*contínuo* e *mutável*" em função da paisagem de ameaças, agentes, técnicas, ferramentas e procedimentos que precisam de ser constantemente atualizados, de forma a garantir um estado elevado de proteção[154].

O grau de maturidade cibernética da Estónia relativamente à larga maioria dos Estados da UE é elevado, muito devido aos ciberataques lançados em 2007 e 2017 que empolaram o desenvolvimento de capacidades na área da SI e cibersegurança num curto período de tempo. Como segundo fator de sucesso organizativo desta estratégia apontamos a instalação do Centro de Excelência de Defesa Cibernética Cooperativa da OTAN (CCD COE) em Tallinn, que acabou por regozijar a capacidade de ciberdefesa da Estónia através do espírito de proximidade muito elevado entre instituições. Ator produtor de cibersegurança, pelo menos, por força das lições apreendidas, podemos retirar deste Estado os erros cometidos e repensar a forma de potenciar as capacidades de cibersegurança a médio prazo de forma integrada com as restantes políticas internas nas sociedades ocidentais de forma a prever e decidir com antecipação face a incidentes no ciberespaço.

[154] Instituto da Defesa Nacional, Seminário da Defesa Nacional, in: *idn cadernos*, N.º 32, 2019, p. 22.

4.2 Convenção 108

Em 1981 foi aberta a assinatura da Convenção para a Proteção das pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108), como primeiro instrumento multilateral, legalmente vinculativo, relativo à proteção de dados. Este instrumento serve como garante da proteção contra os abusos relativos ao tratamento automatizado de dados de caráter pessoal e ainda regula a transferência internacional de dados, aplicando-se a todos os tratamentos de dado pessoais, tanto do setor público como do setor privado, tal como dados tratados no âmbito das autoridades do setor policial e judiciário[155]. Esta Convenção foi inovadora em vários sentidos, relativamente à introdução de novos direitos, como por exemplo, o direito ao conhecimento dos dados pessoais detidos e armazenados por terceiros. A possibilidade de restrição ou limitação dos direitos enunciados na Convenção só é admitida em casos de superior interesse dos Estados, como por exemplo, *segurança nacional*, *defesa* e *liberdade de expressão*, consagrados pelas constituições nacionais.

Mais tarde, em 2001, surgiu um protocolo adicional (Protocolo 281), referente às autoridades de Supervisão e Fluxos Transfronteiriços de Dados[156]. Por último, esta Convenção foi atualizada em 2018, quando lhe sucedeu a emenda (N.º 223) ao Protocolo 2018, passando a denominar-se "Convenção 108 +"[157]. Por via desta modernização foi

[155] Hoje temos uma distinção bem clara entre ambas estas duas realidades na UE com o RGPD e com a Diretiva de cooperação policial, abordadas no ponto anterior.

[156] Este novo protocolo foi extremamente importante para garantir o cumprimento e a efetividade da Convenção, relativos à proteção de dados pessoais, fluxos de dados transfronteiriços e ainda aos fluxos de dados transfronteiriços para países terceiros. Sendo que, à partida, os dados pessoais só podem ser transferidos se o Estado destinatário ou organização oferecer um nível de proteção ou garantias adequadas.

[157] O Protocolo que altera a Convecção 108 de 1981 visa alargar o seu âmbito e obter uma maior eficácia no seu o objetivo principal que é a proteção dos direitos e liberdades fundamentais, em especial pelo direito à vida privada. A Comissão Europeia, apresentou a proposta COM (2018) 451 final, onde propunha a autorização dos Estados-Membros a ratificar, no interesse da União Europeia, o Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal. O principal argumento visa uma modernização por via de um modelo europeu de proteção de dados, partindo, desde logo, do RGPD e da Diretiva de Cooperação Policial, sendo que esta adesão garantiria um nível de proteção mais elevado, seja através da disponibilidade de recursos judiciais e extrajudiciais, entenda-se assim a sujeição ao TEDH, ou através de uma fiscalização eficaz pelas autoridades de supervisão dos Estados signatários, o que contribuiria para o intercâmbio de dados com os pressupostos e garantias de segurança adequadas. Um terceiro argumento utilizado versa sobre a futura adesão da UE à Convenção, possibilidade prevista neste Protocolo de alteração. Tendo em conta a proposta da Comissão Europeia e a aprovação pelo Parlamento Europeu, foi publicada a Decisão (UE) 2019/682 do Conselho de 9 de abril de 2019, que autoriza os Estados-Membros a assinar, no interesse da União Europeia, o Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal.

possibilitado a Estados terceiros aderirem à Convenção, aliás como ocorreu já com Cabo Verde, Mauritânia, México, Senegal e Tunísia[158].

Salientamos que a Convenção 108, é o único instrumento internacional juridicamente vinculativo no domínio da proteção de dados (aos Estados parte).

4.3 Diretiva 2013/40/EU

Houve o entendimento global de que a SI e as infraestruturas críticas dos Estados-membros constituíam um elemento fundamental para a normal fluidez política, social e económica no seio da União. Assim, a temática da segurança da informação começava a ganhar contornos cada vez mais expressivos. Destarte, foi publicada a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e, que substitui a Decisão-Quadro 2005/222/JAI do Conselho elencando uma clara intenção de densificação legislativa para prevenir ataques em ambiente digital contra os sistemas de informação, sabendo que a Diretiva em apreço faz parte integrante de um quadro complexo de medidas de prevenção e resposta à cibercriminalidade[159]. O estabelecimento de regras mínimas relativas à definição das infrações penais e previsão sancionatória relativamente aos ataques perpetrados contra os sistemas de informação estão previstas nesta Diretiva bem como o apelo à intensificação da cooperação por parte das autoridades judiciárias. Todavia, aquele que pretendia ser um documento harmónico em todos os membros da EU, acabou por deixar uma ampla margem de discricionariedade interna aos Estados por via da aplicação das "*medidas necessárias*", entenda-se, medidas de segurança dedicadas para amplificar a resiliência dos sistemas de informação, dado o seu teor vago. Deste modo, o grau de perceção do risco em ambiente digital percecionado em cada Estado-membro, e a capacidade de aplicar um adequado nível de proteção nos sistemas de informação ditou uma implementação que ficou há quem das espectativas[160].

[158] Todos os Estados do Conselho da Europa e também da União Europeia são Estados parte deste instrumento multilateral.

[159] Esta seria uma iniciativa do Conselho da Europa inspirada pela Rede 24/7 (vinte e quatro horas por dia e sete dias por semana em permanente contacto) que o G8 estabeleceu em 1988. Este tinha como principal objetivo assegurar a prestação de auxílio imediato quando ocorressem infrações penais e investigações onde fosse convocada a necessidade de proceder à recolha de prova em ambiente digital.

[160] Pedro Freitas e Nuno Gonçalves, *Illegal access to information systems and the Directive 2013/40/EU*, in: *International Review of Law*, Computers & Technology, Routledge: Taylor & Francis Group, 2015, Vol. 29, Nº 1, p. 50-62.

No parágrafo 23 da Diretiva em análise é notória a promoção da cooperação entre o setor público e privado de forma a promover em conjunto o aumentar da resiliência digital na União.

Em matéria atinente ao combate à cibercriminalidade, foi proposto aos Estados que fomentassem o diálogo com os Fabricantes e Prestadores de Serviços digitais, de forma a que também estes observassem um conjunto de responsabilidades no exercício das suas funções. Por exemplo, o dever de colaboração com as forças e serviços de segurança aquando da necessidade imediata de perícias informáticas para efeitos de preservação de prova e indícios[161], identificação de infrações e infratores, ou encerramento de sistemas ou suspensão de serviços.

4.4 Regulamento (UE) n.º 910/2014

Também na vertente política as preocupações em garantir aos cidadãos da UE uma economia digital aberta e sem riscos ou ameaças de segurança foi evidente. Nesse sentido, em 2014, foi publicado o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, que revogou a Diretiva 199/93/CE. Na sua essência, este Regulamento estabeleceu um novo sistema para a realização de interações eletrónicas em condições seguras em toda a União Europeia compreendendo cidadãos, empresas e autoridades públicas. Num segundo plano, visou o reforço da confiança nas transações eletrónicas em todo o espaço da União e aumentou a eficácia dos serviços públicos e privados em linha, de um modo geral, reforçou a segurança nos sistemas de comércio eletrónico. Sobre este último, importa acrescentar que a parte relacionada com a segurança digital do e-commerce (relativa à segurança dos dispositivos, segurança da informação, integridade dos dados, confidencialidade, disponibilidade, entre outros), constitui um conjunto de medidas necessárias para salvaguardar todos os ativos neste processo segundo uma avaliação de risco, em particular nas fases de transação (fase de informação, fase de negociação, fase de pagamento e fase

[161] A investigação ciminal de indícios em ambiente digital passará a ser um realidade tão mais presente, quanto maior for o grau de dependência tecnológica da sociedade, pois tenderão a ser perpetrados mais crimes neste domínio.

de entrega). No processo de e-commerce, especificámos algumas das mais usuais medidas, como a verificação da identidade, controlos de acesso, contrato de identificação seguro e assinaturas digitais ativas ou encriptação.

Todavia, com o reforço da presença das organizações em ambiente digital puxou a que também as medidas de segurança fossem (continuam a sê-lo) um fator diferenciador e característica de confiança para os potenciais clientes, que por vezes estão localizados em continentes distintos do local da compra do produto em linha. Deste modo, o e-commerce necessita de fortes medidas de segurança para que o cliente final, independentemente da sua localização se sinta seguro ao realizar a sua compra. Por exemplo, recurso ao controlo de acessos[162], recurso a esteganografia[163], utilização de comunicações seguras[164] e aplicação de modelos algorítmicos preditivos[165]. A utilização de métodos de segurança reforça a privacidade dos utilizadores-consumidores utilizando protocolos seguros e metodologias modernas de segurança para fazer face ao acesso, uso, alteração ou destruição não autorizados no e-commerce[166]. Por último, este Regulamento eliminou obstáculos existentes à utilização da IDe[167] na União.

[162] Existem várias tecnologias que podem ser usadas para controlar acessos e aceder a recursos da Intranet e da Internet. O controlo de acessos inclui autenticação, autorização e medidas como as digitalizações biométricas, bloqueios de rede, assinaturas digitais, criptografia, controlo e monitorização de barreiras física por seres humanos ou sistemas automatizados.

[163] Descreve o processo de ocultar informações inserida em outra informação (criptografia), além de fornecer uma maneira de ocultar um arquivo criptografado dentro de outro arquivo. As mensagens ocultas que recorrem à esteganografia são de difícil deteção.

[164] A segurança das comunicações é um dos controlos adotados para negar informações a pessoas não autorizadas. A segurança das comunicações é subdividida em quatro vertentes:

I. Segurança criptográfica: garante a confidencialidade e autenticidade da mensagem;
II. Segurança de emissões: proteção resultante de todas as medidas tomadas para negar informações a pessoas não autorizadas;
III. Segurança física: consiste na componente de segurança das comunicações que resulta de todas as medidas físicas necessárias para proteger os equipamentos classificados, sistemas ou processos de acessos não autorizados.
IV. Segurança de transmissão: componente da comunicação de segurança resultante da aplicação de medidas destinadas a proteger transmissões de interceção e exploração por outros meios que não análise criptográfica (por exemplo, salto de frequência e espectro de propagação).

[165] Para melhor a segurança no e-commerce e aumentar a segurança dos consumidores foram elaborados diversos estudos sobre os tipos de ameaças no ciberespaço relativamente a este domínio. Nesses estudos, verificaram-se que existem diferentes tipos ameaças e, para identificá-las foram utilizadas técnicas recorrendo à previsão, tais como a modelagem estatística e a modelagem algorítmica.

[166] Ramjee Prasad e Vandana Rohokale, E-commerce, In: *Ciber Security: The Lifeline of Information and Communication Technology*, Springer Series in Wireless Technology, Springer, 2020, p. 182-184.

[167] Identificação eletrónica (IDe) - formas tangíveis ou intangíveis de identificação que contém dados de identificação pessoal que são utilizadas para autenticação de um serviço em linha.

4.5 Regulamento (EU) 2016/679

A temática da proteção de dados pessoais na União Europeia assenta base legal das disposições do artigo 16.º do TFUE e nos artigos 7.º e 8.º na Carta dos Direitos Fundamentais da União Europeia. Sendo a proteção dos dados pessoais um tema assumido pela UE em termos transversais em toda a linha de políticas e, do ponto de vista social tendo vindo para permanecer na ordem do dia é da importância máxima o estudo da relação entre a privacidade e a proteção de dados na Era tecnológica[168][169].

No âmbito da proteção dos direitos dos titulares dos dados pessoais e da privacidade ao nível comunitário foi publicado o Regulamento Geral de Proteção de Dados (doravante, RGPD),que veio dar enfâse ao quadro legislação aprovada em 2016, fruto da rápida evolução tecnológica e profunda alteração na comunidade internacional dos serviços em linha, em especial na recolha, acesso e tratamento de dados pessoais. Ao fim de três anos de negociações entre o Parlamento Europeu (a nível de comissão) e o Conselho (a nível de embaixadores) foi publicado o novo diploma comunitário de proteção de dados[170].

Assim, a 25 de maio de 2018, tornou-se juridicamente vinculativo o Regulamento Geral de Proteção de Dados (RGPD), revogando a Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, com aplicada diretamente a todos os Estados-membros[171], criando um quadro mais claro e consistente especificamente direcionado à proteção de dados pessoais. Este Regulamento veio permitir um maior controlo dos dados pelos seus titulares, consagrando um direito fundamental, num contexto e em circunstâncias especialmente relevantes, pois a Era digital e os desafios socias correntes requeriam a modernização no sistema regulatório europeu quanto a esta temática. Ao mesmo tempo, o RGPD unificou regras relativas aos negócios e estipula um quadro de figuras necessárias a ter em linha de conta, como por exemplo, a constituição de um EPD[172].

---

[168] Luis García Segura, European Cybersecurity: Future Challenges from a Human Rights Perspective, in: *Security and Defence in Europe*, Martín Ramírez e Jerzy Biziewski (eds), Springer, 2020, pp.40-45.

[169] Face aquilo que tem sido reportado em termos de violações de segurança e queixas apresentadas no âmbito da proteção de dados.

[170] Parlamento Europeu, *Proteção de daos pessoais*, 2017, disponível para consulta em: https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais.

[171] Atualmente, todos os 27 Estados-membros atualizaram as suas leis de proteção de dados ou criaram uma lei de execução nacional que transpõe o RGPD, com maior ou menor margem de aproximação em relação ao Regulamento. Também a aplicação de coimas tem sido uma realidade bem diferente entre os Estados-membros, com disparidades quando a efitivade da aplicação de coimas pelas autoridades de proteção de dados da UE, *v*. https://www.enforcementtracker.com/.

[172] Encarregado de Proteção de Dados.

Este Regulamento veio responder a algum vazio regulatório que se verificava no mercado único digital eliminando alguma burocracia e reforçando a confiança dos consumidores (titulares dos dados)[173]. Entre outros aspetos, o RGPD trouxe algumas inovações e reforço de alguns direitos em relação ao diploma que este revoga, destacamos por exemplo: a forma como os dados pessoas são tratados, de um forma clara e inteligível; o direito à portabilidade[174], para transferências de dados de um titular de dados entre Prestadores de Serviços; o direito de conhecer se os seus dados foram alvo de um violação de segurança, sendo que deve ser notificada a autoridade de supervisão nacional quando este tipo de incidente ocorre; aumentaram também as responsabilidades e a *accountability* sobre as organizações, tanto para RpT, como para subcontratantes; a obrigatoriedade da realização de avaliações de impacto pelos RpT quando existe a possibilidade de determinada atividade de tratamento poder colocar em risco os titulares de dados, nomeadamente os seus direitos e liberdades fundamentais[175]; novas regras para empresas que oferecem serviços aos europeus, mesmo tendo sede fora da União, tendo estas que estar conformes com o RGPD; aplicação da regra *on-stop-shop*, onde as empresas apenas lidam com uma única autoridade de supervisão; aplicação dos princípios *protection by design and by default*; aplicação de um regime de coimas elevado, podendo mesmo chegar a 4% de volume de negócios anual da empresa ou 20.000.000 de euros; ou ainda eliminação de burocracias, nomeadamente relativas a notificações; a possibilidade das organizações verem aprovados códigos de conduta[176] e mecanismos de certificação.

A *softw law* dirigida ao setor da proteção de dados e segurança da informação, tanto do Conselho da Europa como da União Europeia afirmam o seu compromisso com a proteção da identidade digital dos cidadãos, isto fica bem patente por via da emissão de declarações, resoluções, *guilenes*, diretrizes, opiniões, resoluções entre outros instrumentos elaborados à medida que as novas questões tecnológicas se vão materializando em dúvidas concretas, que por vezes derivam de decisões jurisprudências[177].

---

[173] Shakila Bu-Pasha, Cross-border issues under EU data protection law with regards to personal data protection, in: *Information & Communications Technology Law*, Routledge: Taylor & Francis Group, p.227-228.

[174] Direito este reforçado relativamente aos consumidores da UE pelo Regulamento (UE) 2017/1128 do Parlamento Europeu e do Conselho de 14 de julho de 2017 relativo à portabilidade transfronteiriça dos serviços de conteúdos em linha no mercado interno.

[175] Artigo 35.º do RGPD.

[176] Artigo 40.º do RGPD.

[177] Entre outras, destacamos a Assembleia Parlamentar do Conselho da Europa, *v.* https://pace.coe.int/en/ , o comité de ministros, *v.* https://www.coe.int/en/web/cm, as opiniões e estudos da Comissão Europeia para a democracia para além do direito (Comissão Venice), *v.*

4.6.1 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)

O caso *Google Spain*[178], merece lugar de destaque no nosso estudo porque o órgão decisão, neste caso, o TJUE, postulou um decisão história, decidindo de forma procedente à supressão de hiperligações relacionadas a um titular de dados. Foi analisada e decidida a sua aplicabilidade territorial da legislação de proteção de dados fora do espaço da UE, neste caso, em relação à empresa americana *Google Inc*[179], com sede nos EUA. O requerente apresentou uma reclamação à Agência Espanhola de Proteção de Dados contra um jornal regional (*La Vanguardia Ediciones SL*), e outra contra a *Google Spain* e *Google Inc*, por duas publicações de páginas com informação relativa a procedimentos de execução fiscal em débito à segurança social, augurando a ocultação ou remoção dessas informações no motor de pesquisa da operadora em causa. Destarte, o requente solicitou a eliminação dos seus dados pessoais nos motores de busca da *Google Inc* e dos *hiperlinks* associados à notícia publicada no jornal regional, afirmando que havia quitado a dívida em causa há cinco anos e, deste modo, as notícias em causa figuravam como desatualizadas e desprovidas de relevância. Em 2010, a Agência Espanhola de Proteção de Dados viria a indeferir a reclamação referente ao jornal local, justificando a publicação atentando à sua finalidade pública.

https://www.venice.coe.int/WebForms/pages/?p=04_Compilations, e por último, as opiniões e relatórios do Comité para a Convenção 108.
Ao nível da União Europeia, podemos destacar as diversas orientações em forma de opiniões, *guilines*, entre outros do Comité Europeu de Proteção de Dados (CEPD ou EDPB, em inglês), do antigo Grupo de Trabalho do Artigo 29.º, *v*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. O CEPD assume estatuto de um organismo da UE, dotado de personalidade jurídica e com secretariado independente. Entre o leque de competências destacamos a capacidade para decidir os litígios entre as autoridades de controlo nacionais e a intrepertação e orientação sobre o RGPD, *v*. https://edpb.europa.eu/edpb_pt. Por outro lado, as opiniões da Autoridade Europeia para a Proteção de Dados (AEPD, em inglês EDPS), com funções de entidade supervisora independente, que assegura que as instituições e orgãos da UE respeitam as suas obrigações em matéria de proteção de dados, *v*. https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions-prior-check_en.
Quando à segurança da informação, a ENISA tem um vasto reportório temático para toda a sociedade civil sobre os espetros da seguranaça da informação e proteção de dados, *v*. https://www.enisa.europa.eu/publications/sitemap.

[178] Acordão do Tribunal de Justiça da União Europeia, Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Processo C-131/12, de 13 de maio de 2014, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

[179] O caso ficaria conhecido pelo reconhecimento do "direito à desindexação" de dados pessoais em motores de busca.

Distintamente, a AEPD veio deferir a parte respeitante à supressão da informação do requerente apenas relativamente à *Google Spain* e *Google Inc*, uma vez que estas estavam, como assegurando um servido de browser de Internet, estariam sujeitas ao cumprimento das normas de proteção de dados e ao respeito pela dignidade da pessoa humana, enquanto RpT (artigo 2.º, alínea d) da Diretiva 95/46/CE), de dados e intermediários de informação[180]. Estes últimos, recorreram ao STJ onde argumentaram que não realizavam tratamentos de dados pessoais e, tampouco poderiam vir a ser responsáveis porque não teriam controlo sobre os dados. O STJ, por sua vez, remeteu três questões prejudiciais ao TJUE considerando que a competência interpretativa da Diretiva 95/46 era da competência TJUE devolvendo novamente o processo a este órgão decisório, tendo este emitido acórdão em maio de 2014.

O TJUE declarou que um operador de motor de busca da Internet é RpT de dados pessoais disponibilizados nas páginas Web de outras fontes, pois determina as finalidades e os meios dessa atividade, sendo consequentemente considerado RpT como frisado no ponto 33 do acórdão[181]. A operação de um motor de busca constitui uma atividade distinta da publicação de conteúdos num sítio Web, e nesse sentido os resultados de pesquisa podem comprometer o direito de privacidade de um titular de dados e, consequente a operadora atua como subcontratante à luz da Diretiva 95/46/CE (revogada).

Por seu turno, o Tribunal veio esclarecer que quando a pesquisa é realizada a partir de um motor de busca, permite ao utilizador visualizar uma lista de resultados e de informações sobre uma determinada pessoa, informações essas respeitantes a inúmeros dados da vida privada, fator agravado pelo efeito multiplicador da sociedade moderna e da Internet. Advertiu ainda, que a supressão das ligações em causa no processo pode por em causa o legitimo direito de acesso dos utilizadores à informação disponível na Internet, sendo então necessário observar com equilíbrio os direitos fundamentais dos visados nos motores de busca à luz do artigo 7.º e 8.º da CDFUE.

O TJUE determinou que o operador do motor de busca na Internet pode, em determinados casos, ser obrigado a remover hiperligações relacionadas a uma determinada pessoa singular por via de uma pesquisa, sendo que esta obrigação poderá ser observada mesmo quando o nome ou informações de determinada pessoa em causa não tenha sido apagada

[180] Jerome Squires, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) C-131/12, in: *Adelaide Law Review*, The University of Adelaide, N.º 35, 2014, p.465.

[181] O Advogado Geral considerou que o Prestador de Serviços de motor de buca não poderia ser considerado RpT.

do sítio Web. Adicionalmente, esclareceu que o direito a "ver apagado" o seu nome dos resultados de pesquisa pode ser exercido quando a informação é inexata, inadequada, não é pertinente, ou quando é excessiva relativamente à finalidade de tratamento de dados que pretende atingir. Assim, quando o operador recebe um pedido de apagamento de uma pessoa singular, deve proceder a uma avaliação, caso a caso, e ponderar os interesses da pessoa em causa e o interesse público associado à comunidade nessa pesquisa, ou pelos seus dados em específico num motor de busca[182]. Todavia, o TJUE, esclareceu que não deve ser solicitada a remoção de resultados de pesquisa na Internet de forma aleatória ou simplesmente porque as informações disponíveis não são convenientes para o seu titular. Por último, destacamos a interpretação que o TJUE fez relativamente à aplicabilidade extraterritorial da Diretiva[183], e ainda o facto das autoridades de proteção de dados nacionais terem competências para supervisionar as questões relacionadas com as operadoras de motores de busca, uma vez que os motores de busca são efetivamente RpT e a sua atividade pode vir a afetar direitos jusfundamentais.

Em Espanha, a *Audiencia Nacional* validou a decisão da AEPD de 30 de julho de 2010, condenado a *Google Inc.* a eliminar a lista de resultados obtidos pelo motor de busca com referência ao requerente, ou seja, os *hiperlinks* objeto da reclamação. No caso em análise, assistimos ao conflito jurisdicional entre um titular de dados – o qual foram violados direitos fundamentais, como a proteção de dados, e uma empresa multinacional - na qual o modelo de negócios assenta na economia dos dados e informações. Este poderá ter sido o primeiro passo para que os operadores do mesmo ramo de atividade possam controlar e defender os titulares de dados pessoais ao invés de se limitarem a indexar informação nos motores de busca sem qualquer tipo de filtro. O tribunal, teve que decidir em função de uma colisão de direitos de personalidade e o interesse público em causa, e em termos de proporcionalidade foi dado um sinal claro da prevalência dos direitos fundamentais do indivíduo[184], preterindo o interesse público para segundo lugar.

[182] Por exemplo, quando pensamos em políticos, gestores de instituições ou de titulares de órgãos públicos verificamos que os dados pessoais associados a estes em resultados de pesquisa em motores de busca são pertinentes e adequados, pois desempenham cargos de oficiais públicos, e por tal título o interesse público prevalece sobre os interesses de uma pessoa individualmente considerada, sendo à partida, um pedido de desindexação dirigido a um orgão jurisdicional indeferido.

[183] Shakila Bu-Pasha, *op. cit*., p.217.

[184] Ana Azurmendim, Spain: The Right to be Forgotten, The Right to Privacy and the Initiative Facing the New Challenges of the Information Society, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), Springer, 2017, p. 25-27.

4.6.2 Da "Desindexação" ao Esquecimento

A decisão de "desindexação" proferido pelo TJUE no ponto anterior, postulou a figura do direito ao esquecimento, ora, no agora quadro legislativo da UE, a "desindexação" deu lugar ao direito ao apagamento dos dados («direito a ser esquecido»), consagrado no artigo 17.º do RGPD, com uma maior previsibilidade jurídica e amplitude para o exercício deste direito pelos indivíduos.

O titular dos dados pessoais ao exercer o direito ao apagamento[185], obrigada o RpT à avaliação das condições para proceder ao apagamento, a saber:

a) *Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento*;
b) *A retirada do consentimento em que se baseia o tratamento de dados, sem que haja outro tipo de fundamento legal aplicável*;
c) *O exercício do direito em causa prevaleça sobre interesses legítimos que justificassem o tratamento em causa*;
d) *Os dados tenham sido ilicitamente tratados*;
e) *Cumprimento de uma obrigação jurídica da EU ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito*;
f) *Os dados pessoais recolhidos no contexto da oferta de serviços da sociedade da informação não tenham em atenção o critério de idades ou a supressão da capacidade jurídica do menor de 16 anos*[186].

Cabe ainda, aos RpT a tomada de medidas razoáveis, incluindo as de *carácter técnico* e de custo do processo, *tendo em consideração a tecnologia disponível e os custos da sua aplicação respeitantes ao apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos*[187].

Importa então entender a extensão territorial do direito ao apagamento postulados pelo RGPD e quais os critérios que devem ser preenchidos para os titulares dos dados poderem exercer este direito. Com efeito, o diploma europeu não apresenta, intencionalmente, limites de aplicação territoriais ou quanto à nacionalidade dos titulares de dados, mas antes atende os casos em função do tratamento de dados pessoais e do contexto do

[185] Note-se, diferente dos outros direitos subjetivos da proteção de dados.
[186] Artigo 17.º, n.º 1 do RGPD.
[187] Artigo 17.º, n.º 2 do RGPD.

exercício de atividade no seio da União[188]. Importa entender como um titular de dados pode exercer o seu direito de apagamento perante um Estado terceiro ou uma organizacional situada fora do espaço da UE. À luz dos direitos fundamentais enunciados pelo artigo 7.º e 8.º da CDFUE, importa entender qual a sua efetiva aplicabilidade extraterritorial em Estados terceiros e, desse ponto de vista, a extensão do poder sancionatório por via jurisdicional da União nesses Estados terceiros, em especial, naqueles em não existem garantias jurídicas relativamente a um núcleo de direitos fundamentais, como o respeito pelo vida familiar e a proteção de dados pessoais. Numa lógica restritiva do direito ao apagamento, e observando o princípio da prudência, o exercício do direito ao apagamento não pode proceder como interesse essencial por parte do titular de dados ao evitar o acesso à informação de cidadãos de um Estado terceiro à UE. Assim, o titular de dados pessoais deve invocar um *interesse substantivo e merecedor de tutela* jurisdicional efetiva[189].

Quanto ao direito de apagamento em Estados terceiros ou Estados que não sejam signatários de instrumentos normativos internacionais de proteção de dados a compatibilização poderá ser difícil, uma vez que vigora o princípio da não interferência nos assuntos internos dos Estados[190]. Para a própria eficácia a um nível de extensão global do direito ao apagamento, seguimos a opinião de Francisco Lima e Mateus Magalhães, ao vislumbra a técnica do bloqueio geográfico dos utilizadores de modo a vedar ou limitar a ligação a partir do IP, sem menosprezar que este sirva como medida completar de outros métodos, mas este poderá ser o único capaz de compatibilizar o Direito da União Europeia com o Direito Internacional, na medida em que existe a necessidade de obter um equilíbrio entre as legitimas espectativas dos Estados soberanos e a necessária defesa dos direitos dos titulares de dados, independentemente do local e em *conformidade interjurisdicional*.

Segundo Kuner, é necessário tornar o âmbito do direito ao apagamento proporcional à sua aplicabilidade prática, impedindo que se torne tão abrangente ao ponto de se tornar insignificante[191][192]. Neste aspeto, Rui Ataíde sustenta que para efetuar a remoção ou

---

[188] Francisco Lima e Mateus Carvalho, O Direito ao apagamento de dados como realidade global, in: *Anuário de Proteção de Dados*, 2019, CEDIS, p.61-63.

[189] Francisco Lima e Mateus Carvalho, *op. cit.*, p.66-68.

[190] Artigo 7.º, n.º 2 da Carta da Nações Unidas.

[191] Christopher Kuner, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines, in*: LSE Legal Studies Working Paper*, LSE Law, N.º 3, 2015, p. 20-22.

[192] O modo como o apagamento deverá ser realizado pode versar sobre diferentes modelos: a) apagamento global; b) apagamentos baseados no domínio; c) apagamento híbrido fundado na geo-localização. Anuário de proteção dados.

eliminação do nome de um titular de dados das pesquisas no motores de busca, devemos atender a diversos fatores, sem qualquer hierarquia e/ ou interdependências entre si, a saber: a) *papel do titular na vida pública*; b) *natureza da informação*; c) *tipo de informação que indica uma preponderância do interesse público*; d) *fonte*; e e) *tempo*[193]. O mesmo autor suporta ainda que o direito à memoria e à verdade histórica prevalecem sobre o direito ao esquecimento nos casos em que o interesse público da informação se sobrepõe à defesa da honra e dos dados pessoais em causa[194]. Destarte, do ponto de vista técnico pode ser muito difícil, ou mesmo impossível, de proceder a uma ordem judicial que decrete o apagamento de dados pessoas, pois, como é bem sabido todos os dados que são colocados na Internet não desaparecem, nem quando apagados pelo motor de busca, uma vez que existem múltiplas plataformas que agregam toda a informação que dá entrada em ambiente digital (ex: Internet Archive). Destarte, a figura do direito ao apagamento é um importante passo que o RGPD elencou na defesa dos direitos dos cidadãos, todavia surge ainda como figura híbrida pela ponderação de direitos em análise que proclama.

4.7 Diretiva (EU) 2016/1148

A Diretiva (EU) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, relativa às medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, mais conhecida como "Diretiva NIS" apresenta como foco a regulação da segurança das redes e dos sistemas de informação nos Estados-membros. Esta Diretiva reveste especial relevância práticas para os operadores de serviços essenciais e para as infraestruturas críticos nacionais, que estão presentes no quotidiano dos cidadãos europeus e afetam significativamente a sua qualidade de vida e a sua segurança.

Esta Diretiva parte do pressuposto de que existem assimetrias entre os Estados-membros ao nível da cibersegurança, resultando numa gama de heterogeneidade na União Europeia ao nível das redes e sistemas de informação. A Diretiva NIS (ou SRI em português), assenta em três pilares essenciais: a) a resiliência cibernética; b) o reforço das políticas e recursos de defesa cibernéticos da PCSD, nomeadamente ao nível industrial dos recursos tecnológicos; e c) política internacional de cooperação no ciberespaço. A competência

[193] Rui Ataíde, Direito ao esquecimento, in: *CyberLaw by CIJIC*, Edição N.º VII, 2019.
[194] *Ibidem*.

partilhada entre a União Europeia e os Estados-membros nesta matéria demostrou a crescente securitização coletiva digital dos Estados-membros e dos órgãos e agências da União Europeia.

Inicialmente, a proposta de aplicabilidade só incluía três áreas relativas a setores de serviços essenciais: as plataformas online, o setor energético e o setor dos transportes. Posteriormente, os serviços essências foram propostos pela Comissão como serviços essenciais para a manutenção das atividades sociais e económicas da sociedade, constantes no anexo II da Diretiva NIS. Os Estados-membros divergiram no suporte a esta proposta inicial. As empresas multinacionais sentiram uma ameaça, tendo em conta a sua principal atividade de negócio, assentando na oferta de serviços digitais inscritos no artigo 4.º da Diretiva NIS, como *serviços de computação em nuvem*.

Analisando a diretiva por rúbrica, saltam claro algumas obrigações, tais como: i) desenvolvimento/atualização de estratégias nacionais de cibersegurança[195] (artigo 7.º); ii) estabelecimento/definição da autoridade nacional em matéria de segurança das redes e dos sistemas de informação (artigo 8.º); iii) criação de equipas nacionais de resposta a incidentes informáticos (CSIRT)[196], responsáveis pelo tratamento de incidentes e riscos (artigo 9.º) e redes CSIRT (artigo 12.º); iv) inclusão de uma rede de cooperação que será essencialmente uma rede de aplicação da lei composta pelos reguladores nacionais e pela Comissão Europeia (artigo 11.º); v) notificação de incidentes para as empresas (artigo 14); vi) investigações regulamentares e auditorias (artigo 15.º); e vii) imposição de sanções às "*infrações e às disposições nacionais aprovadas* (…)" (artigo 21º).

Quanto aos setores diretamente incluídos, pela estipulação jurídica do artigo 4.º, n.º 4, que designa os *operadores de serviços essenciais*, esclarecesse que se inscrevem nesta definição o setor da energia (eletricidade, petróleo e gás), transportes (transporte aéreo, ferroviário, marítimo e por vias navegáveis interiores e rodoviário), bancário, infraestruturas do mercado financeiro, setor da saúde, fornecimento e distribuição de água potável e infraestruturas digitais.

O legislador europeu tentou propor o mínimo denominador comum com vista a harmonização entre os Estados-membros, todavia no curto prazo este denominador poderá ser insuficiente face ao constante aumento de ciberataques em solo europeu. Por

[195] Esta estratégia deve compreender: i) medidas de preparação e resposta face a ciberataques; ii) elencar um conjunto de funções, responsabilidades e cooperação dos organismos governamentais e de outros intervenientes relevantes; iii) instrução de programas de ensino, sensibilização e formação; iv) planos de investigação e desenvolvimento; e iv) construção de um plano para a identificação de riscos.

[196] Para mais desenvolvimentos, poderá consultar a rede nacional CSIRT, *v.* https://www.redecsirt.pt/.

outro lado, foi dada margem de discricionariedade suficiente para que os Estados-membros pudessem adotar disposições que garantissem um nível mais elevado de maturidade ao nível da segurança do sistema de informação, mas alertamos que esta margem de discricionariedade pode resultar em incongruências jurídicas e operacionais ao nível dos Estados contribuindo para a antagonização da segurança da informação no espaço europeu.

Neste ponto, cabe realçar a importância da figura dos *operadores de serviços* essenciais e dos *prestadores de serviços digitais*, sendo-lhes incumbida a obrigação de notificação de um incidente de segurança e adaptação dos serviços e sistemas de informação para os novos desafios tecnológicos, por forma a elevar a maturidade cibernética e resiliência face a ataques por via digital às organizações operantes no mercado.

4.7.1 Das autoridades nacionais

Quanto ao papel das autoridades nacionais, monitorizam a aplicação da Diretiva, nomeadamente, cabe-lhes: i) avaliar as políticas de cibersegurança dos Estados-membros; ii) supervisionar os prestadores de serviços digitais; iii) participar nos grupos de trabalho, nomeadamente pelas entidades nacionais criadas para o efeito, com a Comissão Europeia e a ENISA; iv) informar o público, sempre que haja necessidade de proceder à tomada de medidas de segurança, de modo a evitar comprometer a segurança da informação, respeitando a confidencialidade; e v) emitir instruções ou diretrizes vinculativas para corrigir anomalias registadas;

Às equipas CSIRT, como inscrito no anexo I da Diretiva, cabe-lhes a obrigatoriedade de assegurar a ampla *continuidade operacional dos serviços de comunicações*, e é-lhes atribuído os deveres de: i) proceder à monitorização de incidentes de cibersegurança e reagir perante estes; ii) proceder à analise de risco dos incidentes e obter o panorama situacional; iii) participar ativamente na rede CSIRT; iv) cooperar com o setor privado; e v) promover a utilização das práticas normalizadas para a gestão de riscos e a classificação de informações[197].

[197] Cfr. ENISA, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary*, 2018, disponível para consulta em: https://www.enisa.europa.eu/publications/csirts-le-cooperation. Por exemplo, os órgãos e instituições da UE seguem um esquema próprio para classificação da informação. Cfr. David Galloway, Classifying Secrets in the EU, in: *Journal of Common Market Studies*, Vol.52, N.º3, pp. 668-683.

4.7.2 Da notificação do incidente

A Diretiva NIS veio proteger as empresas e o mercado único digital e promover uma cultura de gestão de riscos. Nesse sentido, as empresas notificadas na qualidade de *operadores de serviços* essenciais, para além de pertencerem à rede CSIRT nacional, firmam um compromisso tácito no sentido de elevar os padrões de maturidade de segurança da informação e das redes, nomeadamente através de avaliações continuas de riscos e, se o considerarem adequado face ao risco obtido, agir diligentemente, conforme descrito no artigo 14.º da Diretiva. Esta ação deve ser materializada pela notificação, recorrendo aos mecanismos legais previstos e aos canais das próprias entidades, neste caso as autoridades competentes e às equipas CSIRT. Assim, uma vez detetada uma vulnerabilidade ou qualquer incidente relevante, como por exemplo, a deteção de *malware* na rede elétrica deve ser imediatamente reportada. Neste caso, estavam em causa a continuidade do bem-estar e segurança nacional e desse modo o efeito perturbador era significativo, mas exemplos com efeitos perturbados menos significativos como indisponibilidade temporária da rede nacional serviços de saúde, pode ser considera essenciais ou a interrupção no fornecimento de bens devem, de igual modo ser reportadas[198].

De forma suplementar, mesmo que uma organização não tenha sido notificada como operador de serviços essenciais por não caber no âmbito de aplicabilidade nos termos do artigo 4.º, n.º 4 da Diretiva NIS, se a mesma for afetada por incidentes com impacto significativo nos serviços que prestam e, se entenderem que é do interesse público notificar a ocorrência do incidente, podem fazê-lo. Todavia, tal notificação não implica a obrigação da autoridade competente ou CSIRTs procederem a um tratamento da mesma, mas existe um dever de fazê-lo, desde que não implique um encargo desproporcionado ou indevido aos Estados-membros[199].

[198] Os prestadores de serviços digitais importantes, como por exemplo, motores de pesquisa ou serviços de computação em nuvem são destinatários e, por sua vez, devem cumprir os requisitos de segurança e de notificação.
[199] Cfr. Ponto 67 da Diretiva NIS.

4.7.3 Determinação do efeito perturbador

O efeito perturbador deverá ser determinado pelos Estados-membros tendo em conta alguns critérios específicos, como salienta o artigo 6.º, nº 1 e 2 da Diretiva em análise:

1. *O número de utilizadores que dependem dos serviços prestados pela entidade em causa*;
2. *A dependência de outros setores* como a energia, transportes, setor bancário, infraestruturas do mercado financeiro, saúde, fornecimento e distribuição de água potável *em relação ao serviço prestado*;
3. O possível impacto dos incidentes (mensurando a intensidade e duração) nas *atividades económicas,* sociais *ou de segurança pública*;
4. *A quota de mercado dessa entidade*;
5. *A distribuição geográfica* (determinando a zona que pode ser afetada pelo incidente);
6. *A importância da entidade para a manutenção de um nível suficiente de serviço, tendo em conta a disponibilidade de meios alternativos para a prestação de serviço*;
7. *Fatores setoriais específicos* de um setor determinado pelos Estados-membros, desde que, considerados adequados.

4.7.4 Cooperação técnica e sanções

Do ponto de vista sancionatório, os Estados-membros da UE devem proceder à aplicação de sanções *efetivas, proporcionais* e *dissuasivas*, a fim de garantir a aplicação das disposições conforme estabelece no artigo 21.º da Diretiva NIS. A avaliação da abordagem adotada pelos Estados-membros é apresentada pela Comissão ao Parlamento Europeu e ao Conselho, conferindo à Comissão o poder fiscalizador e a consciência situacional geral da *experiência adquirida a nível estratégico e operacional*.

4.7.5) CSIRTs

A Diretiva NIS estabelece um grupo de cooperação, responsável, entre outras tarefas, por: i) fornecer orientações à rede CSIRT; ii) proceder ao intercâmbio de boas práticas na determinação dos operadores de serviços essenciais; iii) apoiar os Estados-membros no desenvolvimento das capacidades de cibersegurança; iv) promover o intercâmbio das melhores práticas em matéria de sensibilização, formação, investigação e desenvolvimento[200]; v) promover o intercâmbio das melhores práticas em matéria atinente a riscos e incidentes; vi) discutir as formas de comunicação, em especial das notificações de incidentes.

Como inscrito no artigo 9.º da Diretiva NIS, as redes CSIRT são composta por representantes nacionais que " (…) *cumpram as obrigações estabelecidas no anexo I, ponto 1, e que abranjam pelo menos os setores referidos no anexo II e os serviços referidos no anexo III, responsáveis pelo tratamento dos riscos e incidentes, de acordo com um processo bem definido*.[201]" As redes CSIRT podem ser criadas no âmbito de autoridades competentes e cabe aos Estados – membros zelar pela sua eficiência, eficácia e segurança.

As redes CSIRT, devem proceder às atribuições e obrigações constantes no artigo 12.º e anexo I da Diretiva NIS. O trabalho serve como forma de intercâmbio e cooperação operacional, tendo em conta que estas devem "(…) *preencher os requisitos essenciais para garantir capacidades efetivas e compatíveis para fazer aos incidentes e aos riscos e para assegurar uma cooperação eficaz a nível da União*.", sendo que também existe a indicação para a participação das CSIRT europeias em redes de cooperação internacional como consta no ponto 34 da Diretiva NIS. Adverte-se ainda, que as atribuições do grupo de cooperação e da ENISA são *interdependentes* e *complementares*[202].

As redes CSIRT (e as autoridades competentes) estão incumbidas do dever de confidencialidade aquando do cumprimento (obrigatório) das notificações, nomeadamente no que toca a informações sobre as vulnerabilidades dos

[200] Destacamos aqui o ciclo de exercícios CyberEurope, onde cabe ao grupo de cooperação as decisões estratégicas respeitantes a este e outros exercícios, em especial, mas não exclusivamente, no que respeita à regularidade da realização do exercício e à conceção dos cenários. Por sua vez, à ENISA compete a organização e realização destes exercícios, tendo que facultar conhecimentos especializados e prestar aconselhamento ao grupo de cooperação e à rede CSIRT. Cfr. Ponto 42 da Diretiva NIS.

[201] Por exemplo, em Portugal, a autoridade competente é o CNCS, que descreve que as CSIRTs como um *"(..) fórum de excelência para a partilha de informação de carácter operacional*", elencado em vários objetivos. Para mais informações, *v*. https://www.cncs.gov.pt/cooperacao/rede-nacional-de-csirt/.

[202] Cfr. Ponto 38 da Diretiva NIS.

produtos/serviços que sejam considerados estritamente confidenciais até à divulgação de medidas de segurança para as resolver[203].

Ao nível dos órgãos e instituições da UE também existe uma equipa de resposta a emergências informáticas a CERT-UE[204].

4.7.6 Posição sumária adotada

A Diretiva NIS representa um importante contributo para a coerência entre atores multinível (Comissão Europeia, Estados-membros, ENISA e grupos de cooperação-formais e informais), orientando uma estratégica de longo prazo para a União Europeia no capítulo da segurança das redes e da informação. Se, por um lado, existem Estados que preferem elevar o seu grau de maturidade de segurança da informação, como a Alemanha, Holanda, França ou Itália, por outro lado, existem Estados que preferem as formas de cooperação sub-regional, como por exemplo a Áustria, que estabeleceu a Central European Cybersecurity Platform (CSCSP) e prefere promove um registo de cooperação entre as respetivas equipas CERTs e as CSIRTs[205].

Houve um efetivo reconhecimento nas discrepâncias entre os Estados-membros, tendo como objetivo a harmonização do quadro europeu e a proteção dos serviços vitais para a sociedade e economia da UE. A importância do compromisso digital aliado à ligação e coerência entre setor privado e público são fundamentais para alcançar níveis de desenvolvimento superiores pelos Estados - membros[206]. A orgânica descentralizada poderá ser assim um aspeto prático ainda limitador do empolamento da resiliência cibernética, pois essa competência, cabe, primeiramente ao Estados-membros através do pelouro da governação e orgânica de segurança interna, enquanto que a União Europeia apoia a consistência, coordenação e desenvolvimento dos recursos e capacidades dos Estados. Resta perceber se em caso de uma cibercrise que afete territorialmente vários

---

[203] Cfr. Ponto 59 da Diretiva NIS.

[204] Existe uma equipa com os mesmos objetivos, mas de âmbito territorial português, a CERT.PT, em funcionamento no CNCS, "*O CERT.PT tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal*". Pedro Veiga, *European Cybersecurity Policy NIS Directive*, p. 10, disponível para consulta em: https://www.cncs.gov.pt/content/files/2017_06_22_-_pedroveiga_-_pt_-_final.pdf.

[205] Helena Carrapico e André Barrinha, *op. cit*., p. 1263-1267; George Christou b), The European Union and Cybercrime, in: *Cybersecurity in the European Union Resilience and Adaptability in Governance Policy*, 2016, p. 121 e ss.

[206] *Ibidem.*

Estados-membros da UE estas formas de cooperação, em particular, se os *fora* de intercâmbio de informações e a coordenação na resposta é bem arquitetada entre os Estados, ou permanece numa lógica puramente unilateral. Parece ainda saltar claro a relação de interdependência entre segurança da informação e proteção de dados, podendo ser tratas de forma autónoma, mas devendo observar-se como complementares naquele que é o objetivo primordial: assegurar a segurança em ambiente digital.

A criação de um mecanismo de certificação, a preparação de um plano operacionalizado de resposta aos desafios da cibersegurança, o investimento na proteção e encriptação[207] dos sistemas que armazenam os dados, as aplicações e redes[208], bem como a proteção dos direitos fundamentais no ciberespaço são vertidos em ações concretas e essenciais ao longo deste documento normativo. Com efeito, foi reconhecido à ENISA o papel de facilitador, concertando a organização a nível supranacional das competências da segurança da informação, onde se inclui a vertente da cibersegurança.

4.8 Pacote de Cibersegurança da UE e desenvolvimentos ulteriores

Em 2017, já com a publicação sobre o livro branco sobre o futuro da Europa: "*Reflexões e cenários para a UE em 2025*" houve a pretensão de recentrar a União no mercado único digital. O Presidente da Comissão Europeia, Jean- Claude Juncker, afirmou, "*In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks.*", aquando do seu discurso sobre o Estado da União[209]. Neste

[207] Nesse sentido, *v*. James Lewis, Denise Zheng e William Carter, *The Effect of Encryption on Lawful Acess to Communicatins and Data*, Center For Strategic & International Studies. Rowman Littlefield, 2017.; Lindsey Sheppard et. alli, *The Spectrum of Encryption: Safety and Security Considerations*, Center For Strategic & International Studies, 2020.

[208] Para uma análise em detalhe sobre a necessidade de uma design de arquitetura que facilite o dia a dia das interaçãoes entre organizações públicas e privadas de modo a obter um modelo de segurança superior, nomeadamente com recurso à criptografia, *v*. Sélinde van Engelenburg, Marijn Janssen e Bram Klievink, Design of a software architecture supporting business-to-government information sharing to improve public safety and security, in; *Journal of Intelligent Information Systems*, Springer, 2017.

[209] Comissão Europeia, *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*, 2017, disponível para consulta em: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.
Entre outras medidas, verificasse o reforço das competências da ENISA, um conjunto de ferramentas para a aplicação da diretiva NIS; um plano de ação para uma resposta eficaz em caso de ciberataques que afetem vários Estados-Membros; reforço da autonomia estratégica da União através de uma maior capacidade de investigação e criação de uma ciberdefesa e ciber-higiene; fomento de competências adequadas na União em rede com parceiros em todo o mundo, incluindo a NATO.

discurso foi lançado um conjunto de instrumentos, apelidos no seu conjunto de "*cybersecurity package*" que tinha como o objetivo central a elevação do grau de resiliência digital na União.

No decorrer de 2018, o Conselho adotou conclusões sobre as condutas ilícitas no ciberespaço, destacando "(…) *a importância de um ciberespaço mundial, aberto, livre, estável e seguro, no qual se apliquem inteiramente os direitos humanos, as liberdades fundamentais e o Estado de direito*"[210], de forma a poder investigar e extinguir todas as ameaças de Estados terceiros e organizações não estatais que tentem minar os objetivos, interesses e valores da União. Os altos dirigentes da União demostraram as suas preocupações com o tema ao pedirem o reforço das ações encetadas perante as ameaças de natureza química, biológica, radiológica e nuclear (NBRN), e mais concretamente perante os ciberataques, perpetrados contra a Organização para a Proibição de Armas Químicas (OPAQ), sediada em Haia[211].

No mesmo ano, tiveram lugar duas iniciativas fundamentais para a construção sustentada de um projeto de SI ao nível comunitário: a atualização do Quadro-Estratégico da UE para a Ciberdefesa[212] e o "Regulamento da Cibersegurança"[213].

O primeiro, resulta da evolução dos desafios em matéria de segurança adotado em 2014, onde a ciberdefesa é mencionada como um domínio prioritário, a par das preocupações da Comissão. Um aspeto fundamental deste quadro estratégico discorre sobre o apoio ao desenvolvimento das capacidades de ciberdefesa dos Estados-membros, cabendo, de modo coordenado ao Serviço Europeu de Ação Externa (SEAE), à Comissão e à Agência Europeia de Defesa a materialização destas capacidades, por via de projetos coordenados entre Estados-membros. Aqui, importa sobretudo monitorizar de forma contínua os riscos e vulnerabilidades internas e as ameaças externas às infraestruturas de informação que apoiam as missões e operações da PCSD, bem como manter a sua operacionalidade em cenários reais onde haja uma efetiva projeção de força (civil, militar ou mista). Uma maior

---

[210] Conselho Europeu e Conselho da União Europeia, *Ciberatividades maliciosas: Conselho adota conclusões*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.

[211] Conselho Europeu e Conselho da União Europeia, *Conselho Europeu, 18 de outubro de 2018*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/meetings/european-council/2018/10/18/.

[212] Conselho da União Europeia, *Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018)*, 2018, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pt/pdf.

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

proteção dos sistemas de comunicação e informação ao nível da PCSD utilizados pelas entidades e órgãos da UE, em especial, para proteção dos sistemas de comunicação e informação da atividade desenvolvida pelo SEAE. Quanto ao desenvolvimento técnico das capacidades de TI resultam de uma cadeia de comando unificada, tem como objetivo último a melhoria na resiliência das redes e sistemas utilizados no âmbito da PCSD[214][215]. Neste domínio, o intercâmbio de informações em termos de boas práticas, pode servir para criar mecanismos de alertas precoce, proceder a avaliações de risco de resposta a incidentes, e desenvolver uma rede holística de ações de sensibilização e exercícios[216] para além das já existentes equipas CERT (que apresentam uma natureza e missão especifica, ligadas a uma extensa rede europeia em ligação com a ENISA), contribuindo para a malha global de redes de informação.

Quanto ao segundo, assenta na disposições do Regulamento (EU) 2019/881 do Parlamento Europeu e do Conselho de 17 de abril de 2019, relativo à ENISA e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (EU) n.º 526/2013, que veio operar uma reforma estrutural à ENISA por outro lado, e por outro veio introduzir um quadro de certificação europeu[217].

Quanto à Ciberdefesa, o Conselho iniciou a ronda de negociações com o Parlamento Europeu, no sentido de criar um regulamento para reforçar a ciber- resiliência estabelecendo um quadro de certificação à escala da UE para produtos e serviços TIC[218].

---

[214] Note-se que esta cadeia de comando unificada já é uma realidade na dimensão operacional da gestão de crises. Veja-se o artigo 3.º, relativo à cadeia de comando e estrutura, da Decisão 2014/219/PESC do Conselho de 15 de abril de 2014 relativa à missão PCSD da União Europeia no Mali (EUCAP Sael Mali), "*1. A EUCAP Sael Mali tem uma cadeia de comando unificada para as operações de gestão de crise.*"

[215] A fim de melhorar a coordenação e reforçar a proteção e a resiliência das redes e dos sistemas de comunicação e informação da PCSD, foi criado em 2018 no SEAE um Conselho interno de cibergovernação sob a direção do secretário geral do SEAE.

[216] O primeiro exercício ocorreu em 2010, com um conjunto de trinta Estados da Europa. Destacamos dos exercícios: a) UE Blueprint, que explica como a cibersegurança, e em particular os mecanismos de gestão devem atuar durante uma crise existente e como são estabelecidos os objetivos e formas de cooperação entre os Estados-Membros; e b) CiberEurope, que visa avaliar os procedimentos operacionais padrão no intercâmbio de informações além-fronteiras, tendo como pano de fundo ataques a infraestruturas críticas como, por exemplo, o setor de energético ou transportes. Para mais informações, *v.* https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme e https://www.enisa.europa.eu/events/artificial-intelligence-an-opportunity-for-the-eu-cyber-crisis-management/workshop-presentations/20190603-ec-blueprint.pdf/view. ; Tribunal de Contas Europeu, *op. cit.*, pp. 38-42, disponível para consulta em: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf.

[217] Comissão Europeia, *The EU Cybersecurity Act*, 2020, dispoonível para consulta em: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

[218] Nesse sentido *v.* Robert Dewar e Ellie Templeton, The impact of regulatory frameworks on the global digital communications industry, in: *Cyber Security Policy Brief*, GCSP Cyber Security Policy Brief, p.11 e ss.

Por um lado, foi criado um sistema de certificação à escala da UE, e por outro reforçados os poderes da ENISA[219]. Quanto ao esquema de certificação previsto, assenta em duas vertentes: i) uma dirigida à certificação nacional dos Estados-membros onde é atribuído um selo de segurança informática e de boas práticas, como já acontece com a França, Reino Unido e Países Baixos; e ii) a implementação do sistema SOG-IS, consistindo no reconhecimento mútuo em doze Estados-membros e na Noruega que integram e desenvolvem um conjunto de perfis e produtos digitais[220]. O objetivo último passa pela segurança do utilizador final da tecnologia, em paralelo com o princípio de governança aberta, transparente e inclusiva reconhecida em todos os Estados-membros da União[221].
Por último, em 2020, a Comissão Europeia lançou um comunicado no sentido de reformar a União Europeia, sob o tema: "*Reparar e preparar para a próxima geração*"[222], congregando um conjunto de medidas encetadas pela reformada estratégia de Cibersesegurança, que cooperará para o aumento do conhecimento ao nível da maturidade das instituições e das capacidades de resiliência ao nível da UE. Num segundo plano está previsto que a nova estratégia possa acompanhar as parcerias industriais e a iniciativa privada de novas empresas (PME) no setor tecnológico. Por último, ficou conjeturada revisão da Diretiva NIS e a apresentação de um conjunto de propostas de medidas direcionadas para as infraestruturas críticas nacionais do Estados-membros[223].

[219] Conselho Europeu e Conselho da União Europeia, *UE mais resistente à cibercriminalidade graças ao apoio do Conselho ao acordo sobre certificação comum e a uma agência fortalecida*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/.
[220] Esta certificação não é obrigatória para os Estados-membros, o regime funciona sob um escopo voluntarista a menos que alguma norma da UE venham dispor a obrigatoriedade da sua implementação. Esta certificação contribui para a normalização da segurança digital e confiança dos consumidores em ambiente digital. Comissão Europeia, *The EU cybersecurity certification framework*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.
[221] Por exemplo, no caso dos equipamentos IoT existe legislação específica aprovada pela União Europeia que lhe é diretamente aplicável. Para mais informações *v.* https://oxil.uk/publications/iotsf-cybersecurity-regulation-ready/. *V*. nota 53.
[222] Comissão Europeia, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Europe's moment: Repair and Prepare for the Next Generation*, disponível para consulta em: https://ec.europa.eu/info/sites/info/files/communication-europe-moment-repair-prepare-next generation.pdf.
[223] Comissão Europeia, *Cybersecurity*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks; Comissão Europeia, *2020 Commission Work Programme*, 2020, disponível para consulta em: https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en.

4.8.1 Ataques em ambiente digital

Ao nível político, os parlamentos nacionais tem sido alvos de ciberataques. Por exemplo, o parlamento alemão foi alvo de uma tentativa frustrada de propagação de *malware* por parte de um site Israelita[224]. Da mesma forma, quando a ENISA tinha em marcha um programa de formação sobre saúde e cibersegurança, evento organizado sob a tutela da presidência de Malta no Conselho, quando um ciberataque bloqueou todos os sistemas de informação de 40 hospitais do Reino Unido. Este ciberataque em concreto não se circunscreveu apenas ao território do Reino Unido, várias organizações de saúde depararam-se com uma mensagem de *ransomware*[225] com um pedido de resgate financeiro nos seus sistemas, tendo posteriormente resultando na perda de dados médicos. Este incidente viria a ser denominado por WannaCry[226], tendo um impacto direito em mais de 150 Estados e 230.000 sistemas de informação, inviabilizando inúmeros atos médicos. Este tipo de ataques tem ganho expressão entre organizações e cidadãos, por isso, entendesse como urgente uma cultura de segurança da informação tanto em ambiente físico e, com maior premência em ambiente digital.

4.8.2 Cibersegurança a diferentes velocidades

A ENISA em conjunto com os Estados-membros coordena a implementação, monitorização e avaliação das estratégias nacionais de cibersegurança[227], tendo em conta as duas premissas na sua elaboração – inclusão (quanto às partes interessadas) e abertura (relativa aos domínios tecnológicos abordados)[228]. Em termos globais, no ano de 2017, mais de noventa e cinco Estados tinham desenvolvido legislação relacionada à cibersegurança, mais de cinquenta Estados tinha desenvolvido capacidades defensivas ao

[224] Reuters, *German parliament foiled cyber attack by hackers via Israeli website,* 2017, disponível para consulta em: https://www.reuters.com/article/us-germany-cyber-idUSKBN1701V3.
[225] Segundo os últimos dados da União realtivos à invesgação criminal no ciberespaço, apontam o *ransomware* como sendo a prioridade das ameaças. EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA)*, 2020, p.24.
[226] Em termos técnicos, resultou de um *ransomware* que afetou uma vulnerabilidade do Windows OS, propagando o caos pela forma massiva de distribuição. Para mais informações *v*., https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.
[227] A ENISA recomendou expressamente a previsão nas estratégias nacionais de cibersegurança a par de outros documentos basilares, a incorporação da definição de responsabilidades. Adicionalmente, foi realçada a visão de segurança além-fronteiras, nomeadamente a incluir as tecnologias emergentes nas estratégias nacionais e ferramentas potencialmente disruptivas, como IoT, *Dig Data*, IA, entre outras.
[228] ENISA, *op. cit.*, p.17.

nível da cibersegurança e mais de trinta Estados tinham já desenvolvido capacidades ofensivas[229].

No seio da União, dependendo do grau de ameaça percecionado, os utilizadores da Internet podem sentir-se mais ou menos seguros no ciberespçao, de acordo com o número de incidentes de segurança da informação e do grau de exposição social dos ciberataques. Fatores estes que contribuem para o sentimento de "ciber-ansiedade"[230]. O termo "ciber-ansiedade" surge ainda como *difuso* e *abstrato*, mas é reflexo de uma meta-narrativa do ciberespaço como reflexo da perpetração e massificação do cibercrime e outras atividades nele praticadas[231]. Os factos revelados por Edward Snowden acerca da vigilância governamental sobre cidadãos caiu com grande estrondo na comunidade internacional, pois tais condutas não se circunscreveram apenas a uma determinada porção geográfica e não se coadunam com os princípios de direito internacional. De acordo com as informações recolhidas podem ter finalidades últimas motivações económicas, por exemplo, espionagem económica ou industrial[232][233].

Contudo, não colocando em causa a trajetória escolhida para a política externa europeia, e tendo em conta as revelações públicas de Edward Snowden, a União terá que se afirmar com um forte compromisso de princípio para com os EUA, caso contrário, poder-se-ão vir a repetir factos desconhecidos de partilha de informações ou recolha de informações desconhecidas pela UE por parte de órgãos dos EUA. A retórica americana seguiu uma estratégia de descredibilização dos factos revelados, baseando o seu argumento no alto

---

[229] Piret Pernik, *National Cyber Security Strategies The Estonian Approach*, International Centre for Defence and Security, 2017.

[230] Katharina Dimmroth e Wolf Shunemann, The Ambiguos Relation Between Privacy and Security in German Cyber Politics, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), 2017, p. 101.

[231] Cfr. Paul Cornish, Deterrence and the Ethics of Cyber Conflict, in*: Ethics and Policies for Cyber Operations: NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Mariarosaria Taddeo e Ludovica Glorioso (eds), Philosophical Studies Series, Vol. 124, Springer, pp. 3-4.

[232] Na Alemanha, a narrativa defendida pelos decisores passa objetivamente pela defesa da indústria nacional através da implementação de medidas defensivas ou outras além destas, caso contrário, poderiam haver perdas a ascender à casa dos biliões de euros colocando em causa a vitalidade da económica alemã. Como sustenta Thomas Oppermann, "*Our corporations are suffering billion dollar losses through economic espionage. We can't protect them from it effectively enough. That's why we have to think about the recovery or at least partial restoration of our technological sovereignty. That means safe networks, secure communication, encryption and further preventive measures*. (. . .) *The NSA affair has to be a wake-up call for all of us*". Thomas Oppermann, Deutscher Bundestag, in: *Stenografischer Bericht*, Berlim, 2013.

[233] Annegret Bendiek a), European Cyber Security Policy, in: *SWP Research Paper*, N.º 5. Disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf.

nível de cooperação ao nível da partilha de informação entre os dois continentes e a prossecução de interesses legítimos de defesa nacional[234].

A cibersegurança poderá apresentam um alto grau de *volatilidade* social incerto no quadro europeu, certamente que colisões de direitos fundamentais, inscritos em instrumentos multinível de proteção de direitos humanos cederão perante a precedência aos legítimos interesses de segurança e defesa nacional dos Estados-membros. Por exemplo, na Alemanha os serviços de informações utilizaram as suas atribuições para garantir que não seriam perpetrados quaisquer incidentes digitais no parlamento, mesmo que para tal, fosse necessário violar a privacidade e direitos fundamentais consagrados em diversas normas regulatórias. Destarte, parecem imperar os valores securitários de defesa e segurança nacional[235] em relação aos direitos fundamentais do indivíduo, conduto salientamos que o excesso de zelo nas competências das autoridades de determinados Estados sob o capote dos objetivos de segurança e defesa nacional não é certo, como sustenta a jurisprudência do TEDH, que tende a ter sempre uma visão do equilíbrio de direitos em causa.

A preterência pelos valores securitários assenta na retórica em que é garantido um bem maior, a *segurança física e digital da coletividade*, lembrando Hans-Dieter Heumann, "(…) *segurança é um requisito da liberdade*"[236]. A larga maioria da doutrina foca o seu objeto na aplicação de medidas tendentes à segurança coletiva, convergindo para a ideia de securitização estatal, ao invés da defesa da primazia da privacidade do indivíduo neste necessário equilíbrio fundamental entre direitos fundamentais e segurança[237].

Especificamente em relação à cibersegurança, na elaboração de uma Lei de cibersegurança a nível nacional é necessário observar o seu contexto geral – à luz quadro regulamentar geral, e em específico – atendendo às práticas estabelecidas e à cultura de determinado Estado[238]. Deste modo, o legislador interno de cada Estado deve atender ao sentido da defesa dos utilizadores das tecnologias de informação e comunicação, não cabendo aos Estados relegar *direitos* (ex. direito à liberdade e à segurança, proteção de

---

[234] Hans-Peter Friedrich afirmou: "*We expect further clarification. But it's also true that the Americans are essential partners to us in the area of terror prevention. We exchange important Information*". Hans Friedrich, in: *Diese Daten helfen uns*, Interview mit Bundesinnenminister, 2013.

[235] Katharina Dimmroth e Wolf Shunemann, *op. cit.*, p. 109-110.

[236] Bundesakademie für Sicherheitspolitik, *Cyber-Realitat zwischen Freiheit und Sicherheit*, 2015, disponível para consulta em: https://www.baks.bund.de/de/aktuelles/cyber-realitaet-zwischen-freiheit-und-sicherheit.

[237] Barry Buzan, Ole Waever e Jaap de Wilde, *Security: A new framework for analysis*, Boulder, Lynne Rienner, 1998.

[238] Lina Jasmontaite e Valentina Pavel Burloui, Lithuania and Romania to Introduce Cybersecurity Laws: Attaining Information Security at the Cost of Individuals Rights, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), 2017, p. 135.

dados pessoais) *liberdades* (ex. liberdade de expressão e informação) e *princípios* (democracia e Estado de Direito) para atender a uma Lei de cibersegurança ultra protecionista. Por exemplo, a Roménia publicou uma Lei de cibersegurança que mais tarde viria a ser declarada inconstitucional[239]. Tal como a CEDH prevê, e o TEDH reafirma no caso Ahmet Yildirim vs Turkey[240], existem pré-requisitos para a limitação ou restrição de direitos dos cidadãos. Este caso tratava de uma decisão de um processo, no qual foi decretado um bloqueio ao *Google Sites* que hospedava determinadas páginas no acesso a serviços em ambiente digital. Foi precisamente por causa de uma destas páginas bloqueadas e hospedadas no *Google Sites* que o requente, que nada tinha que ver com o processo principal em apreciação, foi afetado por uma decisão judicial de um terceiro. O TEDH, ao analisar o quadro regulatório e, em particular, os critérios formais e materiais para bloquear os serviços em ambiente digital, concluiu que houve violação do artigo 10.º da CEDH, considerando que os efeitos da medida em questão foram arbitrários e a revisão judicial do bloqueio de acesso decretado foi insuficiente para evitar abusos. O TEDH veio sublinhar que determinada medida "prevista na lei" necessita de garantir uma certa *qualidade de medida reguladora*. Acrescentou ainda, que tal medida deve ser *precisa*, *acessível ao público*, com *previsibilidade* em relação aos resultados esperados e em *conformidade* com o Estado de Direito. Além desta, a decisão interna foi contestada por não se verificar se uma medida de menor alcance poderia ter sido adotada para bloquear o site em específico, sublinhando, que o tribunal não considerou os vários interesses das partes, em particular de terceiros quanto à necessidade de bloquear todo o acesso ao *Google Sites*. O TEDH rematou, expondo que os tribunais internos deveriam observar que através dos efeitos da decisão tomada tornariam inacessíveis grandes quantidades de informação, afetando diretamente os direitos dos cidadãos utilizadores do *Google Sites* produzindo efeitos colaterais significativos.

[239] Na Roménia, o ministério da administração interna publicou uma Portaria de emergência de forma a reorganizar uma unidade de inteligência militar, facultando a esta a possibilidade de realizar interceções sem mandato judicial nem qualquer mecanismo de controlo.
Ainda em 2016, foi anunciada uma nova proposta de Lei, que passava a exigir o registo obrigatório dos cartões SIM pré-pagos. Esta teria sido a quinta tentativa de implementação deste tipo de Lei, após as três anteriores terem sido rejeitadas pelo parlamento e a quarta declarada inconstitucional, *op. cit.*, p.142-143.
[240] Acórdão do Tribunal Europeu dos Direitos do Homem, 18 de dezembro de 2012, Ahmet Yildirim vs Turkey, Processo n.º 3111/10, disponível para consulta em: https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-4202780-4985142%22]}.

4.8.3 Medidas restritivas

No ano de 2019, o Conselho decidiu estabelecer um quadro que permite à UE impor medidas restritivas especificas para dissuadir e responder a ciberataques que constituam um ameaça à UE ou aos Estados-membros. Estas sanções são semelhantes àquelas que aplicadas a pessoas individualmente consideradas ou a entidades no âmbito da luta contra o terrorismo e criminalidade organizada, podendo resultar mesmo em sanções diplomáticas, embargos de armas, restrições de circulação, congelamento de bens ou sanções económicas. Este tipo de medidas apresenta um modelo de aplicação legal aos autores materiais dos ilícitos que: a) sejam responsáveis por ciberataques ou a sua tentativa; b) prestem apoio financeiro, técnico ou material a tais ataques; e c) participem de qualquer outra forma em ataques com a mesma natureza. A aplicação destas sanções aplica-se igualmente a ciberataques perpetrados contra-estados terceiros ou organizações internacionais, relativamente aos quais se considerem necessárias medidas restritivas para alcançar os objetivos PESC[241].

O Conselho, decidiu, pela primeira vez, impor sanções desde que o mecanismo foi implementado (2017 e renovado em 2019[242]) aplicando as medidas restritivas a cidadãos e empresas. As medidas restritivas desta sanção visaram seis pessoas e três empresas evolvidas em ciberataques, destacamos a aplicação de medidas restritivas por sabotagem à rede da OPCW, pelo lançamento do vírus WannaCry, NotPetya, e pela operação Cloud Hopper[243]. Analisando as pessoas singulares e as pessoas coletivas, entidades ou organismos visados na lista[244], salta claro, a intervenção maliciosa de cidadãos ou

[241]Conselho Europeu e Conselho da União Europeia, *Ciberataques: Conselho pode agora impor sanções*, 2019, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/. ; Conselho da União Europeia, *Decisão do Conselho relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros*, 2019, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/pt/pdf; Conselho Europeu e Conselho da União Europeia, *Declaração da alta representante, em nome da UE, sobre o respeito pela ordem assente em regras no ciberespaço*, 2019, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/.

[242] Conselho Europeu e Conselho da União Europeia, *Cyber-attacks: Council is now able to impose sanctions*, 2019, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

[243] Conselho Europeu e Conselho da União Europeia, *EU imposes the first ever sanctions against cyber-attacks*, 2020, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

[244] Official Journal of the European Union, Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

empresas com origem na China e Rússia. As medidas em causa elencam a proibição de viajar, o congelamento de bens das pessoas singulares e o congelamento de bens para entidades ou organismos. Paralelamente, foi proibido disponibilizar, direta ou indiretamente, fundos aos indivíduos, entidades ou organismos visados na lista publicada pela UE.

4.9 Mercado único digital e comercio eletrónico

As comunicações eletrónicas são essenciais e quase obrigatórias no quotidiano, com a digitalização em massa a interconexão em massa é uma realidade inexorável no trabalho, nas compras, nas viagens e em tantas outras atividades humanas.

Em 1998, com a publicação da Diretiva 98/84/CE, relativa à proteção dos serviços que se baseiam ou consistam num acesso condicional (mediante assinatura pagante) veio proteger os serviços eletrónicos de acesso pago contra a pirataria e, de forma genérica contra atividades ilícitas (artigo 4.º) levas a cabo em ambiente digital. Desta forma, foram introduzidas medidas mitigadoras contra as atividades comerciais que envolvessem o fabrico, a distribuição ou a comercialização de cartões inteligentes (cartões de plástico com microprocessadores ou microchips incorporados) e outros dispositivos que possibilitassem contornar o acesso protegido a serviços pagos de televisão, rádio, Internet, publicações eletrónicas entre outros serviços que requeriam pagamento para visualização.

A preocupação de proteger no mercado do comercio eletrónico na UE ganhava novos contornos e, desta feita, foi publicada a Diretiva 2000/31/CE, que estabeleceu normas comuns na União relativamente a várias questões entre as quais a localização[245], informações básicas a prestar às autoridades e aos destinatários, publicidade[246], spam[247],

[245] A Diretiva estabelece o princípio segundo o qual os operadores de serviços em linha estão sujeitos a regulamentação apenas no Estado da UE onde têm sede registada, e não no Estado onde se encontram os servidores, os endereços de correio eletrónico, ou as caixas de correio eletrónico utilizadas.

[246] É necessário garantir que determinada publicidade é claramente identificável, através que através da qual a pessoa ou a empresa responsável é claramente identificável ou ainda, que os descontos, ofertas e outras promoções são claramente identificáveis ou ainda as condições são facilmente acessíveis e apresentadas com termos inteligíveis.

[247] O *Spam* deve ser claramente identificável, comutativamente as empresas são obrigadas a respeitar os registos de opção negativa (Oup-out), onde as pessoas se podem inscrever para não receber determinado tipo de conteúdo.

contratos em linha[248], encomendas em linha[249], aplicação legislativa pelos operadores[250] e obrigações de responsabilidade dos prestadores de serviços[251].

Mais tarde, em 2002, com a necessidade de regulamentação do setor das comunicações, a UE publicou uma Diretiva-Quadro, que acolhia quatro diretivas[252] específicas destinadas à regulação de aspetos técnicos das comunicações eletróncias, concretizando o "pacote de telecomunicações", que contou ainda com dois Regulamentos[253]. Os Regulamentos foram publicados em 2009 e 2012, tendo posteriormente sido alterados

[248] Em todos os Estados da União, os contratos eletrónicos devem ter um estatuto jurídico equivalente aos contatos em papel e, comutativamente, incluir de forma clara e compreensível: a) as etapas técnicas que os consumidores/destinatários têm de seguir para a celebração do contrato; b) transparência quanto ao armazenamento dos dados pelo prestador e acesso posterior à assinatura por parte do consumidor/ destinatário; c) o modo como o consumidor pode identificar e proceder à correção dos erros de introdução anteriores à ordem de encomenda; e d) as línguas em que o contrato pode ser celebrado.
Os consumidores devem ter a opção de guardar e imprimir os contratos e as suas condições gerais, para mais informações sobre esta temática, *v*. Diretiva 2011/83/UE do Parlamento Europeu e do Conselho de 25 de Outubro de 2011 relativa aos direitos dos consumidores, que altera a Directiva 93/13/CEE do Conselho e a Directiva 1999/44/CE do Parlamento Europeu e do Conselho e que revoga a Directiva 85/577/CEE do Conselho e a Directiva 97/7/CE do Parlamento Europeu e do Conselho.

[249] A Diretiva apresenta a obrigação do prestador de serviços confirmar a receção da encomenda sem atrasos indevidos e por via eletrónica (correio eletrónico ou mensagem eletrónica). Para efeitos de confirmação da receção, a encomenda é considerada recebida quando passível de ser acedida pelo consumidor. Neste sentido, as medidas de segurança relativas à identificação eletrónica e aos serviços de segurança podem ser consultadas através do Regulamento (UE) n.° 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 , relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

[250] A Diretiva aponta para uma autorregulação pelos operadores e uma co-regulamentação pelos Estado-membros. Deste modo, iniciativas como por exemplo códigos de conduta ao nível da UE, ou ainda mecanismos de resolução extrajudicial de litígios, sobretudo quando o vendedor e o comprador se encontram em Estados diferentes. Assim, os Estados apresentam ampla margem de discricionariedade para arquitetarem soluções eficazes e rápidas para os problemas jurídicos resultantes do mercado em linha e da oferta disponível pelos prestadores de serviços eletrónicos e, por outro lado, assegurar a efetiva aplicação de um quadro sancionatório eficaz, proporcional e dissuasor.

[251] Os prestadores de serviços em linha que atuam também nos serviços simples de transporte, armazenamento temporário ("chaching") ou em servidor, não são responsáveis pelas informações que transmitem ou armazenam caso preencham determinados requisitos. Com efeito, os prestadores de serviços em nuvem, ou em linha de armazenagem em servidores tem o dever de vigilância sobre os "intermediários", que por sua vez enviam informações para armazenamento. Este dever inclui a prevenção e a deteção de atividades ilegais, todavia podem imiscuir-se de responsabilidade em determinados casos, por exemplo, a inexistência de conhecimento acerca das atividades ilícitas ou quando não tenham conhecimento da ilicítude da informação armazenada. Se tiverem conhecimento da ilícitude devem atuar com diligência no sentido de retirar ou impossibilitar o acesso às informações e proceder ao respeitvo reporte dos ilícitos.

[252] Diretiva 2002/20/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa à autorização de redes e serviços de comunicações eletrónicas ("diretiva autorização"); Diretiva 2002/19/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa ao acesso e interligação de redes de comunicações eletrónicas e recursos conexos ("diretiva acesso"); Diretiva 2002/22/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas ("diretiva serviço universal"); e Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas ("diretiva relativa à privacidade e às comunicações eletrónicas").

[253] Regulamento (CE) n.º 1211/2009 que cria o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE); e Regulamento (UE) n. ° 531/2012 do Parlamento Europeu e do Conselho, de 13 de junho de 2012, relativo à itinerância nas redes de comunicações móveis públicas da União.

pelas Diretivas "Legislar Melhor" e "Direitos do Cidadão", que compreendem em si um conjunto de normas que visam assegurar e regular um conjunto de procedimentos que atestam a segurança da informação e também a privacidade nas comunicações eletrónicas.[254][255].

4.9.1 Estratégia para o mercado único digital da União Europeia, comércio transatlântico e a Diretiva (EU) 2015/2366

O ano 2015 foi marcado por importantes contributos normativos para o mercado único digital da EU. Foi lançada uma nova estratégia para o *mercado único digital* da União Europeia, que permitiu aos consumidores e às empresas tirarem o pleno proveito das oportunidades oferecidas pela Internet de forma segura. Esta estratégia assenta em dezasseis ações específicas, baseadas em três eixos: i) garantir o melhor acesso dos consumidores aos bens e serviços digitais em toda a União; ii) criação de condições adequadas para impulsionar a concorrência equitativa, o desenvolvimento de redes digitais e serviços inovadores; e iii) otimização do potencial de crescimento da economia digital, permitindo tirar partido do potencial tecnológico que emerge das tecnologias digitais[256].

[254] A diretiva quadro, permitiu a harmonização quanto à regulamentação das redes e comunicações eletróncias, isto é, quanto aos sistemas de transmissão que permitem o envio de sinais por cabo, feixes hertzianos, meios óticos, ou por outros meios eletromagnéticos, incluindo as redes de satélite, as redes terrestres fixas e móveis, os sistemas de cabos de eletricidade, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo. Assim, todos os serviços de comunicações eletrónicas, nos quais fosse possível enviar sinais através de redes, assim como todos os recursos e serviços externos das redes ou dos serviços de comunicações eletróncias.
Foram ainda publicados princípios basilares quanto às Autoridades Reguladoras Nacionais (ARN), nomeadamente, o princípio da independência, o direito ao recurso e da imparcialidade e transparência.

[255] Numa perspetiva da proteção do utilizador e consumidor final este quadro foi revisto em 2015, com o Regulamento (EU) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, que estabelece medidas respeitantes ao acesso à internet aberta e que alerta a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) n.º 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União. Desta forma, foram estabelecidas regras comuns para garantir o tratamento equitativo e não discriminatório do tráfego na prestação de serviços de acesso à Internet e os direitos dos utilizadores finais relacionados com a prestação. É ainda importante referir que as medidas previstas neste Regulamento respeitam o princípio da neutralidade tecnológica, assim, não é imposta a utilização de qualquer tipo de tecnologia específica, nem se estabeleceu qualquer discriminação que a favoreça.

[256] Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões a Estratégia para o Mercado Único Digital na Europa, *Estratégia para o Mercado Único Digital na Europa*, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192.

Esta estratégia, foi uma das prioridades da Comissão à época[257], ainda que o TJUE tenha declarado inválido o quadro legislativo em matéria de proteção de dados entre a União e os EUA - "porto seguro", obrigando a Comissão a negociar com os EUA para efeitos de transferências transatlânticas de dados pessoais para fins comerciais, que deu origem ao "Escudo de Proteção de Privacidade" (tendo sido este último declarado inválido em julho de 2020 pelo TJUE[258][259]). As transferências ao abrigo do acordo "Porto Seguro" viriam a ser declaradas inválidas por decisão jurisprudencial do TJUE, no processo C-362/13, de 6 de outubro de 2015, Facebook Ireland vs Max Shrems. Neste processo foram tecidas várias críticas à Comissão Europeia, essencialmente pelo facto de esta não assegurar contratualmente um nível de proteção adequado dos direitos fundamentais aos titulares de dados (cidadãos europeus). O TJUE sustentou que a Comissão tinha conhecimento de que eram excedidas as finalidades de tratamento pelas quais os dados pessoais de cidadãos da União eram transferidos, não tomou nenhuma ação para mitigar ou interromper o tratamento de dados entre os dois continentes, tornando assim as transferências de dados incompatíveis e não proporcionais face ao objetivo de proteção da segurança nacional alegado pelos EUA[260]. Posto isto, passou a vigorar um regime de cumprimento de obrigações em matéria de segurança da informação e uma obrigação de comunicação perante as autoridades nacionais de proteção de dados, sendo que vigoram as cláusulas contratuais disponibilizadas pela Comissão e pelas autoridades nacionais ao abrigo do considerando 108 e artigo 46.º do RGPD.

Foi ainda publicado o ato legislativo que viria a alterar o panorama da segurança da informação e comunicação em ambiente económico digital na União, postulado pela Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 ("DSP2")[261], relativa aos serviços de pagamento no mercado interno, alterando o

[257]Comissão Europeia, *Migration and Home Affairs*, 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

[258] Acordão do Tribunal de Justiça da União Europeia, Maximillian Schrems vs Data Protection Commissioner,processo C-362/14, de 6 de outubro de 2015, disponível para consulta em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=PT.

[259] O Escudo de proteção de privacidade entre a UE e os EUA reforçou a confiança entre os titulares de dados dos dois continentes, observando quatro marcos fundamentais: i) as obrigações estritas impostas às empresas; ii) os limites bem definidos e claros sobre o acesso aos dados pelo governo americano; iii) a proteção eficaz dos direitos à privacidade dos cidadãos da União Europeia por via das várias possibilidades de recurso a meios de tutela jurisdicional; e iv) apreciação do modelo de intercâmbio de dados com revisão e reapreciação anual conjunta.

[260] Conclusão n.º 78 e 90 do acórdão do TJUE supracitado na nota 113.

[261] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

quadro jurídico europeu aplicável aos serviços de pagamento. Entre outras, a introdução de um quadro normativo de regras de segurança da informação foi uma das principais novidades desta Diretiva, sendo regulado pelo Regulamento Delegado (EU) 2018/389 da Comissão de 27 de novembro, sobre a autenticação forte do cliente e normas abertas de comunicação comuns e seguras[262].

Um outro marco deste ano, consistiu na aprovou da Convenção do Conselho da Europa sobre a proteção jurídica dos serviços que se baseiam ou consistam num acesso condicional[263]. A assinatura da Convenção pela União reafirmou o compromisso da UE nesta matéria e, paralelamente teve como objetivo simbólico o incentivo institucional sob a forma de exemplo para que os Estados-membros do Conselho da Europa procedessem à sua ratificação. Após a publicação do RGPD em 2016, a Diretiva 2002/58/CE viu a necessidade de ser atualizada em função da sua extemporaneidade, tendo assim, por via da Comissão Europeia[264] e da CEPD[265] que proceder à sua alteração.

A UE tem vindo a assumir uma postura reformista em relação às novas tecnologias e aos seus agentes no seu mercado digital europeu, todavia, esse funcionamento eficaz e eficiente da economia dos dados pode ser questionado, não pelo seu tratamento, mas pela sua praticidade. Neste quadro, a União dirigiu uma comunicação onde lançou algumas ideias para fazer face a problemas como a falta de coordenação a nível transfronteiriço, às infraestruturas, às oportunidades insuficientes ou deficitárias, ou ainda ao complexo quadro jurídico, como temos vindo a desdenhar. Destarte, foram sugeridas várias iniciativas, entre as quais: constituição de parcerias público-privadas em matéria de armazenamento de grande volume de dados; criação de uma incubadora de dados abertos para promover e facilitar a criação das PME; a renovação do quadro regulamentar; edificação de centros de excelência na supercomputação, e ainda a criação de uma rede

[262] Para mais desenvolvimentos sobre esta matéria *v*. Francisco Mendes Correia, DSP 2 e Normas Abertas de Comunicação Comuns e Seguras, in: *FinTech II: Novos Estudos Sobre Tecnologia Financeira*, Almedina, 2019, p. 157-169.

[263] Decisão(UE) 2015/1293 do Conselho de 20 de julho de 2015 relativa à celebração, em nome da União Europeia, da Convenção Europeia sobre a proteção jurídica dos serviços que se baseiem ou consistam num acesso condicional.

[264] A Comissão Europeia apresentou já ao Parlamento Europeu e ao Conselho a proposta de alteração, todavia esta ainda não foi aprovada. *v*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017PC0010&from=PT-.

[265] O CEPD, emitiu várias opiniões e declarações, a última foi em março de 2019, onde reforça o apelo "*aos legisladores da UE para que intensifiquem os seus esforços com vista à adoção de um regulamento relativo à privacidade e às comunicações eletrónicas, necessário para completar o quadro da UE relativo à proteção de dados e à confidencialidade das comunicações*". EDPB, *Declaração 3/2019 sobre um regulamento relativo à privacidade e às comunicações eletrónicas*, 2019, disponível para consulta em: https://edpb.europa.eu/sites/edpb/files/files/file1/201903_edpb_statement_eprivacyregulation_pt_0.pdf.

de instalações de tratamento de dados em diferentes Estados-membros da União Europeia[266]. No parecer do Comité Económico e Social Europeu sobre esta comunicação é referido expressamente no ponto 4.13, "*As questões de cibersegurança revestem-se de particular importância, uma vez que as redes informáticas e a computação em nuvem passarão a lidar com volumes crescentes de dados muito importantes do ponto de vista económico e social, incluindo informação sensível, como é o caso dos dados médicos."* , vindo observar uma realidade inexorável da *big data* a nível europeu[267].

4.10 Confidencialidade nas comunicações

No que respeita à preocupação da confidencialidade no setor das comunicações eletrónicas, foi publicada a Diretiva 2002/58/CE do Parlamento e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, também apelidada de "*E-Privacy Directive*". Esta Diretiva veio exigir aos serviços públicos de comunicações eletrónicas salvaguardas suficientes para a defesa da privacidade e confidencialidade na sua utilização por parte

[266] Nesta senda, através de um conjunto de comunicações, entre elas, a "Iniciativa Europeia para a Nuvem- Construir uma economia de dados e conhecimento competitiva na Europa" (*v*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52016DC0178); a Comunicação da Comissão de 10 de maio de 2017, sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital - Um Mercado Único Digital conectado para todos, identifica a computação de alto desempenho como elemento fundamental par a digitalização da indústria e par a economia dos dados (*v*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM:2017:228:FIN); e a Comunicação da Comissão intitulada Europa 2020 -Estratégia para um crescimento inteligente, sustentável e inclusivo- "Estratégia Europa 2020" (*v*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52010DC2020), conjugado com um quadro legal que presta apoio à criação de empresas comuns no âmbito do "Horizonte 2020" (Regulamento (EU) n.º 1290/2013 do Parlamento Europeu e do Conselho e a Decisão 2013/743/EU do Conselho), estabelecendo a Empresa Comum para a Computação Europeia de Alto Desempenho, através do Regulamento (EU) 2018/1488 do Conselho de 28 de setembro de 2018. A EuroHPC JU foi criada ao abrigo do artigo 187.º do TFUE, atualmente constitui o principal elemento para fazer face às autuais limitações ao nível tecnológico, proporcionando a Estados-membros e empresas privadas (HTP4HPC, BDVA e outras partes interessadas) concentrarem esforços na criação de uma infraestrutura à pre-exaescala até 2020, e *para desenvolver as tecnologias e aplicações necessárias para atingir capacidades à exaescala até 2023, promovendo ao mesmo tempo um ecossistema europeu competitivo para a inovação europeia em matéria de computação de alto desempenho*. Para mais informações consultar sobre a temática *v*. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1488&from=EN.

[267] Comité Económico e Social Europeu, *Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Para uma economia dos dados próspera» [COM(2014) 442 final]*, 2015, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52014AE5300.

dos utilizadores. Todavia, esta Diretiva viria a ser revogada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009, assim como alterou a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor. Na sua essência, a então nova Diretiva veio reforçar o quadro da transparência das informações e dos deveres associados aos Estados-membros e às ARN. Este foi um importante passo para as organizações e indivíduos assegurarem um compromisso com a privacidade e respeito pelo tratamento de dados pessoais no setor das comunicações eletrónicas, de modo a garantir a livre circulação de dados, equipamentos e serviços de comunicações eletrónicas na Comunidade Europeia[268].

4.11 Regulamento (UE) 2018/1807

No que respeita ao tratamento de dados eletrónicos não pessoais na UE, o Regulamento (UE) 2018/1807 veio regular a livre circulação e tratamento desses dados por toda a União. A sua aplicação é dirigida a empresas que realizam tratamentos de dados não pessoais e/ou que prestam um serviço a utilizadores residentes na UE e a pessoas singulares ou organizações para necessidades do foro doméstico. Neste Regulamento o princípio geral é o da livre circulação de dados na União, havendo uma obrigação de comunicação dos Estados-membros à Comissão dos projetos de atos que introduzem um novo requisito de localização de dados, ou que modifiquem um requisito existente de localização de dados pelos procedimentos previsto nos artigos 5.º, 6.º e 7.º da Diretiva

[268] De forma complementar, esta Diretiva foi atualizada em 2006, sendo publicada a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Todavia esta foi declarada invalida pelo TJUE, em 8 de abril de 2014, devido à grave interferência na vida privada e na proteção de dados pessoais, bem como o Regulamento (CE) n.º45/2001 relativo ao tratamento de dados pessoais por instituições e órgãos comunitários, vem como outros instrumentos do antigo terceiro pilar com a Decisão-Quadro do Conselho, de novembro de 2008, relativa à proteção de dados pessoais tratados no âmbito da cooperação judicial e da justiça penal.

(UE) 2015/1535 entre outros procedimentos regulamentares descritos no artigo 4.º da Regulamento em análise[269].

Todavia, não é líquido que não possam surgir obstáculos à mobilidade dos dados e, consequentemente quebras de valor no mercado único digital. Os possíveis obstáculos surgem na forma de restrições que têm de ver com os requisitos de localização de dados estabelecidos pelas autoridades dos Estados-membros ou ainda pelas práticas de vinculação a um prestador de serviços no setor privado[270]. Assim, pode, por disposição nacional, regional ou local, haver uma imposição obrigatória de localização geográfica específica para efeitos de tratamento de dados. A nível europeu, a base jurídica para a exclusão à livre circulação de prestação de serviços de tratamento de dados na União e no seu mercado interno encontrasse no artigo 52.º do TFUE, por "(…) *justificadas por razões de ordem pública, segurança pública e saúde pública* (…)", ou no artigo 5.º do TFUE, observando o princípio da proporcionalidade[271].

[269] Neste regulamento, ainda é possível observar a questão da disponibilidade dos dados para as autoridades competentes, a portabilidade dos dados (com incentivo à criação de códigos de conduta) , e o procedimento para a cooperação entre as autoridades, artigos 5.º, 6.º e 7.º respetivamente.

[270] A liberdade de estabelecimento e a livre circulação de prestação de serviços, consagrados no TFUE aplicasse a serviços de tratamento de dados e a todos os tipos de sistemas informáticos, tanto localizados nas instalações do utilizador com externalizados a um prestador de serviços. A aplicabilidade deste Regulamento abrange o tratamento de dados de diferentes escaldas de intensidade, desde o armazenamento (infraestrutura como serviço) até ao tratamento por meio de plataformas (plataforma como serviço) ou aplicações (software como serviço).

[271] Ao nível legislativo, os Estados-membros só poderão invocar a segurança pública como justificação para requisitos de localização de dados. Segundo a interpretação do TJUE, a segurança pública, abrange tanto a segurança interna como a segurança externa de um Estado-membro, ou ainda questões atinentes à proteção pública, nomeadamente a fim de investigar a investigação, deteção e a repressão de infrações penais. É ainda exigido o (…) *pressuposto de uma ameaça real e suficientemente grave que afete um interesse suficientemente grave da sociedad*e (…) *assim como o risco de uma perturbação grave das relações externas ou da coexistência pacífica das nações, ou um risco para os interesse militares."* Assim, o princípio da proporcionalidade também deverá ser adequado tendo em conta a finalidade, não excedendo o necessário para alcançar essa finalidade.

II- Cibersegurança e Direitos Fundamentais

5 Direitos Fundamentais na Era Digital

Os direitos fundamentais e o respeito pela dignidade da pessoa humana pautam a ação da União tanto no quadro interno como externo, consagrando a sua universalidade e indivisibilidade[272]. A Era digital, marcada pelo avanço tecnológico e digitalização das sociedades modernas, apresenta um grande desafio às organizações e aos Estados, sendo que a defesa da indivisibilidade dos direitos humanos e das liberdades fundamentais não pode nem deve ficar de fora deste domínio.

O termo privacidade, foi analisado em 1604 por Edward Coke, no Kings Bench of England, através da célebre expressão "*A home is one's castle* (…)", aludindo à época à noção de separação entre os direitos da vida privada e doméstica, longe dos olhares e escrutínio público do povo. Os desenvolvimentos tecnológicos em matéria de tecnologias de informação e comunicação avançaram a passos largos desde então, bem como a base legal de construção jurídica sobre o tema. No entanto, os quadros regulatórios visam sempre assegurar nos dias de hoje a que não haja uma interferência externa excessiva relativamente à vida privada da pessoa humana – tal como acontecia antigamente sobre os "castelos".

Do ponto visto teórico na UE, o direito à proteção de dados "(…) *was initiality strongly conected to the right to privacy*", pois era este último que vigorava entre as organizações (*maxime* Estados) de forma abundante através do número de bases de dados armazenadas, observando um exercício de liberdade ao governo para "verificar" aspetos da vida privada, inclusive dados sensíveis[273]. Todavia, este entendimento entrou em conflito com os interesses Estatais associados, pois, se por um lado, os cidadãos tinham o direito à privacidade e à não divulgação de dados privados, por outro, os Estados necessitavam deles para proceder a estudos e desenvolvimento de políticas públicas e em último caso governar.

Contemporaneamente, com os diversos instrumentos jurídicos multilaterais, em especial o RGPD no caso da União, o termo "privacidade" vem sendo relegado para segundo plano, acentuando uma mudança no sentido terminológico[274]. O direto à proteção de

[272] Ana Maria Guerra Martins, *Os Desafios Contemporâneos à Ação Externa da União Europeia: Lições de Direito Internacional Público II*, Almedina, 2018, p. 109.
[273] Bart van der Sloot, Legal Fundamentalism: Is Data Protection Really a Fundamental Right?, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p. 5-8.
[274] *Ibidem*.

dados surgiu inserido nos primeiros instrumentos jurídicos criados com o objetivo de defender o direito à privacidade, sendo a proteção de dados inserido num subconjunto de direitos. Por exemplo, a CDFUE postula claramente a diferença entre o direito à privacidade e direito à proteção de dados e consequente, "(…) *specially in EU law, data protection is disconnected from the right to privacy.*" fruto de uma evolução terminológica das disposições jurídicas da União[275].

As obrigações legais consagradas no Pacto Internacional sobre os Direitos Civis e Políticos, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais da União Europeia devem aplicar-se no domínio digital com a mesma efetividade que no domínio físico, sem prejuízo das particulares deste último, nomeadamente para efeitos do âmbito penal.

A CEDH, entrou em vigor em 1953 e é considerada por muita doutrina como o instrumento mais eficaz na luta contra as violações de direitos humanos na Europa, sendo aplicada no foro doméstico dos Estados-membros do Conselho da Europa (47) e, sob a fiscalização do Tribunal Europeu dos Direitos do Homem. Para o tema em concreto, importa refletir sobre o artigo 8.º da CEDH, no qual se inscreve o direito ao respeito pela vida privada e familiar:

1. *Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.*
2. *Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."*

Note-se que a CEDH não especifica a definição de vida privada com precisão, no entanto o entendimento doutrinário sobre a "vida privada" reflete sobre o próprio exercício autónomo e livre do desenvolvimento e realização da personalidade humana sem qualquer interferência externa. Pelas próprias raízes fundacionais e face à evolução tecnológica com a conhecemos hoje, este documento carece de adaptação interpretativa à luz das mudanças sociais e tecnológicas experimentadas de forma a cumprir a sua

[275] *Ibidem.*

missão de "*Proteção dos Direitos do Homem e das Liberdades Fundamentais*", sob pena de tornar um instrumento jurídico obsoleto e ineficaz[276][277].

O Tribunal Europeu dos Direitos do Homem tem sedimentado uma posição bastante ampla em relação à apreciação de processos em que o artigo 8.º é tido como base jurídica de fundamentação nos casos. Assim, processos que tem por base o armazenamento de informações sobre a vida privada de uma pessoa (Leander vs Sweden[278]), videovigilância e interceção de comunicações (Klass and others vs Germany[279]), videovigilância no local

---

[276] Tribunal Europeu dos Direito do Homem, 25 de abril de 1978, Tyrer vs Reino Unido, processo n.º. 5856/72, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57587%22]}. Neste caso o requerente foi submeteu ao TEDH a apreciação de uma alegada violação do artigo 3.º da CEDH, respeitante ao incumprimento de obrigações por parte do Reino Unido, mais precisamente na Ilha de Man (sob a dependência autónoma da coroa britânica no mar da Irlanda). O requerente, Sr. Tyrer (à época, com 15 anos de idade) foi condenado em 1972, por um tribunal local de menores por uma agressão ilegal que causou graves ferimentos a um aluno (adulto) da sua escola. O requerente foi condenado no mesmo dia a três pancadas de bétula, em conformidade com a legislação local. O requerente recorreu da decisão sendo-lhe negado provimento. Procedeu-se à aplicação da sanção, de acordo com a "*section 56 (1) of the Petty Sessions and Summary Jurisdiction Act 1927 (as amended by section 8 of the Summary Jurisdiction Act 1960) whereby": "Any person who shall - (a) unlawfully assault or beat any other person; (b) make use of provoking language or behaviour tending to a breach of the peace, shall be liable on summary conviction to a fine not exceeding thirty pounds or to be imprisoned for a term not exceeding six months and, in addition to, or instead of, either such punishment, if the offender is a male child or male young person, to be whipped.*"

O TEDH considerou que à luz das crenças sinceras por parte dos membros da comunidade local, inclusive pelas indicações que recebeu, que o castigo aplicado era *necessário* na Ilha de Man para manter a lei e a ordem. No entanto, seria necessário apresentar uma prova positiva conclusiva, ao invés de se basear em crenças e opiniões públicas da comunidade local, sendo que esta última não era considerada uma prova. Mesmo com o recurso ao castigo corporal, não existia nenhuma evidência de que não seria possível manter a lei e ordem recorrendo a outra sanção. Na própria Ilha de Man, como já mencionado, a legislação relevante sob esta matéria esteve sob revisão durante muitos anos. Ora, isso lança dúvidas sobre se a aplicação dessa penalidade como sendo um requisito para a manutenção da lei e ordem. A Ilha de Man é constituída por tradições políticas, sociais e culturais de longa data, mas é uma sociedade atualizada. Historicamente, geográfica e culturalmente, a ilha sempre foi incluída na família das nações europeias e deve ser considerada signatária do "*patrimônio comum das tradições políticas, ideais, liberdade e estado de direito*" ao qual o preâmbulo da Convenção evoca. Finalmente, mesmo que a lei e a ordem na Ilha de Man não pudessem ser mantidas sem recurso a sanções corporais judiciais, tais costumes e práticas são incompatíveis com a Convenção. Da mesma forma, na opinião do Tribunal, nenhum requisito local relativo à manutenção da lei e da ordem autorizaria esses Estados para fazer uso de uma sanção contrária ao artigo 3.º da CEDH.

Por tudo isto, o TEDH considerou que não existiam requisitos locais que afetassem a aplicação do artigo 3.º na Ilha de Man e, portanto, a punição corporal judicial do requerente constitui uma violação do artigo 3.º da CEDH.

[277] A este propósito, o Juíz Alito quanto emitiu a sua opinião no caso *United States* vs *Jones*, a 23 de fevereiro de 2012, " *dramatic technological change may lead to periods in which popular expecta tions are in flux and may ultimately produce significant changes in popular attitudes*." Disponível para consulta em: https://supreme.justia.com/cases/federal/us/565/400/.

[278] Acórdão do Tribunal Europeu dos Direitos do Homem, de 26 de março de 1987, Leander vs Sweden, processo n.º 9248/81, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57519%22]}. Cfr. Nota 288.

[279] Acordão do Tribunal Europeu dos Direitos do Homem, de 6 de setembro de 1978, Klass and others vs Germany, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}.

O conjunto dos cinco requerentes alegaram o incumprimento de um quadro legislativo, denominado "*G 10*", que impunha restrições ao sigilo de correspondência, correio e telecomunicações. Os requerentes alegaram a violação do dever notificação das pessoas visadas por este tipo de operações uma vez terminadas

de trabalho (Copland vs the United Kingdom[280]), uso de CCTV em locais públicos (Peck vs United Kingdom[281]), proteção da imagem (Springer and Von Hannover vs Germany

as operações pelas autoridades responsáveis. Adicionalmente, reclamaram da impossibilidade de recurso perante os tribunais superiores após a aplicação de tais medidas restritivas da vida privada, vendo negado o seu direito de defesa, argumentando mesmo que tal prática iria contra a própria essência da CEDH. O TEDH veio esclarecer, relativamente ao artigo 8.º da CEDH a necessidade dos Estados no "(…) *balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole.*" Relativamente ao caso em concreto a decisão do acórdão veio, por unanimidade, considerar que não houve violação do artigo 8.º da CEDH, rematando que "(…) *the Court concludes that the German legislature was justified to consider the interference resulting from that legislation with the exercise of the right guaranteed by Article 8 para. 1 (art. 8-1) as being necessary in a democratic society in the interests of na tional security and for the prevention of disorder or crime (Article 8 para. 2) (art. 8-2). Accordingly, the Court finds no breach of Article 8 (art. 8) of the Convention*.".

[280] Acórdão do Tribunal Europeu dos Direitos do Homem, de 3 de abril de 2007, Copland vs The United Kingdom, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-79996%22]}.

A requerente (Copland), natural do País de Gales, empregada do "*Carmarthenshire College*", foi alvo de monitorização aos equipamentos de trabalho, desde e-mails a registos telefónicos, ordenado pelo então vice-diretor do estabelecimento de ensino. O TEDH realçou que "(…) *the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone" (see Malone v. the United Kingdom, 2 August 1984, § 84, Series A no. 82). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid.). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1 (see Amann, cited above, § 65). Thus, it is irrelevant that the data held by the College were not disclosed or used against the applicant in disciplinary or other proceedings.*". Neste acórdão, o coletivo de Juízes veio a decidir em favor da requerente e, atendendo ao quadro jurídico deu-se como provado que houve efetivamente uma violação do artigo 8.º da CEDH, considerando que "(…) *collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.".*

[281] Acórdão do Tribunal Europeu dos Direitos do Homem, de 28 de janeiro de 2003, Peck vs The United Kingdom, processo n.º 44647/98, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-60898%22]}. Cfr. Nota 287.

(N.º2) 282) ou reputação (Pfeifer v. Austria[283]), o TEDH vem postulando um eixo jurisprudencial uniforme a respeito desta temática.

[282] Acórdão do Tribunal Europeu dos Direitos do Homem, de 7 de fevereiro de 2012, Springer and Von Hannover vs Germany, processos n.º 40660/08 e 60641/08, Estrsburgo, disponível para consulta em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109029%22]}.
A requerente em causa tentou, por várias vezes, na década de 90 impedir a publicação de fotos referentes à sua vida privada expostas na imprensa alemã. Nos processos internos nos tribunais da Alemanha foi-lhe negado o provimento dos seus casos. Mais tarde, com recurso ao TEDH, os processos do foro doméstico foram objeto do acórdão Von Hannover vs Alemanha, de 24 de junho de 2004 (n. 59320/00, TEDH 2004 - VI), no qual o TEDH considerou que as decisões judiciais violavam o direito da requerente no que toca ao respeito pela sua vida privada, direito este consagrado pelo artigo 8.º da Convenção. Neste segundo acórdão em particular estavam em causa fotos retiradas e publicadas na imprensa nacional, o TEDH observou que *"(…) in accordance with their case-law, the national courts carefully balanced the right of the publishing companies to freedom of expression against the right of the applicants to respect for their private life. In doing so, they attached fundamental importance to the question whether the photos, considered in the light of the accompanying articles, had contributed to a debate of general interest.* Todavia notou que "(…)*Whilst the Federal Court of Justice had changed its approach following the Von Hannover judgment, the Federal Constitutional Court, for its part, had not only confirmed that approach, but also undertaken a detailed analysis of the Court's case-law in response to the applicants' complaints that the Federal Court of Justice had disregarded the Convention and the Court's case-law.*". Finalizou, atendendo "*(…) Int those circumstances, and having regard to the margin of appreciation enjoyed by the national courts when balancing competing interests, the Court concludes that the latter have not failed to comply with their positive obligations under Article 8 of the Convention. Accordingly, there has not been a violation of that provision*. (…)".

[283] Acórdão do Tribunal Europeu dos Direitos do Homem, de 15 de novembro de 2007, Pfeifer vs Austria, processo n.º12556/03, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2212556/03%22],%22itemid%22:[%22001-83294%22]}.
O requente (Fürst-Pfeifer) cidadão austríaco, psicólogo especialista assessor do Tribunal em processos judicias em casos que envolviam a custódia viu-lhe serem proferidas alegações difamatórias num artigo de jornal local, com factos respeitantes à sua vida profissional, diretamente relacionados com as suas funções no Tribunal. O requerente alegou que os tribunais austríacos não haviam protegido os seus direitos nos termos do artigo 8º da CEDH.
O TEDH, veio esclarecer que "*The Court has found the publication of a person's photo to fall within the scope of his or her private life even where the person concerned was a public figure*" e ainda que "(…) *a person's reputation, even if that person is criticised in the context of a public debate, forms part of his or her personal identity and psychological integrity and therefore also falls within the scope of his or her "private life". Article 8 therefore applies. This is not disputed by the parties*.". Frisou que estava em causa "(…) *whether the State, in the context of its positive obligations under Article 8, has achieved a fair balance between the applicant's right to protection of his reputation, which is an element of his "private life" and the other party's right to freedom of expression guaranteed by Article 10 of the Convention (...).*" No contexto do caso em análise o TEDH veio esclarecer que a obrigação do Estado de proteger o requerente, nos termos do artigo 8.º da CEDH, poderia surgir no memento em que as declarações públicas ultrapassassem os limites do que seria considerado uma crítica aceitável de acordo com o artigo 10.º da CEDH. O TEDH vem referir no parágrafo 39 do acordão, que a avaliação dos tribunais austríacos proferiram seria no sentido de que as declarações seriam equivalentes a julgamentos de valor em relação ao requerente. Numa das declarações apontadas pelo tribunal, o Sr. "M." escreveu aos assinantes de *Zur Zeit* e ultrapassou os limites aceitáveis, acusando o requerente de atos equivalentes ao comportamento de um criminoso. O TEDH veio a decidir em favor do requerente, afirmando que os motivos invocados pelos tribunais austríacos para a proteção da liberdade de expressão não se sobrepunham ao direito do requerente salvaguardar a sua reputação, rematando que os tribunais nacionais não conseguiram encontrar um equilíbrio justo entre interesses concorrentes envolvidos entre as partes.

O artigo 8.º da CEDH representa simbolicamente "o guardião da privacidade" da pessoa humana e sustenta a tese de que a pessoa humana é livre nas suas relações e escolhas habilitando-a de interagir e relacionar-se como que entender (Niemietz vs Germany[284]). Todavia, o n.º 2, do artigo 8.º da CEDH prevê o regime de exceção à aplicação das disposições enumeradas no primeiro artigo, não sendo este um direito absoluto. Nesse sentido, existe a possibilidade, em face de uma disposição legal e, prosseguindo interesses legítimos de acordo com as necessidades de numa sociedade democrática de derrogação desse direito. Analisemos então os requisitos legais:

a) *Previsão legal* – Qualquer derrogação deve ter uma base legal de fundamentação, de tal modo que esta ingerência na vida privada (equipamentos associados e/ou incluídos) seja determinada com precisão suficiente de modo a que não seja exequível

[284] Acórdão do Tribunal Europeu dos Direitos do Homem, 16 de dezembro de 1992, Niemietz vs Germany, processo n.º 13710/88, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57887%22]}.

por outra via, a obtenção de acesso a essas informações (Amann v. Switzerland[285] e Rotaru vs Romania [286]).

[285] Acórdão do Tribunal Europeu dos Direitos do Homem, de 16 de fevereiro de 2000, Amann vs Switzerland, processo n.º 27798/95, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-58497%22]}. Cfr. nota

A requerente (Aman), empresário que vivia na Suiça e operava no ramo da importação de artigos depilatórios publicitados em revistas para a Suiça. Em 1981, uma cidadã da embaixada Russa em Berna realizou uma chamada para o requerente solicitando um dos aparelhos depilatórios anunciados numa revista. Essa chamada foi intercetada por um Oficial do Ministério Público – *Bundesanwaltschaft*, que informou os serviços de informação de polícia da confederação de Zurique para proceder a uma investigação ao negócio do requerente, bem como aos produtos por este comercializados. No mesmo ano fora elaborado um relatório pelos serviços de polícia da confederação de Zurique que indicava que este constava como inscrito no Registo Comercial desde 1973, sendo que o "*Perma Tweez*" era um aparelho de depilação a bateria, anexando ao relatório o folheto descritivo com a informação do produto em questão.

Mais tarde, em 1990, a população Suíça tomou conhecimento que o MP elaborava um cartão no qual figurava um índice de segurança nacional por confederações e por pessoas com os seus dados pessoais. O requerente do processo em análise exerceu o direito de acesso aos seus dados junto do MP Suiço, todavia as informações chegaram rasuradas por alegadas questões de segurança nacional (uma das partes rasuradas era respeitante aos nomes dos oficiais que obtiveram as informações que constam no cartão e um outra passagem rasurada era respeitante a uma medida de vigilância técnica ordenada contra terceiros). O Provedor de Justiça declarou que recomendaria que o Oficial especial divulgasse as informações rasuradas, uma vez que, na sua opinião o interesse do candidato prevalecia sobre o interesse público em mantê-lo em segredo. Ora, uma vez revelado, tinha inscrito o seguinte: "*from the Zürich Intelligence Service: A. identified as a contact with the Russian embassy according to (...). A. does business of various kinds with the [A.] company. Appendices: extract from the Commercial Registry and leaflet (...)"*. O Oficial destacado do MP decidiu não informar o cidadão, alegando questões de segurança nacional, sustentando a sua posição em disposições de direito interno, mesmo à revelia do Provedor de Justiça.

A ser convidada a apresentar observações escritas, a confederação declarou que, de acordo com as informações fornecidas pelo MP e pelo Oficial destacado, o registo da vigilância não estava nos arquivos da tutela da polícia federal. O advogado da recorrente indicou que o número do processo do cartão, (1153:0)614, era um código que significa "*país comunista*" (1), "*União Soviética*" (153), "*espionagem estabelecida*" (0) e " *vários contatos com o bloco oriental*" (614).

O representante da Confederação afirmou que alguém na antiga embaixada soviética estava sob vigilância e todas as ligações telefónicas seriam identificadas. Deste modo, o requerente foi indentificado, e o foi armazenado o seu cartão e um relatório de monitorização do telefone (Telefon-Abhör-Bericht). Nesse contexto, a representante da Conferação declarou que a maioria dos relatórios havia sido destruída e aqueles que não haviam sido estavam armazenados em sacos, tendo a intenção de proceder à sua destruição, mas quando o cargo de Oficial destacado foi instituído, todos os processos teriam que ser mantidos "*no seu estado atual*". Segundo as informações que a representante da Confederação recebeu do Oficial destacado, os relatórios não foram classificados e seriam necessária uma força de trabalho de cerca de cinco pessoas e um ano de trabalho para examinar o conteúdo de todas os sacos com documentação ainda existente, tendo acabado o Tribunal Federal por negar provimento a todas as reivindicações do recorrente. Rematou, observando que *"(...) a card was drawn up on the plaintiff in connection with the then monitoring of telephone communications with the Soviet embassy for counter-intelligence reasons. As he had contacts with a male or female employee of the Soviet embassy and it was not immediately clear that the 'Perma Tweez' appliance which he sold was a harmless depilatory instrument, the authorities acted correctly in investigating his identity, his circumstances and the 'Perma Tweez' appliance in question and recording the result.*" Em 1996, o cartão do requerente foi removido do índice de segurança nacional e transferido para o Arquivo Federal, o qual não pode ser consultado nos cinquenta anos subsequentes.

O TEDH deu como provado a violação do artigo 8.º da CEDH decorrente da interceção da chamada telefónica, bem como da criação e armazenamento do cartão identificativo.

[286] Acórdão do Tribunal Europeu dos Direitos do Homem, de 4 de maio de 2020, Rotaru vs Romania, processo n.º 28341/95, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-58586%22]}.

Neste processo, o TEDH descobriu uma violação do artigo 8.º da CEHD na lei nacional romena permitia reunir, gravar e arquivar ficheiros com informação que afetava a segurança nacional não estabelecendo limites para o exercício desses poderes, permanecendo ao critério das autoridades competentes.

b) *Prossecução de um interesse legítimo* – O interesse deve justificar a ingerência na vida privada da pessoa, de tal modo que "*seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros*" (Peck v.United Kingdom [287]).

c) *Dever de necessidade* numa "sociedade democrática" – Para atingir determinado fim é necessário agir sob o *valor* e *princípio* de Estado de direito, aplicando a lei em conformidade com a CEDH (Leander v. Sweden[288]).

A fim dos Estados-membros cumprirem as suas obrigações em matéria de adoção de medidas ao abrigo do artigo 8.º, é-lhes concedido uma determinada margem de apreciação na aplicação das medidas ativas ou sentenças. Constitui-se então imprescindível a execução de medidas internas de proteção para defesa das *liberdades fundamentais* e o *comum respeito pelos direitos do homem* por parte dos Estados, nesse sentido, é importante que os Estados cumpram de forma efetiva as medias decretadas pelas decisões do TEDH e projetem os direitos consagrados pela Convenção, sem prejuízo de expandir a proteção conferida para além das relações individuais (e não só entre cidadãos e Estados[289]).

[287] O requente em causa tentou-se suicidar num espaço público do Reino Unido por automutilação, infligindo cortes nos pulsos. Um polícia de serviço visualizou a situação pelo circuito de CCTV e atuou em conformidade, impedindo o cidadão de continuar com a própria mutilação e, consequentemente salvou-lhe a vida. Após este episódio ter ocorrido as imagens do requerente (autor de tentativa do próprio suicídio) foram expostas nos media. O TEDH considerou que não havia motivos razoáveis, nem justificáveis para revelar a identificação do autor das imagens pelas autoridades sem o consentimento do próprio ou por via do recurso à anonimização da sua identidade. O TEDH conclui que foi violado o artigo 8.º da CEDH.

[288] O TEDH decidiu que o escrutínio secreto de pessoas que se candidatavam a vagas de emprego em altas posições no domínio da segurança nacional não seria, por si só, contrário à exigência da conferência necessária da identidade em causa típica numa sociedade democrática. Tendo em conta a ampla margem de apreciação, o Estado respondeu que, no caso das candidaturas, o interesse de segurança nacional prevalecia sobre os direitos individuais do candidato. O tribunal conclui que não houve violação do artigo 8.º da CEDH.

[289] Acórdão do Tribunal Europeu dos Direitos do Homem, de 2 de dezembro de 2008, caso K.U vs Finland, processo n.º 2872/02, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-89964%22]}.
O TEDH clarificou que os Estados têm a obrigação positiva, sob a base legal do artigo 8.º da Convenção de levar a cabo um sistema de proteção dos menores que são alvos de pedofilia (ou sua tentativa) na Internet. O coletivo do Tribunal deliberou no sentido da obrigatoriedade dos Estados criarem bases legais para monitorizar e identificar os criminosos que intentam tais ações na Internet. Perante a recomendação, os Estados que não procedessem à elaboração de um quadro legal nesse sentido falhariam na aceção do dever de proteção e, consequentemente poderiam vir a ser condenados em futuros processos.

5.1 A questão Ética

Tecnologias como a inteligência artificial ou a *Big Data* aparecem desafiando o ritmo de adaptação humano às tecnologias e ao mesmo tempo começam a ganhar espaço na sociedade e a tornar-se imprescindíveis[290][291][292] observando grandes desafios éticos[293].
A máquina é autónoma, no entanto as decisões são baseadas em algoritmos desenhados por humanos e assegurar o cumprimento dos princípios éticos deve estar presente desde o início do processo de conceção algorítmico (ex. imagine-se o recurso à análise algorítmica para decidir questões fraturantes em áreas como a dignidade da vida humana ou não discriminação)[294]. Este dilema ético deve constar *ad inicium* numa abordagem completa e interdisciplinar (política, jurídica, sociológica, entre outros) e atender a avaliações de impacto e, mesmo assim, o risco de exacerbação dos problemas ao nível político poderá ser elevado, perante a introdução deste tipo de tecnologias na sociedade pelo Estado afetando a nível decisivo a vida dos indivíduos[295].

5.2 Convenção sobre o Cibercrime de Budapeste

Em 2001, os Estados signatários da Convenção sobre o Cibercrime firmaram a assinatura de um importante instrumento internacional no combate à criminalidade no ciberespaço,

[290] Wayne Harrop e Ashley Matteson, Cyber Resilience: A review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA, in: *Current and Emerging Trends in Cyber Operations*, Palgrave Macmillans Studies in Cyber Crime and Security, p.151-152.
[291] Cfr. Murat Karaboga, et. alli, *op. cit.*, pp. 52-53.
[292] Cfr. Antonio Kung et. alli., *op. cit*., pp. 189-198.
[293] Sobre este prósito Brant Reilly sustentou, "*The limit of potencial for big data applications is unknown; thus barring collection could limit societal development*". Brant Reilly, Doing More with More: The Efficacy of Big Data in the Intelligence Community, in: *American Intelligence Journal,* N.º32, 2015, p.18-24.
Cabe salientar, para além da IA, existem tecnológicas emergentes que levantas sérias questões éticas e de impututação legal para os Estados, como por exemplo, os sistemas autónomos de guerra, que funcionam com uma base algortima *bottum-up*, na qual não existe intrevnção humana no processo decisão. Nesse sentido, *v*. Anfonso Seixas-Nunes, Sistemas Autóonomos de Guerra: Compatíveis com o Direito Internacional Humanitário?, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, p. 479 e ss.
[294] Cfr. Kate Robertson, Cynthia Khoo e Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, The Citizen Lab, University of Toronto – Faculty of Law e International Human Rights Program (IHRP), 2020.
[295] ENISA a), *op. cit.*, p. 18-19.

designadamente através da adoção de legislação adequada perante os cenários altamente complexos e internacionais experienciados pelas partes[296].

No preâmbulo desta convenção é mencionada a "(...) *cooperação entre os Estados e a indústria privada* (...)", demostrando a assunção do setor privado como agente ativo e produtor de segurança no combate à cibercriminalidade, sobretudo no processo de criação, armazenamento e transmissão de tecnologia.

Com efeito, esta convenção essencialmente visa: a) a implementação de um quadro harmónico entre Estados signatário em matéria de infrações penais; b) a criação de um quadro de auxílio na recolha de prova no ciberespaço; e c) a implementação mecanismo de cooperação internacional de forma a facilitar o tratamento *latu sensu* da prova localizada num Estado que não aquele em que se instaura o procedimento criminal[297].

Um dos principais aspetos que esteou esta Convenção prendeu-se com o acesso à Rede (possivelmente na exclusão do desenhar da computação em nuvem), nomeadamente, para prevenir infrações criminais e ilícitos ligados a redes informáticas e à informação eletrónica para auxílio de produção de prova com recurso a peritagem forense em ambiente digital. Com efeito, a capacidade e solidez da prova digital vem adquirindo uma maior relevância dada a quantidade de sistemas de informação e comunicação existentes e o consequente uso do ciberespaço para perpetração de ilícitos criminais. As capacidades de armazenamento e transmissão de dados e informação são inúmeras, desde logo, a capacidade de interconexão entre vários dispositivos localizados em diversos Estados e, por conseguinte, em diversas jurisdições. Como alerta David Silva Ramalho, para efeitos práticos de recolha de prova, "(...) *o desconhecimento da jurisdição na qual estão armazenados os dados* (...), *muitas vezes acompanhado da certeza de que os mesmos não se encontrem armazenados em território nacional, aliada à impossibilidade jurídica de recolha de prova transfronteiriça a impossibilidade prática de ativação de quaisquer mecanismos de cooperação internacional*", gerando assim um bloqueio na investigação e possivelmente efeitos irreversíveis na curta janela temporal de recolha de prova, mesmo que alguns Estados recorram à doutrina, jurisprudência e disposições nacionais para obter o acesso transfronteiriço e lograr internacionalmente um acesso legítimo aos SI

[296] Note-se dos dos Estados pertencentes ao Conselho da Europa só ainda não ratificaram este instrumento a Irlanda, a Federação Russa e a Suécia, *v.* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ausMoRba.

[297] David Ramalho, *Métodos ocultos de investigação criminal em ambiente Digital*, 2017, Almedina, p. 69-70.

localizados num Estado terceiro, mas sem que para isso tenham um sustentação jurídica[298].

Na tentativa de garantir um equilíbrio adequando entre a aplicação da lei e respeito pelos direitos humanos esta Convenção tenta conferir um ambiente de segurança cooperativo através do combate à cibercriminalidade por via da cooperação internacional em matéria penal de forma *acrescida, rápida e eficaz*. Todavia, boa parte desta Convenção acaba já absorvida pelos restantes instrumentos jurídicos produzidos pelo Conselho da Europa sobre a cooperação em matéria penal, contribuindo para o enredo jurídico e viabilizar a eficácia das investigações, nomeadamente na recolha de prova e demais diligenciais processuais relativas aos ilícitos praticados em ambiente digital pelos Estados signatários da Convenção.

No total a Convenção conta com a ratificação de 65 Estados, um número ainda insuficiente tendo em conta o número de crimes em ambiente digital, longe dos 193 Estados que tem assento na AGNU, o que faz crer que ainda existe uma larga margem de Estados que podem assinar e ratificar a convenção. No Protocolo Adicional à Convenção sobre o Cibercrime, relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos os Estados demostram ainda mais clivagens, e os Estados ainda são mais reticentes quanto à sua adesão, inclusive Estados da UE, como a Bulgária, a Hungria ou a Irlanda[299].

Entre outros argumentos pelos quais os Estados não aderem à convenção, constam a motivação política e o desacordo com base na liberdade de expressão em ambiente digital; os princípios de tratamento e proteção de dados; lacunas ao nível institucional, com falta de capacidade técnica e humana para fiscalização; e argumentos sobre a relatividade cultural e interpretação jurídica, levando à implementação assimétrica, por exemplo, diferenças nas disposições legais de proteção de dados e armazenamento de prova digital[300]. Posto isto cabe clarificar que este instrumento é tanto mais capaz quanto os Estados relevarem eficácia transfronteiriça na execução da Lei, caso contrário, a falta de harmonização e confiança no intercâmbio de dados da Europa só beneficiará os prevaricadores digitais.

---

[298] *Ibidem*, p.77-78.

[299] Conselho da Europa, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, disponível para consulta em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=EmtNHDeW.

[300] George Christou b), *op. cit.*, p. 103-104.

5.3 Carta dos Direitos Fundamentais da União Europeia

Com a adaptação da Carta dos Direitos Fundamentais da União Europeia no pós-TL adquirindo o mesmo valor jurídico dos Tratados, o espetro de direitos civis, políticos, económicos e sociais conferiram uma maior proteção aos cidadãos da UE atendendo às alterações do próprio direito em face "(...) *da evolução da sociedade, do progresso social e da evolução científica e tecnológica.*". Os direitos fundamentais mereceram um lugar de destaque na quadratura tecnológica da União, com efeito, os Estados–membros e a União ponderam equivaler-se no plano dos direitos fundamentais, afirmando um constitucionalismo europeu capaz de proteger qualquer cidadão da União[301]. Por um lado, a aplicação aos órgãos e instituições da União Europeia o princípio da subsidiariedade e indivisibilidade dos direitos fundamentais e, por outro lado, a aplicação efetiva do DUE são essenciais para os Estados observem um conjunto de garantias em prol da segurança e dignidade da vida humana aplicada ao ambiente digital, nomeadamente o respeito pela vida privada e familiar (artigo 7.º, da CDFUE) e a proteção de dados pessoais (artigo 8.º, da CDFUE).

5.3.1 CDFUE e CEDH

A CDFUE é um instrumento de direto primário da UE e observa um amplo sentido de defesa dos cidadãos enunciando (..) "*a proteção de direitos e liberdades de terceiros*", devendo ser interpretado de forma coerente com a CEDH, gozando de efeito direto nos Estados parte. Conscientes do princípio identitário da Carta e ao reconhecimento dos artigos 7.º e 8.º da CDFUE como não absolutos e, por consequência, podendo estar sujeitos a limitações[302]. Esta limitação de direitos e liberdades fundamentais são admissíveis, segundo o disposto no artigo 52.º, n.º 1 da CDFUE, caso se verifique os seguintes requisitos:

a) Provisão em disposição legal;
b) Respeito pela essência dos direitos reconhecidos pela CDFUE;

[301] Nesse sentido *v.*, Acórdão do Tribunal de Justiça da União Europeia, 6 de outubro de 2015, processo C-362/14, Schrems vs Data Protection Commissioner, disponível para consulta em: http://curia.europa.eu/juris/liste.jsf?num=C-362/14.
[302] Bart van der Sloot, *op. cit.*, p. 22.

c) Sejam observados os princípios da necessidade e da proporcionalidade[303];
d) Correspondam efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdade de terceiros.

Relativamente à CEDH também existem limitações, nomeadamente quanto ao direito do respeito pela vida privada e familiar, que proíbe condutas que tentem interferir ou constituir uma interferência na vida privada, a menos que essa interferência: i) Observe uma provisão na legal; 2) prossiga um interesse legítimo; e 3) Proceda de acordo com o respeito pelo princípio da necessidade[304].

Estas condições de admissibilidade, descritas no artigo 8.º, n.º 2 do CEDH, vão de encontro do artigo 52.º, n.º 1 da CDFUE, todavia o foco não está na proibição de uma interferência injustificada, mas nas condições em que são cumpridas para facilitar o tratamento legítimo e legal dos dados pessoais.

São notórias algumas similitudes entre a CDFUE e a CEDH ao nível das limitações de direitos, nomeadamente naqueles que foram objeto de análise neste estudo. A CDFUE, reforça ainda a sua similitude, quando no seu artigo 52.º, n.º 3, acolhendo o *sentido* e o *âmbito* da CEDH, admitindo uma maior proteção pelo DUE nos casos e nas provisões em que tal seja mais favorável à pessoa humana[305].

Apesar desta similitude, existe uma característica interpretativa na CDFUE que não se encontra presente na CEDH, que consiste na aplicação da limitação de determinados direitos e liberdades da Carta, tendo estes que "*respeitar a essência desses direitos e*

[303] Nesse sentido *v*. Olga Mironenko Enerstvedt, Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, in: *Law, Governance and Technology Series*, Sub-series: Issues in Privacy and Data Protection, N.º 37, Pompeu Casanovas, Giovanni Sarrtor e Serge Gutwirth (eds), Springer, 2017, p.178 e ss.

[304] A necessidade invocada pode revestir vários domínios, entre eles, a segurança nacional, a segurança pública, o bem-estar económico do Estado, a defesa da ordem e da prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

[305] No caso Volte e Markus Schecke e Hartmut Eifert, o TJUE julgou a proporcionalidade da publicação feita ao abrigo do Direito da União Europeia, com nomes e montantes auferidos pelos beneficiários de subsídios de apoio à agricultura. O TJUE, referiu que o direito à proteção de dados não é absoluto, argumento que a publicação dos nomes dos agricultores que receberam os dois subsídios e os montantes precisos dos mesmos constituía uma interferência na vida privada, em geral, e uma interferência na proteção dos seus dados, em particular. Todavia, também reconheceu que a publicação dos seus nomes, interferiu na sua vida, violando o artigo 7.º e 8.º da CDFUE, tendo em conta os princípios de transparência que são aplicados à comunidade, e em especial a que recebe esses subsídios. Todavia, o TJUE reconheceu que a publicação dos nomes dos agricultores, bem como os montantes auferidos, pelos mesmos através dos dois subsídios concedidos, constitui uma medida desproporcional e que não cabia no âmbito justificativo do artigo 52.º, n.º 1 da CDFUE. O TJUE declarou parcialmente invalida a legislação europeia respeitante à informação relativa aos beneficiários europeus de subsídios à agricultura.
Acórdão do Tribunal de Justiça da União Europeia, 2011, Volker und Markus Schecke e Hartmut Eifert vs Land Hessen, processo n.º C-92/09 e C-93/09, disponível para consulta em:https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2011.013.01.0006.01.ENG.

dessas liberdades. Por exemplo, de acordo com o TJUE, a legislação que permite às autoridades públicas o acesso às bases de dados com conteúdos de comunicações eletrónicas deve ser considerado como comprometedor da essência dos direitos fundamentais da pessoa humana, nomeadamente pela não conformidade pelo respeito pela vida privada como uma garantia do artigo 7.º da CDFUE (Digital Rights Ireland and Other case, parágrafo 39)[306]. Também o artigo 17.º do Pacto Internacional sobre os Direitos Civis e Políticos reforça a primazia do respeito pela vida privada, família, domicílio ou correspondência, protegendo ainda atentados à honra e reputação pessoal, não admitindo "*ingerências arbitrárias ou ilegais na sua vida privada"* [307].

Nesta senda, se por um lado a UE deu luz verde[308] aos Estados-membros para ratificar, no interesse da União Europeia, o Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, por outro lado, o mesmo não se aplica à adesão da UE à CEDH pois

[306] Foi submetido pela High Court (Irlanda) e pelo Verdassungsgerichtshof (Tribunal Constitucional Austríaco) a apreciação da validade da Diretiva 2006/24/CE, em particular, no que diz respeito ao direito à vida privada e à proteção dos dados pessoais. O TJUE observou que a Diretiva permite o armazenamento de dados suscetíveis de fornecer informações muito precisas sobre a vida privada das pessoas (por exemplo, morada permanente ou temporária, controlo de movimentos, atividades, relações e vida quotidiana).O TJUE reconheceu a interferência de modo particularmente grave nos direitos fundamentais em matéria de respeito pela vida privada e de proteção dos dados pessoais, neste sentido, o TJUE demostrou especial cuidado na ponderação do critério da proporcionalidade tendo em conta o objetivo do interesse geral público (ameaça à segurança nacional). De modo mais particular, o TJUE endereçou algumas críticas: a) reprovou a generalização da Diretiva, criticado o facto de não existir exceções ou limitações, em prol do objetivo de combater a criminalidade grave; b) referiu que a imposição do período de seis meses de armazenamento, sem fazer qualquer distinção, entre as categorias de dados com base nas pessoas em causa ou na sua plausível utilidade em relação aos objetivos prosseguidos; c) criticou a falta de salvaguardas para garantir a proteção eficaz dos sistemas e da informação, nomeadamente quanto às violações de segurança e privacidade; e d) depreciou a falta de previsão quanto à obrigatoriedade da permanência dos dados na UE e a falta de exigência do cumprimento do controlo de conformidade baseado no quadro legislativo europeu. Acórdão do Tribunal de Justiça da União Europeia, de 8 de abril de 2014, processo C-293/12, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN.

[307] "*Adopted and opened for signature, ratification and accession by General Assembly Resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976, in accordance with Article 49:*

…

Article 17

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks."*

Cfr. United Nations Human Rights, International Covenant on Civil and Political Rights, disponível para consulta em: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[308] Comissão Europeia, *Decisão do Conselho: que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (STE 108)*, 2018, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018PC0451&from=EN.

essa ambição é incerta, mesmo depois do parecer 2/94[309] e pelo parecer 2/13[310]. Sendo a CDFUE o principal instrumento de proteção dos direitos fundamentais na Europa, não é plausível que a indefinição quanto à possibilidade de adesão da UE à CEDH venha a dirimir num curto horizonte temporal dadas as questões do foro jurídico e político, pois iria implicar "(…) *o controlo por uma entidade jurídica externa à UE,* o que configuraria "(…) *cedências à soberania dos Estados*"[311][312].

Por último, a consagração destes dois instrumentos é fundamental para todos os cidadãos da EU, assegurando a privacidade e a proteção de dados, expressão de defesa essa que se revela cada vez mais necessária atendendo à massificação das interações do ser humano em ambiente digital.

6 A transição tecnológica dos Estados vs o direito de permanecer offline

A tendência generalizada das sociedades pós-modernas é o da digitalização e interconexão digital permanente dos serviços do Estado e da Administração Pública para com os cidadãos (ex: balcão único). Face ao complexo informacional de permanente interconexão à Rede cada vez mais são colocadas em jogo, por um lado, a capacidade de experimentar máquinas tecnológicas de alta complexidade e, por outro lado, a preservação da privacidade e o direito à autodeterminação informacional[313] por parte dos utilizadores. Se, por um lado, convergimos para a alta industrialização tecnológica dos sistemas públicos e existe uma maioria convergente nesse sentido, por outro, é justo questionar se haverá lugar para um conjunto de indivíduos preferirem permanecer fora deste complexo informacional, evocando a o "direito de permanecer offline"[314].

[309] Cfr. Opinion Pursuant to article 228 of the EC Treaty, Opinion 2/94, de 28 de março de 1996, disponível para consulta em: https://eur-lex.europa.eu/resource.html?uri=cellar:3645916a-61ba-4ad5-84e1-57767433f326.0002.02/DOC_1&format=PDF.

[310] Cfr. Opinion 2/13 of the Court, de 18 de dezembro de 2014, disponível para consulta em: https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?uri=CELEX:62013CV0002&from=EN.

[311] Ana Guerra Martins, *Manual de Direito da União Europeia*, Lisboa, Almedina, pp. 277-279.

[312] Para mais informações consultar: https://www.europarl.europa.eu/factsheets/pt/sheet/146/protecao-dos-direitos-fundamentais-na-ue.

[313] Cfr. Alexandre Sousa Pinheiro, *Privacy e protecção de dados pessoais:a construção dogmática do direito à identidade informacional*, AAFDL, 2015.

[314] Nesta senda, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal e o proclamado no artigo 22.º do RGPD - "*Decisões individuais automatizadas, incluindo definição de perfis*" podem constituir a base de defesa mais próximos e válidos na defesa do "direito de permanecer offline". Murat Karaboga et. alli, *op. cit.*, pp. 32-33.

Idiossincraticamente podemos avaliar a posição dos cidadãos que apelam à aceitação razoável do direito a permanecer offline e, por consequência a defesa da menor interferência do Estado no compromisso digital. Ora, tal entendimento, visa a oposição dos cidadãos à digitalização dos Estados. A migração digital dos serviços públicos de um Estado merece a nossa melhor reflexão, pois consideramos que pode colocar em causa a própria capacidade dos cidadãos em exercer direitos cívicos, em especial, nas populações e comunidades locais, onde as competências digitais são ainda uma realidade distante e que não revestem, à luz da cultura e necessidade local uma relevância prática.

Ao nível europeu, o "direito de permanecer offline" não é abordado em textos jurídicos, isto é, com força jurídica vinculativa, todavia defendemos que este seja o "*status quo*" mais puro da sociedade moderna. Destarte, o leque de direitos que atende à privacidade e à proteção de dados serve para quem, efetivamente, se vê obrigado a recorrer aos meios tecnológicos, gerando uma ação obrigatória de interação digital no sentido de realizar determinada finalidade, sob pena de incorrer em responsabilidade contraordenacional. Ora, para a realização da ação obrigação são necessárias duas condições prévias: os conhecimentos tecnológicos por parte do indivíduo e o acesso a uma máquina com conecção à Rede[315]. O constitucionalismo europeu defende que nenhum cidadão deve ficar privado do acesso aos serviços digitais pela sua condição económica ou social, sendo previsível em instrumentos legais os meios auxiliares do Estado para colmatar estas desigualdades sociais e proceder ao auxílio dos cidadãos. Com efeito, os órgãos e instituições da União Europeia, bem como os Estados-membros, seguem o caminho da forte digitalização, sendo uma opção racional, tendo em vista os custos e a rapidez do ambiente digital. Esperemos não se acentuem desigualdades sociais por via da preferência comunitária em obter uma comunidade conectada e digital, em face de uma franja populacional que cada vez menos se revê representada socialmente na sua preferência de "permanecer offline"[316].

Em 2006, Adam Greenfield, deu um importante contributo nesta matéria com a teoria simples dos cidadãos poderem recursar utilizar os recursos das redes e sistemas ubíquos. Adam Greenfield, *Everyware: The dawning age ubiquitous computing*, Berkeley, New Riders Publishing, 2006, p. 451.

[315] Cfr. Paulo Moniz, *op. cit.*, p. 18-20.

[316] Murat Karaboga et. alli, *op. cit.*, p. 43.

7 Privacidade na sociedade moderna

Os fundadores do conceito de privacidade moderna, Loius Brandeis e Samnuel Warren, determinaram a importância do conceito em relação à vida pessoal, mas também em relação aos riscos associados aos *media*[317][318]. As pessoas esperam estar livres de qualquer vigilância no seu dia a dia bem como nas suas atividades profissionais ou pessoais[319], no entanto, nos casos em que haja fundamento legal, esse direito pode ser derrogado pelas autoridades competentes.

A proteção da privacidade do indivíduo foi mencionada pelo Juiz Cooley, como o "*right to be let alone*"[320], instando à recusa de qualquer prática, medida ou ação que interfira na esfera da vida privada da pessoa humana. Com efeito, o debate contemporâneo reside precisamente no excesso de interferência externa (digital) na esfera da vida privada do indivíduo[321]. O direito à privacidade confere aos cidadãos o controlo sobre os seus próprios dados, mas também relativamente àqueles casos em que este decide transferir ou divulgar publicamente os seus dados perante outras pessoas ou entidades, sem que para isso possa temer a sua inviolabilidade[322]. Constata-se então, que o direito à privacidade não obsta à publicação de assuntos de interesse geral ou do foro do interesse da comunidade, mesmo se estes se circunscreverem a pormenores particulares. Por outro lado, existe ainda a possibilidade de cessar esse direito quando o próprio titular dos dados pessoais revela publicamente os seus dados ou informações ou é obtido o consentimento deste para a publicação[323].

A privacidade pode ser entendida como uma característica indispensável para as interações sociais, defendida por um Estado de direito democrático, que deve ser capaz de defender a identidade (digital) dos seus cidadãos[324]. Nesse sentido, a privacidade digital tem vindo a ser uma área de estudo de vários académicos, entre eles Spiros Simitis,

---

[317] Samuel Warren e Louis Brandeis, The right to privacy, in: *Harvard Law Review*, Vol IV. N.º 5, 1980, p. 195 e ss.

[318] "*If the invasion of privacy constitutes a legal injuria, the elements for demanding redress exist* (…)", neste quadro a ideia de "compensação" pela perda de privacidade é sustentada pela legislação interna dos Estados-membros e a nível supranacional com normas e princípios de direito interno e europeu.

[319] A este respeito, podemos observar a diversa jurisprudência do TEDH, *v.* https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

[320] Samuel Warren e Louis Brandeis, *op. cit*., p. 195.

[321] Ao nível dos Estados é discutida a videovigilância em massa.

[322] Olga Kuznestsova e Natalia Bondarenko, Private Life Safety Provision in Digital Age, in: *ADFS*L, V12, N.º 3, 2017, pp. 77-78.

[323] Samuel Warren e Louis Brandeis, *op. cit*., p. 218.

[324] Julie Cohen, What is Privacy For? , in: *Harvard Law Review*, 2013, p. 126.

que considerou que o processo de automação dos dados poderia colocar em causa a privacidade dos titulares dos dados e o próprio sistema democrático[325]. Sabemos que a recolha de dados ao nível do sistema Estatal e do sistema económico-comercial, ocorre na sua grande maioria por via digital, seja ela através de via direta ou indireta. Assim, através de sistemas e serviços diretamente relacionados com a máquina do Estado ou através de reportes obrigatórios que os cidadãos efetuam no âmbito de determinada finalidade, por exemplo, operações do sistema bancário ou operações de compras online, o Estado (enquanto agregado institucional) é o RpT com maiores responsabilidades de gestão dos dados pessoais dos cidadãos e, por consequência direta é a este a quem compete proporcionar por um lado, a sustentação de mecanismos de segurança da informação adequado e, por outro, defender os direitos fundamentais dos cidadãos na Era digital.

Tanto o direito à privacidade como o direito à proteção de dados são direitos fundamentais que se relacionam e, em certa parte sobrepõem-se. Ambos exaltam valores similares, ainda que de forma autónoma, pela dignidade humana e individual, garantindo a esfera de direitos de personalidade individual, liberdade, desenvolvimento da personalidade, pensamento e partilha de opiniões, como por exemplo, associamos a liberdade de expressão ou a liberdade de associação. No entanto, o Grupo de Trabalho do Artigo 29[326] notou a diferença entre ambos, "*the Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7 thereof and the same is the case at national level in some Member States*."[327].

Nem todas as situações cobertas pelo chapéu da privacidade são protegidas pelo direito à proteção de dados e vice-versa. O tratamento de dados pessoais nem sempre afeta a esfera da vida privada, mas como já mencionado, no caso *Digital Rights Irland Case*[328], onde o

[325] Evgeny Morozov, The Real Privacy Problem, in: *MIT Technology Review*, 2013.

[326] O Grupo de Trabalho instituído pelo artigo 29.º da Diretiva 95/46/CE é um órgão consultivo e independente sobre a proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no 15.º da Diretiva 2002/58/CE. É constituído por representantes das autoridades nacionais de proteção de dados dos Estados-membros, da Autoridade Europeia para a Proteção de Dados (AEPD) e da Comissão. Com a publicação do RGPD, o GT29 deu lugar ao Comité Europeu de Proteção de Dados, *v.*, https://edpb.europa.eu/our-work-tools/article-29-working-party_pt.

[327] Comissão Europeia, Article 29 Working Party, disponível para consulta em: https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

[328] Cfr. Ponto 36 do Acordão do Tribunal de Justiça da União Europeia, de 8 de abril de 2014, Digital Rights Ireland Ltd , Processo C-293/12, disponível para consulta em: http://curia.europa.eu/juris/document/document.jsf;jsessionid=B353DDD86E4D444B43D357F9BA63148A?text=&docid=150642&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=10647136.

TJUE foi chamado a decidir acerca da validade da Diretiva 2006/24/CE à luz dos direitos fundamentais, nomeadamente sobre dados pessoais e sobre o respeito pela vida privada.

O conceito de vida privada, pode ser desmitificado através da interpretação jurisprudencial do TEDH e do TJUE, onde são abordados casos relacionados com a vida privada e onde estão previstas informações de natureza sensível, confidencial, ou informações cuja interpretação ou a perceção pública possam afetar uma pessoa identificável, mesmo em aspetos da vida privada e pessoal relacionados com o trabalho ou comportamento público[329]. Por exemplo, no caso *Volker and Markus Schecje Gbr* e *Harmut Eifert* vs *Land Hessen*, de 9 de novembro de 2010, o TJUE, declarou que o conceito de vida privada "(…) *abrange todas as informações relativas a qualquer pessoa singular identificada ou identificável."*, reforçando ainda que quanto às restrições "(…) *podem ser legitimamente impostas ao direito à proteção dos dados pessoais correspondem às permitidas no quadro do artigo 8.o da CEDH*"[330].

O controlo e promoção da proteção de dados a nível nacional pelas autoridades de controlo e supervisão[331], nas competências de assistência, controlo e correção aos RpT e subcontratantes são fundamentais para a aplicação da *justiça digital.* A intervenção, quando necessária, por exemplo, nos casos de alerta e aplicação de coimas por violação das regras de privacidade e segurança da informação, ou ainda, a decisão de ordenar retificações, bloqueios, ou eliminação de dados pessoais, bem como litigar em tribunal quando são chamadas a intervir ou quando são constituídas como parte de determinado processo, são competências ou obrigações que as autoridades supervisoras que devem estar atentas e exercer de forma exemplar o seu papel, sendo a sua relevância social cada vez mais importante perante a transformação digital.

---

[329] A posição do TEDH parece uniforme quanto ao alcance interpretativo da noção do termo "*vida privada*", assim no caso Niemietz vs Germany (*v.*, nota 294) , o TEDH sustentou que "(…) *it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.*" Neste julgamento em concreto ainda se refletiu sobre a importância das relações laborais e os contactos resultantes destas como sendo enquadradas na vida privada da pessoa. O tribunal acabou por referir que (…) *deny the protection of Article 8 (art. 8) on the ground that the measure complained of related only to professional activities - as the Government suggested should be done in the present case - could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them.".*

[330] *V.*, nota supra 305.

[331] Para obter ligações às várias autoridades de controlo nacionais, *v.*, https://www.cnpd.pt/home/links/links.htm.

7.1 Segurança vs privacidade

A histórica discussão que opõe segurança e privacidade recorre ao fundamento de autoridade pública exercida pelo Estado relativamente à finalidade (inscrita na temática da segurança e proteção dos cidadãos, nomeadamente contra atos terroristas e seus equiparados) à qual o Estado usa os dados dos indivíduos.

Veja-se, no caso Europeu, aquando dos atentados terroristas nas principais metrópoles europeias, onde se verificaram o aumento das medidas de segurança, inclusive, o uso massivo de equipamentos de videovigilância, divergindo inclusive do repto lançado pelo Conselho da Europa, no sentido dos Estados-membros se absterem-se de efetuar videovigilância em massa de forma indiscriminada e desregulada. Em termos jurisdicionais, podemos observar o caso *Szabo and Vissy* vs *Hungary*, onde o requerente foi alvo de videovigilância massiva não segmentada pelas autoridades policiais e, posteriormente o TEDH viria a concluir que a legislação interna húngara violava o artigo 8.º da CEDH, porque não oferecia salvaguardas suficientes contra abusos de privacidade. Este processo fez referência específica ao caso *Digital Rights Ireland* vs *Minister of Communications and Others*[332], assinalando que a vigilância secreta "*may result in particularly invasive interferences with private life",* e que as *"guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices",* defendendo o escrupuloso cumprimento legislativo neste âmbito.

Apesar do grau de discricionariedade, a história, cultura e tradições de cada Estado ajudarem a definir o grau de maior ou menor intervencionismo na esfera da vida privada dos cidadãos, cujo perceção de ameaça pode levar a implementar medidas mais ou menos restritivas para a privacidade dos cidadãos e, por norma o TEDH, tem em consideração a *expressão da identidade*[333] nacional nas suas decisões.

[332] *V.*, nota supra 306.

[333] Sobre o princípio do respeito da identidae nacional *v.*, Ana Maria Guerra Martins, *Manual de Direito da União Europeia*, 2.ª Ed., Almedina, 2017, pp.313-316.

7.2 Privacidade, anonimato e inviolabilidade nas comunicações

Neste seguimento, todas as informações, quer sejam classificadas como informações pessoais ou não pessoais podem ser alvo de ataques em ambiente digital. Assim, destacamos alguns dois direitos que podem ser violados, tendo por base a probabilidade estatísticas recentes:

a) Direito à privacidade e ao anonimato;
b) Direito à inviolabilidade nas comunicações;

Quanto ao primeiro direito em análise, ponto de vista do direito ao anonimato, referimo-nos à liberdade de circular entre um ponto A e B sem ser identificado ou identificável. Deste modo, a autonomia do indivíduo depende do grau de distanciamento e vinculação a determinados produtos, serviços ou obrigações que possam estar associados à necessidade de conhecer a localização de um determinado indivíduo[334].

Podemos dizer que este tipo de práticas não são exclusivamente dos privados, os Estados também entram nesta equação, por motivos fundamentados no exercício da autoridade e ordem pública, por exemplo, com a utilização (em massa) de câmaras de videovigilância[335]. Recordemos o caso *Martin* vs *United Kingdom*, onde a autoridade local instalou uma câmara de videovigilância próximo da casa do requerente de forma a gravar a entrada da sua casa, tendo como objetivo obter prova do seu comportamento antissocial[336]. O TEDH aceitou o requerimento interposto pelo requerente, com base legal

[334] Por exemplo, quando vemos empregadores a efetuarem monitorização pessoal aos trabalhadores e, tal não resulta do contrato inicial assinado pelo mesmo, ou ainda pior, casos em que isso é feito à revelia do trabalhador, sem o seu consentimento ou sequer sem o seu conhecimento, verifica-se um processo extremamente lesivo do ponto de vista dos direitos fundamentais. Veja-se o caso Mirna Aris vs Intermex Wire Trasnfer, LLC, onde uma trabalhadora foi despedida sem uma fundamentação legal após o empregador controlar os empregados 24 horas por dia, 7 dias por semana com uma aplicação, com a possibilidade de monitorização da sua localização. O processo em causa foi instaurando pela requerente por invasão da privacidade dos trabalhadores, retaliação, práticas comerciais ilegais, entre outras. Caso disponível para consulta em: https://www.docketbird.com/court-documents/Arias-v-Intermex-Wire-Transfer-LLC/NOTICE-of-REMOVAL-from-Kern-County-Superior-Court-case-number-S-1500-CV-284763-SPC-by-Myrna-Arias-Filing-fee-400-receipt-number-0972-5988120/caed-1:2015-cv-01101-00001.

[335] William Baude e James Stern, The Positive law model of the fouth amendment, in: *Harvard Law Review*, Vol. 129, N.º 7, 2016, pp. 1883-1884.

[336] Neste sentido, Elisa Orrù afirma que "*These practices are connected to each other through a net of relationships, although there is no common element shared by all of them. Like the members of a family, the different privacy practices all resemble each other, but not necessarily in the same way*". Elisa Orrù, Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p.119.

do artigo 8.º da CEDH, vindo este, em sede de julgamento a observar que a monitorização realizada através da câmara de videovigilância instalada nas proximidades da sua habitação afetou de forme lesiva o seu dia-a-dia e da sua vida familiar interferindo na sua vida privada[337].

Quanto às ameaças relativas à inviolabilidade das comunicações[338], derivam da crescente massificação do uso de aparelhos tecnológicos que possibilitam o envio, interceção e receção de mensagens, nomeadamente os já mencionados IoT´s, que atualmente são consideradas como desafio securitário ao nível da PCSD podendo impactar as missões e operações[339]. Tomemos o exemplo de Edward Snowed, que revelou ao mundo o programa secreto de interceção de e-mails, conversas e correspondência dos norte americanos. Um Estado capaz de levar a cabo este tipo de condutas é potencialmente incapaz de assegurar ou garantir a inviolabilidade das comunicações dos seus cidadãos, caindo em descredito perante a comunidade internacional, e perante a sua própria população, pois ações encobertas como esta devem respeitar um regime próprio de excecionalidade e limitar a sua atuação sob a sua jurisdição, algo que, neste caso em concreto não ocorreu por intenção deliberada.

Num outro caso, *Roman Kaskharov* vs *Russia*[340], o requerente reivindicou a violação do direito à privacidade (artigo 8.º da CEDH) por parte da Federação Russa, alegando terem-lhe sido colocadas escutas telefónicas nas comunicações móveis. Adicionalmente, alegou não ter sido assistido com os meios eficientes de tutela legais. Pode ler-se na sentença que o risco de arbitrariedade numa operação como esta é evidente e, que existe uma necessidade dos Estados, ao desencadearem um processo de vigilância (secreta) a um indivíduo devem desencadear essa operação sob um escopo bastante claro e de acordo com o seu ordenamento jurídico interno, definindo objetivamente o alcance dos poderes exercidos pelas autoridades competentes na aplicação da lei[341]. No desenlace deste caso,

---

[337] Cfr. Acórdão do Tribunal Europeu dos Direitos do Homem, de 24 de outubro de 2006, Martin vs The United Kingdom, processo n.º 40426/98, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-77661%22]}.

[338] Inclusive das informações de natureza confidencial.

[339] Institute for Security Studies, *The CSDP in 2020: The EU's legacy and ambition in security and defence*, Daniel Fiott (ed), Paris, 2020, p. 91-92.

[340] Acórdão do Tribunal Europeu dos Direitos do Homem, de 4 de dezembro de 2015, Zakharov vs Russia, processo n.º47143/06, Estrasburgo, disponível para consulta em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}.

[341] O TEDH veio esclarecer, para informação dos Estados que estes devem ter em conta as salvaguardas mínimas para evitar abusos de poder, assim deve ser previsto no ordenamento jurídico interno: " (…) *the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when*

O TEDH deu como provado a violação da Federação Russa sob o escopo do artigo 8.º da CEDH em favor do requerente.

8 Análise prospetiva

O processo de inovação e desenvolvimento tecnológico elencou várias vantagens na vida do cidadão, desde a capacidade de um processo de recuperação de doentes com maior rapidez à automatização de processos nas indústrias, mas também trouxe desvantagens, tal como a perda de privacidade. Com efeito, talvez não estejamos no contexto em que George Orwell (1949)[342] desenhou, porque os valores da privacidade e da segurança são preservados pelas cidadãos (ou parte deles) e defendidos em sede própria, mas com a constante e sedimentada evolução virtual tornasse cada vez mais evidente a dificuldade ao cidadão comum se adaptar aos novos processos tecnológicos, mesmo ao nível das obrigações Estatais, consequência das crescentes diretrizes digitais impostas por via da digitalização dos Estados.

O tratamento de dados e informação possibilitou um grau de interação e experiência aos internautas nunca antes visto, revolucionando mesmo o processo e o modelo de negócios, dando origem à 4ª revolução industrial, ou Indústria 4.0. Todavia, este tipo de revolução apresenta representa riscos, em especial para a segurança da informação e da privacidade das pessoas. A constante novidade tecnológica gera uma inegável fonte de conhecimento ao ser humano, e em casos práticos, possibilita mesmo uma melhoria da qualidade de vida das populações, porém, podemos observar riscos associados ao uso de tecnologia em

communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed (see Huvig, cited above, § 34; Amann v. Switzerland [GC], no. 27798/95, §§ 56-58, ECHR 2000-II; Valenzuela Contreras, cited above, § 46; Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003; Weber and Saravia, cited above, § 95; and Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 76).”. Um outro aspeto reforçado por este acórdão é a garantia do órgão de supervisão na aplicação destas medidas, neste caso o controlo judicial (através do Juiz), como pode ler-se “ (…) *the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see Klass and Others, cited above, §§ 55-56).”*. Cfr. ponto 233 do acórdão.

[342] George Orwell, 1984 George Orwell. O autor tentou alertar a sociedade britânica e norte americana para os perigos totalitários de controlo político, como uma espécie de “*big broher*” social, em que inegavelmente conduziria a uma a perda da liberdade individual e uma ameaça às democracias. *v*., https://time.com/5602363/george-orwell-1984-anniversary-surveillance-capitalism/.

ambiente digital, bem como práticas ilícitas associadas a estes, inclusive para ameaça ou mesmo violações do direito da vida privada[343].

O fator "humano" continua a constituir a principal fonte de violações de segurança, seja por erro ou comportamento mal-intencionado (dolo) nas ações, sendo que as vulnerabilidades ocorrem sobretudo ao nível dos sistemas de informação[344].

Num quadro dominado pela tecnologia em massa, os deveres gerais devem proteger os interesses gerais, assegurando a proteção dos direitos fundamentais e os princípios democráticos. As novas tecnológicas como a IA apresentam um significativo impacto na melhoria da qualidade de vida dos cidadãos e das infraestruturas críticas dos Estados[345], todavia ainda carecem de aprofundamento técnico (algorítmico) para se poderem instalar em massa na sociedade, sempre observando o respeito pelos direitos fundamentais, o que poderá afigurar-se no mínimo um desafio os Estados da União.

O maior desafio da União ao nível da cibersegurança faz-se sentir ao nível da cooperação institucional, nomeadamente pela complexidade de atores (públicos e privados), instrumentos legais (vinculativos e não vinculativos) e políticas multinível numa base descentralizada[346]. A compreensão partilhada a vinte e sete Estados pode ser de difícil entendimento dado o número de partes interessadas e o potencial económico, político e social.

Quanto maior for o grau de harmonização europeia nas normas de cibersegurança, maior a cooperação neste domínio para as organizações que lidam com a partilha de informações entre Estados da União e países terceiros, caso contrário, poderá acentuar-se a polarização entre as normas internas de Estados-membros e, por sua vez, gerar *desconfiança digital*, no âmbito dos órgãos e agências da UE ou no âmbito da oferta de bens e serviços do comercio online, contribuindo para o enfraquecimento do mercado único digital.

Cumpre observar que o cenário jurídico de cibersegurança no espaço europeu está atualmente em mudança, e espera-se que assim continue dado a massificação tecnológica e a transição digital em curso[347]. Dessa forma, o plano "Next Generation UE" configura

---

[343] Por exemplo, fenómenos como roubos de identidade, extração de dados e bloqueio de sistemas.

[344] Noushin Ashrafi, Christopher Schuetz e Jean-Pierre Kuilboer, *Twenty-second Americas Conference on Information Systems*, San Diego, 2016.

[345] Jacob Sakhnini, et alli., AI and Security of Critical Infrastructure, in: *Handbook of Big Data Privacy*, Kim-Kwang Raymond Choo e Ali Dehghantanha (eds), Springer, 2020, 7 e ss.

[346] Helena Carrapico e André Barrinha, *op. cit.*, p. 1261.

[347] As ações legais instauradas ao abrigo do RGPD, pelas autoridades nacionais, demostram que a repressão e sanção das violações de proteção de dados e segurança da informação configuram um mecanismo que não caiu na simples figura legislativa, isto é, pelo menos para uma boa parte das autoridades nacionais. Para uma visão geral das coimas aplciadas por violação de proteção de dados pelas autoridades nacionais de proteção de dados na UE, *v.*, https://www.enforcementtracker.com/.

um instrumento adicional da Comissão Europeia, que espera um reforço no investimento para uma Europa digital. Por seu turno, os Estados-membros conseguem estimular a economia e criar condições para uma recuperação económica conduzida pelo investimento privado em setores tecnológicos essenciais. Este investimento releva particular importância para o eixo da transição digital na Europa, nomeadamente no comércio online e na transição digital dos Estados[348].

Se, por um lado, a União se tem revelado como um ator produtor de cibersegurança num ecossistema complexo e em constante desenvolvimento, por outro, ainda se verificam altas disparidades entre Estados–membros em algumas matérias com sobreposição de iniciativas do foro técnico-político[349].

A sedimentação de uma posição que salvaguarde os direitos fundamentais dos cidadãos da União perante as novas tecnologias, mais concretamente, perante o tratamento de dados de forma aleatória e automatizada é essencial para a manutenção da unidade dos Estados democráticos, sob pena dos Estados caírem no esquecimento de franjas da população.

[348] A Comissão estima uma necessidade de investimento que ascende pelo menos a 1,5 biliões de euros entre 2020 e 2021.

[349] George Christou a), *op. cit.*, p. 281.

III- Cooperação transatlântica e ameaças

9 Intercâmbio de informações

A informação retirada da fonte e filtrada para a segurança da informação apresenta um tipo de classificação própria[350]. Assim, o tipo de informação no arranjo da segurança da informação pode ser descrito como uma vulnerabilidade[351], uma ameaça[352], uma contramedida[353], um ataque[354], um risco[355] ou um ativo[356][357]. Em relação ao tipo de fonte de dados para a segurança da informação, verifica-se que provém de sites de notícias e blogs (ver anexo B)[358]. Verificasse, através das co-ocorrências, que o tipo de informação que é tratada com mais frequência no círculo interno da segurança da informação inscrevesse na rubrica das vulnerabilidades, incluída em 90% das fontes[359].

Geralmente, verificasse que as fontes de dados de segurança da informação contêm informações sobre vulnerabilidades e ataques e, a par destes existe uma forte ligação entre vulnerabilidades, ataques e ameaças.

Na União Europeia, a cooperação ao nível da troca de informações no âmbito criminal iniciou-se em Maastricht, e desenvolveu-se nos Tratados de Amesterdão, e posteriormente, no Tratado de Lisboa. Todavia, a União enquanto figura jurídica não prevê no seu Tratado qualquer competência legislativa que lhe possibilite avançar na coordenação de um serviço de análise ou *intelligence* de informações. Apesar disso, a UE dispõe do INTCEN, apresentado como um serviço de análise civil no seio da União, integrado no SEAE, e sob a tutela do Alto representante da União para os Negócios Estrangeiros e Política de Segurança. Este serviço fornece uma capacidade analítica de alto nível aos governantes e os seus *outpus* são baseados nas informações fornecidas pelos serviços de informações dos Estados-membros[360]. Não obstante, a cooperação ao nível da

[350] Diferente do tipo de classificação apresentado, por norma, uma taxonomia diferente, por exemplo, Muito Secreta, Secreta, Confidencial ou Restrita, para mais informação acerca das marcas e graus da informação classificada, *v.*, https://www.gns.gov.pt/media/12746/20190910_foheto_gns_v2.pdf.

[351] Informação sobre uma fraqueza de um determinado ativo que pode ser explorada por meio de uma ameaça.

[352] Informação sobre a potencial causa de um incidente indesejado.

[353] Informação relacionada a qualquer controlo administrativo, de gestão, técnico ou jurídico utilizado para neutralizar um risco de segurança da informação.

[354] Informação sobre qualquer tentativa não autorizada de acesso, alteração ou destruição de um ativo.

[355] Informação que descreve as consequências de um evento potencial, como um ataque.

[356] Informação referente sobre qualquer objeto ou característica que tenha valor para uma organização.

[357] Clemens Sauerwein et. alli., An analysis and classification of public information security data sources used in research and practice, in: *Computers & Security*, Vol. 82, 2019, Elsevier, p. 145.

[358] *Ibidem*, p. 147.

[359] *Ibidem*, p. 149.

[360] Para mais informações, *v.*, https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf. Adicionalmente, através do SEAE, existe um serviço que presta o mesmo tipo de missão, mas ao nível militar, o EUMS INT. Para mais informações, *v.*, https://eeas.europa.eu/delegations/new-zealand/5437/the-european-union-military-staff-eums_fr.

troca de informações permanece à disposição das agências de informações na UE numa base de diálogo bilateral e multilateral.

A partilha de informações ao nível da SI com as estruturas existentes baseia-se nas redes CSIRT[361][362]como analisado previamente, legalmente previstas no artigo 12.º da Diretiva NIS.

Os mecanismos de partilha de informações relacionados com as ameaças em ambiente digital carecem de intervenção humana (seja por e-mail, telefone, reuniões, canal dirigido, entre outros) e podem operar sob diferentes escopos, seja a nível nacional, regional ou internacional sempre com uma cultura de segurança da informação baseada na partilha e no risco. Por exemplo, o Cyber Security Information Exchange Framework (CYBEX)[363], foi um dos primeiros mecanismos do género a operar à escala global (2010)[364]. Posteriormente, foram sendo desenvolvidos mecanismos segmentados baseados na

[361] A nível nacional servem de polos agregadores de informação de segurança da informação entre setores, quer de natureza pública ou privada, infraestruturas indispensáveis para a cooperação, troca de informações, tratamento de incidentes transfronteiriços e resposta coordenada a incidentes específicos.

[362] Para mais informações *v*., https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

[363] CYBEX - Cybersecurity Information Exchange Framework. (…) *focuses on cybersecurity information exchange between cybersecurity organizations*". Anthony Rutkowski, Youki Kadobayashi, Inette Furey, *CYBEX – The Cybersecurity Information Exchange Framework (X.1500), ACM SIGCOMM Computer Communication Review*, Vol. 40, N.º 5, 2010, p. 60.

[364] Para o estudo em análise não foi tido em conta outro tipo de programas como o PRISM. Este programa foi concebido pela NSA nos EUA e consistia num sistema de vigilância onde foram recolhidos dados dos utilizadores em várias plataformas e redes sociais entre 2007 e 2013. Cfr. Michael Landon-Murray, Big Data and Intelligence: Applications, Human Capital, and Education, in*: Journal Of Strategic Security*, Vol. 9, n.º 2, 2016, p. 102.

partilha de informações, como a EISAS[365], CIF[366], TAXII[367], STIX, CyBox[368], IODEF[369], RID[370] e o ISAC[371].

Ao nível NATO, foi desenvolvido um programa de partilha de informação de ciberdefesa em colaboração com os membros da aliança - CDXI[372]. A estrutura integrou recursos que forneciam uma infraestrutura única no campo da defesa cibernética. O projeto CDXI definiu um conjunto de onze requisitos[373] de elevado nível técnico para o sistema de troca

---

[365] EISAS - European Information Sharing and Alert System, tem como objetivo *"(…) raise awareness about IT security issues among citizens and SMEs across Europe. A secondary objective is to assess the benefits of enhancing cooperation among existing activities and the added value which would be achieved by these activities as a result.*". ENISA, *EISAS – European Information Sharing and Alerting System*, 2013, p.2.

[366] CIF - Collective Information Framework, "(…) *helps organizations to structure, normalize, store, post process, query, share, and produce data sets related to cybersecurity threats in a single database. More precisely, this intelligence management system combines known malicious threat information from several sources and uses that information for incident response, detection, and mitigation. The majority of the information contained in the CIF repository includes IP addresses, domains, and URLs associated with malicious activity"*. Frederic Lemieux, *op. cit*., p. 134.

[367] TAXII – Trusted Automated Exchange of Indicator Information, "(...) *provides a set of specifications defining the network-level activity of the exchange and defines services as well as messages to exchange data. It supports multiple sharing models including variations of 'hub and spoke' as well as 'peer to peer.' The TAXII enables organizations to share the information they choose about cyber threats with the partners they choose*". *Ibidem*, p. 136

Para mais informações sobre o programa, *v.*, https://us-cert.cisa.gov/ais.

[368] CybOX - Cyber Observable Expression e STIX - Structured Threat Information Expression "(…) *are standards that support data formatting. The STIX language intends to convey the full range of potential cyber-threat information. The STIX architecture consists of eight constructs and 70 object types that capture all the details relating to a malicious actor's campaign, tactics, actions, and targets (Mitre 2013b). These constructs are (1) threat actor; (2) campaign; (3) trusted third party; (4) exploit target; (5) courses of action; (6) incident; (7) indicator; and (8) observable. CybOx is a standardized schema for the specification, capture, characterization, and communication of incidents that are observable in the operational domain.*". *Ibidem.*

[369] IODEF - Incident Object Description Exchange Format, "(…) *it is a standard for representing computer security information commonly exchanged between Computer Emergency Readiness Teams (CERTs) and organizations facing a cyber-security incident."* O objetivo principal do programa consiste em *(..) provide an improved ability to resolve incidents and convey situational awareness by simplifying collaboration and data sharing*.". *Ibidem.*

[370] RID - Real-time Inter-Network Defense, "*RID outlines a proactive inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution.' The IODEF and RID are information-sharing standards in the Multi-national Alliance for Collaborative Cyber Situational Awareness (MACCSA) information-sharing framework*". *Ibidem*, p.136-137.

[371] A FS-ISAC - Financial Services Information Sharing and Analysis Center, "(…) *is dedicated to reducing cyber risk in the global financial system. Serving financial institutions and in turn their customers, the organization leverages its intelligence platform, resiliency resources and a trusted peer to-peer network of experts to anticipate, mitigate and respond to cyber threats*". *Ibidem*. Para mais informações sobreo programa *v*., https://www.fsisac.com/.

[372] Luc Dandurand, *Cyber Defence Data Exchange and Collaboration Infrastructure*, 22nd Annual FIRST Conference, Miami, 2010, disponível para consulta em: https://www.first.org/resources/papers/conference2010/dandurand-slides.pdf.

[373] Os requisitos em análise são: " *1) Provide an adaptable, scalable, secure, and decentralized infrastructure (e.g., allow for flexible access controls, private query, anonymous contribution, data replacement, data exchange review, support of small and large organizations, and knowledge exchange among community of interest); 2) Provide for the controlled evolution of the syntax and semantic of multiple independent data models and their correlation (e.g: allow organizations to implement standardized data*

de informações de forma a elevar a maturidade dos sistemas de informações. O objeto essencial do projeto residiu na facilidade na partilha de informação com recurso à tecnologia de automação. Simultaneamente, pretendia facilitar a produção, refinamento e verificação dos dados e encargos adicionais com a colaboração externa[374]. A dificuldade de integração deste projeto residiu na integração dos diferentes modelos de dados e ontologias utilizadas por cada sistema, dado que a gestão de grandes volumes de informação por si só exige um processo complexo de automatização[375].

A NATO, através da sua agência dedicada exclusivamente às comunicações e informações - NCI[376], observa um conjunto de projetos de matriz defensiva e ofensiva, sendo estes relativos à segurança da informação, cibersegurança ou *intelligence*.

9.1 Programas de intercâmbio de dados da União

Sobre um prisma bilateral e transatlântico são várias as disposições relativamente à proteção dos cidadãos e segurança da informação. A UE tem mantido ao longo das últimas duas décadas negociações, sendo possível obter um quadro legislativo cooperativo, destacando cinco tipos:

models that can be captured by 'independent topic ontologies' through data correlations); 3) Securely store both private and shared data (e.g., allow organizations to use agile data models and correlation capabilities to discriminate private and sharable data); 4) Provide for customizable, controlled multilateral sharing (e.g., allow integration of IPEs from all participating organizations and enable free association of IPEs with communication channels); 5) Enable the exchange of data across non-connected domains (e.g., allow exchange across these 'air gaps' without compromising secured networks); 6) Provide human and machine interface (e.g., allow for the integration and use of graphical user interfaces as well as application programing interfaces); 7) Provide collaboration tools that enable burden sharing for generation, refinement, and vetting of data (e.g., allow organizations to collaborate through threaded discussion mechanisms in order to annotate data and understand context of data modification); 8) Provide customizable quality control process (e.g., allow organizations to share quality control processes in order to ensure collaboration in maintaining data quality assurance); 9) Expose dissension to reach consensus (e.g., allow organizations to correct detected errors and inexactitudes by integrating divergent values that expose multiple truths); 10) Support continuous availability of data (e.g., allow organizations to store and access data locally in case of interruption or disconnection of external networks – resilience); 11) Enable commercial activities (e.g., allow integration of accounting models for data providers and data consumers through commercial contracts)". Frederic Lemieux, op. cit., p. 140.

[374] Luc Dandurand e Oscar Serrano Serrano, *Towards Improved Cyber Security Information Sharing*, 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.), 2013, NATO CCD COE Publications, Tallinn, 2013, disponível para consulta em: https://ccdcoe.org/uploads/2018/10/25_d3r1s5_dandurand.pdf.

[375] Frederic Lemieux, op. cit., p. 141.

[376] Para mais informações, *v.*, https://www.ncia.nato.int/index.html.

I. Quanto a decisões de adequação e nível de segurança, o RGPD atribui, através do postulado no artigo 45.º, o poder decisório à Comissão quanto às transferências internacionais, ou seja, a Comissão avalia o nível de segurança de um Estado terceiro à UE com base na sua legislação interna e compromissos internacionais assumidos.

II. Acordo-quadro UE-EUA[377], também conhecido como "acordo global", que compreende um conjunto harmonizado de medidas de segurança, que visam assegurar um elevado nível de proteção dos dados pessoais transferidos no quadro da cooperação transatlântica no domínio da aplicação da lei (âmbito penal), em especial em matérias de segurança, como o combate ao terrorismo e criminalidade organizada[378][379].

---

[377] Decisão (UE) 2016/920 do Conselho de 20 de maio de 2016, relativa à assinatura, em nome da União Europeia, do acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais.
Este acordo prevê a salvaguarda da proteção dos direitos dos titulares dos dados no âmbito da transferência transatlântica entre autoridades polícias e judicias, este quadro inclui: a) *limitações claras sobre a utilização dos dados* (os dados pessoais só podem ser utilizados para efeitos de prevenção, investigação, deteção e repressão de infrações penais); b) *restrições impostas a transferências ulteriores* (as transferências ulteriores para países que não sejam os EUA, países não pertencentes à UE, ou organizações internacionais devem ser aprovadas pela autoridade competente do país que realizou a transferência inicial dos dados pessoais); c) *períodos de conservação* (os dados pessoais apenas podem ser conservados durante o período considerado necessário ou adequado. Estes períodos de conservação devem ser publicados ou tornados do domínio público; d) *o direito de acesso aos dados pessoais e o direito de retificação* (todas as pessoas têm o direito de aceder, em determinadas condições, aos dados pessoais que lhes digam respeito e podem solicitar a retificação dos dados inexatos); e) *a notificação em caso de violação da segurança dos dados* (obrigatoriedade da existência de um mecanismo que assegure assegurar que a autoridade competente e, se for caso disso, o titular dos dado é notificado de qualquer violação da segurança dos dados); e f) *o recurso judicial e a aplicabilidade dos direitos* (garantir aos cidadãos da UE o direito adicional de interpor recurso judicial junto dos tribunais dos EUA se as autoridades deste país negarem o acesso aos seus dados pessoais, a retificação dos mesmos, ou se procederem à divulgação ilícita desses dados). Além disso, os cidadãos da UE titulares dos dados podem invocar os direitos de recurso judicial já existentes nos EUA. Para consultar o acordo, *v.*, https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:280601_1 e https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_2040.

[378] Este acordo está coberto pelas principais normas de proteção de dados do quadro legislativo europeu, assim: a) normas quanto ao *tratamento de dados* (como por exemplo, qualidade, integridade dos dados e da sua segurança, mesmo no seu processo de intercâmbio); b*) garantias e limitações* (como por exemplo, finalidades e restrições de utilização e conservação de dados); e c) garantia efetiva *dos direitos dos titulares de dados* (como por exemplo, a aplicação da possibilidade do titular dos dados exercer os seus direitos de acesso, retificação, recuso administrativo e judicial).
A par da aplicação deste quadro legislativo, é garantido o princípio da supervisão independente, nomeadamente quando à condução de investigações, com poder decisório sob queixa individual quanto ao não cumprimento do acordo e a revisão periódica conjunta. Para mais informações, *v.*, https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:3104_8&from=PT e https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31925.

[379] No estrito cumprimento do papel do Parlamento, nos termos do artigo 218.º, n.º1, do TFUE, decidiu solicitar um parecer ao TJUE numa Resolução de 25 de novembro de 2014. Em resposta, o TJUE, em 26 de julho de 2017, considerou que o "acordo PNR" não poderia ser concluído na sua forma existente, já que possuía várias disposições incompatíveis com o DUE.

III. Escudo de Proteção de Privacidade (em inglês, *Privacy Shield*[380]), reconhecido pela Decisão (EU) 2016/1250[381], reforçando a proteção dos dados pessoais dos cidadãos da EU transferidos para os EUA (invalidado pelo TJUE[382]).

Os dados da *Privacy Shield* são mantidos e disponibilizados, através da comunicação e cumprimento de regras específicas de uma lista de organizações que se encontram a cumprir os elevados padrões de proteção de privacidade exigidos pelo escudo, tendo estas organizações que passar pelo crivo do Departamento do Comércio dos Estados Unidos[383].

IV. No âmbito bilateral, a UE assinou acordos quadro sobre registos de identificação de passageiros (PNR) com os EUA[384], Austrália[385] e Canadá[386]. Os dados contidos

---

[380] Comissão Europeia, Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting, 2016, disponível para consulta em: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_2040.

[381] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

[382] Este acordo foi declarado inválido pelo TJUE no caso Data Protection Commissioner v. Facebook & Max Schrems, processo C-311/18, de julho de 2020, Disponível para consulta em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=10414552.

Com esta decisão jurisprudencial, assistimos a um impasse jurídico quanto à transferência de dados entre os EU-EUA. Este acórdão representa uma derrota em toda a linha para a Comissão, nomeadamente ao nível da avaliação do nível da proteção assegurado no contexto de uma transferência de dados para um Estado terceiro. Assim, a autoridade nacional de controlo de proteção de dados tem a competência do poder decisório quanto à suspensão ou proibição de transferências para Estados-terceiros, desde que:

a) Sejam fundadas pelas cláusulas-tipo de proteção de dados adotadas pela Comissão;
b) As cláusulas contratuais associadas à transferência de dados em específico não são ou não podem ser respeitadas nesse Estado terceiro e a proteção de dados transferidos não pode ser assegurada por outros meios, atendendo às disposições regulatórias do DUE, em especial, nos artigos 45.º e 46.º do RGPD e a CDFUE.

Este acórdão suspende o envio de dados pessoais de empresas e cidadãos para os EUA em vigor desde 2016, deixando empresas localizadas nos dois lados do atlântico num vazio jurídico.

[383] *V.*https://www.privacyshield.gov/welcome.

[384] Jornal Oficial da União Europeia, *Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados*, 2012, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22012A0811(01)&from=EN.

[385] Jornal Oficial da União Europeia, *Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano*, 2012, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22012A0714(01)&from=EN.

[386] Antes da votação final do acordo bilateral entre a UE-Canadá sobre o tratamento de dados PNR, o Parlamento Europeu solicitou um parecer ao TJUE, nos termos do artigo 218.º, n.º 1, do TFUE, sob a forma de resolução de 25 de novembro de 2014. Em 2017, a resposta do TJUE veio considerar que os termos do Acordo que iria ser firmado não poderia ser concluído daquela forma, uma vez que as suas disposições eram incompatíveis com o direito fundamental à proteção de dados pessoais. Pode ler-se que os tratamentos de dados associados: "*consubstanciam uma ingerência no direito fundamental ao respeito da vida privada. Do mesmo modo, o acordo projetado contém uma ingerência no direito fundamental à proteção dos dados pessoais.",* ainda assim, salientou que "*as ingerências são justificadas pela prossecução de um objetivo de interesse geral (garantia da segurança pública no âmbito da luta contra infrações terroristas e a*

nas reservas, no controlo de voos ou outros quaisquer recolhidos pelas transportadoras aéreas podem ser utilizados no âmbito da aplicação da lei de fiscalização, como por exemplo, pelas autoridades responsáveis pelo combate ao terrorismo e criminalidade organizada.

V. Programa de deteção de financiamento ao terrorismo (TFTP), consiste num acordo bilateral entre a UE e os EUA sobre o tratamento e transferência de informações relativas a mensagens de pagamentos da UE para os EUA, tendo como finalidade a prevenção do financiamento a ilícitos praticados com vista à prática de infrações terroristas[387][388].

criminalidade transnacional grave), todavia "*várias disposições do acordo não se limitam ao estritamente necessário e não preveem regras claras e precisas.".* No mesmo ano foram abertas negociações.
Tribunal de Justiça da União Europeia, Parecer 1/15, de 26 de julho de 2017, disponível para consulta em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084pt.pdf; Conselho da União Europeia, *Recomendação de Decisão do Conselho que autoriza a abertura de negociações de um acordo entre a União Europeia e o Canadá para a transferência e utilização dos registos de identificação dos passageiros (PNR) para fins de prevenção e luta contra o terrorismo e outros crimes transnacionais graves, de 23 de outubro de 2017*, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-13490-2017-INIT/pt/pdf.

[387] Jornal Oficial da União Europeia, *Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo*, 2010, disponível para consulta em: https://www.cnpd.pt/home/direitos/EU_EUA_AGREEMENT_TFTP_2_pt.pdf.

[388] O Parlamento Europeu, em 2013, adotou uma Resolução sobre o programa de vigilância da Agência Nacional de Segurança dos Estados Unidos, os órgãos de vigilância em diversos Estados-membros e o seu impacto na privacidade dos cidadãos da UE (2013/2682(RSP)). Esta ação foi enquadrada na sequência dos factos revelados em 2013, sobre a alegada espionagem dos EUA a alguns Estados-membros da União. Foi realizado um extenso inquérito, pelo Parlamento Europeu, sobre a vigilância eletrónica em larga escala aos cidadãos da União Europeia. A alegada espionagem, abrangia, entre outros programas equivalentes, o programa PRISM, que configuravam uma violação grave do direito fundamental à privacidade, à proteção de dados dos cidadãos, o direito à vida privada e familiar, à confidencialidade das comunicações, à liberdade de expressão, à liberdade de informação e à liberdade empresarial, atos altamente condenáveis, inclusive previstas na Convenção de Viena sobre as Relações Diplomáticas. Com este cenário, a União Europeia viu-se obrigada a agir para restabelecer a confianças nos fluxos de dados transferidos com os EUA. Para tal, decidiu adotar um pacote de medidas de reforma sobre proteção de dados (dando origem ao RGPD e à Diretiva de Cooperação Policial), reforçar a esfera de segurança no sistema "Porto Seguro" (que deu origem a uma comunicação da Comissão ao Parlamento Europeu e o Conselho com treze recomendações, *v.* https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52013DC0847, e mais tarde viria a ser considerado inválido, dando origem ao "Escudo de Proteção de Privacidade", e a reforçar as garantias em matéria de proteção de dados pessoas sob um quadro cooperativo previamente estabelecido entre os serviços repressivos, inclusive o "acordo-quadro". Como supra visto, este Escudo viria a ser decradado inválido.

9.2 Cooperação ao nível transatlântico e resiliência das infraestruturas críticas nacionais de informação

As infraestruturas críticas de informação denominam-se por " (...) *quaisquer sistemas de tecnologias da informação que suportem ativos fundamentais e serviços das infraestruturas nacionais.*"[389], enquanto que as infraestruturas críticas nacionais representam " *a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.*"[390][391].

O encontro de uma plataforma de intercâmbio de dados em ambiente seguro e ao mesmo tempo cooperativo pode ser um desafio bastante complexo, principalmente ao nível transatlântico[392]. Podemos apontar os conhecidos escândalos que envolviam espionagem americana em solo europeu[393][394], ou do ponto de vista jurisdicional, nomeadamente nos acórdãos em que o TJUE declarou que não foram asseguradas as garantias adequadas aos cidadãos da UE, tendo em conta as cláusulas tipo de proteção de dados que supostamente beneficiariam os cidadãos da União com um nível de proteção substancialmente equivalente ao garantido pela União Europeia. O último desenvolvimento ao nível jurisdicional, deu conta da invalidação da Diretiva de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade EU-EUA por parte do TJUE[395].

A troca de informações é considerada um elemento fundamental para a melhoria e monitorização da correlação, identificação e disseminação de informação elevando os participantes a um patamar de conhecimento situacional superior. No entanto, existem algumas limitações à partilha de informação, principalmente de informações respeitantes

[389] Tim Maurer e Robert Morgus, Compilation of Existing Cybersecurity and Information Security Related Defintions, in: *Open Technology Institute New America*, 2011, p. 44.
[390] Resulta do Decreto-Lei n.º 62/2011, de 9 de maio, que estabelece os procedimentos de identificação e proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social nos sectores da energia e transportes e transpõe a Diretiva n.º 2008/114/CE do Conselho, de 8 de dezembro.
[391] Traduzido para português através do sítio institucional do CNCS, *v*., https://www.cncs.gov.pt/recursos/glossario/.
[392] U.S Department of State, *A New Transatlantic Dialogue*, 2020, disponível para consulta em: https://www.state.gov/a-new-transatlantic-dialogue/.
[393] Russell Buchan, *Cyber Espionage and International Law*, HART, 2019, p. 70 e ss.
[394] David Omand, Understanding Digital Intelligence: A British View, in*: National Security and Counterintelligence in the Era of Cyber Espionage*, Eugenie de Silva (Ed), IGI, 2016, pp. 99 e ss.
[395] Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

a incidentes no ciberespaço[396]. A falta de um registo técnico e respetiva partilha de informação em momento adequado pode comprometer a mitigação de qualquer ataque informático de grande escala. Assim, elenca-se o *registo* e *reporte* como primeiro grande desafio das infraestruturas críticas nacionais de informação[397].

Em segundo, apontamos a *duplicação informacional*. A duplicação de sistemas de troca de dados resulta na deterioração da partilha de informações e incentiva à acumulação de informações, contribuindo para o *ruído informacional*, devendo-se principalmente a uma sobrecarga na troca de informações num determinado canal de comunicação entre transmissores e recetores. De forma a poder ser considerada útil, a troca de informações deve ocorrer sob um escopo rigoroso de critérios, aplicando *filtros informacionais*, de modo a que seja apenas a informação mais importante transmitida, sem duplicações para auxiliar de forma correta a gestão de determinada emergência[398]. Não menos importante será mencionar a capacidade de visualizar, tratar e estruturar os dados compartilhados, podendo ser um decisivo contributo para o aumento ou diminuição de ruído, um pouco à luz da qualidade dos dados que são rececionados e o seu grau de confiabilidade[399].

Em terceiro, apontamos a fricção institucional, ou seja, o atrito entre os diferentes participantes num determinado sistema. Os participantes centram o foco na partilha de informação sobre o mesmo segmento ou nicho de mercado e, nesse sentido poderá ser despoletado um nível competitivo e conflituante nos interesses em jogo, que poderá acabar por limitar a partilha de informação[400]. Por outro lado, a troca de informação em ambiente digita distribuí dividendos para todos, pois a vantagem competitiva retirada da partilha de informação sobre as ameaças cibernéticas é muito maior do que o custo de uma não participação. Tratando-se de um sistema de base voluntarista, a troca de informação dependerá, em último caso da decisão do participante em partilhar informação e, nesse aspeto os sistemas de partilha de informação ainda são limitados, salvo se houver regulamentação associada com obrigações de *reporte informacional*.

Na perspetiva das relações internacionais, Thierry Balzacq e Benjamin Puybareau escrevem sobre a economia do segredo ("Economy of Secrecy"), uma narrativa de controlo e domínio da informação projetada pela ambição hegemónica dos EUA pela informação, recorrendo a alianças políticas e modulação da informação entre vários

[396] Frederic Lemieux, *op. cit.*, p. 131.
[397] *Ibidem.*
[398] *Ibidem, p. 132.*
[399] *Ibidem.*
[400] *Ibidem, p.133.*

Estados. De modo semelhante, o impacto negativo do caso Snowden, onde as ondas de choque internacionais sobre alegada espionagem em diversos Estados contribuíram para um ambiente disfuncional na economia do segredo na cena internacional[401]. Ora, através deste cenário somos levados novamente a questionar a colaboração da UE com os EUA, dado o registo comprometedor da política externa dos EUA em relação à metodologia na obtenção de informações de cidadãos da UE. Destacamos também o impacto e a infrações aos direitos fundamentais dos cidadãos europeus com a *economia do segredo*, recordemos o parágrafo 60 do acórdão do TJUE, *Maximillian Schrems vs Data Protection Commissioner* declarando que, "(…) *a União é uma União de Direito cujas instituições estão sujeitas à fiscalização da conformidade dos seus atos, nomeadamente, com os Tratados, com os princípios gerais do direito e com os direitos fundamentais*". Adicionalmente, neste acórdão, foi postulado a desarmonia entre os diferentes ordenamentos jurídicos nos Estados-membros relativamente à execução da lei e, consequente invalidação de prova digital em processo penal.

Neste sentido, os órgãos jurisdicionais da União representam o último bastião da defesa contra eventuais ingerências nos direitos fundamentais dos cidadãos na União. A decisão de partilha informacional, terá que ser precedida de uma análise dos direitos e do valor associado ao potencial efetivo da informação transmitida, nomeadamente entre o direito à vida privada e proteção de dados e a prossecução de interesses legítimos do Estado, como é o caso da segurança ou defesa nacional.

9.3 Mecanismos de cooperação policial e judiciária europeia

A partilha de informação do foro policial apresenta um enquadramento legislativo e operativo definido ao nível da União, que posteriormente é vertido para o ordenamento jurídico interno dos Estados-membros[402]. Na UE existem diversos mecanismos de informação e comunicação entre as autoridades de aplicação da lei, primariamente da responsabilidade das autoridades competentes dos Estados-membros.

[401] *Ibidem*.

[402] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

No âmbito do ELSJ relativo à partilha de informações destacamos o *SIS II*[403], mecanismo de partilha de informação respeitante a cidadãos estrangeiros, com indicações de pessoas e objetos, como disposto no n.º 2, artigo 1.º, da Decisão do Conselho da UE n.º 2007/533/JAI de 12 de junho de 2007. No mesmo diploma verifica-se o contributo que este mecanismo poderá ter para no intercâmbio de informações complementares para efeitos de cooperação policial e judiciária em matéria penal. Quanto à segurança da informação e das infraestruturas existe um conjunto de responsabilidades a adotar pelos Estados–membros e pelas autoridades de gestão para assegurar a conformidade técnica, a segurança, e a confidencialidade.

Quanto existe uma necessidade de comunicação é necessário garantir as condições necessárias de confidencialidade, integridade e disponibilidade da informação, e para tal efeito é utilizado o mecanismo *SIENA*[404], assegurando o intercâmbio seguro de informações sensíveis e restritas ao nível da Europol, como por exemplo na luta contra o terrorismo[405].

Ainda no eixo europeu destacamos o mecanismo *EIXM*[406], subdivido na *Iniciativa do Reino da Suécia*[407] e na *decisão Prum*[408]. Quanto à primeira, estabeleceu um conjunto de regras para a partilha de dados e informações em matéria de investigação criminal. Quanto à segunda, apresenta o seu foco na cooperação policial e judicial ao nível da partilha de informação transfronteiriça em matéria penal, em particular entre as autoridades com competências de prevenção e repressão criminal[409]. O tipo de informação partilhada nesta plataforma tem que ver com características pessoais e dados sensíveis, como por exemplo, o ADN, ou informação adjetiva, como por exemplo, matrículas de veículos, matéria relacionada a grandes eventos nacionais nos Estados de

[403] Regulamento (CE) n.º 1987/2006 do Parlamento Europeu e do Conselho, de 20 de Dezembro de 2006, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II).

[404] EUROPOL, *Secure Information Exchange Network Application*, 2020, disponível para consulta em: https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena.

[405] *Ibidem*.

[406] Comissão Europeia, *European Information Exchange Model (EIXM)*, 2020, disponível para consulta em: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/eixm_en.

[407] Decisão-quadro 2006/960/JAI do Conselho, de 18 de Dezembro de 2006 , relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia.

[408] Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras.

[409] Cfr. Marie McGinley e Roderick Parkes, Rights vs. Effectiveness? The Autonomy Thesis in EU Internal Security Cooperation, in: *Journal European Security*, Vol.16, 2007, pp. 255-257.

forma a poder evitar atos terroristas e outras medidas de prevenção e cooperação policial ao nível da União[410].

Sob a égide da Europol foram ainda estabelecidos alguns programas específicos, a saber:

I. *Sistema de Informações da Europol* (EIS), constituído por uma central de base de dados e informações criminais. Abrange todas as áreas de criminalidade mandatadas pela Europol, incluindo o terrorismo. É um sistema de referência que pode ser usado para verificar informações sobre uma determinada pessoa ou objeto de interesse (ex: um veículo, um telefone ou uma mensagem de e-mail) para além das jurisdições nacionais[411]).

II. *Europol Analysis Projects*, sistema que prestando apoio aos Estados–membros no âmbito da luta contra as formas graves de criminalidade internacional e de terrorismo. Além disso, colabora com países terceiros e organizações internacionais. O trabalho, predominantemente analítico, fornece apoio às operações policiais e serve como plataforma de armazenamento de informações sobre atividades criminosas, apresentando ainda uma valência de competências em matéria de aplicação da lei[412].

III. *Centro Europeu de Cibercriminaldade* (EC3) e *Joint Cybercrime Action Taskforce* (J-CAT), com equipas de apoio que permanecem em constante funcionamento (24/7) no auxílio ao Estados-membros, nomeadamente a nível transnacional, elevando a ideia da securitização coletiva da área na previsão e repressão da criminalidade digital pelos órgãos de polícia criminal[413].

IV. *Centro Europeu de Luta Contra o Terrorismo* (ECTC), opera num centro de especialização que reflete a necessidade crescente de a UE em reforçar a sua resposta ao terrorismo e, presta apoio operacional, mediante pedido de um Estado-Membro da UE, para investigações direcionadas às diversas temáticas do terrorismo.

V. *Joint Operational Team Mare* (JOT Mare), especializada em matéria de identificação, apoio ao asilo, partilha de informação em investigações criminais e

---

[410] Adérito Grazina Rodrigues, O papel do Ponto Único de Contacto para a Cooperação Policial Internacional face ao quadro de ameaças e riscos, in: *Instituto Universitário Militar*, Curso de Estado Maior Conjunto, 2019, Lisboa, pp. 6-20.

[411] EUROPOL, *Europol Information System (EIS)*, 2020, disponível para consulta em: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system.

[412] EUROPOL, *Europol Analysis Projects*, 2020, disponível para consulta em: https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects.

[413] George Christou a), *op. cit.*, pp. 290-293.

na acusação de redes criminosas de tráfico de seres humanos[414]. É constituído por especialistas de Estados-membros da União e opera através da troca de informações em tempo real para desmantelar as redes de contrabando que operam com base na Turquia, Líbia e outros Estados do norte de África[415].

Posto isto, cabe realçar que existem diversos mecanismos sob a forma de canais de intercâmbio de informação e comunicação na União ao nível policial. Por esta ordem de razão, foi considerada e implementado um sistema capaz de melhorar a eficácia e o intercâmbio de informações de forma articulada entre os vários órgãos de polícia internacionais, o PUC-CPI[416], funcionando sob pedidos de informação às autoridades competentes. Este órgão constitui o "(...) *centro operacional responsável pela coordenação da cooperação policial internacional, que assegura o encaminhamento dos pedidos de informação nacionais, a receção, o encaminhamento e a difusão nacional de informação proveniente das autoridades policiais estrangeiras, a transmissão de informação e a satisfação dos pedidos por estas formulados*"[417].

Relativamente ao número de mecanismos analisados, podemos observar que boa parte dos dados e informações são armazenadas em mais que uma base de dados, ou seja, duplicação informacional, o que pode ser uma limitação ao cumprimento dos princípios inscritos no artigo 4.º da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. A garantia de um constante monitorização e atualização das bases de dados deve obedecer rigidamente ao *registo cronológico*[418], inscrito no artigo 25.º do mesmo

---

414 Europol, *European Migrant Smuggling Centre*, 2020, disponível para consulta em: https://www.europol.europa.eu/about-europol/european-migrant-smuggling-centre-emsc.

415 *Ibidem*.

416 Em Portugal opera no âmbito do Sistema de Segurança Interna, na dependência e sob coordenação do Secretário-Geral do Sistema de Segurança Interna.

417 Decreto Regulamentar n.º 7/2017, de 7 de agosto de 2017, disponível para consulta em: https://dre.pt/home/-/dre/107963497/details/maximized.

418 "*Artigo 25.º*
Registo cronológico
1.Os Estados-Membros preveem que sejam conservados em sistemas de tratamento automatizado registos cronológicos pelo menos das seguintes operações de tratamento: recolha, alteração, consulta, divulgação — incluindo transferências —, interconexão e apagamento. Os registos cronológicos das operações de consulta e divulgação permitem determinar o motivo, a data e a hora dessas operações e, na medida do possível, a identificação da pessoa que consultou ou divulgou dados pessoais, e a identidade dos destinatários desses dados pessoais.

diploma, uma vez que na maior parte dos mecanismos analisados são armazenadas categorias especiais de dados, que devem ser objeto de *garantias de segurança no tratamento*, dispostas nos n.ºs 1 e 2 do artigo 29.º do referido diploma[419].

10. Quadro de ameaças

O quadro complexo de ameaças internas e externas à vida privada e à segurança da informação estão presentes quer no espaço físico, quer no espaço digital com o intuito de interferir na esfera privada das pessoas, organizações e Estados. Nesta senda, somos confrontados com equipamentos e dispositivos altamente intrusivos, como são as câmaras de videovigilância[420], ou microfones nos aparelhos digitais, aos quais, por uma questão de segurança pessoal e coletiva, devemos observar um conjunto de regras de segurança quanto ao manuseio do *hardware* e do *software.*

Posto isto, e atendendo ao conceito de "segurança humana" elencado e desenvolvido pelas Nações Unidas no início dos anos 90, e às suas várias dimensões exploradas, entre as quais a económica, alimentar, sanitária, ambiental, pessoal, comunitária e política, adicional a digital. Defendemos a segurança digital como uma das dimensões ou tipologias integradas da segurança humana, sendo que é cada vez premente assumir o domínio digital como essencial para a segurança do Ser Humano, quer pelos níveis de intensidade ou pela teoria dos efeitos que avançaremos no último capítulo. Como defendemos esta nova dimensão – segurança digital, integrada na segurança humana

2.Os registos cronológicos são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo e garantia da integridade e segurança dos dados pessoais, bem como para ações penais.

3.O responsável pelo tratamento e o subcontratante disponibilizam os registos cronológicos à autoridade de controlo, a pedido desta."

[419] *Como menciona o n.º1, artigo 29.º, "Os Estados-Membros preveem que o responsável pelo tratamento e o subcontratante, tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos de probabilidade e gravidade variáveis que este tratamento representa para os direitos e liberdades das pessoas singulares, apliquem medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco. (…)*".

[420] Note-se que o próprio entendimento sobre videovigilância não é fechado do ponto de vista epistemológico. Contemporaneamente, o uso de tecnologia para efeitos de videovigilância e para outro tipo de finalidades começa a criar dificuldades do ponto de vista da real funcionalidade dos equipamentos ou tecnologias associadas a este. Assim, a tecnologia ou equipamento em causa deve ser avaliado de acordo com as suas funções primárias e secundárias tendo em linha de conta as reais capacidades de recolha de dados, por exemplo a capacidade de uso de microfones ou câmara de vídeo. Elisa Orrù, Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, pp. 11-116.

tende a proteger os valores fundamentais consagradas pela Comunidade Internacional, e que corresponde à nova quadratura do século XXI.

Numa sociedade altamente interconectada, é cada vez mais difícil recusar ou simplesmente permanecer offline, quer por via da alteração de paradigma mundial, as interações sociais que se vão multiplicando em ambiente digital em inúmeros aspetos da vida dos cidadãos, assumem uma dependência digital difícil de contestar.

Todavia, é sempre necessário criticar e revindicar meios que assegurem a segurança, confidencialidade e privacidade dos cidadãos quando se ligam à Rede, pois as opções tomadas, mesmo ao nível das infraestruturas devem obedecer a critérios que tenham em linha de conta o estudo do risco associada às ameaças. Os Estados assumem neste campo especiais responsabilidades para com os indivíduos, na medida em que devem empreender ações para manter um ambiente digital seguro, como meio e instrumento de público que facilite a vida dos indivíduos[421]. Uma segunda responsabilidade resvala na aplicação da defesa do Estado de Direito[422][423] e dos direitos fundamentais no ciberespaço, como adiante aprofundaremos[424].

Neste novo mundo tecnológico existem realidades altamente disruptivas que só podem ser compreendidas pela consciencialização social, por exemplo, um simples *software* aplicacional que tenha a capacidade de armazenar dados pessoais ou informação classificada (ou confidencial) necessita, de forma permanente, de obter atualizações e obedecer a um conjunto de regras básicas de SI, caso contrário pode desenvolver uma

---

[421] No mesmo sentido, Murat Karaboga, "(…) *Since they serve a basic democratic function – which nowadays also includes informing the public about risks and benefits of technology*.". Murat Karaboga et. alli., *op. cit.*, p. 35.

[422] Note-se, do ponto de vista do exercício da autoridade pública do Estado, algumas ações que envolvem a capacitação tecnológica das autoridades podem ser bastante questionáveis. Por exemplo, em Fresno, na Califórnia, a polícia usa um sistema de pontuação de ameaças denonimado "*BEWARE*", que analisa um conjunto de dados, entre os quais as publicações em redes sociais de forma a atribuir aos residentes um nível de ameaça, recorrendo, portanto, a uma definição de perfis em massa dos residentes. A sala de controlo de todos os movimentos na cidade tem 57 monitores de forma a manipular as 200 camaras instalas em toda a cidade.

Cfr. Marco Krüger, The impact of video tracking routines on crowd behaviour and crowd policing, in: Protests in the Information Age: *Social Movements, Digital Practices and Surveillance*, Lucas Melgaço e Jeffrey Monaghan (eds), Routledge Studies in Crime, Security and Justice, Routledge, 2018, pp. 136 e ss.

[423] A este porpósito, surgiu o "Privacy 2030: Una nuova visione per l'Europa", definindo-se como um manifesto para a União Europeia. Este documento estimula os cidadãos e as instituições democráticas pesarem nos direitos humanos, na ética e na dignidade humana em ambiente digital. Cfr. IAPP e Garante per la protezione dei dati personali, *Privacy 2030: Una nuova visione per l'Europa*, 2020, disponível para consulta em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9456977.

[424] Murat Karaboga, "(…) *Since they serve a basic democratic function – which nowadays also includes informing the public about risks and benefits of technology*.". Murat Karaboga et. alli. *op. cit.*, pp. 54-55.

série de problemas relacionados com *data breaches* com valor significativo para atores mal-intencionados[425].

A exposição pessoal e coletiva em redes sociais com várias categorias de dados e informações partilhados na internet acabam por expor importantes fragmentos para um prevaricador. Tudo o tipo de informação pessoal ou não pessoal que entra na Internet apresenta um valor, e poderá ser utilizado na preparação de um ataque em ambiente digital dada a facilidade com que as ferramentas OSINT[426][427] se utilizam e multiplicam.

Relembramos que os direitos como a proteção de dados não são direitos absolutos e, por conseguinte, podem ser limitados em razão de alguns exceções, entre as quais a segurança nacional, o bem estar social e económico dos Estados, para prevenir ilícitos criminais, para proteger a saúde e a moral ou ainda, na defesa ou proteção de direitos e liberdade de terceiros.

10.1 5G

A incapacidade da União em prever riscos e eventos tecnológicos pode ser um grande gap, pois poderá chegar atrasada a corridas internacionais em que os seus pares já arrancaram, exemplo notório é o da dependência da tecnologia 5G. Por um lado, a pressão Chinesa por uma tecnologia de ponta, potencialmente com menores custos e potencialmente com maiores riscos tecnológicos, por outro a escolha do velho aliado transatlântico que indica o caminho a seguir sob pena de afastamento na cooperação institucional, fazem com que a União seja relegada para um segundo plano, sendo um mero espectador de bancada ao invés de ser um ator determinante numa área que afeta o

[425] Ugo Pagallo, Massimo Durante e Shara Monteleone, What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IOT, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p. 58-62.

[426] OSINT é um termo em inglês que serve para designar uma fonte ou um canal de informação, em qualquer que seja o contexto, na qual exista uma necessidade de lidar com uma ameaça humana imprevisível. Para aceder a algumas das OSINT disponíveis em fontes abertas, *v.* https://osintframework.com/. Para além destas, existem outros canais que utilizam o recurso à *intelligence* como disciplinas, a saber: Geoint, Masint, Sigint, Techint, Cybint/Dnint ou Finint.

[427] Cfr. Pompeu Casanovas, Cyber Warfare and Organised Crime, *A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT)*, Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative, Mariarosaria Taddeo Ludovica Glorioso (eds), Philosophical Studies Series, Springer, Vol.124, pp.142-145.

futuro de gerações e põe em causa setores e infraestruturas críticas na comunidade europeia.

A reforma das telecomunicações deu o mote para a entrada em vigor da implementação da tecnologia 5G no espaço da União Europeia. Esta é a última geração de redes de comunicações móveis, caracterizada por um elevado débito de dados, menor latência, menor consumo de energia, menores custos, maior capacidade de sistema e maior concetividade de dispositivos, visando modernizar as comunicações entre cidadãos, organizações e Estados, resultando numa melhoria da qualidade de vida das sociedades[428][429][430].

A Diretiva (UE) 2018/1972 que estabeleceu o Código Europeu das Comunicações Eletrónicas criou um conjunto de regras harmonizadas para a regulação das redes de comunicações eletróncias, dos serviços de comunicações eletrónicas e dos recursos e serviços conexos[431][432]. A estimulação da concorrência e competitividade europeia no 5G permite que cidadãos e empresas beneficiem de alta conectividade e qualidade de serviços comunicacionais, e ainda possam disfrutar de um leque de escolhas digitais mais alargado. Esta Diretiva surge no pacote legislativo sobre comunicações eletrónicas que inclui o Regulamento (UE) 2018/1971, criando o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE) e a Agência de Apoio ao ORECE (Gabinete ORECE).

O Conselho transcreveu as suas preocupações relativamente às implicações do 5G na economia europeia e a necessidade de atenuar os riscos de segurança, pois a atualização destas redes estará diretamente interligada com a aquisição de equipamento para as

[428] Note-se que esta reforma vinha sendo preparada, por exemplo, na Decisão n.º 243/2012/UE, postulando a perspetiva de longo prazo para a implementação da Internet banda larga ultrarrápida em 2020.

[429]Conselho da União Europeia, de 4 de dezembro de 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/12/04/better-connectivity-eu-adopts-telecoms-reform/.

[430]Ficha informativa da Comissão Europeia, de 6 de junho de 2018, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/more-and-better-internet-connectivity-requires-investments-high-speed-and-quality-networks.

[431] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas.

[432] Esta Diretiva veio assegurar maior proteção aos consumidores, nomeadamente no que toca à subscrição dos pacotes de comunicações; da obrigação de proporcionar aos consumidores um acesso adequado e o acesso a um preço acessível de banda larga, independentemente da localização e nível de rendimentos do consumidor; da obrigação dos Estados-membros da UE implementarem um sistema de alerta ao público, para transmitir, por telemóvel, alertas aos cidadãos sobre catástrofes ou fenómenos semelhantes existentes na sua área; a obrigação dos Estados assegurarem aos operadores uma previsibilidade regulatória em matéria de direitos de utilização do espetro de radiofrequências para serviços de banda larga sem fios, pelo menos, durante um período de 20 anos; ou ainda, regras de acesso dos operadores a redes para promover a concorrência e promover a aquisição de novas infraestruturas de elevada capacidade pelas empresas que realizem essa exploração.

infraestruturas críticas nacionais, e consequente manutenção dos setores vitais dos Estados da União Europeia[433][434].

Cada Estado-membro concluiu uma avaliação de risco das suas infraestruturas de rede ao 5G e transmitiu os resultados à Comissão e à ENISA. Com base nestas avaliações de risco nacionais, foi publicado um relatório sobre a avaliação de risco coordenada da UE sobre Cibersegurança nas redes 5G. Por seu turno, o Grupo de Cooperação NIS publicou um conjunto de medidas de mitigação de risco[435], e Comissão posicionou-se relativamente à implementação segura de 5G na UE, lançando um primeiro relatório sobre o estado de arte da implementação das medidas destinadas a reduzir o risco nos Estados-membros[436]. Com efeito, também se tem veiculado sobre os potenciais riscos que a tecnologia 5G (fornecidos por uma multinacional chinesa) poderão ter em território da União, alertando em especial para os riscos na região das Balcãs[437][438].

Nesse sentido, é necessário criar e desenvolver uma cadeia de confiança na UE de modo a que tanto Estados, como empresas e indivíduos possam ser capazes de utilizar as redes e equipamentos tecnológicos para concretizar as suas atividades com os recursos adequados e em segurança[439]. A UE está empenhada em melhorar as suas capacidades e regras em matéria de cibersegurança, para tal, a implementação de medias no domínio da luta contra a criminalidade organizada, no domínio da política externa e de segurança

[433]Conselho da União Europeia, *Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G*, 2019, https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[434] Em 2008, a OCDE emitiu aos Estados recomendações ao nível da SI, de entra as quais se destacaram: a) referências aos *stakeholders* para a implementação de uma política de segurança da informação, no sentido de empreender uma cooperação mútua entre ambos; b) garantir a transparências na decisões e na delegação de competências entre o setor público e privado; c) a revisão sistemática e coordenada das políticas e marcos legais; c) detetar e reprimir, no que toca à resposta a incidentes. Para mais informações *v*., https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf.

[435] Comissão Europeia, *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[436] NIS Cooperation Group, *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

[437] Por exemplo, a Lituânia em 2025 pensa implementar a rede 5G em todas as zonas urbanas, nos corredores aéreos internacionais, nas principais linhas ferroviárias, aeroportos e portos marítimos, portanto algumas das suas infraestruturas críticas nacionais terão esta cobertura, de modo que é necessário assegurar segurança na aquisição e implementação tecnológica.

[438] Maya Guzdar e Tomas Jermalavicius, *op. cit*., pp.1- 4.

[439] Os ataques perpetrados por meio de *ransomware* triplicaram entre 2015 e 2017. O impacto económico da cibercriminalidade quintuplicou entre 2013 e 2017 e a cibercriminalidade é vista como um grande desafio para a segurança interna da UE por 87% dos Europeus.

comum e no domínio da ciberdefesa, exprimindo como objetivos a resiliência, dissuasão e defesa da cibersegurança ao nível da UE.

10.2 Cabo de Conexão do Ártico

Bem sabemos que as interdependências internacionais são imprescindíveis e, no último reduto podem configurar-se como fator colateral nos mecanismos de paz entre Estados, em especial do mercado chinês, onde são evidentes as tendências de crescimento no setor tecnológico. Além da China, existem outras potências mundiais ao nível tecnológico (como Japão, EUA ou Israel), tendo a geopolítica internacional vindo a demonstrar como a diplomacia indireta e pode constituir-se como uma vantagem competitiva entre Estados. Nesta senda, é crucial para a União Europeia afirmar a sua autónima estratégica, nomeadamente a segurança e autonomia digital (dados e infraestruturas) relativamente ao novo Cabo de Conexão do Ártico (ver anexo C). Este, a par do 5G, são desafios emergentes que necessitam de maior clarificação europeia, em particular dos Estados-membros no sentido de garantir segurança e privacidade aos dados que circulam e ligam continentes. A União e os seus Estados-membros não devem ficar dependentes de Estados terceiros como a China ou a Rússia em matéria de cabos submarinos, sendo que em termos geopolíticos, estes atores podem intervir nas comunicações de forma ameaçadora para a União e os seus cidadãos. Ora, se o projeto da ligação entre a UE e a Ásia avançar e a ligação submarina passar por cabo de fibra ótica de origem chinesa pode comprometer os princípios básicos de SI, colocando em causa a independência dos dados trocados entre a UE e a Ásia, daí advém um principio primordial: recorrer às técnicas criptográficas mais avançadas[440]. O cabo de conexão submarino poderá servir de base de operações vigilância submarina chinesas ou lograr com potenciais vantagens na Rota do Mar do Norte, local do qual a Rússia apresenta já uma estratégia de exploração, quer ao nível oceânico quer ao nível das telecomunicações podendo constituir-se como uma zona de conflito[441]. Nem só o fator económico deve ser ponderado em questões geoestratégicas, como afirma Frank Jüris, "*Internet cables, meant to connect people in cyberspace, can become a dividing factor, if countries participating in the Artic Connect project want to protect the cable*

[440] Martti Lehto, et. alli, Arctic Connect Project and cyber security control, ARCY, in: *Informaatioteknologian tiedekunnan julkaisuja*, Pekka Neittaanmäki (ed), University of Jyväskylän, N.º 78, 2019, p. 14-22.
[441] Martti Lehto, et. alli, *op. cit.*, p. 12-13.

from outside intrusion and the outsiders try to improve their capabilities to have access to the data transferred through them. This could lead to the militarisation of the Arctic and increase the probability of conflict in the region"[442].

10.3 Ciberterrorismo

O processo socioeconómico no efeito pós-globalização exibe sérios riscos e ameaças às populações, desde logo a própria perpetração destas não reconhecer fronteiras visíveis ou um agente identificável. Desta forma, cabe aos Estados a necessidade de percecionar, detetar e dissuadir os riscos internos e regular a forma como a atividade digital se desenvolve no seu Estado, nomeadamente por meio de infraestruturas, salvo disposição supranacional ou internacional em contrário.

Os desafios da União Europeia no aspeto securitário em ambiente digital são bastante complexos, onde existe um prolongamento ou extensão dos desafios anteriormente experienciados em ambiente físico, falamos por exemplo no combate ao terrorismo, que ganha um novo enquadramento através da noção de ciberterrorismo, ou ainda da criminalidade organizada transnacional que funciona em redes online bem organizadas no submundo do crime digital. Quanto ao ciberterrrorismo, auxiliamo-nos na definição de Mark Pollitt, caracterizando o fenómeno como um ato "(..) *deliberate, politically motivated attack carried out by non-state groups or clandestine agents against information, computer systems, software, and data at the result of what the people not participating in the fighting experience the violence*"[443]. A ação terrorista perpetrada no domínio do ciberespaço tira partido do uso de tecnologia para incutir ameaças, medo e violência numa determinada população, meio ou grupo, sendo conduzida na esfera virtual de forma inadvertida por parte dos agentes criminosos, tal como ocorre em meio físico. A intimidação e coerção dirigida a determinados grupos específicos como governos, associações ou empresas sectoriais pretende alcançar a sua expressão máxima por meio do recurso à violência empregue a pessoas ou infraestruturas, causando uma alteração da

[442] Frank Jüris, Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic, *Sinopsis: China in Context and Prespective*, 2020, p. 8 e ss.
[443] Mark Pollitt, Cyberterrorism – Fact or Fancy?, in: *FBI Laboratory*, disponível para consulta em: https://cs.georgetown.edu/~denning/infosec/pollitt.html.

ordem pública através do medo incutido às vítimas e sociedade[444]. Como Alexandre Guerreiro sustenta, "*A emergência de ameaças associadas à ciberactividade é diretamente influenciada pela atividade desencadeada por agentes da ameaça com vista à exploração das vulnerabilidades geradas pela meteórica evolução de plataformas digitais com limites ainda desconhecidos*"[445].

A União através do foro legislativo tem caminho progressivamente para agilizar os processos de investigação criminal no que toca ao cibercrime. Nesse sentido, veja-se a Diretiva 2014/41/UE, onde no seu artigo 4.º são enunciadas as obrigações de cumprimento de procedimentos de investigação criminal, inclusive com referências à jurisdição e ao direito interno dos Estados.

A utilização da Internet como meio para perpetrar um ataque terrorista, tendo em conta os baixos custos associados ao material necessário, não envolvendo as tradicionais quantias de dinheiro em armamento de natureza militar (ex. granadas ou bombas), ou objetos convencionais do dia-a-dia (ex. armas brancas ou veículos).

A limitação da aplicação clássica territorial do Estado é um conceito que ganhará uma nova adaptação, pois a maior parte das operações levadas a cabo no ciberespaço são encobertas e de escala transnacional, transpondo os limites territoriais e jurisdições de diferentes Estados. O problema prático fica ainda mais complexo quando pensamos no acesso a dados promovidos e armazenados em sistemas de computação em nuvem (*infraestruture as a service*), uma vez que os diferentes ordenamentos jurídicos apresentem previsões diferentes para a preservação e integridade da prova digital[446]. A particularidade de alguns casos, como casos de cibercrimes investigados em Estados estrangeiros, portanto, situados fora do espaço comunitário, implicam a necessidade de reconhecimento da soberania dos Estados, o que poderá conflituar com alguns princípios de Direito Internacional, como por exemplo, o princípio da igualdade entre Estados, o princípio da territorialidade e o princípio da não ingerência interna.

O ciberterrorismo pode ter ainda contornos indefinidos pelo seu domínio, todavia, pode constituir-se como uma séria ameaça à União pelo pela teoria dos efeitos, sendo

---

[444] Cfr. Neil Rowe, Challenges of Civilian Distinction in Cyberwarfare, in: *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Mariarosaria Taddeo Ludovica Glorioso (eds), Philosophical Studies Series, Springer, Vol. 124, p. 46.

[445] Alexandre Guerreiro, Direito Internacional e o combate ao terrorismo e ao ciberterrorismo, in: *O Direito Internacional e o uso da força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, p. 337.

[446] Nesse senttido, *v*. Giuseppe Vaciago, Worksop - *The Death of Computer Forensic: Digital Forensic after the singularity*, Milão, 2011.

necessária uma posta num quadro cooperado multinível, em particular entre as forças e serviços de segurança.

IV- Conflito Inter-estatal no ciberespaço

11 Operações levadas a cabo no ciberespaço

Ao longo da história da humanidade sempre existiram divergências entre atores na cena internacional, originando confrontos, que por sua vez deram origem a diversos fenómenos como "guerras" ou "terrorismo", posteriormente regulados por normas internacionais, como por exemplo, no Direito dos Conflitos Armados ou Direito Internacional Humanitário. No entanto, contemporaneamente, assistimos no placo que é o ciberespaço a confrontos que ainda são objeto de regulamentação clara e precisa pela sua natureza difusa, complexa e metamórfica[447]. Nesse sentido, algumas das tecnologias e máquinas que coabitam no ciberespaço, acessíveis à sociedade, representam bens que podem constituir-se como objetos de perpetração de factos ilícitos no ciberespaço, dependendo da finalidade que lhe é dada pelo utilizador[448].

As ações perpetradas no ciberespaço, para o estudo em concreto, circunscrevem-se a atos ou condutas praticadas pelos sistemas de informação e comunicação (através de sistemas e redes), que sejam passíveis de imputação de responsabilidade a um leque distinto de atores, sejam Estados, organizações internacionais, grupos armados ou indivíduos. Tais condutas ilícitas, podem consubstanciar um ato ou uma prática que viola uma norma primária de direito internacional no domínio do ciberespaço[449][450]. Aqui é então necessário proceder à analise do regime jurídico aplicável ao ciberespaço e, nesse sentido, à vinculação[451]ao Direito Internacional, à Carta da Nações Unidas e ao Direito da União Europeia e seus Estados-membros, no caso deste último, partindo da base jurídica que regula esta relação, segundo artigo 3.º, n.º 5, o artigo 21.º, 23.º e 42, n.º1 do TUE. A União assumiu de forma explícita o seu compromisso com a segurança internacional, contribuindo para a paz, bem-estar, desenvolvimento internacional e proteção dos direitos

[447] Eduardo Gelbstein, The War of Attrition in Cyber-Space or "Cyber-Attacks", "Cyber-War" and "Cyber-Terrorism", in: *Conselho de Segurança da ONU*, idn nação e defesa, Instituto da Defesa Nacional, n.º 135, N.º 135-5ª Série, p. 125.

[448] Por exemplo o telemóvel, é um bem útil para efetuar comunicações e interconectar pessoas, todavia pode ser considerado como um equipamento assimétrico pelos seus recursos, por recolha fotografias, armazena dados do utilizador e de terceiros, sinal de GPS, ligação à Internet e poderá ser usado por atores mal intencionados, como terroristas, *hacktivistas* ou *hackers* com diversas motivações, entre as quais, a perpetração de ataques terroristas.

[449] Frederic Lemieux, *op. cit*., p.1.

[450] Operação cibernética pode ser definida por "(…) *as having a set of comprehensive cyber operational goals that are carefully designed and planned to serve a long-term offensive or defensive purpose* (…)". Frederic Lemieux, *op. cit*., p.19.

[451] Em relação à CNU pode fazê-lo a título proclamatório e axiológico, uma vez que não é um Estado. Em relação ao direito internacional, como sujeito de direito internacional e, por ato unilateral, pode declarar que se vincula a determinadas obrigações. Cfr. Ana Maria Guerra Martins, *op. cit.*, p. 109-110.

do Homem em diferentes dimensões na sua ação externa[452]. Acrescentamos ainda, que em matérias atinentes ao direito internacional humanitário, à prevenção de conflitos internacionais, combate ao terrorismo, à proibição do uso da força, entre outras matérias, a União vem construindo uma postura pró-ativa na criação de regras, mediação de conflitos e a apresentação de represálias a atores estatais e não estatais na comunidade internacional que violam os ditames do direito internacional[453]. Destarte, a UE na prossecução da sua política externa vem afirmando o respeito e promoção dos princípios da Carta das Nações Unidas, do Direito Internacional[454] e, como sustentaremos adiante por uma conduta diligente e mediadora no ciberespaço.

Epistemologicamente, cabe encontrar um justa definição para descrever uma operação cibernética, o que poderá ser espinhoso e arriscado dado o múltiplo leque de áreas do saber convocadas, entre elas, as ciências do comportamento, o direito, a ciência política, as relações internacionais, as engenharias, matemática entre outras, extensos ramos do conhecimento que encontram aplicação no ciberespaço e às suas interações[455]. Mas vale tentar encontrar uma subdivisão para o estudo em concreto. Deste modo, podemos definir uma operação cibernética defensiva, que visa a prevenção e dissuasão (*ciberdefesa passiva*) de ameaças em ambiente digital, ao passo que uma operação cibernética de natureza ofensiva tem como principal foco o recurso ao uso da força, envolvendo o lançamento de uma contra-operação cibernética, preemptiva ou preventiva, contra a fonte (*ciberdefesa ativa*)[456][457].

---

[452] Panos Koutrakos, The EU Common Security and Defense Policy, In: *European Journal of International Law*, Julia Schmidt (ed), 2013, Oxford, Oxford University, p. 1257 e ss.; Aurel Sari, International Law Aspects of the EU´s Security and Defense Policy, With a Particular Focus on the Law of Armed Conflict, in: *European Law Review*, Fredrick Naert (ed), 2011, pp. 451-453. Nesse sentido *v.* Sven Biscop and Per M. Norheim- Martinsen, CSDP: The Strategic Perspective, in: *Explaining the EU's Common Security and Defence Policy: Theory*, Action, Xymena Kurowska e Fabian Breuer (eds), 2013, Palgrave Studies in European Union Politics, p.65.

[453] Ana Maria Guerra Martins, *op. cit.*, p. 90-91.

[454] *Ibidem*, p. 94.

[455] Por exemplo, o papel do politólogo será centrado no exame da política atual e emergente relacionada com as operações cibernéticas e seus atores de forma a poder interpretar o exercício da influência de poder e estratégia destes no ciberespaço. De forma distinta, o jurista irá focar o seu exame nas normas jurídicas e nas matérias substantivas aplicadas ao ciberespaço. Cfr. Eriksson e Giacomello, Introduction: Closing the gap between International Relations theory and studies of digital-age security, Erickson and Giancomello (eds), in: *Internacional relations and security in digital age*, Routledge, New York, p. 1-29; Sofia Casimiro, Contributos para uma Estratégia Nacional de Ciberdefesa, Paulo Viegas Nunes (coord), in: *idn cadernos*, 2018, N.º 28, p.47-49.

[456] CNCS, *Recursos*, disponível para consulta em: https://www.cncs.gov.pt/recursos/glossario/.

[457] Frederic Lemieux, *op. cit.*, p.2.

Neste sentido, as operações no ciberespaço conduzidas por atores estatais devem observar condutas responsáveis no ciberespaço, preconizando o *direito à igualdade soberana*[458]. Com efeito, é necessário observar vários aspetos teóricos neste domínio, como por exemplo, quais os atores do ciberespaço? Que tipo de efeitos este pode observar nos Estados e no indivíduo? Poderá ser atribuída responsabilidade internacional? Se sim por quem? os Estados devem respeitar a soberania digital dos demais Estados da comunidade internacional? Qual o papel particular das suas infraestruturas críticas, que suportam a Internet e estão sujeitas à jurisdição territorial destes?[459]. Destarte, os Estados são confrontados com a crescente interoperabilidade e interdependência dos sistemas de comunicação e informação localizados em várias jurisdições convocando uma conduta de *responsabilidade digital coletiva.*

11.1 Tipo de atores e níveis de intensidade das operações no ciberespaço

O ciberespaço é um domínio operacional definido pelas interações digitais e tecnológicas entre pessoas humanas através das máquinas e pela arquitetura de sistemas e redes que os suporta[460]. O tipo de atores que atua no ciberespaço é dividido em dois grandes grupos, Estatais e não Estatais. A categorização do nível de intensidade empregue numa operação cibernética no ciberespaço é definida pelo tipo de ato ou conduta perpetradas pelos atores, mais ou menos hostis.

11.1.1 Tipo de atores

O ciberespaço é composto por uma miríade de atores que podem violam normas internacionais e, por consequência, incorrem em responsabilidade internacional. Os

[458] Cfr. André Gonçalves Pereira e Fausto de Quadros, *Manual de Direito Internacional Público*, Almedina, 3ª Ed, 2011, p. 332.
[459] Harold Hongju Koh, International Law in Cyberspace Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, in: *Harvard International Law Journal*, Vol. 54, 2012, p. 6.
[460] *Ibidem*, p. 30.

atores no ciberespaço podem ser categorizados em dois grandes grupos: atores estatais e não estatais[461].

11.1.1.1 Atores estatais

Atores estatais são compostos por indivíduos, grupos ou organizações, que agem diretamente ou sob a orientação[462] ou autoridade de um Estado, levando a cabo operações cibernéticas de forma pública ou encoberta[463].

Os atores estatais que prossigam condutas que recorram ao uso de força no ciberespaço circunscrevem-se, à priori, como arguiremos adiante, sob a alçada do direito internacional e, por essa via, podem estar sujeitos a repercussões ao nível diplomático, militar ou jurisdicional como resultado das suas condutas[464].

11.1.1.2 Não Estatais

Atores não estatais podem ser constituídos por indivíduos, grupos ou empresas privadas, que desenvolvem práticas ou condutas cibernéticas sem a autoridade, orientação, patrocínio direto ou indireto de Estados.

Atores não estatais, podem configurar grupos *hacktivistas*[465] e *hackers*, geralmente atuam com base em considerações políticas, ideológicas, patrióticas[466] ou de ordem financeira. Dentro da categoria de *hackers*, devemos distinguir um subgrupo, tipicamente utilizados pelas organizações ou Estados para detetar vulnerabilidades e proceder à sua defesa, quer

---

[461] *Ibidem*.

[462] Neste sentido,"*The notion of "direction or control" is limited to the conduct of specific operations, rather than merely supplementing a state's activities or assuming responsibility for performing a particular function, as in the case of "instruction*.". Assim, e para efeitos desta noção, "*Russia's silent endorsement of the 2007 cyber attacks against Estonia, demonstrated, inter alia, by its refusal to assist Estonian authorities in related criminal proceedings pursuant to the Agreement on Mutual Legal Assistance, did not suffice to attribute the attacks to Russia*". Michael Schmitt e Liis Vihul a), *op. cit.*, pp. 63-64.

[463] *Ibidem*.

[464] A União Europeia refletiu isso mesmo, observando uma interpretação extensível relativamente ao regime jurídico aplicável, incluindo o Direito Internacional Humanitário.

[465] Segundo a ENISA, podem representar *"(...) atores de ameaças "orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais*.". ENISA, *ENISA Threat Landscape Report 2018*, 2019, p.121.

[466] Frederic Lemieux, *op. cit.*, p. 31.

seja nos sistemas e ou nas redes, denominados de *ethical hackers,* podendo entrevir nos processos de cibersegurança (organizações) ou ciberdefesa (Estado)[467][468].

A participação dos atores não estatais em controvérsias no ciberespaço apresenta preocupações crescentes, uma vez que estes não apresentam limitações morais ou éticas, ou pelo menos, na maior dos casos estas não são reveladas, o que não ocorre ao nível dos atores estatais regulados pelos Tratados e atos jurídicos unilaterais[469][470].

A inexistência de marcos limitativos convoca um sério risco da ocorrência de escaladas de conflitos e, invariavelmente, ao provável recurso à utilização de força por ambos os atores (no caso de um Estado poderia haver o recurso à legítima defesa, *ultima ratio*, podemos idealizar um cenário de guerra total no domínio do ciberespaço iniciada por um ator não Estatal[471], encontrando-se a sua respetiva aplicação do campo do direito dos conflitos armados internacionais).

Na comunidade internacional é sabido que atores estatais podem, de forma pública ou secreta, dirigir, apoiar ou omitir a presença de atores não estatais no ciberespaço[472].

11.1.2 Níveis de intensidade

O primeiro nível de intensidade na escala de conflitos no ciberespaço é o *passivo*, considera-se o tipo menos hostil de operação no ciberespaço e pode ser associado, por exemplo, à espionagem no ciberespaço, ou atividades destinadas à recolha de informações para fins competitivos, por exemplo, no domínio das informações ou

[467] No caso do ciberataque à Estónia em 2007, a maior parte da reconstrução da infraestrutura de rede e sistemas recaiu sobre agentes privados do mercado da segurança da informação e da cibersegurança.

[468] Para mais desenvolvimentos sobre o tipo de atores não estatais, *v.*, Luís Elias, Ciberameaças e (in)segurança, in; *CyberLaw by CIJIC*, Edição N.º VII, 2019.

[469] Frederic Lemieux, *op. cit.*, p. 31.

[470] Os atores não-estatais na condução de ciberataques contra Estados apresentam uma potencial capacidade para elevar os níveis de violência executadas para a disputa no campo de batalha físico. *Ibidem*.

[471] Cfr. Carl Clausewitz, *On War*, Michael Howard e Peter Paret (Eds), in: *Princeton University Press*, Princeton, 1976.

[472] Neste caso em particular destacamos a Federação Russa, que parece aprovar tacitamente as ações de *hackers* patrióticos na condução de ataques contra Estados como a Estónia ou a Geórgia, sem qualquer tipo de sanções interna conhecido. Do ponto de vista do direito interno russo, foram identificadas as pessoas que conduziram tais operações no ciberespaço e, no entanto, não resultaram em qualquer consequências, ao fazê-lo, deu um claro final sobre a sua posição em relação à sua vinculação às normas de direito internacional aplicadas ao ciberespaço. A inação de responsabilização por factos internacionalemnte ilícitos de atores que foram identificados na jurisdição da Federação Russa ecuou na comunidade interancional, todavia não houve efetividade do ponto de vista sacnionatório para os perpetradores do ciberataque. Frederic Lemieux, *op. cit*., p. 33.

segredos de negócio das empresas. Nesse cenário, atores estatais e não estatais tentam ganhar uma vantagem competitiva através da recolha de informações.

O segundo nível, *provocativo*, é mais hostil que o anterior no sentido em que os atores estatais e não estatais usam o ciberespaço para transmitirem uma mensagem ou divulgar informações que possam comprometer, influenciar ou polarizar a opinião pública internacional em relação a outro ator. Neste cenário constam casos como o de Julian Assange e Edward Snowden, que através da exposição de informação pública sobre condutas dos seus governos originaram grande eco na comunidade internacional. O grupo terrorista ISIS, através da propaganda no ciberespaço, em particular em revistas online[473] e plataformas[474] digitais aliciava novos recrutas através da propaganda e narrativas ideológicas[475][476]. A este nível as operações no ciberespaço são conduzidas de modo a que as informações ou mensagens transmitidas para a comunidade tenham uma ação consequente em terceiros.

O terceiro nível, *disruptivo*, refere-se à perpetração de atos ou práticas hostis para dominar e paralisar momentaneamente um alvo. Este tipo de operações, por norma, configuram o roubo de dados pessoais em massa ou ataques distribuídos de negação de serviços (DDoS). Por exemplo, a Rússia foi acusada de lançar ataques DDoS contra servidores na Estónia e na Geórgia. Ambos paralisaram infraestruturas críticas nacionais, como sites governamentais, o setor financeiro ou a rede de telecomunicações.

Por último, o quarto nível, *destrutivo*, refere-se às operações cibernéticas que visam provocar a destruição física de sistemas, redes, ou qualquer sistema que opere com sinais codificados nos canais de comunicação. Estes ataques podem, potencialmente, causar

473 Cfr. Halil Bisgin, Hasan Arslan e Yusuf Korkmaz, Analyzing the Dabiq Magazine: The Language and the Propaganda Structure of ISIS, in: International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, Springer, 2019.

474 As técnicas descentralizadas de recrutamento são hoje uma realidade (terrorismo 3.0). Por exemplo, o denominado ISIS 2.0, elenca o foco no recrutamento através das plataformas sociais mais conhecidas, como Facebook, Twiiter, Instagram, entre outras. O uso astuto de plataformas que permitem a anonimização como o telegram, ou os seus ensinamentos através de revistas como a *daqib* ou mesmo, os post de vídeos realizados nos blogs constituem a nova realidade do recrutamento das células terroristas.

475 Rebeca Wilson e Anthony Lemieux, An Information, Motivation, and Behavioral Skills Perspective on Terrorist Propaganda, in: *Online terrorist propaganda, recruitment and radicalization*, Ed. John Vacca, CRC Press, Taylor & Francis Group, 2020, p. 227-238.

476 Marina Shorer-Zeltser e Galit Margalit Ben-Israel, Developing Discourse and Tools for Alternative Content to Prevent Terror, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, Eugenie de Silva (ed), Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series, IGI, p. 148-155.

danos[477] a seres humanos, levando mesmo à sua morte[478]. O exemplo mais próximo de uma operação cibernética disruptiva foi experimentado pelo vírus *Stuxnet*, levando à destruição de centrais nucleares. Este vírus teve como alvo um sistema de controlo de um programa nuclear do Irão, presumindo que o número de conexões e o nível de segurança são inversamente proporcionais[479]. Esta operação cibernética disruptiva revelou as possíveis consequências de um ciberataque numa infraestrutura crítica (vulnerável), evidenciando os efeitos que um *malware* inserido num sistema de controlo, supervisão e recolha de dados (SCADA), pode proporcionar. Ataques cibernéticos coordenados que interrompem várias ou mesmo todos as infraestruturas críticas nacionais de um Estado altamente digitalizado (*alta dependência digital*) por um período prolongado de tempo provavelmente atingirão o nível de intensidade máximo.

11.2 Responsabilidade por factos internacionalmente ilícitos no ciberespaço

Nas relações internacionais entre Estados está previsto uma obrigação geral de abstenção, ameaça, recurso ao uso de força contra a integridade territorial ou independência política. A questão da aplicabilidade (ou não) de determinada violação das normas jurídicas internacionais por um Estado relativamente a outro no ciberespaço ainda não é clara no seio da comunidade internacional. Primeiramente, é importante entender se determinada conduta ilícita no ciberespaço por parte de um Estado constitui uma violação de uma

[477] "*what is meant by harm inflicted in or from cyberspace, and how can it be measured? This question points to a deeper uncertainty as to the effects (physical, human, psychological) of cyber conflict and how those effects might be prioritised both internally and relative to the effects of other forms of conflict and coercion (such as state-sanctioned organised violence, terrorism and the effects of crime), and relative to the effects of natural hazards and disasters (such as extreme weather events, volcanic eruptions and earthquakes, for example). Without some understanding of the nature and scale of harm which could result from cyber conflict it cannot be possible to answer the most basic of ethical questions to do with conflict and coercion; where is the threshold at which the harm resulting from a cyber action of some sort moves from the tolerable (e.g. inconvenience, discomfort, disruption) to the unacceptable (e.g. multiple deaths, irreversible physical damage, or even social collapse).*" Paul Cornish, *op. cit*., p. 6.

[478] Helbert Lin, Offensive Cyber Operations and the Use of Force, in: *National Security Law and Policy*, 2010, p. 39-60, *apud*. Frederic Lemieux, *op. cit*., p. 7.

[479] Eugenie de Silva, *op. cit*, p. 222-223.

obrigação internacional, por uma ação ou omissão[480], ou se essa conduta é ou não conforme com uma regra internacional de carácter consuetudinário[481].

A aplicação do direito internacional ao ciberespaço fez já correr muita tinta, pois existem quadrantes bastantes diferentes de Estados que não partilham as mesmas premissas fundacionais relativamente a este domínio. Tais divergências ficam patentes em sede do grupo de especialistas governamentais ah hoc da ONU (GEG), ou em instrumentos regionais ou nacionais, como por exemplo observou a França na sua revisão da estratégia de cibersegurança[482]. Contemporaneamente, ainda que possa haja reticências nesta questão, existem uma maioria doutrina, entre estes, jus-internacionalistas que defenm a aplicação do direito internacional ao ciberespaço, onde por exemplo se enquadra Harold Hongju Koh, onde defende a aplicação dos princípios do direito internacional ao ciberespaço[483]. Adicionalmente, defende o direito dos conflitos armados e a sua aplicação ao ciberespaço, bem como a necessidade de entendimentos comuns e regras a aplicar em ambiente digital para manutenção da paz e segurança internacionais.

O processo de imputação de responsabilidade pela prática ilícita em ambiente digital é complexo. No caso de um incidente no ciberespaço, por meio da perpetração de um ataque armado a um ou mais Estados vigoram as normas internacionais que regulam a relação entre Estados em caso de conflitos, quer na vertente da *jus ad bellum*, quer na

---

[480] Como normalizado no direito internacional, "(…) *qualquer Estado encontra-se sujeito a um dever de impedir que o seu território seja utilizado por movimentos ou bandos armados em operações contra um Estado vizinho* (…) assinalado pela Declaração sobre os Princípios de Direito Internacional da Assembleia Geral na Resolução 2625 em AGNU, v., https://unispal.un.org/DPA/DPR/unispal.nsf/0/25A1C8E35B23161C852570C4006E50AB. Eduardo Correia Baptista, *op. cit.*, pp. 556-557. Nesta senda, o TIJ, no caso de Estreito de Corfu, postulou "every State´s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States". Tribunal Internacional de Justiça, The Corfu Channel case, 1949, Reports of Judgments, Advisory Opinions and Orders, disponível para consulta em: https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf. No caso do ciberespaço a noção de "Estado vizinho" do TIJ pode necessitar de adequação, pese embora esta alusão clássica aos limites territoriais dos Estados, no ciberespaço, a informação circula entre vários Estados e jurisdições, desde o armazenamento de dados em vários proxis por diferentes Estados, à localização mascarada de atores que atuam com navegação anónima e localização geográfica.

[481] Nguyen Dinh, Patrick Dailler, Alain Pellet, *Direito Internacional Público*, 2.ª Edição, Fundação Calouste Gulbenkian, 2003, p.782.

[482] Para mais informações *v*., https://www.un.org/disarmament/group-of-governmental-experts/. Este grupo será alvo de maior aprofundamento num ponto autónomo neste nosso estudo.

[482] "*Le cyberespace n'est pas totalement dépourvu de normes et de regles, dans la mesure ou celles du droit international ou les grandes principes qui regissent les relations entre Estats s´y appliquent*". Secrétariat Général de la Défense et de la Sécurité Nationale, Revue stratégique de cyberdéfense, 2018, p.35, disponível para consulta em: http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

[483] Harold Hongju Koh, *op. cit.*, pp.2-3.

ótica da *jus in bellum*[484]. Com efeito, as normas internacionais determinarão os tramites nos quais se iniciará e desenvolverão os conflitos[485][486].

No âmbito de um ataque perpetrado através de redes e sistemas tecnológicos, podemos aplicar, à priori, o quadro legal do direito internacional e, alternativamente aos actos jurídicos unilaterais das organizações internacionais. Dependendo das relações que cada Estado se encontra vinculado ao nível regional (ex: Tratado do Atlântico Norte, ou Tratado da União Europeia), poderá ser determinante para efeitos de determinação da possível ação do uso de força pelo/s Estado/s alvo do ataque cibernético[487]. Destarte, como supramencionado, ainda não exista uma clara certeza jurídica quanto à base legal a aplicar em sede de concertação internacional ao ciberespaço. Na sua máxime, podemos apontar a CNU, para efeitos de resolução de litigância entre Estados desavindos no ciberespaço.

Na maioria dos casos, somente o Estado alvo de ataque perpetrado no ciberespaço e pressupondo que sofreu um grave prejuízo, imediato ou mediato, encontra-se no direito de invocar a responsabilidade do autor (materialmente da autoria de um indivíduo ou um conjunto de indivíduos) de um facto internacionalmente ilícito[488]. Posto isto, os Estados, tem o direito exclusivo de imputação (ou não) de determinada operação cibernética baseada nos seu próprios procedimentos, investigações e interesses (políticos). No entanto, para efeitos de imputação do ataque é necessários indícios que suportem a imputação de responsabilidade de um ciberataque[489], como nota Eduardo Gelbstein, o maior problema continua a provir da "(…) the lack of international harmonization of cybercrime legislation"[490]. A atribuição de um ciberataque pressupõe a existência clara e inequívoca de indícios que um ou mais Estados (ou atores não estatais) foram responsáveis pelo uso de força ilícito em território soberano de outro Estado[491].

---

[484] Sofia Casimiro, *op. cit*., p. 50.
[485] *Ibidem*.
[486] O problema da imputação também está subjacente a muitos dos problemas na aplicação da vertente da *jus in bellum*
[487] A ONU, dotada de competências coercitivas, pode decretar a obrigatoriedade de execução de obrigações a um Estado em matérias que lhe são incumbidas responsabilidades, e por essa via, as organizações internacionais, como por exemplo a UE ou a NATO, podem auxiliar um determinado Estado nessa tarefa.
[488] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, , p. 820.
[489] Dennis Broeders, Els Busser e Patryk Pawlak, Three tales of attribution in cyberspace: Criminal law, international law and policy debates, in: *The Hague Program For Cyber Norms*, Policy Brief, 2020, p. 3.
[489] Eduardo Gelbstein, *op. cit.*, p. 119.
[490] *Ibidem*.
[491] No 6.º parágrafo da declaração pode ler-se, "(…) *NATO reiterates that international law applies in cyberspace and must be respected. All states have an important role to play in promoting and upholding voluntary norms of responsible state behaviour and in countering destabilising and malicious cyber*

Os atos praticados com recurso a meios informáticos, nomeadamente redes e sistemas de informação e comunicação, tende a ser equiparado a atos praticados noutros domínios (mar, terra, ar). Esta tendência é verificada através da doutrina internacional, que concentra no Manual de Tallin[492] a interpretação dos princípios e regras internacionais aplicadas aos conflitos no ciberespaço. Este manual, apesar de apresentar uma natureza doutrinária, e por essa via, considerado uma fonte mediata de Direito[493], não lhe retira a importância que assume na comunidade internacional, exemplo disso é a sua referência nos principais fora de discussão internacionais, constituindo um marco doutrinário indiscutível a nível internacional[494].

Por seu turno, a NATO reconheceu expressamente a aplicabilidade do direito internacional e o direito internacional humanitário ao ciberespaço, em sede da declaração da Cimeira de Gales[495], corria o ano de 2014, onde foi declarado "Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace"[496]. As conclusões não se ficariam por aqui, foi ainda postulado no parágrafo 72, que um ciberataque poderia constituir um ataque armado, suscetível de aplicação do artigo 5.º do Tratado do Atlântico Norte pelos aliados, "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis"[497]. Esta posição foi reiterada em diversos fora, nomeadamente na Cimeira de Varsóvia, em 2016, que enquadrou o domínio da ciberdefesa como uma nova dimensão operacional, a par dos domínios

activities". NATO, *op. cit.*, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

[492] O Manual de Tallin é um documento doutrinário e não vinculativo sobre a aplicabilidade da lei internacional na resolução de conflitos cibernéticos, desenvolvido por especialistas independentes a convite do Centro de Excelência de Ciberdefesa Cooperativa da NATO (CCDCOE) em Tallinn, todavia não representa a opinião institucional da NATO.

Os eventos cibernéticos não ocorrem num vazio legal, pelo que os Estados possuem direitos e obrigações de acordo com o direito internacional. O manual aborda uma ampla gama de princípios e regimes de direito internacional que regulam eventos no espaço cibernético incluindo princípios gerais de direito internacional, como a soberania, o princípio da devida diligência, a jurisdição territorial entre outros. A lei da responsabilidade de Estado é examinada detalhadamente no contexto das operações cibernéticas, incluindo os direitos humanos, o direito do ar, o direito do espaço, o direito do mar e o direito diplomático e consular. João Barbas e Carolina Sancho, Cibersegurança e Políticas Públicas: Análise Comparada dos casos chileno e português, in: *idn cadernos*, n.º 29., p.62.

[493] Cfr. André Gonçalves Pereia e Fausto de Quadros, *op. cit*., p. 273.

[494] Sofia Casimiro, *op. cit*., p. 51.

[495] Piret Pernik, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies, 2014, p.5.

[496] NATO, *Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 2014, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[497] *Ibidem*.

clássicos, e na qual a aliança atlântica deve-se defender de forma eficaz tal como acontece nos outros domínios.

Não existindo uma vinculação jurídica dos Estados a normas internacionais que regulem expressamente as relações e a conduta dos Estados no ciberespaço, ou um compromisso vinculativo internacional que crie obrigações jurídicas entre as Partes neste domínio de forma adequada e completa, dificilmente se poderá obter segurança jurídica no ciberespaço, em especial, quando se trata na atribuição de responsabilidades e mecanismos sancionatórios internacionais por ciberataques. Com efeito, a determinação da ilicitude e natureza da obrigação violada poderá ser difícil de provar em sede dos instrumentos multilaterais jurídicos existentes, mas não se pense que este é um domínio anárquico.

Na nossa tese defendemos que a atribuição de responsabilidade no ciberespaço a um Estado é admitida, desde que, o comportamento denunciado emane de pessoas ou de órgãos sob a sua "autoridade efetiva" (do Estado responsabilizado), com isto, o facto ilícito é atribuído ao Estado em nome do qual agiu o autor do ato ou do comportamento ilícito no ciberespaço[498]. Neste sentido, Michael Schmitt e Liis Vihul, sustem a aplicabilidade do direito internacional, mais concretamente, a responsabilidade internacional dos Estados[499] por factos ilícitos no ciberespaço, desde que provado o nexo de causalidade e a subordinação dos atores materiais do facto internacionalmente ilícito que gera responsabilidade internacional[500].

A obtenção de prova relativamente a um determinado agente particular que agiu em co-autoria, por orientação, subordinação ou por solicitação de um Estado do qual era executor de ordens talvez seja um dos maiores desafios emergentes da comunidade jurídica internacional. De outro modo, os factos apontados a particulares, como princípio geral, nunca poderão responsabilizar um Estado, porque os seus atos não lhe podem ser atribuídos[501]. Como sustenta Nuno Ferreira, "A orientação mais ceite em relação aos actos hostis de indivíduos ou grupos de pessoas aponta para que o Estado que exerce o controlo sobre um território responda por ter violado o seu dever institucional de prevenir ou

[498] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 788.
[499] Cfr. United Nations, International Law Commission, Report of the International Law Commission, *Draft Articles of State Responsibility*, A/56/10, 2001, disponível para consulta em: https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf.
[500] Michael Schmitt e Liis Vihul a), *op. cit*., pp. 63-64.
[501] *Ibidem*, p.793.

mesmo reprimir penalmente esses actos[502] (diligência devida). Assim, e sob o esquema clássico do direito internacional, o Estado alvo do ciberataque endereça uma reclamação àquele alegado perpetrador do facto ilícito, desde que exista um nexo de causalidade entre o facto internacionalmente ilícito – violação da integridade territorial ou a independência política – e o dano – inviabilização de infraestruturas críticas nacionais, violação da integridade de redes e sistemas, mortes, entre outros prejuízos graves que possam por em causa a segurança, defesa e soberania nacional[503][504].

Neste seguimento, no âmbito do ciberespaço um Estado é, à priori, obrigado, de forma imediata, a cessar uma conduta ofensiva (um ato) ou cumprir com o dever exigido (uma omissão) e fazer uma reparação completa ao Estado que sofreu a violação, tal como ocorre nos domínios clássicos. Esta fórmula é igualmente aplicável aos Estados perante a verificação de um ato internacionalmente ilícito no ciberespaço por um ator não estatal sob a sua jurisdição, devendo atuar com a devida diligência de forma a cessar o uso de força ou ataque.

Destarte, são necessárias intensificar as conversações e negociações ao nível regional e internacional, na medida em que assistimos à emergência da não aplicabilidade de uma responsabilidade internacional dos Estados por um vácuo jurídico que regule expressamente, e de forma completa as condutas dos Estados no ciberespaço.

11.2.1 Plano do direito internacional

O direito internacional ajuda a resolver litigâncias entre atores desavindos no plano internacional, sendo que, visa garantir que o perpetrador do ataque digital se possa retratar pelo seu comportamento ou ato ilícito no ciberespaço. Por norma, no direito internacional

[502] Nuno Ferreira, A Responsabilidade Internacional: Evolução na Tradição, in: *Revista da Ordem dos Advogados*, Vol II, Set. 2006, disponível para consulta em: https://portal.oa.pt/publicacoes/revista/ano-2006/ano-66-vol-ii-set-2006/doutrina/nuno-ferreira-a-responsabilidade-internacional-evolucao-na-tradicao/.

[503] Nguyen Dinh, Patrick Dailler e Alain Pellet, *op. cit*., p. 819.

[504] Note-se que os indivíduos, à priori, e apesar de não serem os principais sujeitos de direito internacional, podem responder penalmente tendo em conta o Direito Internacional vigente. Eduardo Correia Baptista, *Direito Internacional Público*, Vol. II, AAFDL, 2015, p. 430.

sancionatório podem aplicar-se duas modalidades de sanções: contra o ato e contra o autor do ato[505].

Encontrar indícios sólidos para atribuir a responsabilidade de um Estado por factos internacionalmente ilícitos de acordo com o direito internacional é complexo nos domínios clássicos, com o domínio ciber essa tarefa pode vir a dificultar-se, muito por culpa da intervenção dos atores não estatais que atuam em co-autoria com um Estado, ou sob as suas ordens. Do ponto de vista técnico-processual, a apresentação de indícios sólidos, como por exemplo, conseguir provar que os proxies que se encontram no domínio de privados agem sob ordens ou instruções de determinado Estado pode despoltar uma operação complexa no ciberespaço, que convoca esforços vários no domínio da ação judicial. A natureza e a conexão entre um Estado e um operador proxy poderá apontar para atores não estatais encobertos pelas ordens de um Estado, mas essa factualidade deverá ser vertida em indícios para a condução da imputação de responsabilidade internacional (ou não), ao nível dos atores e operadores do proxy.

Os Estados têm um dever positivo de agir, no sentido de procurar cumprir os deveres e obrigações internacionais perante as condutas ilícitas dos indivíduos no ciberespaço sob a sua jurisdição[506]. Como sustentado supra, regra geral, o Estado (sujeito com capacidade jurídica plena[507]) nunca é responsável pelos factos dos particulares, no entanto, um Estado poderá ser responsabilizado pelos factos dos particulares sob a sua jurisdição, quando se venha a provar que estes agem sob o seu controlo ou orientação. Harold Koh sustenta que, "If a state exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the state assumes responsibility for the act, just as if official agents of the state itself had committed it. These rules are designed to ensure that states cannot hide behind putatively private actors to engage in conduct that is internationally wrongful"[508]. Podemos então inferir que um Estado poderá ser responsabilizado internacionalmente quando não tenha tomado as devidas diligências para prevenir um incidente de escala apreciável ou para proteger vítimas, tendo este prévia identificação e conhecimento da atuação ilícita dos atores privados no ciberespaço509.

[505] Jorge Bacelar Gouveia, *op. cit.,* p. 32.
[506] Este entendimento é corroborado pelo relatório final da Nações Unidades A/70/174 do grupo de peritos governmentais ao nível das Nações Unidas, *v.*, https://undocs.org/A/70/174.
[507] Cfr. André Gonçalves Pereia e Fausto de Quadros, *op. cit*., p. 327.
[508] Harold Hongju Koh, *op. cit.*, pp. 6-7.
[509] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 794.

No entanto, voltamos a assinalar, que não existe uma certeza jurídica clara quanto à base legal para desencadear os procedimentos de responsabilidade internacional de um ataque em ambiente digital sob o escopo das normas de direito internacional. O foco da responsabilização no direito internacional é determinante para verificar os direitos e obrigações dos Estados pelas partes em diferendo, e posteriormente na imposição de consequências, uma vez dado como provado o facto internacionalmente ilícito.

Reconhecidamente, as qualidades dos elementos probatórios ao nível digital servem de garantia de igualdade entre as partes em diferendo, sendo este um desafio para o Estado alvo do ciberataque, pois é a este que cabe a apresentação do ónus da prova. Nesta senda, as modalidades da invocação de responsabilidade internacional iniciam-se pelos meios de resolução não jurisdicional, se todas as modalidades falharem, o diferendo poderá ser resolvidas pelas vias jurisdicionais competentes[510].

O ciberespaço expõe vulnerabilidade civis e militares dos Estados e, nesse sentido, devem ser dadas respostas multidimensionais entre o domínio civil e militar, entre os aliados e parceiros internacionais na esperança de mitigar os riscos e as ameaças, contribuindo para a paz e estabilidade internacionais.

Por último, perspetivamos o dilema político relacionado às consequências intencionais ou não intencionais da imputação de responsabilidade de um ciberataque. Os Estados atribuem (ou não) ataques cibernéticos em função de vários fatores, entre eles a organização geopolítica como veremos adiante.

11.2.2 Do plano político

O ciberespaço tem sido um marco para o desenvolvimento económico e social nas democracias, contribuindo para o acesso livre ao conhecimento, informação e partilha de ideologias[511] – um espaço onde impera a liberdade de expressão.

Um ciberataque, independentemente do tipo de ator perpetrador e do nível de intensidade deste, poderá tornar-se uma arma de arremesso político. Embora não conheçamos os números oficiais de ciberataques entre Estados, muitos destes não são de natureza pública,

[510] *Ibidem*.
[511] Paulo Moniz, *op. cit*., p. 20.

todavia outros são amplificados e tornados públicos. Além disso, a maior parte dos ataques cibernéticos conhecidos tiveram como alvo os EUA e os seus aliados, curiosamente Estados que participam ativamente na construção de regras de segurança da informação e cibersegurança, presentes em diversos fora, para tentar encetar negociações no sentido de tornar vinculativas normas internacionais de modo a regular o comportamento (ir)responsável dos Estados no ciberespaço. Parte da doutrina preocupa-se com as reações, ou falta delas, para enfrentar ataques cibernéticos maliciosos que colocam em causa o normal funcionamento das instituições democráticas e o normal funcionamento da sociedade.

A imputação pública de operações cibernéticas é um processo que pode servir diferentes objetivos aos atores na cena internacional. Um dos objetivos é moldar o espaço operacional[512], residindo sobretudo no plano diplomático e no plano do processo jurídico. Outro dos objetivos visa o estabelecimento de uma estratégia de contra-ameaças, ou seja, o uso estratégico de atribuição de um ciberataque para combater certos adversários políticos específicos (recorrendo à estratégia política).

Enquanto no plano jurídico os elementos dos processos atendem a elevados padrões para fazer prova do facto internacionalmente ilícito, no plano político o critério parece ser o da plausibilidade em retirar dividendos da comunidade internacional utilizando a análise estratégica. Efrony e Shany mostraram que a maioria das imputações públicas de ciberataques não fizeram referência ao direito internacional, ou se o fizerem, foi apenas nos termos mais gerais e sem citar quaisquer princípios, base legal ou violação específica[513], podendo configurar uma mensagem a transmitir para o adversário político e seus aliados[514].

A decisão de imputação (ou não) de ataques cibernéticos aos Estados, por norma, compreende um processo de decisão mais do foro político do que jurídico. Há muitas fatores que determinam a tomada de decisão de um Estado, entre os quais: a) os recursos técnicos disponíveis para detetar e determinar com exatidão um ataque cibernético e o seu autor; b) a capacidade das instituições e serviços de informações em obter acesso a indícios sólidos de entre os seus parceiros de confiança; c) a geopolítica, com a necessidade de atender aos aliados políticos e às coligações internacionais; e d) as

[512] *Ibidem*.
[513] Dan Efrony e Yuval Shany, A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, in: *American Journal of International Law*, N.º 4, 2018 pp. 583-657, *apud* Dennis Broeders, Els De Busser and Patryk Pawlak, *op. cit*. p. 10.
[514] *Ibidem.*

consequências previsíveis, pois determinadas posições assumidas perante a comunidade internacional podem resultar em retaliação em dossiês no campo diplomático.

Para a cena política, o processo jurídico pode observar uma prioridade secundária, dado que o mais importante poderá ser mesmo ganhar a discussão na opinião pública internacional. Se a tática subversiva de determinado Estado versar sobre desonestidade pública de outro Estado, então bastará a acusação pública, pois uma campanha internacional de informações pode valer mais que a própria resolução do litígio perante os órgãos jurisdicionais, servindo, esta última, apenas de requisito de complementaridade e ação formal para capitalizar credibilidade internacional no momento da acusação pública.

11.3 Resolução de controvérsias sem eficácia obrigatória

A resolução de controvérsias pela via pacífica sob um esquema de natureza político, ou seja, uma resolução na ótica não jurisdicional "(…) constitui uma obrigação que entra em vigor em resultado do desencadear de uma controvérsia sobre responsabilidade"[515]. Uma vez que o uso de força nas relações internacionais observa uma proibição costumeira, exceto quando existe uma causa de exclusão da ilicitude, ou a habilitação do CSNU[516], a resolução pacífica de controvérsias constitui a única alternativa conforme o direito internacional[517].

Nesta base, segundo o espírito da CNU e as bases jurídicas inscritas no artigo 2.º, n.º 3 e o artigo 33, n.º 1 da mesma, constata-se o dever da resolução pacífica das controvérsias internacionais àquelas entidades vinculadas pelo princípio[518].

Quanto aos meios destituídos de eficácia obrigatória, podemos observar a negociação, tanto a nível bilateral ou multilateral tendo na sua génese um fundamento consuetudinário obrigacionista para resolução do litígio, esperando-se o mínimo entre as duas partes para resolver pacificamente qualquer conflito, sem que para tal se devam subordinar ao direito

[515] Eduardo Correia Baptista, *op. cit.*, p. 683.
[516] As prerrogativas deste órgão encontram-se previstas no artigo 24.º, n.º 1, da CNU.
[517] Eduardo Correia Baptista, *op. cit*., p. 683; Jorge Bacelar Gouveia, *Encicploédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (coord.), Almedina, 2015, pp. 342-346.
[518] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 691.

internacional, desde que não entrem em contradição com normas iuris cogentis[519][520]. Por exemplo, quando existem fortes indícios de um ciberataque perpetrado por um Estado B ao Estado A, este último, alvo do ciberataque, pode entrar em negociações com o Estado B, por sua vez, se B aceitar, iniciam as negociações. Tendo em vista a suscetibilidade de entendimento do mesmo, que "(…) pode assumir a modalidade de um sistema de consultas, podendo dela decorrer três resultados: a transação, a aquiescência e a desistência"[521].

As partes em controvérsia, e uma vez agudizadas as conversações diretas entre ambas têm menos possibilidades de alcançar um acordo, assim existe a prática corrente de apelar ou de uma terceira parte ofertar a sua participação com as partes controvertidas. Neste sentido, a resolução das controvérsias através do recurso aos bons ofícios e à mediação, constituem outro tipo de instrumentos negociais que podem ser determinantes para a resolução do conflito no universo pacifista[522]. Aqui entram uma terceira parte do diálogo que poderá ser particularmente relevante, dada a clivagem de poder negocial e influência internacional das partes em conflito sentadas à mesa de negociações. A participação de um terceiro Estado pode ser importante para evitar uma escalada de poder e desbloquear qualquer situação no decorrer das negociações para que se possa chegar a um acordo negocial, ou a um princípio de acordo. A principal diferença entre ambos reside no papel ativo da parte externa, na medida em que esta propõe soluções para o processo negocial de forma ativa.

Por outro lado, podemos observar o recurso ao inquérito, que consiste numa investigação externa sobre os factos que estiveram na origem da discórdia, constatando a sua materialidade, natureza e circunstâncias que os acompanham e, no final é entregue um relatório às partes[523].

Por fim, temos o recurso à conciliação, traduzindo-se na formação de uma comissão, que " (…) possa analisar a natureza e os pormenores do conflito, incumbindo-lhe propor uma solução jurídica (..)"[524]tendo em vista a justa resolução[525][526].

---

[519] *Ibidem*, p. 694.
[520] *Ibidem*, pp. 844-847.
[521] Jorge Bacelar Gouveia, *op. cit.*, p. 36.
[522] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 849.
[523] *Ibidem*, p. 850.
[524] Jorge Bacelar Gouveia, *op. cit.*, p. 37.
[525] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 852.
[526] Eduardo Correia Baptista, *op. cit.*, p. 698.

O CSNU assume a responsabilidade maxime da manutenção da paz e da segurança internacional, inscrita no artigo 24.º da CNU conferindo-lhe tal atribuição, gizando de um papel ímpar num sistema de segurança coletiva e pública. Por esta via, os Estados ou outras partes envolvidas na controvérsia poderão interpelar o CSNU, e não existindo um acordo preliminar entre as partes, atribuirá ao Conselho um carácter de uma intervenção oficiosa. Destarte, o CSNU poderá apelar aos meios não jurisdicionais de resolução pacifica de litígios (ex: recurso aos bons ofícios ou a meios disponíveis pelas organizações internacionais) por via de recomendações. Opcionalmente, poderá ser criado um órgão subsidiário, que lhe esteja diretamente subordinado, tendo como principal tarefa assistir o CSNU na resolução da controvérsia[527].

De forma suplementar, a AGNU, embora possa ser uma instância de resolução, como órgão plenário, assume uma tribuna essencialmente dominada pela agenda política internacional. Todavia, segundo o artigo 10.º da CNU, atribui-lhe uma competência geral, e nos artigos 11.º, 12.º e 13.º são definidas as possibilidades dessa intervenção, ainda que limitada[528].

11.4 Resolução de controvérsias com eficácia obrigatória

Neste tipo de forma de resolução litigiosa existe a adoção de um ato obrigatório para as partes na controvérsia, com a intervenção de uma entidade jurisdicional, que atua com independência e imparcialidade relativamente às partes em conflito, com base num processo contraditório[529]. Quanto aos meios, temos o recurso a um tribunal permanente ou arbitral e, nesse caso, imposta aos Estados uma solução por terceiros com todos as etapas processuais daí subjacentes. O recurso às varas dos tribunais é facultativo e, salvo disposição num Tratado em contrário, não existe nenhum dever de sujeitar uma controvérsia a uma resolução judicial[530].

O recurso à arbitragem implica um consentimento que deverá ser suficientemente claro e preciso de forma a constituir uma verdadeira obrigação jurídica internacional, pois "todo o compromisso é arbitrável se for vontade das partes". Assim, para dirimir um litígio no

[527] Na maior das situações são órgãos *ad hoc.*
[528] Nguyen Dinh, Patrick daillier e Allain Pellet, *op. cit.*, pp. 865-868.
[529] Jorge Bacelar Gouveia, *op. cit.*, p. 37.
[530] Eduardo Correia Baptista, *op. cit.*, p. 700.

ciberespaço com recurso à arbitragem é necessário a vontade livre dos Estados e um acordo entre as partes para a constituição de um órgão arbitral ad hoc ou permanente, responsável pela resolução.

O recurso à via judicial por um tribunal internacional permanente, mormente o TIJ, principal órgão judicial das Nações Unidas e, simultaneamente o mais importante tribunal existente[531][532], para além da função contenciosa, dispõe de uma função consultiva, emanando pareces sobre qualquer questão jurídica, todavia destituídos de efeitos obrigatórios[533][534]. Em caso de resolução do diferendo pelo TIJ, nomeadamente na fase escrita do processo, o Estado que sofreu o ciberataque terá que apresentar os indícios concretos que provocaram os factos internacionalmente ilícitos, conforme as regras da apresentação de prova de um determinado órgão de resolução de controvérsias. Sobre estas, note-se, a impossibilidade de determinar qual o grau de indícios necessário para obter um teor probatório suficiente. O TIJ aplica a abordagem do padrão de prova claro e convincente, todavia a comunidade internacional ainda procura uma interpretação quanto a esta abordagem[535]. Nesse sentido, o Manual de Tallinn 2.0, sugere a adoção da análise ao ciberataque caso a caso na ausência de um padrão universal de prova, segundo o entendimento de que as ações que um Estado toma devem ser atendidas conforme o costume razoável e atendendo à tradição de reposta dadas as circunstâncias em concreto[536]. Deste modo, deverá ser atendida a avaliação dos direitos conflituantes, o nível força empregue nas operações cibernéticas, as limitações, a proporcionalidade, a necessidade e entre outros princípios que são objeto de análise no Manual[537].

Como sugerem Dennis Broeders, Els De Busser e Patryk Pawlak, uma das soluções alternativas poderá passar pela interpretação do requisito do TIJ - claro e convincente –

[531] Ibidem, p. 705.
[532] Artigo 92.º da CNU
[533] Artigo 96.º da CNU.
[534] Eduardo Correia Baptista, *op. cit.*, pp. 700 e ss.
[535] Marco Roscini a), Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in: *Texas International Law Journal*, 2015, pp. 248; Mary Ellen O'Connell, Rules of Evidence for the Use of Force in International Law's New Era, in: *Proceedings of the Annual Meeting* (American Society of International Law), 2006, pp. 44-47, *apud*, Dennis Broeders, Els De Busser e Patryk Pawlak, *op. cit*. p. 7.
[536] "A base de validade do costume é o uso ou a prática", sendo que, geralmente, " (…) o uso, para que possa servir de base para a formação do costume, deve ser geral e constate.", enquanto que a prática, deve atender aos precedentes, caso que o ocorreu caso Estreito de Corfu, onde o TIJ, atendeu a estes para concluir que determinada prática geralmente admitida era suscetível de gerar o costume. Andrés Gonçalves Pereira e Fausto de Quadros, *op. cit.*, pp. 159-161.
[537] Michael Schmitt b), Tallinn Manual 2.0 on the international law applicable to cyber operations, in: Cambridge University Press, Cambridge, 2017, pp.111-134.

de forma específica e desenvolver um padrão de prova por meio da prática judicial ao nível Estatal[538].

A impunidade no ciberespaço é uma questão urgente. Os litígios ao nível das relações internacionais centram-se cada vez mais nos conflitos em ambiente digital, podendo ser observada pela comunidade internacional um domínio no qual reina um impasse jurídico internacional. Nesta senda, os Estados não são conduzidos a recorrerem aos meios pacíficos de resolução de conflitos internacionais pelas reduzidas hipóteses de aplicação sancionatória por uma violação internacional[539]. Por outo lado, se vários Estados adotarem como prática a referência ao direito internacional e, por esta ordem de razão, assumirem a sua aplicabilidade ao ciberespaço poderá, no longo prazo, contribuir para a formação de um ramo do direito internacional dedicado à regulação de controvérsias entre Estados no ciberespaço[540].

12 Uso de força, ataque armado e legítima defesa

Segundo a gradação do sistema resolução de controvérsias, tradicionalmente, variando das medidas pacíficas, por via não jurisdicional e jurisdicional, até ao recurso da força, sendo esta última preterida face às primeiras, todavia necessária quando não é possível assegurar a soberania do Estado nas relações internacionais convocando esta faculdade[541]. Todo o ato de coação entre Estados constitui, em termos virtuais, um perigo para a segurança internacional[542]. Assim, afigura-se importante para o estudo em concreto a interpretação do conceito de uso da força, inscrito no n.º 4, artigo 2.º da CNU e ataque armado, postulado no artigo 51.º da CNU à luz da contemporaneidade. Poderemos partir desta base normativa, com o auxílio das competências do CNSU, para perspetivar o uso de força ou o recurso à legítima defesa pelo Estado alvo de um ciberataque.

---

[538] Ibidem.
[539] Cfr. Jorge Bacelar Gouveia, *op. cit*., p. 32.
[540] Adicional à Convenção de Budapeste ou Convenção sobre o cibercrime.
[541] Não entraremos em considerados alongadas, apenas destacamos o facto do ponto de vista histórico, do uso de força nem sempre ter observado um princípio "juridicalista", ou seja, em vez de servir a defesa dos interesses juridicamente protegidos dos Estados não raras vezes serviu de justificativo para utilização do uso de força em grau apreciável de coação. Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, p. 952; Cfr. Carlos Blanco de Morais, O Direiot ao Uso de Força pelos Estados em tempos de Unilateralismo Multipolar, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, p.45-93.
[542] *Ibidem*.

Michael Schmitt sugeriu mensurar a dimensão do uso de força através do uso do *critério da escala dos efeitos cinéticos* provocados pela operação cibernética, ao qual, por outras palavras, apelidamos de níveis de intensidade no início deste capítulo[543][544]. Assim, este sustenta que quando os efeitos de uma operação cibernética sejam equivalentes aos efeitos cinéticos provocados nos domínios clássicos dever-se-á aplicar a CNU. Por exemplo, um ataque cibernético que cause danos materiais para o Estado alvo, como por exemplo, destruição ou inoperância definitiva de infraestruturas críticas nacionais, provocando destruição de sistemas vitais para o normal funcionamento de um Estado democrático, aí poder-se-ia aplicar a CNU à controvérsia no ciberespaço.

12.1.1 Uso de força

O uso de força no direito internacional público esteia-se essencialmente pela CNU, em particular pelo CSNU, órgão central das Nações Unidas, e nesta matéria tem o poder exclusivo externamente e internamente, cabendo-lhe a faculdade de atribuir sanções[545][546]. Como mencionado, existiu uma consagração progressiva do princípio da interdição do recuso ao uso de força[547], no qual o artigo 2.º, n.º 4 da CNU postula a proibição com todo o recuso à força, do qual a guerra não é senão uma forma extrema, tese esta corroborada pelos pactos regionais de e segurança e defesa mútua, onde observam o sentido lato do termo e do seu âmbito de aplicação[548][549]. Ainda, no caso Atividades Militares e

[543] De poderá ser observada como aleternativa àquela que foi apresentada no início deste capítulo, atinente aos níveis de intensidade.
[544] Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, in: *Columbia Journal of Transnational Law*, N.º 37, 1999, pp. 885-937, a*pud* Marco Roscini, *op. cit*., p. 44-68.
[545] Processo sujeito a vários tipos de princípios do tipo procedimental e material, que segue diferentes etapas: iniciativa, apreciação e decisão.
[546] Jorge Bacelar Gouveia, *op. cit.*, p. 63-65.
[547] Esta proibição jurídico–internacional da proscrição do uso da força assentou em quatro momentos fundamentais: 1) Na Convenção Drago-Porter em Haia, nomeadamente da proibição do uso de força na cobrança de dívidas contratuais; 2) Na afirmação de moratória de guerra no âmbito do Pacto da Sociedade das Nações; 3) Na renúncia geral ao uso da força no pacto Briand-Kellog; e 4) Na proibição geral inscrita na CNU. Cfr. Jorge Bacelar Gouveia, *op. cit.*, 54 e ss; Patrícia Galvão Teles, O Contributo da Comissão de Direito Internacional das Nações Unidas no que respeita à Proibição do Uso de Força, Direito Internacional Humanitário e Direito Penal Internacional, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, pp.504-505.
[548] Nguyen Dinh, Patrick daillier e Allain Pellet, *op. cit*., p. 957.
[549] O artigo 2.º, n.º 4 da CNU é frequentemente identificado como norma de *ius cogens*, nesse sentido vai o comentário da Comissão de Direito Internacional (ILC) sobre o Projeto de Artigos sobre o Direito de

Paramilitares na e contra Nicarágua, o TIJ afirmou que a proibição do uso de força era um princípio fundamental ou cardinal do Direito, e que o Estado alvo de ataque tem que efetivamente declarar, não cabendo a este fazer a avaliação da situação e partir para a legítima defesa (individual ou coletiva)[550].

Perante este cenário, se forças ou contingentes militares de um Estado conduzirem uma operação física que resulte na morte de cidadãos ou destruição física de infraestruturas de outro Estado, esta controvérsia internacional cabe no âmbito de atuação da CNU, nomeadamente na resolução através da ação oficiosa do CSNU. Poder-se-á argumentar que o uso de força tende a observar um uso múltiplo de aplicação, assim, condutas políticas ou sanções económicas podem observar consequências indiretas, como mortes ou destruição física de uma infraestrutura, que por sua vez, podem resultar em prejuízos ainda mais graves que uma operação militar clássica.

Destarte, Maro Roscini, sustenta que artigo 2.º, n.º 4 da CNU proíbe claramente o recurso à ameaça e ao uso de força, todavia o termo "uso de força" é pouco luminoso, ainda mais quando convocado em sede do ciberespaço. O autor sustenta, através do *Blacks Law Dictionary*, uma associação a "*poder, violência ou pressão dirigida contra uma pessoa ou coisa*"[551]. Neste sentido, residente um âmbito de aplicação lato, não convergente com a doutrina que circunscreve o termo "uso de força" de forma exclusivamente às forças armadas, podendo, por deste modo, referir-se a conceções mais abrangestes como a coerção política ou económica[552]. De forma divergente, este termo pode ser interpretado em sentido restritivo, pela aplicação exclusiva do termo "força" em relação ao uso da força armada, pois o preâmbulo da CNU dispõe "(…) *que a força armada* (…)", e desta forma, o artigo 2.º da CNU deve ser interpretado como sendo uma referência à força armada clássica (forças armadas), vedando a sua aplicabilidade ao ciberespaço. Ainda, documentos da ONU, como a Declaração de Relações Amistosas de 1970[553], a Declaração de 1974 sobre a Definição de Agressão[554] e a Declaração de 1987 sobre o Não

---

Tratados, «a lei da Carta relativa à proibição do uso da força constitui um exemplo notável de uma norma de direito internacional com caráter de *ius cogens*».

[550] Manuel de Almeida Ribeiro, A ONU e o uso da força pelos Estados: da letra da Carta aos novos desafios do século XXI, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, pp.460-461.

[551] Marco Roscini b), *op. cit.*, p. 45.

[552] *Ibidem*.

[553] United Nations, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, A/RES/2625, XXV AGNU, 1970, disponível para consulta em: https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf.

[554] United Nations, *Declaration on the Definition of Aggression*, A/RES/3314, XXIX AGNU, 1974, disponível para consulta em: https://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf.

Utilização da Força[555] suportam a opinião de que o artigo 2º, n.º 4 da CNU refere-se apenas à força armada[556].

Todavia, argumenta-se que se houvesse intenção do legislador em referir especificamente "força armada", entenda-se em sentido militar, restritivamente, este o teria expressamente mencionado, o que não ocorreu, concedendo uma interpretação ampla e corroborada pela inscrição do objetivo último "(…) *preservar as gerações vindouras do flagelo da guerra* (…)", independentemente do domínio aplicado à CNU.

Neste ponto interessa discutir o momento no qual uma operação cibernética assume que é utilizada "força armada", porque uma intervenção cibernética coercitiva não é por si só suficiente para identificar operações cibernéticas como um uso de força armada. Nestes termos, entendesse por *força armada* uma forma extrema de intervenção caracterizada pela intenção do Estado coercitivo obrigar o Estado alvo de coerção a proceder (ou não proceder) a determinada conduta, constituindo-se assim uma interferência nos seus assuntos internos[557].

Na perspetiva da corrente clássica as operações cibernéticas não caberiam no uso da força nos termos do artigo 2.º, n.º 4 da CNU, mesmo quando resultassem em danos físicos para os Estados alvo[558]. Sob uma perspetiva diferente, argumentasse que as operações cibernéticas atingem o limiar do uso de força armada quando são conduzidas contra uma infraestrutura crítica nacional, independentemente do meio utilizado[559].

Nesta senda, importa aferir se a utilização de meios no ciberataque, ou seja, a "arma", tradicionalmente associada a um objeto físico, pode ser considerada como sendo uma infraestrutura digital – um computador, um telemóvel ou outro aparelho tecnológico. A Federação Russa sustenta claramente que "(…) *currently the ICTs do not fit the definition of a weapon*"[560]. Embora não haja uma definição de "arma" através das vertentes de *jus*

---

[555] United Nations, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, A/Res/42/22, 1987, disponível para consulta em: https://digitallibrary.un.org/record/152626#record-files-collapse-header.

[556] Marco Roscini b), *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014, p. 46.

[557] Como enfatizado pelo TIJ *"[t] he element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force' directly or indirectly (Nicaragua, para 205)*. Marco Roscini b), *op. cit.*, p.46.

[558] Stephanie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare", in: *Stanford Journal of International Law,* N.º 48, 2012, pp. 226 e ss; Matthew Waxman, "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions', in: *International Law Studies,* N.º 89, 2013, p 111, *apud*, Marco Roscini b), *op. cit.*, p.46.

[559] Marco Roscini b), *op. cit.*, p.47.

[560] United Nations, *Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*, Moscow, 2020,

ad bellum ou *jus in bello*, o *Black's Law Dictionary* define arma como *"*(…) *instrumento usado ou projetado para ser usado para ferir ou matar alguém*"[561]. Um Estudo de direito Internacional Humanitário define armas como "(…) *meios para cometer atos de violência contra forças inimigas humanas ou materiais*"[562]. O HPCR Manual on International Law Applicable to Air and Missile Warfare, frisa a característica principal de uma arma: a capacidade de causar ferimentos, morte, dano ou destruição de objetos[563]. O mínimo denominador comum das visões supramencionadas são as potências consequências violentas produzidas pela arma, portante o *nível de intensidade* ou a *teoria dos efeitos*, aplicada às consequências do uso de uma "arma" no ciberespaço.

Se o uso de força armada nos termos do artigo 2, n.º 4, da CNU requer o uso de armas, a próxima questão a responder é se um software malicioso - *malware* pode ser qualificado como tal. O TIJ, numa opinião consultiva sobre a legalidade da ameaça ou uso de armas nucleares, deixou claro que os artigos 2.º, n.º 4, 42.º e 51.º da CNU não refere quaisquer armas específicas, sendo aplicáveis a qualquer uso de força, independentemente das armas empregues[564]. Ian Brownlie, discorre que produtos químicos e armas biológicas são comumente referidas como armas de "guerra" e a forma como estas podem ser usados para destruir vidas humanas e propriedades – tal argumento pode servir de base análoga para a propagação de um *malware* malicioso na infraestrutura crítica de um Estado.

Vários Estados incluíram tecnologias cibernéticas nas suas doutrinas militares, referindo-se ao ciberespaço como um domínio de guerra (ciberdefesa), e por essa via dispuseram unidades militares com experiência cibernética, centradas na hipótese de deflagrar um conflito armado cibernético que recairá na *jus in bello,* daí a necessidade de distinguir alvos e objetivos de ataque (militares ou civís)[565]. O Ministro dos Negócios Estrangeiros

disponível para consulta em: https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

[561] *Black's Law Dictionary*, 9ª Edição, Bryan Garner (ed), West, 2009, p.1730.

[562] Jean-Marie Henckaerts e Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge University Press, Cambridge, 2005, Vol. I, Rule 6, p. 23, *apud*, Marco Roscini, *op. cit*., p. 49.

[563] HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge University Press, Cambridge, 2013, p. 49, *apud*, Marco Roscini b), *op. cit.*, p. 49.

[564] "*These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons."* International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, , 1996, ICJ Reports, disponível para consulta em: https://www.icj-cij.org/public/files/case-related/95/7497.pdf.

[565] Harold Hongju Koh, sustenta que "(…) *We must distinguish military objectives—that is, objects that make an effective contribution to military action and whose destruction would offer a military advantage—from civilian objects, which under international law are generally protected from attack.*". Harold Hongju Koh, *op. cit.*, p. 5.

da Rússia alertou para o efeito destrutivo das armas de informação, "(…) *pode ser comparável a das armas de destruição em massa*"[566]. Por sua vez, Espanha relembrou o perigo do "*uso da Internet como meio de lançamento de uma arma, ou seja, o seu uso configuraria um meio de lançamento de ataques contra sistemas de informação a infraestrutura críticas ou a da própria infraestrutura da Internet*"[567]. A estratégia de segurança nacional do Reino Unido enfatiza que a "a*tividade no ciberespaço" é "uma arma militar para uso dos Estados e possivelmente de outros (…)"*[568], por seu turno, o subsecretário de segurança e contraterrorismo do Reino Unido declarou que um ataque cibernético que destrua uma central elétrica seria considerado um ato de guerra.

A abordagem que recebeu maior apoio doutrinário é baseada nos *efeitos da ação*: o uso da força poderá apresentar diferentes níveis de intensidade e, que por sua vez nos diz que um ataque cibernético pode conduzir a danos sobre a propriedade e pessoas, tal como acontece nos domínios clássicos[569]. Desta forma, qualquer operação cibernética que cause, ou seja passível de causar consequências prejudiciais na mesma escala que aquelas que são normalmente produzidas por armas cinéticas considera-se empregue o uso da força[570].

De forma semelhante Harold Koh, sustenta que "*se as consequências físicas de um ataque cibernético resultarem num dano físico, por meio do acionamento de uma bomba ou disparo de um míssil, esse ataque cibernético deve igualmente ser considerado pelo recurso ao uso da força*[571]. Convergentemente, Michael Schmitt e Liis Vihul, sustentam que certas operações cibernéticas, atendendo à teoria dos efeitos não apresentam consequências destrutivas ou prejudiciais, todavia recorrem ao uso de força, e porventura violam normas internacionalmente consagradas e princípios como o da soberania e da não-intervenção nos assuntos internos, como por exemplo, através do exercício do

---

[566] Cfr. Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, UN Doc A/C.1/53/3, 1998, p 2, disponível para consulta em: https://undocs.org/en/A/C.1/53/3.

[567] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/64/129, 2009, p.10, disponível para consulta em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/396/33/PDF/N0939633.pdf?OpenElement.

[568] United Kingdom, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, p. 29, disponível para consulta em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

[569] Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict and Security Law*, N.º 17, *2012*, p. 212; Heather Harrison Dinniss, Cyber Warfare and the Laws of War, in*: Cambridge University Press*, 2012, p. 74.

[570] Marco Roscini b), *op. cit.*, p. 51.

[571] Harold Koh, *op. cit*., p. 4.

controlo sobre infraestrutura, ou por via de atividades cibernéticas dentro de um território de outro Estado[572]. Portanto, operações cibernéticas, seja de natureza defensiva ou ofensivamente, conduzidos pelos órgãos de defesa cibernética daqueles Estados são atribuídos aos mesmos Estados, mesmo quando a ação desse órgão seja *ultra vires*[573].

Após a verificação da retórica dos termos empregues, e à luz da contemporaneidade, afirmamos que a propagação de *malware*, apesar de não caber nos regimes jurídicos como arma, segundo a teoria dos efeitos ou o nível de intensidade determinado, poderá potencialmente, equivaler ao uso de força nas relações internacionais e constituir-se como uma arma pelo seu potencial alto nível de intensidade destrutivo e inclusive disruptivo, em especial numa sociedade com alta dependência tecnológica, e inevitavelmente um futuro incerto quanto à segurança ao nível cibernético[574].

12.1.2 Ataque armado

A primeira frase do artigo 51.º da CNU, estabelece que "(…) *nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais*".

A noção do termo "ataque armado" à luz do desenvolvimento tecnológico experimentado convoca a necessidade de escrutinar a complexidade dos fenómenos perpetrados através do ciberespaço e, mais importante, os seus efeitos para um determinado território e para uma população. Destarte, esta figura embora difusa, poderá configurar "(…) *qualquer*

[572] De acordo como os especialistas do Manual de Tallin, é convergente a ideia de que uma operação cibernética de um Estado contra outro Estado que que cause danos à infraestrutura críticas nacionais violaria a soberania do Estado alvo, enquanto o mera monitorização digital não. Todavia não existe concordância sobre a colocação de malware numa infraestrutura crítica ou numa eventual alteração ou destruir de dados. Deste modo, uma operação cibernética lançada pelo Estado A que altere os dados armazenados num servidor no território do Estado B viola a soberania do Estado B. Contudo, se o estado B armazenar os mesmos dados no Estado C, a operação do Estado A violaria apenas a soberania do Estado C. Michael Schmitt e Liis Vihul a), *op. cit.*, pp. 59-60.

[573] Vills, *op. cit*., p. 61.

[574] Noran Shafik Fouad, *The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016)*, p. 635.

operação ou ato com o efeito de infligir um prejuízo ou um dano no Estado e nos seus elementos fundamentais"[575].

Cabe então analisar a posição soberana dos Estados à luz da sua interpretação. Em caso de conflito da "*informação do ciberespaço*", a Rússia reivindica o direito de legítima defesa individual ou coletiva, através da "(…) *implementação de quaisquer opções e meios* (…)" de acordo com as normas e princípios do direito internacional[576]. O Estado Italiano afirmou que os Estados podem proteger infraestruturas críticas nacionais de ataques externos conforme a com lei[577].

De acordo com o artigo 51.º da CNU, o Estado alvo de uma operação cibernética terá o direito inerente de legítima defesa apenas na medida em que tal operação possa ser descrita como um "ataque armado". Destarte, o requisito é aplicável aos meios cibernéticos na medida em que equivale a um uso da força nos termos do n.º 4 do artigo 2.º da CNU. No caso de Nicarágua, o TIJ reconheceu que a definição de "ataque armado" não é comtemplada na CNU[578]. Suportando-nos no Parecer Consultivo do TIJ, onde este órgão decisório assume a *flexibilidade* do termo um "ataque armado", esclarecendo que o artigo 51.º da CNU é aplicável a "*qualquer uso da força, independentemente do tipo de armas empregues*"[579], rematado que "«*o uso de qualquer dispositivo ou número de dispositivos que resulte numa considerável perda de vidas humanas e/ou destruição de propriedade deve ser apta a preencher os pressupostos de um ataque armado* »"[580].

O uso de qualquer dispositivo tecnológico, que resulte na perda considerável de vidas e/ou destruição considerável de propriedade deve, portanto, *implet totum* as condições de um ataque armado[581]. Da lista exemplificativa na Resolução n.º 3314 (XXIX) da AGNU, de 14 de dezembro de 1974, o uso de força não é admitido à luz do direito internacional

---

[575] Jorge Bacelar Gouveia, *op. cit.*, p. 76.

[576] Ministry of Defence of the Russian Federation, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, 2000, p. 12, disponível para consulta em: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

[577] Ministero dell'Istruzione Ministero dell'Università e della Ricerca, *La posizione italiana sui principi fondamentali di Internet*, 2012, p. 5, disponível para consulta em: http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf.

[578] Cfr. *Nicaragua*, para 176, *apud*, Marco Roscini b), *op. cit.*, p. 71.

[579] Cfr. *Nuclear Weapons*, para 39, *apud*, Marco Roscini b), *op. cit.*, p. 71.

[580] Alexandre Guerreiro, *op. cit*, p. 339.

[581] Consistindo este "(…) *um ato ilícito perpetrado por um Estado que atenta contra a independência política ou a integridade territorial de outro Estado*". Sofia Santos, Enciclopédia de Direito e Segurança, Jorge Bacelar Gouveia e Sofia Santos (coord.), 2015, Almedina, p. 41.

dos conflitos armados, definindo no artigo 3.º alínea a)[582], b)[583], c)[584] e g)[585], os atos considerados como agressão (com recurso ao uso de força) e, comutativamente ataques armados. Em particular, o artigo 3.º, alínea b), refere-se ao "*bombardeamento por forças armadas de um Estado do território de outro Estado* (…)", demonstrando o amplo sentido da definição em escrutínio. Por outro lado, o bloqueio de portos ou costas não é, *per se*, um ato de agressão que equivale a um ataque armado[586].

Relativamente ao nível de dano aplicado ao ciberespaço, uma operação cibernética que consiga bloquear o acesso à Internet de todos os cidadãos de um determinado Estado, sem causar danos físicos, patrimoniais ou inoperância dos serviços essenciais daquele Estado, não equivaleria a um ataque armado, e, portanto, o direito à legitima defesa não deveria ser aplicado. Alertamos para as linhas muito ténues nas fronteiras quando se qualifica o ataque armado ao nível cibernético, a mensuração do dano pode revelar-se inquantificável para efeitos da qualificação de ataque armado pois tenderá à relativização.

O TIJ identificou "*as formas mais graves do uso da força*", entre as quais o ataque armado, corresponde ao uso máximo de força armada, isto em termos de nível de intensidade a fim de distingui-los[587]. Como consequência, o uso da força é somente considerado "ataque armado" quando atinge o patamar mais elevado ao nível da intensidade (efeitos), isto é, atinge o nível disruptivo.

Em termos doutrinários Avra Constantinou tentou caracterizar os ciberataques através de um padrão de *escala* e *efeitos*[588], argumentando que um ataque armado é "*um ato ou o começo de uma série de atos de força armada de magnitude e intensidade consideráveis* (escala), *que têm como consequências* (efeitos) *a imposição ou destruição de elementos importantes no Estado alvo, ou seja, da população, das infraestruturas e da unidade*

---

582 "(a) *The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof*";

583 "(b) *Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State*";

584 "(c) *The blockade of the ports or coasts of a State by the armed forces of another State*";

585 "(g) *The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein*";

586 Marco Roscini b), *op. cit.*, p.72.

587 *Ibidem*.

588 Ao nível dos efeitos, Dinstein sugeriu alguns exemplos de ataques cibernéticos onde é aplicada a escala dos *efeitos* de forma para obter qualificação de como ataques armados: a) número de mortes causadas pela inoperância de computadores que controlam sistemas; b) tempo de interrupção da rede elétrica, repercutindo-se em consideráveis repercussões nacionais; destruição ou alteração de informação de computadores que controlam centrais hidráulicas, barragens ou centrais nucleares. Yoram Dinstein, Computer Network Attacks and Self-Defense, in: *Computer Network Attack and International Law*, Michael Schmitt e Brian O´Donnell (eds), International Law Studies, Vol. 76, p. 105.

governativa"[589]. Nesta linha, considera-se que tanto a escala como os efeitos do uso da força determinam a possibilidade da ocorrência de um ataque armado. Um exemplo ilustrativo desta situação poderá ocorrer quando é perpetrado um ataque DDoS massivo que envolve milhões de *botnets* que interrompe uma infraestrutura crítica nacional por um período reduzido de tempo, considera-se, quanto à sua escala como bastante significativo, mas os seus efeitos são de pouco impacto, pois são pouco repercutidos ao nível dos danos causados a um Estado[590]. Por outro lado, quando o uso de força é direcionado para a inoperância da infraestrutura, tendo em vista a inoperância funcional para qual esta foi concebida, poderá ser equiparado a um ataque armado, caso se revele um grau de dano muito apreciável[591]. Com efeito, um ataque DDoS de ampla *escala* numa infraestrutura crítica nacional do ramo financeiro, que inviabilize o funcionamento da estrutura de mercado financeiro de determinado Estado, causará certamente graves perturbações nacionais e externalidade impactantes, colocando em causa a segurança (económica) do Estado. Pode haver uma qualificação de ataque armado neste caso? A resposta é incerta, e poderá, atendendo à teoria do nível de intensidade ou da teoria dos efeitos só passível de mensuração real no médio-longo prazo, dada a necessidade de contabilizar com a máxima verisimilhança possível o nível de dano causado ao Estado.

Assim, ainda que seja qualificado de ataque armado, não é líquido que o Estado alvo dos ataques cibernéticos possa avançar para o recurso à legítima defesa nos termos do artigo 51.º da CNU, e, mesmo quando tal aconteça devem ser observados determinados critérios, nomeadamente a necessidade, a proporcionalidade e o imediatismo de modo a repelir o ataque.

Foi doutrinariamente convergente a tese no Manual de Tallin na ideia de que o ciberataque *Stuxnet* envolveu uso de força, todavia não houve consenso em qualificar este ciberataque como um "ataque armado"[592]. O Irão considerou que foram violados princípios da CNU e o direito internacional, qualificando o ciberataque como uma forma de "terrorismo nuclear", todavia, atendendo ao nível de dano causado, não considerou grave o suficiente para determinar a existência de um "ataque armado" e, consequente passível de recorrer ao direito inerente à legítima defesa[593].

[589] Marco Roscini b), *op. cit.*, p. 73.
[590] *Ibidem*.
[591] *Ibidem.*
[592] Michael Schmitt b), *op.* cit., *pp.* 107-139.
[593] Iranian Foreign Minister's address to the UN Security Council, 2012, disponível para consulta em: http:// iran un.org/en/2012/09/28/28-september-2012-2/, *apud,* Marco Roscini b), *op. cit*., p. 76.

Um ataque armado requer *animus agressionis* – neste contexto a invocação da intenção deliberada de causar danos à propriedade, pessoas ou sistemas de um determinado Estado. De acordo com o TIJ, um ataque armado deve ser realizado "*com a intenção específica de causar dano*"[594]. No contexto cibernético, a intenção hostil pode ser inferida de "(…) *fatores como persistência, sofisticação dos métodos utilizados, direcionamento de sistemas especialmente sensíveis, e o dano real causado*"[595].

Se um ataque armado perpetrado pelo Estado A contra o Estado B também produz consequências prejudiciais não intencionais sobre a propriedade, pessoas ou sistemas no Estado C, uma reação em legítima defesa pelo estado C não seria necessária, pois o Estado A provavelmente cessará a ação de C[596]. O problema será mais complexo se o Estado A ataca B passando-se por Estado C (manipulando dados de transmissão e localização para parecer que eles se originaram no Estado C), reagindo B em legítima defesa contra o Estado C. Como sugere o Manual de Tallinn, o fato que uma operação cibernética ser lançada ou encaminhada através de uma infraestrutura cibernética governamental de um Estado não é, *per se*, indício suficiente para efeitos de atribuição de responsabilidade da operação, e por sua vez, não é líquida a atribuição de responsabilidade direta do ciberataque a determinado Estado. Marco Roscini, acrescenta se um Estado de forma conhecedora e consciente, permitir que outro Estado utilize as suas infraestruturas cibernéticas, com a finalidade de conduzir uma operação cibernética equivalente a um ato de agressão num outro Estado, então, o Estado conhecedor da ação também violaria a proibição do uso da força, mas não cometeria um ataque armado.

Com efeito, apesar de existir uma distinção de alvos (militares/civis) um ciberataque, qualificado como "ataque armado" pela comunidade internacional em determinado território soberano e, seguindo a teoria do *nível de intensidade* e a teoria dos *efeitos*, guiam a nossa investigação no sentido de que, independentemente dos alvos, o Estado alvo deverá recorrer à figura da legítima individual ou coletiva para repelir o evento, sob pena de não saber se a ameaça ou ataques cibernéticos se continuariam a registar no seu território e, consequentemente viver com um grau de incerteza quando a futuros danos tendo que conviver com um "inimigo ativo"[597]. Todavia, advertimos, que esta ação de

[594] Cfr. *Oil Platforms*, para 64, *apud*, Marco Roscini b), *op. cit.*, p.77.
[595] Cfr. US DoD, *An Assessment*, p. 21. *Ibidem*.
[596] Marco Roscini b), *op. cit.*, p. 77.
[597] Dinstein, 'Computer Network Attacks', p. 106, *apud*, Marco Roscini b), *op. cit.*, p.33.

legítima defesa deverá ser exercida pelo ciberespaço, e atender aos critérios da necessidade, proporcionalidade e imediatismo.

12.1.3 Legítima defesa

A legítima defesa constitui um direito inerente a todo o sistema jurídico e no cunho jurídico-internacional está previsto no artigo 51.º da CNU, postulado no Capítulo VII, adstrito à segurança pública e coletiva[598][599][600].

Os pressupostos de legítima defesa relacionam-se com a perpetração de um "ataque armado", sendo este último um ato ilícito contra os bens dos sujeitos internacionais[601].

Como vimos anteriormente, o uso de força nas relações internacionais é proibido, todavia, o efeito da violação desta norma pode originar o direito inerte à legítima defesa, que constitui uma causa de exclusão de ilicitude[602].

Adverte-se para as limitações do exercício da legítima defesa, nomeadamente, " (…) *medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao CSNU e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais*."[603]. Posto isto, radica do artigo 51.º da CNU, que o direito à legítima defesa no caso de um operação no ciberespaço por parte de um Estado para fazer cessar um ataque armado não deve ser invocado, senão enquanto o CSNU não tenha tomado as medidas necessárias para manter a paz, ou uma vez exercido pelos Estado (segundo o imediatismo a imprimir na ação) deve ser imediatamente comunicadas as medidas tomadas ao CSNU. Neste caso em específico, a seu carácter é provisório, controlado e subsidiário deduzido no CSNU como expressão

[598] Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit.*, pp. 959-960.
[599] Constitui-se como *subsidiária, provisória* e *controlada*. Cfr. Nguyen Dinh, Patrick Dailler, Alain Pellet, *op. cit*., p. 961.
[600] Como bem sustenta Nico Schrijver "(…) *Part of the process restricting and regulating the use of force was the specification of exceptions under which use of force would be justified and unavoidable*.". Nico Schrijver, The Ban on the Use of Force in the UN Charter, in: *The Oxford Handbook of The Use of Force in International Law*, Marc Weller (ed), Oxford University Press, 2015, p. 473.
[601] Jorge Bacelar Gouveia, *op. cit.*, 76.
[602] Eduardo Correia Baptista, *op. cit.*, p. 648.
[603] Jorge Bacelar Gouveia, *Direito Internacional da Segurança*, Almedina, 2015, p. 75.

máxima da comunidade internacional no exercício da legítima defesa[604] que deverá ser diligente. No entanto, sabemos que um veto de um membro permanente do CSNU ou as divergências políticas podem pôr em causa o seu exercício de legítima defesa ou a sua paralisação quando esteja numa situação que não permita tomar medidas corretivas, sendo que a legítima defesa serve de bastião da defesa soberana para os Estados[605][606].

O direito à legítima defesa, é um *direito limitado de autotutela* do Estado assegurado no direito internacional[607], previsto e reconhecido pelo artigo 51.º da CNU, sendo ao mesmo tempo um direito natural. Nestes termos, "(…) *somente agressão armada* – e não qualquer coação – *justifica o recurso à força a título de legítima defesa*"[608].

Verifica-se que a invocação por parte de um Estado alvo de ciberataque, portanto *"*(…) *objeto de uma violação em escala apreciável da proibição do uso da força nas relações internacionais por uma entidade vinculada por esta* (…) *ou, em relação a Estados terceiros, um movimento armado*", sendo que esta violação deve "(…) *assumir uma forma grave, não apenas de agressão, mas de ataque armado*", conduzindo por usa vez à aplicabilidade de determinado regime jurídico[609].

Em termos práticos, o exercício da legítima defesa pressupõe um quadro de ataque armado (a decorrer ou atual)[610]. Assim, o ataque deve se ter iniciado "(…) *e ainda se encontrar em curso, ou, no mínimo, ter sido extraordinariamente grave e existirem riscos sérios de se encontrarem iminentes outros ataques*" para o Estado alvo poder recorrer a este meio, caso contrário poderemos falar em represália, sendo esta última ilícita[611].

A legítima defesa no âmbito de um ataque no ciberespaço pode ser exercida por meios físicos ou digitais (*latu sensu*), como sustentamos defendemos o meio domínio na aceção da figura da legítima defesa. A legítima defesa física poderá utilizar armas tradicionais (militares) para atingir a infraestrutura cibernética do perpetrador do ciberataque, como

---

[604] Nguyen Dinh, Patrick daillier e Allain Pellet, *op. cit.*,p. 962.
[605] *Ibidem*.
[606] Ainda a este respeito, em 1986, no processo relativo às *Atividades militares e paramilitares na Nicarágua e contra esta*, o TIJ, esclareceu o regime de legítima defesa no direito internacional, nomeadamente quanto às condições necessárias ao exercício do direito à legítima defesa e quato às suas modalidades. *Ibidem.*
[607] José Pina Delgado, Legítima Defesa, in*: Enciclopédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (coord.), Almedina, 201 5, p. 253.
[608] Nguyen Dinh, Patrick daillier e Allain Pellet, *op. cit.*,p. 960.
[609] Eduardo Correia Baptista, *op. cit.*, p. 649.
[610] Cfr. nota de rodapé 1167 relativa à legítima defesa preemptiva em: Eduardo Correia Baptista, *op. cit.*, p. 650.
[611] Eduardo Correia Baptista, *op. cit.*, pp. 650-651.

os servidores de origem dos ataques, ou outros alvos físicos de acordo com os princípios de necessidade e proporcionalidade[612].

O desafio do sistema internacional encontra dois desafios, o primeiro relativo à perceção da figura da legítima defesa e retaliação por parte dos Estados alvo dos ciberataques, o segundo desafio é relativo ao momento a partir do qual é aceitável iniciar uma ação de legítima defesa[613] no domínio do ciberespaço e mais complexo, como o poderá fazer em relação à figura da legítima defesa preventiva e preemptiva. Quanto ao primeiro, de forma consuetudinária, a figura da autotutela defensiva assume a justificação do uso da força lícita contra determinados atos ilícitos, o que poderá configurar um meio mais liberal, com menores limitações que o recurso à legítima defesa, e que poderá ser um recurso com maior *relevância prática* do ponto de vista da repressão de um ciberataque, sendo que se enquadra no âmbito da exclusão da ilicitude de atos de defesa. Quanto ao segundo, no âmbito de um ataque digital poderá ser bastante complexo, ou o Estado alvo apresenta uma maturidade ao nível da cibersegurança e ciberdesa altíssimos, inclusive com redundância de recursos.

13 Princípios da necessidade, proporcionalidade e imediatismo

A legítima defesa contra operações cibernéticas equivalentes a ataques armados, como qualquer reação em autodefesa deve de atender aos requisitos de *necessidade*, *proporcionalidade* e *imediatismo*[614]. Embora o artigo 51.º da CNU não lhes faça

[612] Harold Hongju Koh, aprofunda o princípio da proporcionalidade, referindo que este "(…) *prohibits attacks that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects that would be excessive in relation to the concrete and direct military advantage anticipated*". Descreve ainda alguma regras de aplicação deste princípio: "(1*) the effects of cyber weapons on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or a power grid) that would affect civilians*; (2) *the potential physical damage that a cyber attack may cause, such as death or injury that may result from effects on critical infrastructure*; e (3) *the potential effects of a cyber attack on civilian objects that are not military objectives, such as private, civilian computers that hold no military significance, but may be networked to computers that are military objectives*". Harold Hongju Koh, op. cit., p. 4. Cfr. ICRC, *Protocol Additional: to the Geneva Conventions of 12 august 1949*, pp. 41 e ss.

[613] Destarte, a doutrina norte americana afirmou na sua Estratégia de Defesa do Ciberespaço de 2011, que sempre que tal se justificasse, recorreriam ao uso de força para responder a atos hostis no ciberespaço tal como faria com qualquer outra ameaça. United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, 2011, p.14.

[614] Cfr. Regra 23 do Tallinn Manual 2.0, Michael Schmitt, *op. cit*., pp. 127-130.

referência expressa, o TIJ, sustenta que "(…) *a submissão do exercício do direito de legítima defesa às condições de necessidade e proporcionalidade é uma regra de direito consuetudinário internacional* " e " *a sua dupla condição aplica-se igualmente ao artigo 51.º da CNU, quaisquer que sejam os meios de força empregues*"[615].

No contexto cibernético, os Estados Unidos reafirmaram que o uso da força em legítima defesa contra um ataque cibernético "*deve ser limitado ao que é necessário para lidar* com um ataque iminente ou ataque armado real, devendo este ser proporcional à ameaça concreta"[616]. Por se turno, o secretário de Estado dos negócios estrangeiros do Reino Unido sustentou que "*a necessidade para os governos agirem proporcionalmente no ciberespaço e de acordo com direito nacional e internacional*"[617]. A Holanda também declarou que o uso da força em resposta a um "*ataque cibernético armado*" deve cumprir os requisitos de necessidade e proporcionalidade[618].

13.1.1 Necessidade

A necessidade do uso de força como último recurso e a única maneira eficaz de repelir o ataque armado obriga o Estado que exerce a legítima defesa ou a autotutela defensiva a proceder à imputação do ciberataque. Conforme o artigo 51.º da CNU expõe expressamente, uma reação em legítima defesa, não se coaduna necessária se o CSNU apresentar medidas para manter ou restaurar a paz e a segurança internacional. Por outro lado, se a medida de legítima defesa se demonstrar ter sido ineficaz contra o ataque armado, esta não significa que não foi necessária, todavia se fosse claro *ex ante* que a reação de legítima defesa não servisse o propósito de repelir o ataque armado, aí poderíamos constatar uma ação ilícita por parte de um Estado que recorreu a esta figura.

---

[615] Cfr. *Nuclear Weapons*, para 41, *apud*, Marco Roscini b), *op. cit.*, p.88.
[616] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/66/152, 2011, p.19, disponível para consulta em: https://undocs.org/A/66/152.
[617] Marco Roscini b), *op. cit.*, p. 89.
[618] Advisory Commite on Public Internacional Law, Government Response to the AIV/CAVV, Report on Cyber Warfare, p. 5, disponível para consulta em: https://www.advisorycommitteeinternationallaw.nl/publications/government-response/2012/04/06/cyber-warfare.

13.1.2 Proporcionalidade

A proporcionalidade está intimamente relacionada à necessidade. O *quantum* do uso de força usada na ação defensiva pode ser mensurado pela *escala* e pelos *efeitos* do ataque armado perpetrados no Estado alvo dos ciberataques, sempre com o propósito de repelir o ataque que se encontra em ação ou, que uma vez cessado, ainda apresenta sérios e iminentes riscos de serem perpetrados outros ataques. A proporcionalidade tende a fundir-se com a necessidade. Proporcionalidade, não significa que é permitido uma resposta cinética e cibernética a um ataque cibernético, bem como uma resposta cibernética a um ataque cinético[619]. Posto isto, uma resposta em espécie contra um ataque cibernético nem sempre é possível ou eficaz. Se um Estado que exerce a legítima defesa não possuir a tecnologia capaz para responder aos desafios tecnológicos apresentados pelo Estado perpetrador ou quando o Estado onde será empregue a força de legítima defesa é independente das redes e sistemas tecnológicos, isto é, sem claras infraestrutura críticas que possam ser alvos de semelhantes danos infligidos sobre o seu território, ou possui um baixo grau de dependência digital, então poderá ter que ser repensada a proporcionalidade[620].

O problema com o cálculo da proporcionalidade no contexto cibernético reside na velocidade e natureza imprevisível dos ataques cibernéticos: pode ser difícil estabelecer de forma precisa a sua *escala* e *efeitos* (danos)[621]. A proporcionalidade poderá ser difícil de calcular com antecedência devido à interconectividade das informações nos sistemas. Imagine-se que um Estado em legítima defesa lança um *malware* com o intuito de fazer cessar um ataque cibernético a decorrer, sendo que esse *malware* está programado para determinado sistema informático, mas, por acaso, é lançado nos sistemas informáticos que possuem o controlo de uma arma biológica, que por sua vez reproduzir-se-ia de forma descontrolada. Neste caso, era observando um grau incalculável de proporcionalidade no exercício de legitima defesa, constituindo-se uma reação desproporcional, que não seria, *per se*, transformar uma medida de legítima defesa numa represália ilícita, mas qualificaria " (…) *o Estado que exerceu o direito de legítima defesa por um ato de excesso*

[619] Cfr. Marco Roscini b), *op. cit*., p. 90.
[620] *Ibidem*.
[621] Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, in: *Boston College International and Comparative Law Review*, 32, Issue 2, 2009, p 452, disponível para consulta em: https://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16/.

(ou abuso) de legítima defesa"[622]. Em suma, atender ao critério de proporcionalidade é essencialmente uma questão técnica: reações cibernéticas personalizadas de legítima defesa são possíveis atendendo ao objetivo último que é arquitetado, neste caso cessar todos os ciberataques[623].

13.1.3 Imediatismo

A exigência de imediatismo na ação de legítima defesa, reflete a rápida diligência tendo em vista a ação de repelir ou fazer cessar um ataque armado[624]. O imediatismo não significa "instantaneidade" e deve ser aplicado de forma flexível, ou seja, "(…) *não deve haver um lapso de tempo indevido entre o uso de força ou o ataque armado e o exercício da resposta de legítima defesa ou autotutela do Estado*"[625].

O imediatismo (e também a proporcionalidade) ficou postulado no exercício da legítima defesa pela doutrina *Caroline*, que decorreu de um conflito entre um navio dos EUA e as forças armadas da Grã-Bretanha, em 1837[626]. Neste conflito, a marinha britânica destruiu o navio Caroline dos EUA, posteriormente Daniel Webster sustentou que o recurso à legítima defesa deve ficar reservada para os casos em que a "«*necessidade daquela legítima defesa é imediata, avassaladora e não deixa outra alternativa nem outro momento para decidir*»"[627].

Alguma flexibilidade na avaliação do imediatismo (em termos temporais) é especialmente exigida nos casos em que os efeitos de um ciberataque causem danos apreciáveis nas redes e sistemas de informação militares de um Estado, sendo espectável que estes possam atuar num quadro de tempo razoável face ao dano provocado e à necessária conduta a providenciar.

[622] Marco Roscini b), *op. cit.*, p. 91.
[623] Como por exemplo planear um determinado *software* malicioso, com um alto nível de precisão e informações tendo em conta o alvo a atingir, de resto, foi o que ocorreu no ataque Stuxnet.
[624] Marco Roscini b), *op. cit.*, p. 91.
[625] *Ibidem*.
[626] Alexandre Guerreiro, *op. cit*., p.333.
[627] *Ibidem*.

13.2 Princípio da diligência devida

Os Estados, as organizações e os cidadãos interagem constantemente sem interrupções, sob as mais diversas formas no ciberespaço, por esse mesmo motivo, apresentam quota parte de responsabilidade pelo bom funcionamento do mesmo. As dependências que o ciberespaço criou na nossa sociedade demostra a imprescindibilidade das práticas de segurança da informação para a manutenção da ordem e segurança nacional e internacional no ciberespaço, enfrentando múltiplos desafios do foro legal, técnico, político e militar.

A vida social, política, cultural, económica e o bem-estar da sociedade dependem em certa medida do bom funcionamento da Internet, isto é, do correto funcionamento das estruturas operacionais do ciberespaço. Espera-se então, perante um ideário simbiótico de utilizadores e prestadores de serviços de Internet e sistemas de rede que haja uma atitude coletiva responsável de entre todos os atores do ciberespaço, de forma a promover a operacionalidade de sistemas e redes de modo a que não seja comprometida a confidencialidade, integridade e disponibilidade.

A responsabilização coletiva, entre os diversos atores do ciberespaço, desde os utilizadores o indivíduo até ao Estado, necessitam de adotar práticas preventivas, consideradas internacionalmente como seguras e aprovadas amplamente pela comunidade internacional no contexto em ambiente digital[628]. A responsabilidade objetiva no ciberespaço coloca o ônus nos Estados e, considerando a dificuldade de prevenção[629] de intrusões cibernéticas e a facilidade com que os equipamentos digitais (ex. computadores ou telemóveis) podem ser controlados remotamente através da manipulação de identidades falsas ou roubos de identidades[630] e cruzando diferentes jurisdições perspetivamos que a prevenção e a fiscalização em ambiente digital possam vir a ser objeto de massificação na comunidade internacional, em especial pelas autoridades judiciárias.

[628] Nesse sentido, *v.* Ana Maria Guerra Martins, *op. cit*., p. 399.

[629] Em várias áreas de responsabilidade, em diferentes fases de implementação e em diferentes níveis de participação.

[630] Por essa via, Estados podem vir a assumir responsabilidade por operações cibernéticas de servidores hospedados nos seus Estados, mas a autor material da perpetração do ciberataque pdoerá estar localizado num Estados terceiro, servindo-se da localização digital do primeiro para perpetração de ataques cibernéticos.

A adoção do princípio da *due deligence*[631] como um princípio internacional emergente é essencial no ciberespaço, onde cabe aos Estados a responsabilidade de proteger pessoas e infraestruturas de informação e sistemas nacionais contra danos ou uso indevido, deste modo, tenderá em afirmar-se na comunidade internacional e, em particular, nas organizações internacionais. Sob o escopo deste princípio, a AGNU sugeriu aos Estados algumas medidas a ter em conta no domínio do ciberespaço corroborando este princípio, a saber[632]:

" *(a) Os Estados devem assegurar que a sua legislação e procedimentos internos não constituem um refúgio seguro para aqueles que usam indevidamente as tecnologias de informação*;

(b) *Cooperação em matéria de execução da lei, investigação e ação penal, nomeadamente àqueles crimes relacionados com as tecnologias de informação devem observar a coordenação entre todos os Estados interessados*;

(c) *As informações devem ser trocadas entre os Estados sobre os problemas que enfrentam no combate ao crime perpetrado em ambiente digital*;

(d) *Os aplicadores da lei devem obter formação e equipamentos adequados para lidar com os crimes e criminosos que utilizam indevidamente as tecnologias de informação no ciberespaço*;

(e) *Os sistemas jurídicos devem proteger a confidencialidade, integridade e disponibilidade dos dados e sistemas de computador contra danos e acessos não autorizados, de modo a garantir que os criminosos sejam sancionados*;

(f) *Os sistemas judiciais devem permitir a conservação e o acesso rápido aos dados eletrónicos atinentes a investigações criminais específicas*;

(g) *Os regimes jurídicos de assistência mútua devem garantir a investigação oportuna do alegado criminoso, a recolha e intercâmbio oportuno de indícios nestes casos*;

(h) *O público em geral deve ser informado da necessidade de prevenir e combater este tipo de crimes em ambiente digital*;

(i) *Na medida do possível, as tecnologias da informação devem ser projetadas para ajudar a evitar e detetar prevaricadores no ciberespaço, monitorizar criminosos e recolher indícios*;

---

631 Cfr. Regra 7 do Manual de Tallin 2.0, pp. 43- 50.

632 United Nations, *Combating the criminal misuse of information technologies*, A/Res/55/63, 2000, disponível para consulta em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

(j) *A luta contra o uso indevido das tecnologias da informação requer o desenvolvimento de soluções que levem em consideração tanto a proteção das liberdades individuais, como a privacidade, ao mesmo tempo que preserva a capacidade dos governos no combate a este tipo de crimes.*

Adicionalmente, o relatório do Conselho da Europa, atendeu ao carácter transnacional do cibercrime, e veio esclarecer que a *due deligence* equivale a "*razoáveis esforços de um Estado para se informar sobre as componentes factuais e legais que se relacionam com interrupções ou interferências transfronteiriças, com a infraestrutura da Internet e, nesse sentido, tomar as medidas adequadas em tempo útil para resolvê-los. Tais medidas incluem, em primeiro lugar, a formulação de políticas destinadas a prevenir e responder a interrupções ou interferências no ciberespaço de modo a minimizar o risco ou consequências desses eventos e, em segundo lugar, a implementação dessas políticas*"[633]. A diligência devida exige a implementação e aplicação de um quadro normativo interno nos Estados-membros, com liberdade de ação para investigar, iniciar ações judiciais, recolher indícios suficientes fortes e proceder à dedução de acusações contra os responsáveis pelos crimes perpetrados no ciberespaço, sem esquecer a diligente cooperação das investigações com Estados alvo de ataques cibernéticos[634]. Atualmente, esta é já uma realidade entre os Estados-membros da UE que apresentam bases normativas e autoridades policiais com unidades específicas dirigidas ao cibercrime, todavia a principal crítica que vem sendo veiculado salienta a fraca harmonização entre os sistemas jurídicos, nomeadamente quanto à prova digital[635].

[633] Council of Europe, *International and multi-stakeholder co-operation on cross-border Internet*, Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, 2010, disponível para consulta em: www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf.

[634] Christopher Lentz, A State's Duty to Prevent and Respond to Cyberterrorist Acts, in: *Chicago Journal of International Law,* 10, 2010, pp. 820 e ss, *apud*, Marco Roscini b), *op. cit.*, p. 88.

[635] A título de exemplo, no caso português, as competências preventivas e repressivas do informáticos são reservadas à competência da Polícia Judiciária, através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T). Cfr. Polícia Judiciária, Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), disponível para consulta em: https://www.policiajudiciaria.pt/unc3t/.

14 O Grupo de Especialistas Governamentais

A temática da segurança da informação está inscrita na agenda da ONU desde 1998, quando a Federação Russa apresentou um projeto de resolução sobre o assunto ao Primeiro Comitê da AGNU. Foi então adotada, sem proceder a votação pela Assembleia Geral a Resolução n.º 53/70[636] da ONU. Desde 2004, foram formados cinco Grupos de Especialistas Governamentais (GEG) para discutir a existência de riscos e ameaças ao nível do ciberespaço a fim de poderem chegar a um entendimento comum quanto às medidas a adotar para a sua mitigação. Três desses grupos concordaram nos relatórios apresentados ao nível das conclusões e recomendações que foram emitidas a todos os Estados da ONU. Os relatórios do GEG foram bem-recebidos pela AGNU. O relatório de 2015[637], aprovado por consenso alargado na Resolução n.º 70/237[638], "*exorta os Estados Membros a serem orientados no uso das tecnologias de informação e comunicação pelo relatório de 2015 do Grupo de Peritos Governamentais*". No relatório foram expostas as preocupações quanto às ameaças, nomeadamente quanto à capacidade disruptiva dos atores não estatais[639], ao desenvolvimento de capacidades dos Estados no domínio militar (ciberdefesa)[640], a preocupação com as infraestruturas críticas nacionais[641] ou as vulnerabilidades causadas pela disparidade de recursos entre Estados[642].

Destacamos o ponto 13 deste relatório, de onde é possível retirar alguns avançados práticos no entendimento da comunidade internacional, concretamente, são recomendadas condutas aos Estados numa base voluntarista e não vinculativa um conjunto de regras e princípios visando a promoção de um ambiente digital aberto, seguro,

---

[636] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/RES/53/70, disponível para consulta em: https://undocs.org/A/RES/53/70.
[637] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/RES70/174, disponível para consulta em: https://undocs.org/A/70/174.
[638] United Nations, *Developments in the field of information and telecommunications in the context of international security*, A/RES/70/237, disponível para consulta em: https://undocs.org/A/RES/70/237.
[639] "*The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy*". Ponto 7, A/RES/174 da AGNU.
[640] "*A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely*". Ponto 4, A/RES/174 da AGNU.
[641] "The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.". Ponto 5, A/RES/174 da AGNU.
[642] "*Different levels of capacity for ICT security among States can increase vulnerability in an interconnected world*". Ponto 8, A/RES/174 da AGNU.

estável e pacífico[643]. Observamos ainda como o grupo inferiu sobre a aplicabilidade do direito internacional, incluindo a CNU aos Estados membros da ONU relativamente ao uso das tecnologias e informação e comunicação[644].

---

[643] " (a*) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security*;
(b) *In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences*;
(c) *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs*;
(d) *States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect; (e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression*;
(f) *A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public*;
(g) *States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions; (h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty*;
(i) *States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions*;
(j) *States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure*;
(k) *States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity*". Ponto 13, da A/RES/174 da AGNU.

[644] "(a) *States have jurisdiction over the ICT infrastructure located within their territory*;
(b) *In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms*;
(c) *Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group recognized the need for further study on this matter*;
(d) *The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction*;
(e) *States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts*;
(f) *States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.* Ponto 28 da A/RES/174 da AGNU.

Com efeito, a Federação Russa declarou a aceitação da aplicabilidade do direito internacional e da CNU à esfera das tecnologias de informação e comunicação, ao mesmo tempo que sustenta que não estão previstas especificações desta aplicabilidade, em particular, por quem, como e em que condições lhe é aplicável, indiciando que, na prática tais normas internacionais ficam condicionadas de aplicação ao ciberespaço, rematando que tais aspetos merecem uma maior atenção por via de um instrumento jurídico internacional que regule expressamente as regras aplicáveis às TIC, concluindo então pela existência de um vazio jurídico[645].

Por seu turno, em sede da discussão do relatório final do grupo aberto de trabalho, a União Europeia e o seus Estados-membros decidiram comentara o "pré-draf", incluindo na sua comunicação algumas posturas partilhadas. Nesta comunicação, ficou reiterada a subordinação de toda a estrutura de cibersegurança no ciberespaço sob o escopo do direito internacional, incluindo a CNU e o direito internacional humanitário. Deste modo, destacam-se os princípios da humanidade, necessidade, proporcionalidade e distinção aos Estados em relação às TIC no que concerne à promoção da redução dos riscos, à responsabilização, transparência e manutenção da paz e segurança internacional no longo prazo. Nesta senda, a UE defendeu, atendendo às circunstâncias internacionais, à não criação de novos instrumentos legais para o ciberespaço, velando antes pela aplicação das estruturas jurídicas já criadas[646], alertando para o risco de minar os efeitos práticos que se vão sentido no ciberespaço enquanto tal discussão se oferece na comunidade internacional. Por último, salientou a necessidade de um maior entendimento das normas de responsabilidade aplicadas ao ciberespaço.

Destacamos a comunicação Estado Australiano pela sua postura pró-ativa neste domínio, zelando pela manutenção e expansão das estruturas de responsabilidade estatal direcionada especificamente ao ciberespaço[647]. Acrescenta, que a discussão esteve

---

645 United Nations, *op. cit.*, https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

646 Em especial normas internacionais, onde se inclui o CSNU e o TIJ.

647 Destaque-se, o Estado Australiano, alvo de uma mega ciberataque em junho de 2020, confirmando publicamente ser dirigido de um Estado pela natureza sofisticada e segmentação técnica utilizada. O centro de cibersegurança australiano, tinha já advertido para uma série de riscos que se tinham vindo intensificar. Apesar do presidente Australiano ter veiculado um Estado como ator perpetrador dos ciberatatques não fez qualquer imputação pública sobre o mesmo, preferindo referir que a escala do ataque afetou todos os ministérios do governo, infraestruturas críticas nacionais e operadores de serviços essenciais. Cfr. Prime Minister, Minister for Home Affairs and Minister for Defence, *Statement on malicious cyber activity against Australian networks*, 2020, disponível para consulta em: https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks.

centrada nas "*normas*", advertindo que estas não devem ser confundidas com o "*quadro normativo*". Rematou, afirmando a necessidade de criar acordos vinculativos, seja a nível bilateral ou multilateral, a par da importância da reflexão acerca dos pontos convergentes por todos os Estados[648].

Verifica-se o contributo que este grupo tem dado à orientação dos Estados no ciberespaço, através da possibilidade de diálogo público internacional, a par da definição de importantes guias de conduta para atuação dos Estados, tentando com que estes se possam vincular à manutenção de um ciberespaço estável, contribuindo para manutenção da paz e segurança internacionais. Sem prejuízo das metas já alcançadas, a seu funcionamento predomina essencialmente uma base de *soft law* aplicada à conduta dos Estados no ciberespaço, o que em termos práticos não cria obrigações jurídicas para os Estados, podendo, na prática servir de antecâmera para um acordo internacional ou um placo de acusações internacionais entre Estados.

15 Quadratura Europeia face a um ciberataque

A União Europeia tem desempenhado um papel ativo na promoção da defesa e segurança do ciberespaço. A nível supranacional conta uma complexa rede de órgãos e instituições que comtemplam na sua missão principal ou adjetiva o reforço da cibersegurança ou ciberdefesa[649], ao nível civil, militar ou ambos[650].

A União, através da AED tem um janela de oportunidade aberta para os Estados-membros cooperarem e elevarem o seu nível interno de cibersegurança e ciberdefesa através do centro de capacidades e ciberdefesa da UE, cometido à AED, ou ainda por via do

A par deste ciberataque não podemos deixar de salientar a relevância estratégica que a Estratégia de cibersegurança da Austrália concebeu, sendo alocados 1,67 biliões de dólares neste decano, *v*. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy.

[648] OEWG Virtual Meeting, Australian Intervention, 2020, disponível para consulta em: https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-australia-2-july-2020.pdf.

[649] Estruturalmente a União Europeia na rubrica no setor da paz, segurança e justiça conta com as agências da EUROPOL (EC3), EUROJUST e EU-LISA; ao nível do mercado único conta com a ENISA, as redes CSIRT e a CERTU-EU; e na PESC e PCSD, conta com a AED, GSA, SEAE, SIAC e a ERCC.

[650] Estados da UE como a Alemanha, Reino Unido, Espanha e França apresentam declaradamente unidades militares responsáveis pela condução de operações no ciberespaço.

estabelecimento da CEP[651], onde é possível verificar o alinhamento entre várias linhas de financiamento europeu para a edificação de projetos com o cunho de Estados europeus[652]. A estratégia de cibersegurança da União Europeia admite que *"[Um] incidente ou ataque cibernético particularmente grave pode constituir a base suficiente para um Estado-membro invocar a Cláusula de Solidariedade da UE*"(artigo 222.º do TFUE)[653], embora nenhuma menção fosse feita ao artigo 42.º, n.º 7 do TUE, que proclama o "*dever de auxílio e assistência por todos os meios ao seu alcance, em termos semelhantes ao artigo 51.º da CNU "em caso de agressão armada*"". O artigo 222.º do TFUE prevê que a União Europeia mobilize todos os instrumentos ao seu dispor, incluindo os recursos militares dos Estados-membros para fazer face a certas ameaças, em especial, ataques terroristas, ou catástrofes de causadas pelo homem ou de origem natural. A cláusula de solidariedade é suficientemente ampla para justificar uma resposta militar ao nível da ciberdefesa, de forma coordenada, que de acordo com a estratégia de cibersegurança da UE, onde inclui "*incidentes ou ataques cibernéticos particularmente graves*", apelando, portanto, à *mutualização da partilha de recursos e informações* entre os Estados-membros.

Nesta senda, o artigo 222.º do TFUE pode ser invocado no caso de qualquer "*grave incidente ou ataque cibernético*", enquanto que o artigo 42.º, n.º 7 do TUE parece ser, potencialmente aplicável aos ataques cibernéticos que equivalham a uma "agressão armada". Tendencialmente, o artigo 42.º, n.º 7 do TUE assemelhasse ao artigo 5.º do Tratado do Atlântico Norte e subordina a sua própria operação aos "*compromissos sob a Organização do Tratado do Atlântico Norte*", sendo que, para os Estados-membros de ambas as organizações, continuam a ser as bases jurídicas para a defesa coletiva ao nível regional em caso de ataque armado no ciberespaço.

Sob esta linha de raciocínio, constitui-se inteiramente legítimo e possível que a cláusula de solidariedade mútua seja desencadeada fruto de um ataque cibernético perpetrado contra um Estado-membro da UE, tendo este, segundo o nível de força ou a teoria dos efeitos, causado danos na propriedade, perda de vidas humanas, ou forte perturbação do funcionamento das infraestruturas críticas nacionais de um Estado ou de vários Estados–membros. Esta opção do uso de força, não prejudicaria uma eventual ação de ciberdefesa

[651] Decisão (PESC) 2017/2315 do Conselho de 11 de dezembro de 2017, que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados-Membros participantes.
[652] Para consultar a lista de projetos em curso, *v.* https://pesco.europa.eu/.
[653] European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013, p. 19, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

ativa nos termos do artigo 42.º, n.º 7 do TUE, que ao contrário de uma ação conduzida sob o escopo do artigo 222.º do TFUE, seria puramente intergovernamental e não exigiria a coordenação ao nível da UE, pois estaríamos no âmbito da PCSD. Recorde-se que utilização do uso de força em ambiente digital pelo Estados-membros deveria ser sempre aplicado à luz dos princípios da necessidade, proporcionalidade e imediatismo como supra descritos.

15.1 A articulação com a NATO

A doutrina NATO inscreve nas suas preocupações e desafios de segurança ao nível civil e militar a cibersegurança e ciberdefesa. Esta realidade, começou por ganhar lugar no conceito estratégico da NATO de 2010 (Cimeira de Lisboa), sendo uma das principais prioridades para os membros da aliança atlântica. Em 2011, a NC3A lançou a iniciativa multinacional para o desenvolvimento de uma capacidade de ciberdefesa (MNCD2), onde foram identificadas seis grandes áreas de capacitação para a ciberdefesa: 1) deteção de atividade maliciosa[654]; 2) prevenção, mitigação e eliminação de ataques[655]; 3) análise dinâmica de riscos, ataques e danos[656]; 4) recuperação de ciberataques[657]; 5) tomada de decisão em tempo real[658]; e 6) gestão de informações de ciberdefesa[659]. Em linha com esta iniciativa, foi estabelecida a Cyber Rapid Reaction (CRR) como sendo estratégico no auxílio à aliança de forma permanente (24/7), com duas equipas de especialistas que se dedicam à coordenação e execução de missões de defesa no ciberespaço. A UE firmou com a NATO um acordo técnico entre os centros de resposta a incidentes cibernéticos, constituindo o primeiro passo para uma cooperação mais alargada a outras vertentes[660]. A constituição deste tipo de equipas já existe ao nível dos Estados-membros, auxiliados

[654] Compilação de dados de sensores, avaliação de entidades, avaliação de situação e visualização para análise.
[655] Reconfiguração de tipologia, controlo de fluxo de tráfego, defesa ativa e coordenação da resposta externa.
[656] Análise de riscos, valoração dos ataques, avaliação de danos, consciencialização da situação.
[657] Restaurar a integridade dos sistemas, integridade da informação, restaurar a disponibilidade de serviço e o registo de informação comprometida.
[658] Opções, coordenação e disseminação da decisão.
[659] Recompilação e partilha de informação de ciberdefesa, garantia de qualidade da informação e compilação e exploração de dados.
[660] Luís Camelos dos Santos et. alli, *op. cit.*, p 45.

por órgãos da União, o que indica coerência, coordenação e complementaridade ao nível intergovernamental e supranacional no âmbito da ciberdefesa.

Na prática, a NATO já afirmou que o direito internacional é aplicável ao ciberespaço[661], o que é conforme com a visão da União, aplicando princípios defensivos e ofensivos semelhantes àqueles que são aplicados nos domínios clássicos. Os aliados assinaram um compromisso de defesa cibernética em julho de 2016, para aprimorar as capacidades cibernéticas, demostrando a importância emergente do domínio. Ainda no mesmo ano NATO e UE firmaram um acordo técnico sobre a defesa no ciberespaço. À luz dos desafios comuns, a NATO e a UE estão a reforçar a cooperação na ciberdefesa, nomeadamente nas áreas de intercâmbio de informações[662], formação de pessoal e simulação de exercícios em ambiente digital.

Em 2018, na Cimeira de Bruxelas, os aliados concordaram em criar um novo Centro de Operações Ciberespaciais como parte da Estrutura de Comando reforçada da NATO[663][664], iniciativa esta regozijada por todos os ministros da defesa dos Estados da aliança[665]. Nessa mesma Cimeira, os aliados advertiram para o perigo que as ameaças cibernéticas representavam para a segurança da aliança, inclusive foi alertado que estas estavam a ganhar dimensões significativas, descrevendo-as como complexas, destrutivas e coercitivas. Como descrito pela própria organização, a NATO serve em três eixos essenciais: a defesa coletiva, a gestão de crises e a segurança cooperativa – esteados no princípio da indivisibilidade da segurança e, por essa via, nem só o artigo 5.º do Tratado

---

661 "*We reaffirm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable*". NATO, *Brussels Summit Declaration*, 2018, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20; Federico Yaniz, NATO-EU Cooperation Milestones and Challenges Ahead, in: *Security and Defence in Europe*, Martín Ramírez e Jerzy Biziewski (Eds), Springer, 2020, pp. 221-225.

662 Cfr. Tribunal Europeu de Contas, *op. cit*, p. 43-47.

663 "*Individual Allies may consider, when appropriate, attributing malicious cyber activity and responding in a coordinated manner, recognising attribution is a sovereign national prerogative. We are determined to deliver strong national cyber defences through full implementation of the Cyber Defence Pledge, which is central to enhancing cyber resilience and raising the costs of a cyber attack*". NATO, *op. cit.,* disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

664 O centro proporcionará consciência situacional e coordenação da atividade operacional da NATO no ciberespaço. Os Aliados concordaram que a NATO poderia recorrer às capacidades cibernéticas nacionais para a prossecussão das missões e operações. Os Aliados também se comprometeram a elevar a resiliência nacional por meio do compromisso de defesa no ciberespaço.

665 "(..) *NATO defence ministers endorsed a NATO guide that sets out a number of tools to further strengthen NATO's ability to respond to significant malicious cyber activities. NATO needs to use all the tools at its disposal, including political, diplomatic and military, to tackle the cyber threats that it faces. The response options outlined in the NATO guide will help NATO and its Allies to enhance their situational awareness about what is happening in cyberspace, boost their resilience, and work together with partners to deter, defend against and counter the full spectrum of cyber threats*. NATO, *Cyber defence*, 2020, disponível para consulta em: https://www.nato.int/cps/en/natohq/topics_78170.htm.

do Atlântico Norte serve de base jurídica no caso de ameaça ou mesmo um "ataque armado" no ciberespaço a qualquer um dos aliados[666]. Com efeito, como inscrito no artigo 3.º do Tratado em análise, " (…) *as Partes, tanto individualmente, como em conjunto, manterão e desenvolverão, de maneira contínua e efetiva, pelos seus próprios meios e mediante mútuo auxilio, a capacidade individual e coletiva para resistir a um ataque armado*", demostrando o compromisso entre os aliados em trabalhar, individualmente ou coletivamente, para obter capacidades para, tanto a nível civil (cibersegurança) ou militar (ciberdefesa) enfrentarem o uso de força no ciberespaço. Da mesma forma, os aliados concertam uma posição cooperativa no ciberespaço, dada a aplicabilidade do artigo 4.º do Tratado, sempre que "(…) *estiver ameaçada a integridade territorial, a independência política ou a segurança de uma das Partes*". A posição do Conselho do Atlântico Norte, para além de observar reiteradamente a aplicação seu próprio Tratado fundacional e pedra basilar da organização, reitera a adesão às normas e princípios de direito internacional em relação ao ciberespaço[667].

A par de todos estes esforços políticos, a NATO tem promovido uma cooperação estreita com o setor industrial, em especial com o setor privado, entendido como crítico para o sucesso ao nível da segurança da informação no ciberespaço, tentando aproximar-se das redes CERT e representantes nacionais da indústria privada, convocando sinergias para várias atividades nas vertentes da formação e implementação de projetos relativos à *smart defence*[668][669][670].

---

[666] NATO, *NATO's role in cyberspace*, 2019, disponível para consulta em: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

[667] NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, 2020, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

[668] Para mais desenvolvimentos *v.*, https://nicp.nato.int/nato-cyber-defence/index.html.

[669] Cyber Defence Smart Defence Projects Conference, *Multinational Cyber Defence Capability Development (MNCD2)*, 2016, disponível para consulta em: https://academiamilitar.pt/images/CDSDP2016/Apresentacoes/1.NATO-CD-Smart-Defence-Projects_MNCD2.pdf.

[670] No âmbito da partilha de informação, Portugal participa num projeto de *smart defence* no âmbito da NATO, liderado pela Bélgica – Malware Information Sharing Platform (MISP), *v.* https://www.nato.int/cps/en/natolive/news_105485.htm.

15.2 Diplomacia digital

A política externa dos Estados é desenvolvida sob um quadro dinâmico e multifacetado, onde a centralidade de atuação baseia-se nas informações e na influência internacional. Bem sabemos que a influência internacional e o recursos dos Estados no ciberespçao não são iguais e, por essa via, como bem sustenta Justin Morris, "*For international law to operate successfully as an institution of international society it is necessary for those states which possess the greatest power to acknowledge and act commensurate to the responsibilities which flow from their status*"[671].

Os novos desafios públicos da diplomacia dependem cada vez mais da informação, assim "*Diplomats will have to rethink what is "information," and see that a new realm is emerging— the noosphere[672], a global "realm of the mind"—that may have a profound effect on statecraft."[673].* As circunstâncias da *realpolitik* podem não servir de forma tão eficaz os Estados e as suas estratégias diplomáticas clássicas, "(…) *and will instead favor the emergence of a new diplomacy based on what we call noopolitik (nü-oh-poh-li-teek) and its preference for "soft power"*"[674]. Como argumenta Paul Cornish, primariamente, o ciberespaço deverá ser um assunto de discussão política, para que caso se venha a ocorrer um conflito no ciberespaço, as normas éticas e os princípios estejam bem definidos, assim, deverá ser objeto de apreciação negocial entre os Estados, mormente através de compromissos[675].

A diplomacia clássica é alvo de transformação por via da digitalização e das técnicas mais avançadas em linha. A informação como ativo mais importante ao nível diplomático é também aquele que permite influência e persuasão ao nível da *softw law* internacional. Contemporaneamente, a lógica da partilha de informação em rede, entre atores estatais e

---

[671] Justin Morris, Law, power and force in an unbalanced world, in: *International Conflict and Security Law*, Essays in Memory of Hilaire McCoubrey, Richard Burchill, Nigel White e Justin Morris (eds), Cambridge University Press, 2009, p. 298.

[672] Acerca da definição de *"Noosphere*": "*This term, from the Greek word noos for "the mind," was coined by French theologian and scientist Pierre Teilhard de Chardin in 1925, and spread in posthumous publications in the 1950s and 1960s. In his view, the world first evolved a geosphere, and next a biosphere. Now that people are communing on global scales, the world is giving rise to a noosphere—what he variously describes as a globe-circling realm of "the mind," a "thinking circuit," a "stupendous thinking machine," a "thinking envelope" full of fibers and networks, and a planetary "consciousness." In the words of Julian Huxley, the noosphere is a "web of living thought.*". David Ronfeldt e John Arquilla, Noopolitik: A New Paradigm for Public Diplomacy, in: *Routledge Handbook of Public Diplomacy*, Nancy Snow e Philip Taylor (eds), Routledge International Handbooks, p. 354.

[673] Cfr. *Ibidem*, *op. cit*., p. 352.

[674] *Ibidem*.

[675] Paul Cornish, *op. cit.*, pp.1-16.

não-estatais e a sua utilização como fonte de poder enceta um novo caminho nas relações internacionais de *soft power* – a *ciberpolitik*.

O cruzamento de áreas do saber como direito, economia, política, estratégia, informática, matemática ou as ciências militares assumem a centralidade da atuação no ciberespaço pelos diversos atores da cena internacional. Esta ascensão gradual do *soft power* por via da digitalização estatual tende a ser uma realidade na política externa, com o aumento do número de exercícios ao nível da cibersegurança, ciberdefesa e troca de informação entre Estados, organizações internacionais e outros atores internacionais.

Em 2017, os Estados não chegaram a um consenso em sede do GEG quanto ao estabelecimento de um Conselho de atribuição dos ataques em ambiente digital (de natureza política, técnica e legal). Este teria como missão principal a identificação e imputação, de forma inequívoca do perpetrador dos ataques cibernéticos através da troca de informações ao nível das equipas CERT e por via das agências e serviços de informações[676]. Desde então, a relação entre Estados tem variado de acordo com a *geopolítica aplicada ao ciberespaço*, antevendo o exercício predominante de cooperação a nível bilateral, veja-se que ao nível do G7 e G20, os Estados tentam concertar posições de natureza benéficas entre todos[677].

A frequência de fenómenos de guerra híbrida em Estados da União foi inaugurada no segundo decano deste século e observa ciberataques contra infraestruturas de telecomunicações e informações do governo alemão, através da utilização de ciberespionagem[678][679], furto de propriedade intelectual, entre outros ataques emparelhados pela paralisação do sistema de segurança e de comunicação de forma

[676] Annegret Bendiek b), The EU as a Force for Peace in International Cyber Diplomacy, in: *SWP Commnet*, N.º19, 2018, disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf

[677] Sobre este tipo de cooperação, o WWF estabeleceu um conselho global para a cibersegurança, que tem como missão o fortalecimento da colaboração global para enfrentar os desafios sistémicos de cibersegurança, melhorar a confiança digital e proteger a inovação, instituições, empresas e indivíduos. Para mais informações *v*., https://www.weforum.org/communities/the-future-of-cybersecurity.
Ao nível da proteção da proteção dos cidadãos e da sociedade cívil em geral, as agências de cibersegurança ou qualquer órgão com competências atribuídas nesta área tem uma função pedagógica de alerta, independentemente. Destacamos as ameaças transnacionais pela capacidade de afetar o foro doméstico do indivíduo através dos seus equipamentos pessoais. Cfr. FBI e Internet Crime Complaint Center , *Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide*, 2020, disponível para consulta em: https://www.ic3.gov/Media/Y2018/PSA180525.

[678] Potencialmente perturbador da ordem internacional, em especial nas relações bilaterais entre EUA e China.

[679] Para mais desenvolvimentos sobre a matéria *v*., Russell Buchan, *Cyber Espionage and International* Law, HART, p. 15-17.

subversiva[680]. Este não é exemplo isolado ao nível do aparelho político-diplomático, após um ataque a dois cidadãos com um gás nervoso (Novichok[681]) em Londres, os chefes de governo e de Estado declararam solidariedade ao Reino Unido e ameaçaram a Rússia com consequências que visavam a retaliação digital (*hackback*)[682].

A postura diplomática em relação a operações defensivas ou ofensivas em ambiente digital na Alemanha é vertida na sua estratégia de cibersegurança, onde é possível observar o estabelecimento de uma força de reação rápida, integrada no BSI[683], capaz de responder a ataques contra infraestruturas críticas nacionais ou a outras ameaças que possam colocar em causa o Estado e as suas instituições democráticas. A base de sustentação legal e política foi obtida através do parlamento em 2015 e 2016, e neste último ano, o ministério da defesa nacional entendeu estabelecer uma nova unidade militar dedicada ao ciberespaço.

Na Dinamarca, por exemplo, foi nomeado um embaixador para a ciberdiplomacia, ação política que demostra a importância da postura nacional (soberana) face aos acontecimentos internacionais de largo espetro, como a discussão da aplicabilidade das normas internacionais, proteção de dados, *governance* na Internet, acordos mútuos internacionais, entre outros.

Recordemos que a UE apresentou uma proposta em forma de pacote de medidas para auxiliar a resposta diplomática a atividades maliciosos em ambiente digital em complemento à Diretiva NIS, visando a proteção e segurança do mercado único. Além disto, este pacote apresentou instrumentos que podem ser utilizadas pela UE ao abrigo da PCSD, por exemplo, a utilização de sanções restritivas como supra mencionado neste estudo. As diferentes categorias de medidas tomadas pela União podem ser consideradas

[680] Annegret Bendiek b), *op. cit*., disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf.

[681] Gás com orgime na Sibéria e de natureza militar, produzido pela ex-URSS, entretanto descontinuado de produção.

[682] Estados Unidos, França, Canadá e Alemanha consideram que, em última instância, o presidente da Federação Russa seria o responsável por esta operação.

[683] Para mais informações consultar *v.*, https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html.

como: preventivas[684], cooperativas[685], de estabilização[686] e restritivas[687] com o apoio dos Estados-membros ao nível legislativo[688].

A União tem se posicionado de forma preventiva, promovendo uma cultura de fortalecimento da paz ao nível cibernético internacional por via da prevenção e guiada pelos valores inscritos no artigo 2.º do TUE em sede dos principais *fora* especializados, mas também, ao nível interno através da PESC e PCSD.

A UE define uma política de continuidade preventiva (ao nível da regulamentação) e deteção (atores/ameaças existentes e emergentes) de natureza civilística, mas não militar. A seu tempo esta abordagem pode não ser suficientemente eficaz para fazer face a um número elevado de ciberataques a Estados europeus. Por outro lado, sabemos que o cunho militar está indiretamente presente nesta "política de paz e diplomacia" da UE, quer seja por via dos instrumentos ao abrigo da PCSD, e poderá vir a revelar-se uma importante antecâmera, servindo de último bastião da defesa supranacional.

Nesta senda, Josep Borrell sustentou que "*member states have repeatedly signalled their concern and denounced malicious behaviour in cyberspace. Such behaviour is unacceptable as it undermines international security and stability and the benefits*

---

[684] Ao nível político existe uma tentativa de diálogo com países terceiros para a construção de soluções globais, sob a forma de associação ou parceria numa perspetiva cooperativa.

[685] Por exemplo, através de uma delegação da UE pode transmitir uma nota diplomática (*démarche*) ao governo de determinado Estado, sob permissão e acompanhamento da AR/VP. O chefe de representação da delegação diplomática pode entregar uma proposta para conduzir conversas abrangentes ou simplesmente transmitir ideias chave.

[686] Essas medidas têm uma função de alerta para o Estado visado para se abster de tomar qualquer ação maliciosa em ambiente digital. O Conselho Europeu pode tomar uma ação ou posição em representação da UE, mas apenas por unanimidade. Também pode publicar uma resolução para implementar tal ato. Nesse caso, a votação por maioria qualificada aplicar-se-ia, exceto para atos de implementação relativos à ação militarizada ou de defesa (artigo 31, n.º 2 do TUE).

Outra alternativa possível visa a intervenção da AR/VP, podendo esta emitir uma declaração em nome União, por norma concertada com os 27 Estados-membros, todavia, se a situação assim o exigir, pode-o fazer sem proceder à consulta.

[687] A UE pode reprimir a conduta de autores de graves ciberataques por via da imposição de medidas restritivas (sanções). Estas medidas podem ser dirigidas a funcionários governamentais de Estados terceiros, empresas Estatais ou outras pessoas físicas ou jurídicas. Nesta situação é obrigatório o voto por unanimidade no Conselho, sendo que o ato deve ser conforme os objetivos da PESC ao abrigo do artigo 24.º, n.º 1 do TUE. A imposição de medidas restritivas ocorrer por duas vias, a saber: 1) as sanções autónomas da UE; e 2) aquelas que a UE, de forma subsidiária, tem a obrigação de impor na sequência de uma resolução do CSNU.

[688] O TL inclui cláusulas de solidariedade e assistência mútua, que podem ser invocadas por um Estado-membro caso venha a ser alvo de um ciberataque, caso a situação assim o permita.

A cláusula de solidariedade (artigo 222.º do TFUE) estipula que os Estados Membros da UE fornecem apoio mútuo, se um, ou vários deles forem vítimas de ataques terroristas, ou vítimas de uma catástrofe natural ou de origem humana (ex. ciberataque de escala ou nível de intensidade apreciável).

A cláusula de assistência mútua, inscrita no artigo 42.º, n.º 7 do TUE, corresponde aproximadamente aos desígnios do artigo 5.º da NATO, embora nem todos os membros da NATO são membros da UE, sendo que a primeira tem precedência face à segunda face a um ciberataque, todavia, dependo de quais os Estados em causa, pois estes são soberanos para decidir nesta matéria.

provided by the Internet and the use of Information and Communication Technologies (ICTs). We strongly promote a global, open, stable, peaceful and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply, supporting the acceleration of social, political and economic development."[689].

Esta vertente da diplomacia europeia, com sustentação jurídica no artigo 21.º do TUE, e posteriormente no Regulamento 2019/796, promove a aplicação da justiça no ciberespaço numa jurisdição capaz de dar um sinal a nível internacional da capacidade de deter e reprimir os criminosos no ciberespaço.

Porventura, uma postura mais aberta e assertiva, por meio de um diálogo bilateral com a Rússia, China ou Irão, ou mesmo, tentar encontrar espaço para acordos bilaterais com estes Estados poderia reforçar a posição construtiva e ativa União no ciberespaço[690]. Paralelamente, a UE poderia reforçar a cooperação com atores congéneres ao nível inter-regional, em especial, com a OSCE, ASEAN, OAS e União Africana, de forma a perceber quais seriam as suas agendas e objetivos, ao mesmo tempo que promovia os seus valores e ambições[691]. A UE poderia liderar estes diálogos de forma a ser um ator promotor da mediação regional e até internacional, capitalizando politicante a sua abertura para o diálogo e incentivando as organizações ao intercâmbio de informações[692].

O primeiro desafio que a comunidade internacional, e particularmente a UE enfrenta, passa pela aproximação de um mecanismo capaz de vincular regional e internacionalmente os Estados, de forma a que seja exigias responsabilidades face a factos internacionalmente ilícitos perpetrados no ciberespaço. Isso acontece, por exemplo, ao nível do Conselho da Europa na Convenção de Budapeste, todavia este não serve como a necessária eficaz face aos desafios de prova digita atuais, paralelamente, Estados como a Rússia não assinaram nem ratificação este instrumento e, por essa via não são criadas obrigações jurídicas para estes Estados, sem prejuízo de todos aqueles que já aderiram e se vincularam internacionalmente a esta Convenção.

---

[689] Conselho Europeu e Conselho da União Europeia, *Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace*, 2020, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace/.

[690] Para um consulta completa aos alegados ciberataques lançados pela Rússia contra a Geórgia, *v*., https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/.

[691] Annegret Bendiek b), *op. cit*., disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf.

[692] *Ibidem.*

O segundo desafio versa sobre os baixos custos políticos de lançar um ciberataque, isto é, as facilidades com que alguns atores internacionais conseguem utilizar o ciberespaço para perpetrar graves danos aos Estados. Aqui a monitorização dos nichos tecnológicos pode ser uma ferramenta importante naquilo que toca ao arsenal cibernético que os Estados possuem e promovem dentro de portas. Essa monitorização poderia ser levada a cabo por via da monitorização estatística da indústria tecnológica dos Estados, podendo ajudar a prever o impacto que uma determinada controvérsia no ciberespaço pudesse vir a constituir, e em última análise poderia vir a ser integrado no sistema de alerta precoce de conflitos da UE[693]. Segundo a Privacy International, a análise de dados do setor industrial ou a videovigilância industrial, a nível europeu, apresenta números com alguma expressão, sendo o Reino Unido o local onde se encontra o maior número destas organizações a operar (ver anexo D).

16 A importância da produção de informações no âmbito do apoio à decisão em contexto multidimensional: o caso da Federação Russa

O *homini* já experienciou vários tipos de sociedades da informação, pelo menos desde a Idade do Bronze, Era que marcou a invenção da proto escrita (Quarto Milênio a.C), final do Neolítico na Mesopotâmia e noutras regiões do mundo. Todavia, tem sido veiculado que se vem assistindo à revolução das informações[694]. Neste sentido é importante esclarecer que fruto da entrada do domínio *ciber* na vida humana foram operadas drásticas mudanças no estilo de vida das sociedades, sendo que o bem-estar individual e social passou a depender, em grande medida, da boa gestão e eficiência do ciclo de vida das informações[695][696].

[693] Este mecanismo funciona com sustentação jurídica assente no artigo 21.º, n.º 2, alínea c) do TUE e sob a égide da SEAE. Para mais informações V, http://www.eeas.europa.eu/archives/docs/cfsp/conflict_prevention/docs/201409_factsheet_conflict_earth_warning_en.pdf.

[694] Segundo Rui Pereira e Alice Feteira, as informações podem ser " (...) *entendidas como um conjunto de elementos disponíveis, devidamente "recortados", valorados e interpretados, representam um instrumento de auxílio à tomada de decisão política, de natureza estartégica e tática, e uma garantia na defesa dos valores estruturantes do Estdo de Direito democrático*". Rui Pereira e Alice Feiteira, Enciclopédia de Direito e Segurança, Jorge Bacelar Gouveia e Sofia Santos (coord.), Alemedina, 2015, p. 340.

[695] Luciano Floridi, *Information: A Very Short Introdution*, Oxford University Press, 2010.

[696] *Ibidem*.

Os dados e a informação sempre representaram um certo valor697 e interesses a diferentes subgrupos de atores, entre eles os espiões (indústria), criminosos (fraude, roubo, extorsão) ou às autoridades estatais (analistas de dados, monitorização, planeamento)698699. A utilização de novas tecnologias pode constituir uma ameaça se o propósito da sua utilização for mal-intencionado, com por exemplo, o uso de inteligência artificial com "falsos positivos" 700, colocando em causa a forma como são obtidos os nossos dados e informações e, em última análise podem colocar em causa a dignidade humana e a própria identidade digital dos indivíduos.

A informação é o elemento central para comandar o ciberespaço (em tempos de paz e em temos de conflito), e de igual importância é a infraestrutura que permite que a informação flua no palco internacional. Assim, a tríade que compõe a "guerra da informação", é composta pelas "armas tecnológicas", o controlo comunicacional e ciberataques, que se encontram distribuídos pelas infraestruturas críticas nacionais com componentes defensivas e ofensivas701.

Existe um desequilíbrio quando se trata de gestão de informação e modelos de atuação pública no ciberespaço. A guerra ideológica é levada ao extremo, ideologias podem despoletar grandes desafios com a massificação da interconectividade global, mesmo ao nível militar, com a adequação de conceitos e conceções sobre a guerra tradicional, agora aplicada ao ciberespaço. Em termos práticos, estamos perante um "(…) challenge for information strategy, a concept that calls for knowing the enemy, shaping public consciousness, and crafting persuasive messages for friend and foe alike. It is about getting the contents of those messages right, while finding the best conduits. It is about deploying inviting, meaningful narratives to win the battle of the story702.

O desafio contemporâneo para os Estados concerta-se em primeiro por perceber a qualidade do agente responsável que veicula a retórica digital pela via dos media, observando um nível de conflitualidade muito particular, conceptualizando as estratégias

---

697 Nesse sentido, *v*. K. Williams, Dana-Marie Thomas, Latoya Johnson, The Value of Personal Information, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, Eugenie de Silva (ed), Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series, IGI, p. 163-174.

698 Eduardo Gelbstein, *op*. *cit*., p.123.

699 Cfr. Philip Taylor, Public Diplomacy and Strategic Communications, in: *Routledge Handbook of Public Diplomacy*, Nancy Snow e Philip Taylor (eds), Routledge International Handbooks, pp.12-16.

700 ENISA, *Strengthening Network and Information Security and Protecting Against Online Disinformation* ("Fake News"), 2018, p. 4.

701 Mariarosaria Taddeo, Just Information Warfare, in*: Ethics and Policies for Cyber Operations: NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Mariarosaria Taddeo e Ludovica Glorioso (eds), Philosophical Studies Series, Springer, p.68-72.

702 *Ibidem*.

da Informação. A informação como "arma" e como recurso enceta desafios à sua própria modelação em plena época histórica da humanidade em que experimentamos a transação digital, assumindo uma preponderância elevada para os cidadãos. Ora, se no meio da transação digital os media são coaptados pelas estratégias de informação laterais dos estados, a sua perceção passa a ser enviesada, o ciberespaço passa a considerar-se como o placo do autoritarismo digital.

Vicente Freire e Alexandre Caldas sintetizam, "(…) a Estratégia da informação dá sentido a ação a ser conduzida, proporcionando um contexto e contribuindo para maximizar os seus efeitos"703. A Rússia inscreve na sua doutrina militar "(…) exerting simultaneous pressure on the enemy throughout the enemy's territory in the global information space (…)", revendo a sua longa história de desinformação que alude à época dos Czares. Valeri Gerasimov, chefe do Estado-Maior das Forças Armadas Russas, afirmou que "as regras da guerra "eles próprios mudaram significativamente, as opções não militares passaram a desempenhar um papel mais importante na realização de objetivos políticos e estratégicos e, em algumas situações, são muito superiores ao poder das armas"704.

A influência e propaganda dos Estados, por meio de agências ou órgãos sob a égide destes passa a ser prática comum em território interno e em território estrangeiro705. A segurança da informação em ambiente digital, apesar de apresentar uma vertente técnica do ponto de vista da ciência informática, é reconhecida pela sua vertente estratégia para os atores internacionais que se posicionam de forma destacada no ciberespaço e, através da geopolítica aplicada ao ciberespaço tentam ganhar uma posição dominante. Por exemplo, uma das estratégias de guerra da informação da federação russa, a Maskirovka706 (traduzido significa camuflagem ou engano), representa uma técnica utilizada tanto em tempos de paz como em tempos de guerra, sendo aplicada

---

703 Vicente Freire e Alexandre Caldas, *op. cit*., pp.129-133.

704 Michael Connell e Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA Analysis & Solutions*, www.dtic.mil/get-tr-doc/pdf?AD=AD1019062*; Nicholas Fedyk, "Russian 'New Generation' Warfare: Theory, Practice, and Lessons for U.S. Strategists," Small Wars Journal,* http://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D warfaretheory-practice-and-lessons-for-us-strategists., *apud*, James Lewis, op. cit., p.7.

705 Realçamos que esta condição não é exclusiva dos Estados, outros atores da Comunidade Internacional, como grupos não governamentais ou organizações internacionais utilizam a estratégica comunicacional para se posicionar e ganhar influência ao nível internacional. Para mais informações, *v*. Marc Jungblut, *Strategic Communication and its Role in Conflict News*, Springer VS, 2019.

706 Trata-se de uma técnica que visa influenciar o inimigo, dando-lhe uma falsa sensação de controlo sobre a situação, fazendo-o assim agir de uma forma previsível, forma essa que é prejudicial aos seus próprios interesses.

correntemente à desinformação707708. Historicamente, a Federação Russa no seu ramo militar e na sua elite política apresenta especialistas experientes na aplicação desta técnica709, nomeadamente através do serviço FSB, onde agentes altamente treinados tentam influenciar e persuadir no ciberespaço com um determinado propósito, seja ele de ordem política-ideológica, financeira, ou outra710.

Neste sentido, os ciberataques perpetrados por hacktivistas russos ao Estado estoniano em 2007, associada à transferência de um monumento militar soviético na capital de Tallin representaram as novas formas de utilização tecnologia em favor dos regimes em linha com os seus objetivos geoestratégicos, ficando postulada a extensão entre o domínio físico e virtual num conflito. Ambos os acontecimentos observaram a participação ativa de operações psicológicas, por via de campanha de informações, a diversos níveis, por agentes locais e nacionais sob influência pró-russa. Além das interferências altamente intrusivas e destrutivas nos sistemas de informação e comunicação da Estónia, haviam "(…) prominent visual reminders of information command and control.". Por exemplo, "there were defacements of Georgian governmental websites with scurrilous portraits of President Shakashvili looking like Adolf Hitler."711.

Durante a anexação da Crimeia pela Federação Russa, e mesmo durante os incidentes na zona oriental da Ucrânia ocorreram ciberoperações psicológicas em sítios da Internet, como blogs pró-defesa da Rússia. Quem criticasse a doutrina pró-russa era sujeito a violentos ataques em ambiente digital, entre outras formas de desinformação, utilização de bots de spam, até à propaganda massiva russa nos blogs, redes sociais e media em geral, em vários idiomas e de forma segmentada712. Como sustenta James Lewis, "The Russians adopted traditional disinformation techniques to the new technologies and

---

707 Cerwyn Moore, Russia and Desinformation: Maskirovkam, in: *Centre for Research and Evidence on Security Threats (CREST)*, University of Birmingham, 2019, pp. 4-12.

708 A complexidade da investigação no ciberespçao convoca esforços mulitlareais, nomeadamente quando os indícios podem ser encobertos sob o dorso Estatal, como alegadamente ocorre na Federação Russa , através da "*Russian Internet Research Agency*" pela utilização de tecnologias emergentes com potencial efetivo desconhecido, mas que pode observar uma esclada nesfasta com impacto na Comunidade Interancional, em particular, nas instituições democráticas. Parlamento Europeu, *Regulating disinformation with artificial intelligence: Effects of disinformation initiatives on freedom of expression and media pluralism*, 2019, p.12-19.

709 Roland Heickero, Russia´s Information Warfare Capabilities, in: *Current and Emerging Trends in Cyber Operations*, Palgrave Macmillans Studies in Cybercrime and Security, 2015, p.76.

710 Serviço federal de segurança - órgão executivo com a competência de implementar políticas governamentais de segurança, sob a supervisão do presidente da federação russa, *v*., http://government.ru/en/department/113/. Cfr. Sanjay Sharma, *Data Privacy and GDPR Handbook*, Wiley, 2020, pp. 372-379.

711 Roland Heickero, *op*. *cit*., p.78.

712 *Ibidem*.

honed their skills by first using trolls, fake news, and damaging leaks again domestic opponents in the first years of Putin's rule. Influenced by both traditional Russian espionage techniques and by new military doctrines, Russia has used the internet as a weapon against the West"713.

O controlo dos média, nas várias franjas da comunidade nacional, regional ou internacional é a pedra angular de uma estratégia informacional extensa, que vai desde a propaganda e manipulação, até à distorção de informação, que sustenta ou amplifica a projeção de forças terrestres convencionais e atinge a sua máxima expressão quando ocorre um cenário de guerra híbrida, capaz de envolver tanto pessoas singulares de um Estado como as suas forças armadas714715. Este tipo de ameaça híbrida, por via do emprego de técnicas de desinformação, combinadas com outro tipo de técnicas, mais ou menos coercivas, mais ou menos subversivas, mais ou menos militarizadas, mantem-se abaixo do limiar de guerra (formalmente declarada), todavia empregam meios e utilizam as informações para atingir as vulnerabilidades de atores não Estatais, mas sobretudo atores estatais de forma a minar o processo de tomadas de decisão e criar instabilidade, desconfiança, ambiguidade e incerteza nos cidadãos e nas instituições. Fica claro o tipo de ameaça difusa que a União e os seus Estados-membros enfrentam, todavia cabe na responsabilidade dos Estados zelar pela segurança e bem estar dos cidadãos, capacitando recursos humanos e lógicos para prevenir e reprimir este tipo de ameaças e velar pela manutenção da lei e da ordem individual e coletiva716.

A combinação de uma estratégia conjunta, entre mundo físico e operações em ambiente digital, concerta uma técnica avançada da federação russa, à qual alguns analistas consideram como a sexta geração de guerra717.

A superioridade em relação ao controlo das informações constituí uma vantagem competitiva em relação aos demais interessados e deriva da aliança entre, por um lado, o sucesso no domínio físico (envio de efetivos militares para ocupação de um espaço físico e agentes no teatro de operações) e, por outro lado, no domínio do ciberespaço (ações

[713] James Lewis, *Cognitive Effect and State Conflict in Cyberspace*, Center for Strategic & International Studies, 2018, p.6.
[714] Luís Camelo dos Santos et. alli, Defesa do Ciberespaço, Contributos para uma estratégia nacional de ciberdefesa, in: *idn cadernos*, p.33.
[715] Cfr. Mark Kilbane, Military Psychological Operations as Public Diplomacy, in: *Routledge Handbook of Public Diplomacy*, Nancy Snow e Philip Taylor (eds), Routledge International Handbooks, p. 187-191.
[716] Cfr. Ana Maria Guerra Martins, *op. cit*., p. 407.
[717] *Ibidem*, p.76.

estrategicamente plantadas para um determinado público), este último, decisivo para o sucesso da operação pelo seu modus operandi inovador e difuso.

Charlotte Wagnsson e Maria Hellman, suportadas pelo estudo da East StratCom Task Force e a Desinformation Digest, sugerem que a União deve preocupar-se da forma como representa a Federação Russa na sua comunicação, sugerindo operar uma reforma na abordagem à estratégia russa, pela promoção de vozes alternativas que contestem a governança, seja a nível local, regional ou nacional718. Adiantam ainda a forma como é importante expor as alegadas violações de princípios e normas internacionais, sem que para isso se recorra à inferiorização da Federação Russa719720.

As operações cibernéticas lançadas contra a Estónia e a Geórgia foram bem coordenadas, demonstrando um conhecimento prévio das vulnerabilidades dos ativos e dos alvos de ataque. Um conhecimento situacional da realidade apurado, mesmo ao nível do risco e das vulnerabilidades associado a cada Estado implicou graves danos aos sistemas de redes e infraestruturas críticas nacionais.

Os civis e grupos nacionalistas que perpetraram os ataques (DDoS, injeções SQL e desfiguração de sites) na Geórgia são cidadãos altamente especializados, recrutados em redes sociais ou redes equivalentes, motivados pelos ganhos financeiros, com assistência de organizações criminosas (ex: Russian Business Network – RBN ou o grupo Rock Phish) para o fornecimento de malware específico. Uma vez recrutados, aplicam a técnica de forma inovadora em agências governamentais, sites de notícias e instituições financeiras721. Os ataques diminuíram a capacidade de defesa da Geórgia por via da divisão de recursos em diferentes áreas face às emergências vividas, associada à lacuna informacional dos media que não foi deteta ou interpretada.

Como sustenta Roland Heickero, "*These events show a new course of action that may become normative for future cyber conflict."*[722]. Atendendo às circunstâncias do Estado Estoniano à época dos ataques, com baixa maturidade em termos de ligação e dependência à rede e infraestruturas críticas, as consequências resultaram num nível de

---

[718] Charlotte Wagnsson e Maria Hellman, Normative Power Europe Caving in? EU Under Pressure of Russian Information Warfare, in: *JCMS: Journal of Common Market Studies*, Vol. 56, Issue 5, 2018, pp. 1161-1172.

[719] *Ibidem*.

[720] A posição da Federação Russa vem nesse sentido, e apela ao cuidado político da imputação de ciberataques e a respetiva necessidade de demostração de indícios técnicos, tendo que avançar com uma fundamentação antes de partir para uma acusação pública, *v*. https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

[721] Roland Heickero, *op*. *cit*., p.76.

[722] *Ibidem*, p.81.

perturbação baixo, todavia, se um Estado com maior dependência no acesso à Rede e infraestruturas digitais for alvo de um ataque análogo pode ser altamente disruptivo a todos os níveis experimentados.

A componente da guerra da informação está a ganhar um peso no cenário internacional, sendo decisiva para a Federação Russa, que decide em função do espetro informacional que retira das técnicas empregues no seio da Comunidade Internacional. No final da guerra fria, a Rússia desenvolveu um conjunto de técnicas e operações contínuas de informações para aplicação quer em tempo de paz, quer em atos preparatórios de conflito, ou mesmo durante o decorrer dos mesmos[723]. Este tipo de estratégia assenta no controlo da narrativa através da componente das informações difundidas através dos media e, uma vez obtido esse controlo é possível guiar e manipular a informação de forma a ganhar poder e influência sobre os adversários internos e/ou internacionais[724]. Mas repare-se que a estratégia russa não visa diretamente causar danos às instituições do ocidente, mas despertar as desigualdades e descontentamento social, que levam ao sentimento de mudança social e revolta afetando indiretamente instituições e órgãos democráticos.

[723] Uma dessas técnicas remonta ao século XIX, com a utilizam da técnica do "*controlo reflexivo*", enquanto que na Europa e América predomina o vocábulo "operações de informação", que assentam na aplicação de processos cognitivos de modo a afetar e moldar o pensamento dos oponentes e neutrais, sendo este processo descrito como central da doutrina militar russa. James Lewis, *op. cit*., 2018, pp.6-7.

[724] De forma semelhante, o extremismo online tem uma forma muita própria de ser disseminada nos media. Cabe aos Estados a tarefa central e necessária de desconstruir a mensagem transmitida de forma a mitigar este tipo de fenómenos na Internet, dai a urgente aposta na literacia digital e alerta para a necessidade de verificar e questionar as fontes. Para mais informações *v*. Rachel Briggs e Sebastien Feve, Policy Briefing: Countering The Appeal of Extremism Online, in: *Institute for Strategic Dialogue*, 2013, p. 5-22.

Conclusão

A segurança da informação encontra no ordenamento jurídico da União Europeia a sua previsão em várias normas, que se refletem também na ligação umbilical com a proteção de dados para a proteção dos seus cidadãos.

Segurança da informação, proteção de dados e privacidade podem ser tratados de forma independente, todavia face à conjuntura tecnológica devem ser alvo de tratamento e interpretação conjunta e complementar, mesmo por força do amplo quadro regulatório. A informação, baseada nos dados, representa um determinado valor, e por essa via, é alvo da perpetração de crimes no ciberespaço, convocando à responsabilização coletiva dos agentes que nele coabitam. Os princípios subjacentes a um Estado de Direito podem ser fortemente colocados à prova no ciberespaço, sendo este último caracterizado por um ecossistema errático, complexo, difuso e interdependente, operado por máquinas físicas que interligam indivíduos virtualmente.

Existe ainda um importante e necessário trabalho a promover na defesa dos direitos fundamentais no ciberespaço, papel que cabe não só às autoridades complentes pela aplicação da lei, mas também muito dependente da alteração do paradigma social para a segurança da informação na sociedade, sendo que este último determinará o sucesso da segurança digital da comunidade.

O Estado, como principal sujeito da Comunidade Internacional multipolar, enfrenta responsabilidades primárias e ultra desafiantes, desde logo no plano interno na proteção das infraestruturas críticas nacionais, e no plano externo na afirmação de um quadro jurídico que estabeleça obrigações para os demais Estados. Convocamos à reflexão de conceitos tradicionais como jurisdição, território, soberania, uso de força, ataque armado, legítima defesa ou diplomacia. A harmonização destes conceitos regionalmente e ao nível da Comunidade Internacional é preponderante para o compromisso de garantir um espaço seguro e aberto para todos os indivíduos nas relações internacionais.

O equilíbrio contemporâneo de forças no ciberespaço convoca sinergias entre público e privado, pela sua aplicação integral à sociedade. Os perigos veiculados pelas tecnologias emergentes, podem colocar em causa valores basilares da Nações, isso fica bem patente na discussão de implementação da tecnologia 5G ou no novo projeto de cabo submarino para o ártico.

Fechamos com a perceção incerta quanto ao futuro do ciberespaço, inferimos, porém, a certeza de uma sociedade e cultura muito mais dependentes à Rede, ameaçando a soberania (digital) dos Estados por via da geopolítica de informações nas relações internacionais.

Bibliografia

Adérito Grazina Rodrigues, O papel do Ponto Único de Contacto para a Cooperação Policial Internacional face ao quadro de ameaças e riscos, in: *Instituto Universitário Militar*, Curso de Estado Maior Conjunto, 2019, Lisboa, pp. 6-20.

Advisory Commite on Public Internacional Law, Government Response to the AIV/CAVV, Report on Cyber Warfare, p. 5, disponível para consulta em: https://www.advisorycommitteeinternationallaw.nl/publications/government-response/2012/04/06/cyber-warfare.

Alastair Black e Rodney Brunt, Information Management in MI5 Before the Age of the Computer, *Journal Intelligence and National Security*, Vol. 16, Issue 2, 2010, p.158-165.

Alexandre Guerreiro, Direito Internacional e o combate ao terrorismo e ao ciberterrorismo, in: *O Direito Internacional e o uso da força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, p. 337.

Ana Azurmendim, Spain: The Right to be Forgotten, The Right to Privacy and the Initiative Facing the New Challenges of the Information Society, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), Springer, 2017, p. 25-27.

Ana Guerra Martins, *Manual de Direito da União Europeia*, Lisboa, Almedina, pp. 277-279.

Ana Maria Guerra Martins, *Os Desafios Contemporâneos à Ação Externa da União Europeia: Lições de Direito Internacional Público II*, Almedina, 2018, p. 109.

Annegret Bendiek a), European Cyber Security Policy, in: *SWP Research Paper*, N.º 5. Disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf.

Annegret Bendiek b), The EU as a Force for Peace in International Cyber Diplomacy, in: *SWP Commnet*, N.º19, 2018, disponível para consulta em: https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf.

Anthony Rutkowski, Youki Kadobayashi, Inette Furey, *CYBEX – The Cybersecurity Information Exchange Framework (X.1500), ACM SIGCOMM Computer Communication Review*, Vol. 40, N.º 5, 2010, p. 60.

Barry Buzan, Ole Waever e Jaap de Wilde, *Security: A new framework for analysis*, Boulder, Lynne Rienner, 1998.

Bart van der Sloot, Legal Fundamentalism: Is Data Protection Really a Fundamental Right?, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p. 5-8.

Black's Law Dictionary, 9ª Edição, Bryan Garner (ed), West, 2009, p.1730.

Brant Reilly, Doing More with More: The Efficacy of Big Data in the Intelligence Community, in: *American Intelligence Journal*, N.º32, 2015, p.18-24.

Bundesakademie für Sicherheitspolitik, *Cyber-Realitat zwischen Freiheit und Sicherheit*, 2015, disponível para consulta em: https://www.baks.bund.de/de/aktuelles/cyber-realitaet-zwischen-freiheit-und-sicherheit.

Carlos Blanco de Morais, O Direiot ao Uso de Força pelos Estados em tempos de Unilateralismo Multipolar, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, pp.45-93.

Center for Digital Strategies: Tuck at Dartmouth, Cyber/information Security in the Digital Age: A Roundtable Overview European Chapter Discussion, in: *Roundtable on Digital Strategies*, p. 4 e ss.

Centro Nacional de Cibersegurança, Recursos, disponível para consulta em: https://www.cncs.gov.pt/recursos/glossario/.

Cerwyn Moore, Russia and Desinformation: Maskirovkam, in: *Centre for Research and Evidence on Security Threats (CREST)*, University of Birmingham, 2019, pp. 4-12.

Charlotte Wagnsson e Maria Hellman, Normative Power Europe Caving in? EU Under Pressure of Russian Information Warfare, in: *JCMS: Journal of Common Market Studies*, Vol. 56, Issue 5, 2018, pp. 1161-1172.

Christian Reus-Smit, Culture, Diversity and Technology, in: *Technologies of International Relations Continuity and Change*, Carolin Kaltofen, Madeline Carr e Michele Acuto (eds), Plagrave Macmillanm, 2019, p.72.

Christopher Kuner, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines, in*: LSE Legal Studies Working Paper*, LSE Law, N.º 3, 2015, p. 20-22.

Christopher Lentz, A State's Duty to Prevent and Respond to Cyberterrorist Acts, in: *Chicago Journal of International Law,* 10, 2010, pp. 820 e ss, *apud*, Marco Roscini, p. 88.

Comissão Europeia, Article 29 Working Party, disponível para consulta em: https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

Comissão Europeia, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Delivering an area of freedom, security and justice for Europe's citizens - Action Plan Implementing the Stockholm Programme*, COM/2010/0171 final, disponível para consulta em: https://ipexl.europarl.europa.eu/IPEXL-WEB/dossier/document.do?code=COM&year=2010&number=171&extension=FIN&appLng=PT.

Comissão Europeia, Comunicação conjunta ao Parlamento Europeu e ao Conselho*: Resiliência, dissuasão e defesa: reforçar a cibersegurança na EU*, 2017, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia da União Europeia para a cibersegurança:Um ciberespaço aberto, seguro e protegido*, 2013, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT.

Comissão Europeia, Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões a Estratégia para o Mercado Único Digital na Europa, *Estratégia para o Mercado Único Digital na Europa*, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52015DC0192.

Comissão Europeia, *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Comissão Europeia, *Decisão do Conselho: que autoriza os Estados-Membros a ratificar, no interesse da União Europeia, o Protocolo que altera a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de*

Dados de Caráter Pessoal (STE 108), 2018, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018PC0451&from=EN.

Comissão Europeia, *European Information Exchange Model (EIXM)*, 2020, disponível para consulta em: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/eixm_en.

Comissão Europeia, *Growth, competitiveness, employment: The challenges and ways forward into the 21st century*, 1994, disponível para consulta em: https://op.europa.eu/en/publication-detail/-/publication/0d563bc1-f17e-48ab-bb2a-9dd9a31d5004.

Comissão Europeia, Joint EU-U.S. press statement following the EU-U.S. Justice and Home Affairs Ministerial meeting, 2016, disponível para consulta em: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_2040.

Comissão Europeia, *Migration and Home Affairs*, 2019, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

Comissão Europeia, *State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks*, 2017, disponível para consulta em: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193.

Comissão Europeia, *The EU Cybersecurity Act*, 2020, dispoonível para consulta em: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

Comité Económico e Social Europeu, *Parecer do Comité Económico e Social Europeu sobre a «Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Para uma economia dos dados*

próspera» [COM(2014) 442 final], 2015, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52014AE5300.

Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*", 2009, disponível para consulta em:https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

Conselho da Europa, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, disponível para consulta em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=EmtNHDeW.

Conselho da União Europeia, *Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G*, 2019, https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

Conselho da União Europeia, de 4 de dezembro de 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/12/04/better-connectivity-eu-adopts-telecoms-reform/.

Conselho da União Europeia, *Decisão do Conselho relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros*, 2019, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/pt/pdf.

Conselho da União Europeia, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 2020, disponível para consulta em: https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.

Conselho da União Europeia, *Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018)*, 2018, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pt/pdf.

Conselho da União Europeia, *Recomendação de Decisão do Conselho que autoriza a abertura de negociações de um acordo entre a União Europeia e o Canadá para a transferência e utilização dos registos de identificação dos passageiros (PNR) para fins de prevenção e luta contra o terrorismo e outros crimes transnacionais graves*, de 23 de outubro de 2017, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-13490-2017-INIT/pt/pdf.

Conselho Europeu e Conselho da União Europeia, *Ciberataques: Conselho pode agora impor sanções*, 2019, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

Conselho Europeu e Conselho da União Europeia, *Ciberatividades maliciosas: Conselho adota conclusões*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/04/16/malicious-cyber-activities-council-adopts-conclusions/.

Conselho Europeu e Conselho da União Europeia, *Conselho Europeu, 18 de outubro de 2018*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/meetings/european-council/2018/10/18/.

Conselho Europeu e Conselho da União Europeia, *Cyber-attacks: Council is now able to impose sanctions*, 2019, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions/.

Conselho Europeu e Conselho da União Europeia, *Declaração da alta representante, em nome da UE, sobre o respeito pela ordem assente em regras no ciberespaço*, 2019, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2019/04/12/declaration-by-the-high-representative-on-behalf-of-the-eu-on-respect-for-the-rules-based-order-in-cyberspace/.

Conselho Europeu e Conselho da União Europeia, *Declaration by the High Representative Josep Borrell on behalf of the EU: European Union response to promote international security and stability in cyberspace*, 2020, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-eu-european-union-response-to-promote-international-security-and-stability-in-cyberspace/.

Conselho Europeu e Conselho da União Europeia, *EU imposes the first ever sanctions against cyber-attacks*, 2020, disponível para consulta em: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

Conselho Europeu e Conselho da União Europeia, *UE mais resistente à cibercriminalidade graças ao apoio do Conselho ao acordo sobre certificação comum e a uma agência fortalecida*, 2018, disponível para consulta em: https://www.consilium.europa.eu/pt/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/.

Council of Europe, *International and multi-stakeholder co-operation on cross-border Internet*, multi-stakeholder co-operation on cross-border Internet, 2010. www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf.

Council of Europe, *International and multi-stakeholder co-operation on cross-border Internet*, Interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet, 2010, disponível para consulta em: www.coe.int/t/dghl/standardsetting/media/MC-S-CI/MC-S-CI%20Interim%20Report.pdf.

Cyber Defence Smart Defence Projects Conference, *Multinational Cyber Defence Capability Development (MNCD2)*, 2016, disponível para consulta em: https://academiamilitar.pt/images/CDSDP2016/Apresentacoes/1.NATO-CD-Smart-Defence-Projects_MNCD2.pdf.

Cyberspace, 2013, p. 19, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

Dan Efrony e Yuval Shany, A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice, in: *American Journal of International Law*, N.º 4, 2018 pp. 583-657, *apud* Dennis Broeders, Els De Busser and Patryk Pawlak, p. 10.

Dário Moura Vicente e Sofia de Vasconcelos Casimiro, Data Protection in the Internet: General Report, in: *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law, Springer., Vol. 38, 2020, p.1.

David Kim e Michael Solomon, *Fundamentals of Information Systems Security*, Information Systems Security, 3rd Edition, 2018, p. 51.

David Omand, Understanding Digital Intelligence: A British View, in*: National Security and Counterintelligence in the Era of Cyber Espionage*, Eugenie de Silva (Ed), IGI, 2016, pp. 99 e ss.

David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Almedina, Lisboa, 2017, p.51.

David Ronfeldt e John Arquilla, Noopolitik: A New Paradigm for Public Diplomacy, in: *Routledge Handbook of Public Diplomacy*, Nancy Snow e Philip Taylor (eds), Routledge International Handbooks, p. 354.

Dennis Broeders, Els Busser e Patryk Pawlak, Three tales of attribution in cyberspace: Criminal law, international law and policy debates, in: *The Hague Program For Cyber Norms,* Policy Brief, 2020, p. 3.

Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Georgetown University, p.3.

Eduardo Correia Baptista, *Direito Internacional Público*, Vol. II, AAFDL, 2015, p. 430.

Eduardo Gelbstein, The War of Attrition in Cyber-Space or "Cyber-Attacks", "Cyber-War" and "Cyber-Terrorism", in: *Conselho de Segurança da ONU*, idn nação e defesa, Instituto da Defesa Nacional, n.º 135, N.º 135-5ª Série, p. 125.

Elisa Orrù, Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance, in: *Data Protection and Privacy: (In) visibilities and*

Infrastructures, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p.119.

Elisa Orrù, Minimum Harm by Design: Reworking Privacy by Design to Mitigate the Risks of Surveillance, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p. 11-116.

ENISA, *Cyber espionage ENISA Threat Landscape*, 2020, p. 3.

ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2018, pp. 26-29.

ENISA, *EISAS – European Information Sharing and Alerting System*, 2013, p.2.

ENISA, *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps*, Presidency progress report N.º 14711/16, 2016, disponível para consulta em: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf.

ENISA, *ENISA overview of cybersecurity and related terminology*, 2017, disponível para consulta em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

ENISA, ENISA Threat Landscape Report 2017, 2017, disponível para coinsulta em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

ENISA, *ENISA's Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity*, 2016, p. 11.

ENISA, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*, 2012, p. 4.

ENISA, *Status of Privacy and NIS course curricula in Member States*, 2015, disponível para consulta em: https://www.enisa.europa.eu/publications/status-of-privacy-and-nis-course-curricula-in-eu-member-states.

ENISA, *Strengthening Network & Information Security & Protection Against People Online Disinformation ("Fake News")*, 2018, disponível para consulta em: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/fake-news/.

ENISA a), *Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents*, v.1.0, 2018, p. 17.

European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013, p. 19, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

European Security and Defence College, *Hanbook on CSDP Missions and Operations the Commons an security and Defence Policy of the European Union*, Jochen Rehrl e Galia Glume (ed), 2015, p.197.

European Strategy and Policy Analysis System e European Union Institute for Security Studies, *Global Trends to 2030: Challenges and Choices for Europe*, 2020, disponível para consulta em: https://www.iss.europa.eu/sites/default/files/EUISSFiles/ESPAS_Report.pdf.

Europol, *European Migrant Smuggling Centre*, 2020, disponível para consulta em: https://www.europol.europa.eu/about-europol/european-migrant-smuggling-centre-emsc.

Europol, *European Union Terrorism Situation and Trend Report 2020*, 2020, disponível para consulta em: https://www.europol.europa.eu/tesat-report.

Europol, *Europol Analysis Projects*, 2020, disponível para consulta em: https://www.europol.europa.eu/crime-areas-trends/europol-analysis-projects.

Europol, *Europol Information System (EIS)*, 2020, disponível para consulta em: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system.

Europol, *Internet Organised Crime Threat Assessment (IOCTA*), 2016, disponível para consulta em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2020, p.24.

Europol, *Secure Information Exchange Network Application*, 2020, disponível para consulta em: https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena.

Europol, *The EU Serious and Organised Crime Threat Assessment (SOCTA)*, 2017, p. 29.

Evgeny Morozov, The Real Privacy Problem, in: *MIT Technology Review*, 2013.

Federico Yaniz, NATO-EU Cooperation Milestones and Challenges Ahead, in: *Security and Defence in Europe*, Martín Ramírez e Jerzy Biziewski (Eds), Springer, 2020, pp. 221-225.

Ficha informativa da Comissão Europeia, de 6 de junho de 2018, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/more-and-better-internet-connectivity-requires-investments-high-speed-and-quality-networks.

Francisco Lima e Mateus Carvalho, O Direito ao apagamento de dados como realidade global, in: *Anuário de Proteção de Dados,* 2019, CEDIS, p.61-63.

François Delerue, Xymena Kurowska e Patryk Pawlak, Reflections on the Pre-draft of the report of the OEWG on developments in the field of ICTs in the context of international security, in: *Research in Focus, EU Cyber Direct: Supporting EU Cyber Diplomacy*, 2020.

Frank Jüris, Handing over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic, *Sinopsis: China in Context and Prespective*, 2020, p. 8 e ss.

Freedom House, *Freedom on the NET 2019*, 2019, p. 24, disponível para consulta em: https://freedomhouse.org/issues/technology-democracy.

George Christou a), The collective securitization of cyberspace in the European Union, in: *West European Politics*, Routledge, Vol. 42, N.º 2, 2019, pp. 285-286.

George Christou b), The European Union and Cybercrime, in: *Cybersecurity in the European Union Resilience and Adaptability in Governance Policy*, 2016, p. 103-104.

Gouvernement of Canada, *Canada's Cyber Security Strategy: For a stronger and more prosperous Canada*, p.7-8.

Hannes Ebert, Contested Cyberspace and Rising Powers, in: *Third World Quarterly*, Routledge, Vol. 34, N.º 6, 2013, p. 1054.

Hans Friedrich, in: *Diese Daten helfen uns,* Interview mit Bundesinnenminister, 2013, disponível para consulta em: https://www.baks.bund.de/de/aktuelles/cyber-realitaet-zwischen-freiheit-und-sicherheit.

Harold Hongju Koh, International Law in Cyberspace Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, in: *Harvard International Law Journal*, Vol. 54, 2012, p. 6.

Heather Harrison Dinniss, Cyber Warfare and the Laws of War, in*: Cambridge University Press*, 2012, p. 74.

Helbert Lin, Offensive Cyber Operations and the Use of Force, in: *National Security Law and Policy*, 2010, p. 39-60, *apud*, Frederic Lemieux, p. 7.

Helena Carrapico e André Barrinha, The EU as a Coherent (Cyber)Security Actor?, in: *Journal of Common Market Studies*, Vol. 55, N.º 6, 2017, p. 1259.

HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge University Press, Cambridge, 2013, p. 49, *apud*, Marco Roscini, p. 49.

Iguehi Ikenwe, Osahon Igbinovia e Ademakhe Elogie, Information Security in the Digital Age: The Case of Developing Countries, in: *Chinese Librarianship: an Internacional Eletronic Journal*, N.º 42, disponível para consulta em: http://www.white-clouds.com/iclc/cliej/cl42IIE.pdf.

Institute for Security Studies, *The CSDP in 2020: The EU's legacy and ambition in security and defence*, Daniel Fiott (ed), Paris, 2020, p. 91-92.

Instituto da Defesa Nacional, Seminário da Defesa Nacional, in: *idn cadernos*, N.º 32, 2019, p. 22.

International Telecommunication Union, Global Information Infrastructure terminology: Terms and definitions, *Y.101*, 2000, p. 37.

Iranian Foreign Minister's address to the UN Security Council, 2012, disponível para consulta em: http:// iran un.org/en/2012/09/28/28-september-2012-2/, *apud*, Marco Roscini, p. 76.

Jacob Sakhnini, et alli., AI and Security of Critical Infrastructure, in: *Handbook of Big Data Privacy*, Kim-Kwang Raymond Choo e Ali Dehghantanha (eds), Springer, 2020, 7 e ss.

James Lewis, *Cognitive Effect and State Conflict in Cyberspace*, Center for Strategic & International Studies, 2018, p.6.

Jean-Marie Henckaerts e Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge University Press, Cambridge, 2005, Vol. I, Rule 6, p. 23, *apud*, Marco Roscini, p. 49.

Jerome Squires, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) C-131/12, in: *Adelaide Law Review*, The University of Adelaide, N.º 35, 2014, p.465.

João Barbas e Carolina Sancho, Cibersegurança e Políticas Públicas: Análise Comparada dos casos chileno e português, in: *idn cadernos*, n.º 29, p.62.

John Ikenberry, The Future of the Liberal World Order: Internationalism After America, in: *Foreign Affairs*, Vol. 90, N.º. 3, 2011, p. 56.

Jorge Bacelar Gouveia, *Direito Internacional da Segurança*, Almedina, 2015, p. 75.

Jorge Bacelar Gouveia, *Encicploédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (coord.), Almedina, 2015, pp. 342-346.

Jornal Oficial da União Europeia, *Acordo entre a União Europeia e a Austrália sobre o tratamento e a transferência de dados do registo de identificação dos passageiros (PNR) pelas transportadoras aéreas para o Serviço Aduaneiro e de Proteção das Fronteiras australiano*, 2012, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22012A0714(01)&from=EN.

Jornal Oficial da União Europeia, *Acordo entre a União Europeia e os Estados Unidos da América sobre o tratamento de dados de mensagens de pagamentos financeiros e a sua transferência da União Europeia para os Estados Unidos para efeitos do Programa de Detecção do Financiamento do Terrorismo*, 2010, disponível para consulta em: https://www.cnpd.pt/home/direitos/EU_EUA_AGREEMENT_TFTP_2_pt.pdf.

Jornal Oficial da União Europeia, *Acordo entre os Estados Unidos da América e a União Europeia sobre a utilização e a transferência dos registos de identificação dos passageiros para o Departamento da Segurança Interna dos Estados*, 2012, disponível para consulta em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22012A0811(01)&from=EN.

José Martins et. alli, Modelo Integrado de atividades para a Gestão de Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais, in: *CyberLaw by CIJIC*, Edição N.º V – 2018, p. 34-59.

José Pina Delgado, Legítima Defesa, in*: Enciclopédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (coord.), Almedina, 201 5, p. 253.

Julie Cohen, What is Privacy For? , in: *Harvard Law Review*, 2013, p. 126.

Justin Morris, Law, power and force in an unbalanced world, in: *International Conflict and Security Law*, Essays in Memory of Hilaire McCoubrey, Richard Burchill, Nigel White e Justin Morris (eds), Cambridge University Press, 2009, p. 298.

Katharina Dimmroth e Wolf Shunemann, The Ambiguos Relation Between Privacy and Security in German Cyber Politics, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), 2017, p. 101.

Lina Jasmontaite e Valentina Pavel Burloui, Lithuania and Romania to Introduce Cybersecurity Laws: Attaining Information Security at the Cost of Individuals Rights, in: *Privacy, Data Protection and Cybersecurity in Europe*, Wolf Schunemann e Max-Otto Baumann (eds), 2017, p. 135.

Lino Santos, *Enciclopédia de Direito e Segurança*, Jorge Bacelar Gouveia e Sofia Santos (Cord), Almedina, 2015, pp. 65.

Luc Dandurand e Oscar Serrano Serrano, *Towards Improved Cyber Security Information Sharing*, 5th International Conference on Cyber Conflict K. Podins, J. Stinissen, M. Maybaum (Eds.), 2013, NATO CCD COE Publications, Tallinn, 2013, disponível para consulta em: https://ccdcoe.org/uploads/2018/10/25_d3r1s5_dandurand.pdf.

Luc Dandurand, *Cyber Defence Data Exchange and Collaboration Infrastructure*, 22nd Annual FIRST Conference, Miami, 2010, disponível para consulta em: https://www.first.org/resources/papers/conference2010/dandurand-slides.pdf.

Luciano Floridi, *Information: A Very Short Introdution*, Oxford University Press, 2010.

Luís Camelo dos Santos et. alli, Defesa do Ciberespaço, Contributos para uma estratégia nacional de ciberdefesa, in: *idn cadernos*, p.33.

Luis García Segura, European Cybersecurity: Future Challenges from a Human Rights Perspective, in: *Security and Defence in Europe*, Martín Ramírez e Jerzy Biziewski (eds), Springer, 2020, pp.40-45.

Luísa Santos e Mário Marques, Gestão de Risco Aplicada à Segurança da Informação, in: *CyberLaw by CIJIC*, Edição N.º VII, 2019.

Luukas Ilves et alli, European Union and NATO Global Cybersecurity Challenges: A Way Forward, in: *PRISM*, Institute for national Strategic Security, Nacional Defense University, Vol. 6, N.º 2, p.128.

Manuel de Almeida Ribeiro, A ONU e o uso da força pelos Estados: da letra da Carta aos novos desafios do século XXI, in: *O Direito Internacional e o Uso de Força no Século XXI*, Maria Luísa Duarte e Rui Tavares Lanceiro (coord.), AAFDL, 2018, p.460-461.

Marco Roscini b), *Cyber Operations and the Use of Force in International Law*, Oxford, Oxford University Press, 2014, p. 46.

Marco Roscini a), Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in: *Texas International Law Journal*, 2015, pp. 248.

Mariarosaria Taddeo, Just Information Warfare, in*: Ethics and Policies for Cyber Operations: NATO Cooperative Cyber Defence Centre of Excellence Initiative*, Mariarosaria Taddeo e Ludovica Glorioso (eds), Philosophical Studies Series, Springer, p.68-72.

Marina Shorer-Zeltser e Galit Margalit Ben-Israel, Developing Discourse and Tools for Alternative Content to Prevent Terror, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, Eugenie de Silva (ed), Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series, IGI, p. 148-155.

Mark Pollitt, Cyberterrorism – Fact or Fancy?, in: *FBI Laboratory*, disponível para consulta em: https://cs.georgetown.edu/~denning/infosec/pollitt.html.

Martti Lehto, et. alli, Arctic Connect Project and cyber security control, ARCY, in: *Informaatioteknologian tiedekunnan julkaisuja*, Pekka Neittaanmäki (ed), University of Jyväskylän, N.º 78, 2019, p. 14-22.

Mary Ellen O'Connell, Rules of Evidence for the Use of Force in International Law's New Era, in: *Proceedings of the Annual Meeting (American Society of International Law)*, 2006, pp. 44-47, *apud*, Dennis Broeders, Els De Busser e Patryk Pawlak, p. 7.

Matthew Hoisington, Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, in: *Boston College International and Comparative Law Review*, 32, Issue 2, 2009, p 452, disponível para consulta em: https://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16/.

Matthew Waxman, "Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions', in: *International Law Studies,* N.º 89, 2013, p 111, *apud*, Marco Roscini, p.46.

Maya Guzdar e Tomas Jermalavicius, Between the Chinese Dragon and American Eagle: 5G Development in the Baltic States, in: *Internacional Center for Defense and Security*, 2020, p.1, disponível para consulta em: https://icds.ee/en/between-the-chinese-dragon-and-american-eagle-5g-development-in-the-baltic-states/.

MI5, *Cyber*, Disponível para consulta em: https://www.mi5.gov.uk/cyber.

Michael Connell e Sarah Vogler, "Russia's Approach to Cyber Warfare," *CNA Analysis & Solutions,* www.dtic.mil/get-tr-doc/pdf?AD=AD1019062*; Nicholas Fedyk, "Russian 'New Generation' Warfare: Theory, Practice, and Lessons for U.S. Strategists," Small Wars Journal*, http://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D warfaretheory- practice-and-lessons-for-us-strategists., *apud*, James Lewis, p.7.

Michael Schmitt e Liis Vihul a), Proxy Wars in Cyberspace, in: *Fletcher Security Review*, Vol I, Issue II, 2014, pp. 63-64.

Michael Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, in: *Columbia Journal of Transnational Law*, N.º 37, 1999, pp. 885-937, a*pud* Marco Roscini, p. 44-68.

Michael Schmitt b), Tallinn Manual 2.0 on the international law applicable to cyber operations, in: *Cambridge University Press*, Cambridge, 2017, pp. 111 - 134.

Ministero dell'Istruzione Ministero dell'Università e della Ricerca, *La posizione italiana sui principi fondamentali di Internet*, 2012, p. 5, disponível para consulta em: http://download.repubblica.it/pdf/2012/tecnologia/internet.pdf.

Ministry of Defence of the Russian Federation, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, 2000, p. 12, disponível para consulta em: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Ministry of Defence, Cyber Security Strategy Cyber Security Strategy Committee, 2008, disponível para consulta em: http://www.sicurezzacibernetica.it/db/[Estonia]%20%20National%20Cyber%20Security%20Strategy%20-%20old%20-%202008%20-%20EN.pdf.

Murat Karaboga et. alli, Is There a Right to Offline Alternartives in a Digital World?, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Law Governance and Technology Series, N.º 36, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Springer, 2016, p. 48.

NATO, *Brussels Summit Declaration*, 2018, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

NATO, *Cyber defence*, 2020, disponível para consulta em: https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO, *NATO's role in cyberspace*, 2019, disponível para consulta em: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, 2020, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

NATO, *Wales Summit Declaration: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*, 2014, disponível para consulta em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

Nguyen Dinh, Patrick Dailler, Alain Pellet, *Direito Internacional Público*, 2.ª Edição, Fundação Calouste Gulbenkian, 2003, p.782.

Nico Schrijver, The Ban on the Use of Force in the UN Charter, in: *The Oxford Handbook of The Use of Force in International Law*, Marc Weller (ed), Oxford University Press, 2015, p. 473.

NIS Cooperation Group, *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*, 2020, disponível para consulta em: https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity.

Noran Shafik Fouad, *The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016)*, p. 635.

Noushin Ashrafi, Christopher Schuetz e Jean-Pierre Kuilboer, *Twenty-second Americas Conference on Information Systems*, San Diego, 2016.

Nuno Ferreira, A Responsabilidade Internacional: Evolução na Tradição, in: *Revista da Ordem dos Advogados*, Vol II, Set. 2006, disponível para consulta em:

https://portal.oa.pt/publicacoes/revista/ano-2006/ano-66-vol-ii-set-2006/doutrina/nuno-ferreira-a-responsabilidade-internacional-evolucao-na-tradicao/.

OEWG Virtual Meeting, Australian Intervention, 2020, disponível para consulta em: https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-australia-2-july-2020.pdf.

Olga Kuznestsova e Natalia Bondarenko, Private Life Safety Provision in Digital Age, in: *ADFS*L, V12, N.º 3, 2017, pp. 77-78.

Ott Velsber, Ulrika Westergren e Katrin Jonsson, *Exploring smartness in public sector innovation – creating smart public services with the Internet of Things*, in: European Journal of Information Systems, 2020.

Oxford University, *A Dictionary of Comupting*, 2004, p. 269.

Panos Koutrakos, The EU Common Security and Defense Policy, In: *European Journal of International Law*, Julia Schmidt (ed), 2013, Oxford, Oxford University, p. 1257 e ss.; Aurel Sari, International Law Aspects of the EU´s Security and Defense Policy, With a Particular Focus on the Law of Armed Conflict, in: *European Law Review*, Fredrick Naert (ed), 2011, pp. 451-453.

Parlamento Europeu, *Parlamento trabalha em prol da cibersegurança europeia (infografia)*, 2019, disponível para consulta em mais informações: https://www.europarl.europa.eu/news/pt/headlines/security/20190307STO30713/parlamento-trabalha-em-prol-da-ciberseguranca-europeia-infografia.

Parlamento Europeu, *Proteção de daos pessoais*, 2017, disponível para consulta em: https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais.
Parlamento Europeu, *Regulating disinformation with artificial intelligence: Effects of disinformation initiatives on freedom of expression and media pluralism*, 2019, p.12-19.

Parlamento Europeu, *Report de 16 de julho de 1996*, 1996, disponível para consulta em: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A4-1996-0244+0+DOC+XML+V0//EN.

Paulo Moniz, Impacto do Ciberespaço na Sociedade em Rede, Contributos para uma estratégia nacional de ciberdefesa, in: *idn cadernos*, 2020, p. 21-22.

Pedro Freitas e Nuno Gonçalves, *Illegal access to information systems and the Directive 2013/40/EU*, in: *International Review of Law*, Computers & Technology, Routledge: Taylor & Francis Group, 2015, Vol. 29, Nº 1, p. 50-62.

Pedro Veiga, *European Cybersecurity Policy NIS Directive*, p. 10, disponível para consulta em: https://www.cncs.gov.pt/content/files/2017_06_22_-_pedroveiga_-_pt_-_final.pdf.

Piret Pernik, *Improving Cyber Security: NATO and the EU*, International Centre for Defence Studies, 2014, p.5.

Piret Pernik, *National Cyber Security Strategies The Estonian Approach*, International Centre for Defence and Security, 2017.

Ramjee Prasad e Vandana Rohokale, Artificial Intelligence and Machine Learning in Cyber Security, In: *Ciber Security: The Lifeline of Information and Communication Technology*, Springer Series in Wireless Technology, Springer, 2020, pp. 234-242.

Ramjee Prasad e Vandana Rohokale, E-commerce, In: *Ciber Security: The Lifeline of Information and Communication Technology*, Springer Series in Wireless Technology, Springer, 2020, pp. 182-184.

Rebeca Wilson e Anthony Lemieux, An Information, Motivation, and Behavioral Skills Perspective on Terrorist Propaganda, in: *Online terrorist propaganda, recruitment and radicalization*, Ed. John Vacca, CRC Press, Taylor & Francis Group, 2020, p. 227-238.

Republic of Estonia Ministry of Foreign Affairs, *Cybersecurity Strategy Republic of Estonia*, p.10.

Resolução do Parlamento Europeu, de 13 de junho de 2018, sobre ciberdefesa (2018/2004(INI)), disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018IP0258&from=EN.

Reuters, *German parliament foiled cyber attack by hackers via Israeli website,* 2017, disponível para consulta em: https://www.reuters.com/article/us-germany-cyber-idUSKBN1701V3.

Roland Heickero, Russia´s Information Warfare Capabilities, in: *Current and Emerging Trends in Cyber Operations*, Palgrave Macmillans Studies in Cybercrime and Security, 2015, p.76.

Rui Ataíde, Direito ao esquecimento, in: *CyberLaw by CIJIC*, Edição N.º VII, 2019.

Rui Pereira e Alice Feiteira, Enciclopédia de Direito e Segurança, Jorge Bacelar Gouveia e Sofia Santos (coord.), Alemedina, 2015, p. 340.

Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", *Journal of Conflict and Security Law,* N.º 17*, 2012*, p. 212.

Russell Buchan, *Cyber Espionage and International Law*, HART, 2019, pp. 70 e ss.

Samuel Huntington, Culture, Power and Democracy, in: *Globalization, Power, and Democracy*, Marc Plattner e Aleksander Smolar (ed), John Hopkins University Press, Baltimore, 2000, p.6.

Samuel Warren e Louis Brandeis, The right to privacy, in: *Harvard Law Review*, Vol IV. N.º 5, 1980, pp. 195 e ss.

Secrétariat Général de la Défense et de la Sécurité Nationale, Revue stratégique de cyberdéfense, 2018, p. 35, disponível para consulta em: http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

Sérgio Ferreira, *Sistemas de informação em Segurança*, Editora e Distribuidora Educacional S.A.,2017, pp.51-52.

Shakila Bu-Pasha, Cross-border issues under EU data protection law with regards to personal data protection, in: *Information & Communications Technology Law*, Routledge: Taylor & Francis Group, pp. 227-228.

Sofia Santos, Enciclopédia de Direito e Segurança, Jorge Bacelar Gouveia e Sofia Santos (coord.), 2015, Almedina, p. 41.

Stephanie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare", in: *Stanford Journal of International Law*, N.º 48, 2012, pp. 226.

Thomas Oppermann, Deutscher Bundestag, in: *Stenografischer Bericht*, Berlim, 2013.

Tim Maurer e Robert Morgus, Compilation of Existing Cybersecurity and Information Security Related Defintions, in: *Open Technology Institute New America*, 2011, p. 44.

Tribunal de Contas Europeu, *Desafios à eficácia da política de cibersegurança da UE*, 2019, pp. 42-43.

Tridas Mukhopadhyay, Sunder Kekre e Suresh Kalathur, Business Value of Information Technology: A Study of Electronic Data Interchange, in: *MIS Quarterly*, Vol.19, N.º 2, 1995, pp.137-156.

U.S Department of State, *A New Transatlantic Dialogue*, 2020, disponível para consulta em: https://www.state.gov/a-new-transatlantic-dialogue/.

Ugo Pagallo, Massimo Durante e Shara Monteleone, What is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IOT, in: *Data Protection and Privacy: (In) visibilities and Infrastructures*, Ranald Leenes, Rosamunde van Brakel, Serge Gutwirth e Paul De Hert (Eds), Law Governance and Technology Series 36, Springer, 2016, p. 58-62.

United Kingdom, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, p. 29, disponível para consulta em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

United Nations, *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development*, 2020, p.52.

United Nations, *Statement by the representative of the Russian Federation at the online discussion of the second "pre-draft" of the final report of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security*, Moscow, 2020, disponível para consulta em: https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-the-russian-federation-15-june-2020.pdf.

United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 94.

Vicente Freire e Alexandre Caldas, *O Ciberespaço: Desafios à Segurança e à Estratégia, Segurança Internacional: Perspetivas Analíticas*, Imprensa Nacional-Casa da Moeda e Instituto de Defesa Nacional, Lisboa, 2013, p.81.

Wayne Harrop e Ashley Matteson, Cyber Resilience: A review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA, in: *Current and Emerging Trends in Cyber Operations*, Palgrave Macmillans Studies in Cyber Crime and Security, p.151-152.

William Baude e James Stern, The Positive law model of the fouth amendment, in: *Harvard Law Review*, Vol. 129, N.º 7, 2016, pp. 1883-1884.

World Economic Forum, *The Global Risks Report 2020*, 2020, disponível para consulta em: https://www.weforum.org/reports/the-global-risks-report-2020.

Yoram Dinstein, Computer Network Attacks and Self-Defense, in: *Computer Network Attack and International Law*, Michael Schmitt e Brian O´Donnell (eds), International Law Studies, Vol. 76, p 105.

ANEXOS

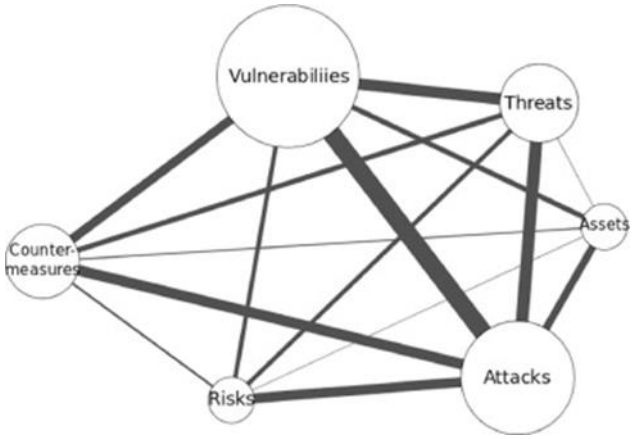
ANEXOS

Critical control 1	Inventory of authorised and unauthorised devices
Critical control 2	Inventory of authorised and unauthorised software
Critical control 3	Secure configurations for hardware and software
Critical control 4	Continuous vulnerability assessment and remediation
Critical control 5	Mahvare defences
Critical control 6	Application software security
Critical control 7	Wireless device control
Critical control 8	Data recovery capability
Critical control 9	Security skills assessment and appropriate training to fill gaps
Critical control 10	Secure configurations for network devices
Critical control 11	Limitation and control of network ports, protocols and services
Critical control 12	Controlled use of administrative privileges
Critical control 13	Boundary defence
Critical control 14	Maintenance, monitoring and analysis of security audit logs
Critical control 15	Controlled access based on the need to know
Critical control 16	Account monitoring and control
Critical control 17	Data loss prevention
Critical control 18	Incident response capability
Critical control 19	Secure network engineering
Critical control 20	Penetration tests and red team exercises

Anexo A - Guia de controlos de segurança da informação para as organizações do Reino Unido.

Fonte: Wayne Harrop e Ashley Matteson, Cyber Resilience: A review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA, in: *Current and Emerging Trends in Cyber Operations*, Palgrave Macmillans Studies in Cyber Crime and Security, p. 157.

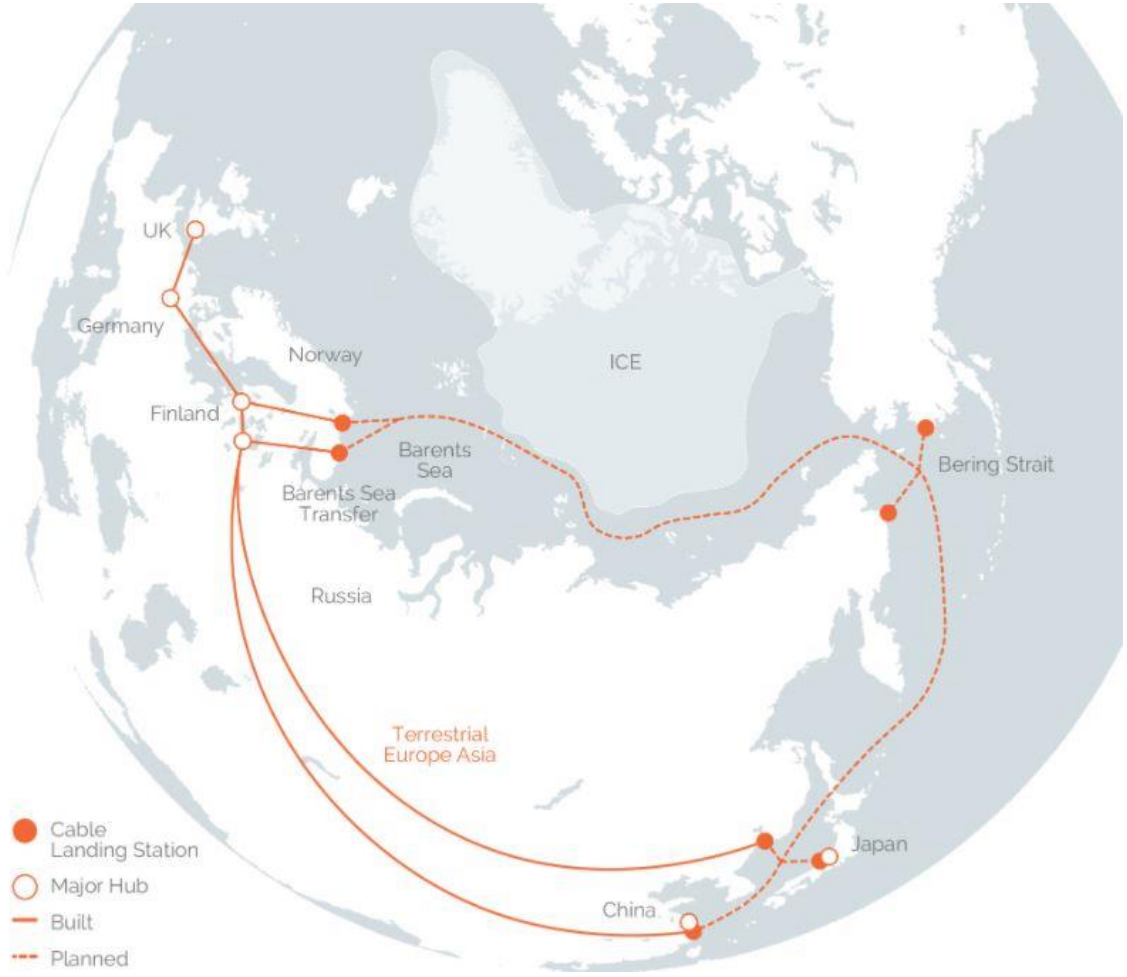
ANEXOS



Anexo B – Relação dos diferentes tipos de informações de segurança e frequência das suas co-ocorrências.

Fonte: Clemens Sauerwein et. alli., An analysis and classification of public information security data sources used in research and practice, in: *Computers & Security*, Volume 82, Maio 2019, Elsevier, p. 149.

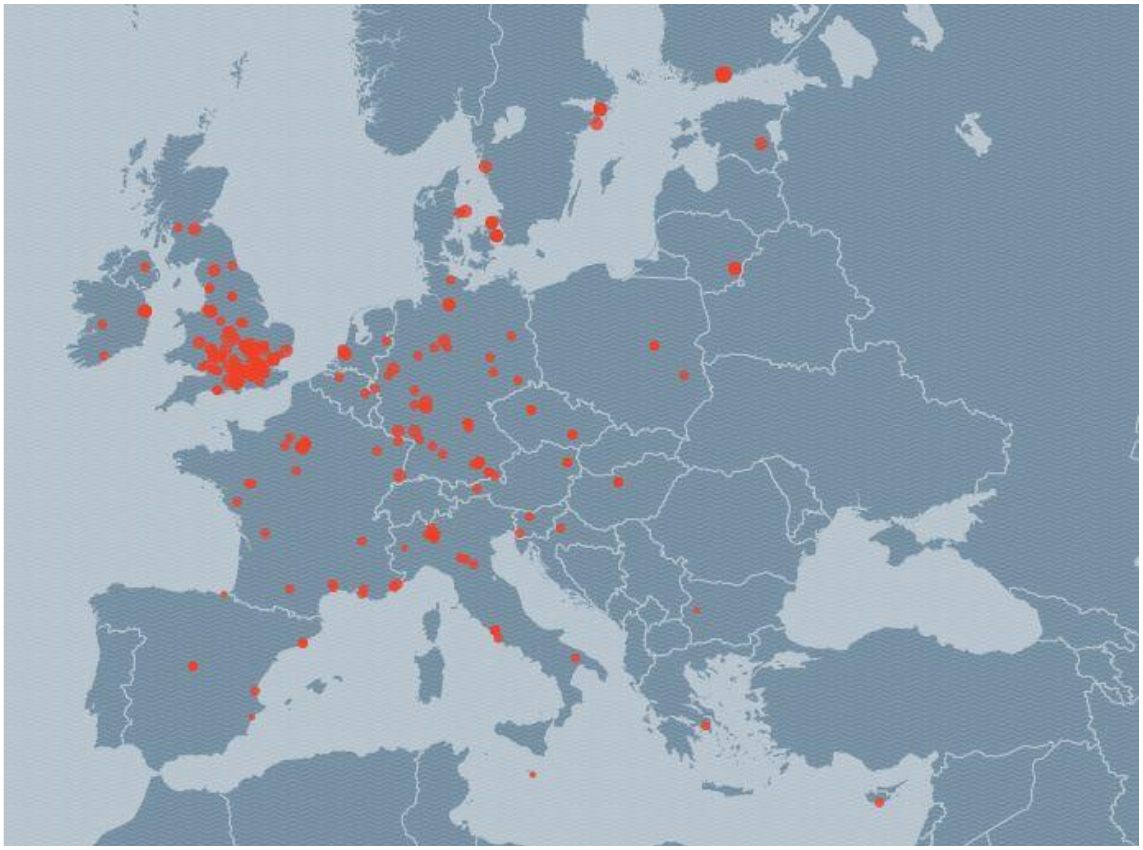
ANEXOS



Anexo C – Rota planeada para o novo cabo submarino do ártico.

Fonte: Submarine Cable Networks, *MegaFon Begins Offshore Survey for the Arctic Connect Subsea Cable Project*, disponível para consulta em: https://www.submarinenetworks.com/en/systems/asia-europe-africa/arctic-connect/megafon-begins-offshore-survey-for-the-arctic-connect-subsea-cable-project.

ANEXOS



Anexo D– Distribuição das organizações que operam em vigilância industrial na UE.

Fonte: Privacy Internacional, The Global Surveillance Industry, disponível para consulta em: https://privacyinternational.org/explainer/1632/global-surveillance-industry.

Índice