INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Trabalho Individual Final do
VI Curso de Direção e Estratégia Policial

O POLICIAMENTO NA ERA DIGITAL: A ESTRATÉGIA ANTI-INFODÉMICA DA EUROPOL

Estudo Teórico

Autor: Roberto Narciso Andrade Fernandes, Intendente
Orientador: Professor Doutor Luís Manuel André Elias, Superintendente
Número do auditor: 100219

Funchal, 31 de agosto de 2024

O Decreto-Lei n.º 243/2015, de 19 de outubro, que aprova o estatuto profissional do pessoal com funções policiais da Polícia de Segurança Pública (PSP), consagra a carreira de oficial de polícia como uma carreira especial de complexidade funcional de grau 3. Nos termos da lei, os oficiais de polícia desempenham, fundamentalmente, funções de comando, direção ou chefia e de inspeção e assessoria, bem como desenvolvem atividades de natureza especializada e instrução próprias das respetivas categorias, na estrutura orgânica da PSP ou em outros organismos nacionais ou internacionais.

O presente Trabalho Individual Final (TIF) foi desenvolvido no âmbito do VI Curso de Direção e Estratégia Policial (CDEP), ministrado pelo Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI), enquanto condição especial para a ascensão na carreira de oficial de polícia ao posto de Superintendente. Conforme consignado no n.º 3, do Artigo 4.º do Regulamento do CDEP, em anexo ao Despacho n.º 33/GDN/2023, de 14 de novembro de 2023, o TIF consiste numa exposição escrita, individual, orientada e inédita sobre um tópico relevante para a segurança interna. *Ex vi* do n.º 2 e n.º 4, do Artigo 4.º, da Portaria n.º 245/2016, de 7 de setembro, a lista de temas para o TIF dos auditores do VI CDEP foi aprovada por despacho do Diretor Nacional da PSP, sob proposta do Diretor do ISCPSI, nos termos do Ofício n.º 217/SECDE/2023, de 28 de dezembro de 2023. Uma vez escolhido o tópico da investigação, elaborou-se o projeto de TIF, o qual foi previamente submetido à apreciação e validação do Diretor do ISCPSI. Cognominado "O Policiamento na Era Digital: A estratégia anti-infodémica da EUROPOL", o corrente estudo enquadra-se na linha de investigação III. Policiamento, no subtema V. Ciberpoliciamento e especificamente no ponto 1. Prevenção dos fenómenos criminais.

Ficha técnica:

Título:	O Policiamento na Era Digital: A estratégia anti-infodémica da EUROPOL
Autor:	Roberto Narciso Andrade Fernandes CIÊNCIA ID 7A17-C4C6-519E | ORCID iD 0000-0002-3649-8694
Orientador:	Professor Doutor Luís Manuel André Elias
Curso:	VI Curso de Direção e Estratégia Policial
Estabelecimento de ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Data:	2024

Dedicatória

À Noémi, pela sua generosa candura e suavidade.
Que a bondade e delicadeza continuem a inspirar e a encantar
todos os que atravessam o seu caminho.

Agradecimentos

Expresso a minha mais profunda gratidão ao Professor Doutor Luís Manuel André Elias, Superintendente da PSP, pela sua inspiração, orientação e apoio incansáveis ao longo de todo o processo de elaboração desta investigação, desenvolvida no âmbito do VI Curso de Direção e Estratégia Policial. A sua experiência precursora, enquanto Oficial de Ligação do Ministério da Administração Interna junto da EUROPOL, impulsionou-nos na edificação desta *visão de futuro* quanto a uma problemática atual e fraturante da segurança europeia e mundial.

Agradeço, por fim, à minha esposa e aos meus filhos, pela paciência e apoio incondicional aos meus recorrentes empreendimentos académicos e profissionais, tantas vezes em detrimento das próprias necessidades e anseios. Estou eternamente grato pela vossa generosidade.

Resumo

A pandemia de Covid-19 e o conflito russo-ucraniano aceleraram a proliferação da desinformação *online*, impactando significativamente na segurança doméstica e internacional. A investigação examina a instrumentalização da "infodemia" pela Rússia como tática não convencional para desestabilizar a Europa e, sobretudo, a convizinha Ucrânia. O constructo de desinformação e propaganda pró-Kremlin assume uma expressão global, híbrida e instrumentalizada na corrupção do ecossistema de informação contemporâneo, inundando o envolvente digital com quantidades massivas de informações manipuladas, falsas e meias-verdades que intoxicam os sistemas democráticos ocidentais (Bertolin, 2015).

No contexto do policiamento pan-europeu da era digital, o estudo analisa a estratégia europeia anti-infodémica, designadamente os produtos de inteligência disponibilizados pela EUROPOL para combater a infodemia, enfatizando a contribuição dos oficiais de ligação envolvidos no reforço estratégico da partilha de informações credíveis, na identificação e desmembramento de redes de desinformação e no apoio à sensibilização pública.

Os resultados deste trabalho visam contribuir para uma melhor compreensão dos complexidades apresentadas pela infodemia e prospetivar estratégias específicas a serem empregues pelas forças de segurança no seu enfreamento. Espera-se que as conclusões informem o desenvolvimento de políticas e práticas eficazes no combate à propagação da "censura moderna pelo ruído" que ameaça os Direitos Humanos e a integridade da informação.

Palavras-chave

Era digital, desinformação, geopolítica, infodemia, policiamento.

Abstract

The Covid-19 pandemic and the Russian-Ukrainian conflict have accelerated the proliferation of disinformation online, significantly impacting domestic and international security. The research examines Russia's use of the 'infodemic' as an unconventional tactic to destabilise Europe and neighbouring Ukraine. The construct of disinformation and pro-Kremlin propaganda takes on a global, hybrid and instrumentalised expression in the corruption of the contemporary information ecosystem, flooding the digital environment with massive amounts of manipulated information, falsehoods and half-truths that intoxicate Western democratic systems (Bertolin, 2015).

In the context of pan-European policing in the digital age, the study analyses the European anti-infodemic strategy, namely the intelligence products made available by EUROPOL to combat the infodemic, emphasising the contribution of the liaison officers involved in strategically strengthening credible information sharing, identifying, and breaking up disinformation networks and supporting public awareness.

The results of this work aim to contribute to a better understanding of the complexities presented by the infodemic and to prospect specific strategies to be employed by police forces in tackling it. It is hoped that the findings will inform the development of effective policies and practices to combat the spread of 'modern censorship by noise' that threatens human rights and the integrity of information.

Keywords

Digital age, disinformation, geopolitics, infodemic, policing.

Índice

Dedicatória ii
Agradecimentos iii
Resumo iv
Abstract v
Índice vi
Lista de Anexos vi
Lista de Siglas, Abreviaturas e Acrónimos vii
Glossário ix
1. INTRODUÇÃO 1
2. A ERA DIGITAL E O 'POLÍCIA CIENTÍFICO' 9
3. INFODEMIA: A EPIDEMIA DE INFORMAÇÃO DESORDENADA 15
4. A ROLETA-RUSSA DE DESINFORMAÇÃO E PROPAGANDA 20
5. A EUROPOL NA VANGUARDA DO POLICIAMENTO NA ERA DIGITAL 27
6. CONCLUSÃO 34
6.1. Instigações geopolíticas ao policiamento moderno 34
6.2. Dinamismos da cooperação policial transfronteiriça 36
6.3. Uma União em defesa da informação fidedigna 38
6.4. A singularidade dos subsídios da EUROPOL 39
6.5. Complexidades da criminalização da desinformação em Portugal 41
6.6. Prospetivas de ação para a PSP 43
Referências 45
Anexos 75

Lista de Anexos

Figura 1 – A confiança e a Pandemia. 75
Figura 2 – Um planeta em aquecimento 75
Figura 3 – Os grandes desafios do próximo decénio 76
Figura 4 – A expansão dos riscos nucleares. 76
Figura 5 – A infodemia de Putin 77
Figura 6 – Países responsáveis por ciberataques e outros incidentes conexos. 77
Figura 7 – Países europeus mais vulneráveis ao cibercrime. 78

Lista de Siglas, Abreviaturas e Acrónimos

AFIS	*Automated Fingerprint Identification System*
CCPA	Centros de cooperação policial e aduaneira
CIA	Agência Central de Inteligência
CNCS	Centro Nacional de Cibersegurança
COT	Crime organizado transnacional
DDoS	*Distributed Denial-of-Service*
ECAT	Centro Europeu para Transparência dos Algoritmos
EDMO	*European Digital Media Observatory*; Observatório Europeu dos Meios de Comunicação Digitais
EFCSN	*European Fact-Checking Standards Network*
EIS	*Europol Information System*
EM	Estados-Membros
EMPACT	*European Multidisciplinary Platform Against Criminal Threats*
EPE	*Europol Platform For Experts*
ERC	Entidade Reguladora para a Comunicação Social
ESCTF	*East StratCom Task Force*
EUA	Estados Unidos da América
EUROJUST	Agência da União Europeia para a Cooperação Judiciária Penal
EUROPOL	Agência da União Europeia para a Cooperação Policial
FMI	Fundo Monetário Internacional
FSB	*Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii*; Serviço Federal de Segurança da Federação Russa
GNR	Guarda Nacional Republicana
GRU	*Glavnoye razvedyvatel'noye upravleniye*; Diretoria Principal de Inteligência
HUMINT	*Human intelligence*; inteligência humana
IA	Inteligência artificial
ICPOL	Centro de Investigação (*Police Research Center*) do ISCPSI
ID&I	Investigação, desenvolvimento e inovação
IFCN	*The International Fact-Checking Network*; Rede Internacional de Verificação de Factos
INFOSEC	*Information security*; Segurança da Informação

INTERPOL	Organização Internacional de Polícia Criminal
IoT	*Internet of Things*; *Internet* das Coisas
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
JADs	*Joint Action Days*
JIT	*Joint Investigation Team*
KGB	*Komitet Gosudarstvennoy Bezopasnosti SSSR*; Comité de Segurança do Estado da União das Repúblicas Socialistas Soviéticas
MAI	Ministério da Administração Interna
MJ	Ministério da Justiça
MNE	Ministério dos Negócios Estrangeiros
NU	Nações Unidas
OLMAI	Oficiais de ligação do Ministério da Administração Interna
OLMJ	Oficiais de ligação do Ministério da Justiça
OMC	Organização Mundial do Comércio
OMS	Organização Mundial da Saúde
ONG	Organizações não governamentais
OSCE	Organização para a Segurança e Cooperação na Europa
OSINT	*Open source intelligence*; inteligência de fonte aberta
OTAN	Organização do Tratado do Atlântico Norte
OTF	*Operacional Task Force*; Grupo de Trabalho Operacional
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
QUERCUS	Associação Nacional de Conservação da Natureza
SEAE	Serviço Europeu para a Ação Externa
SIENA	*Secure Information Exchange Network Application*; Aplicação de rede de intercâmbio seguro de informações
SOMA	*Social Observatory for Disinformation and Social Media Analysis*; Observatório social para a análise da desinformação e dos media sociais
Spetsnaz	*Voiska spetsialnogo naznacheniya*; Unidades para fins especiais (forças especiais)
StratCom	*Strategic Communications and Information Analysis Division*; Divisão de Comunicações Estratégicas e Análise de Informação

SVR	*Sluzhba Vneshney Razvedki*; Serviço de Inteligência Estrangeiro
TECHINT	*Technical intelligence*; inteligência tecnológica
TIC	Tecnologias de Informação e de Comunicação
TIJ	Tribunal Internacional de Justiça
UE	União Europeia; União

Glossário

Ameaça	Causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer dos sistemas por ela utilizados. Estas ameaças podem ser acidentais ou intencionais e caracterizam-se por elementos ameaçadores, alvos potenciais e métodos de ataque (Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013; Decisão (UE, Euratom) n.º 2015/444 da Comissão, de 13 de março de 2015; CNCS, 2022, p. A).
Ameaças híbridas	"(…) Ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação, combinando atividades convencionais e não-convencionais, militares e não militares, de forma coordenada, levadas a cabo por sujeitos estatais e não-estatais, recorrendo ainda a campanhas multidimensionais que combinam medidas coercivas e subversivas, com vista ao alcance de objetivos políticos" (Pereira, 2018, p. 10). As ameaças híbridas podem abranger diferentes formatos e tonalidades. Podemos classificá-las em dois grandes grupos: as de ação cinética – *i.e.*, guerras por procuração; conflitos não declarados; e grupos paramilitares – e as de ação não cinética – nomeadamente, as operações de narração e armamento dos média, onde se inclui a propaganda, a desinformação e a contrainformação, as fugas de informação estratégicas e as agências noticiosas estatais ou paraestatais; o financiamento; a pressão económica; e os ciberataques. As conjugações da pluralidade das ações não cinéticas

	com a disrupção do ciberespaço aproveitam o uso malicioso da infodemia (Duarte, 2020).
Ataque	Qualquer tipo de atividade maliciosa que tenta recolher, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si (Paulsen & Byers, 2019; CNCS, 2022, p. A).
Autenticidade	Num contexto informacional, é a propriedade de uma informação cuja origem e integridade são garantidas (CNCS, 2022, p. A).
Avaliação do Risco	Identificação das ameaças e vulnerabilidades e realização da análise de risco conexa, ou seja, a análise da probabilidade e do impacto (Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013; CNCS, 2022, p. A).
Botnet	Rede de computadores infetados por *software* malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados (União Europeia, 2019; CNCS, 2022, p. B).
Bots	Consistem em contas de redes sociais não humanas, programadas para publicar rápida e repetidamente conteúdos em várias redes sociais em linha.
Cheap Fake	Manipulação audiovisual criada com *software* barato e acessível (ou nenhum). Falsificações baratas podem ser "renderizadas" através do *Photoshop*, semelhantes, recontextualizando imagens (CNCS, 2022, p. C).
Ciber	Termo que conota uma relação com as tecnologias da informação (Paulsen & Byers, 2019; CNCS, 2022, p. C).
Ciberataque	Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente (CNCS, 2022, p. C).
Ciberbullyng	*Bullying* realizado através da *internet* ou telemóvel, envolvendo mensagens ofensivas ou maliciosas, *e-mails*, *chats* ou comentários, ou mesmo, em casos extremos, *websites* construídos com intenções

	maliciosas contra indivíduos ou certos grupos de pessoas (CNCS, 2022, p. C).
Cibercrimes	Factos qualificados como crimes, previstos na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa. O 'cibercriminoso' é o agente destes crimes. Todavia, no âmbito dos atores de ameaças, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas (Lei n.º 109/2009, de 15 de setembro; Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho; CNCS, 2022, p. C).
Ciberdefesa	Atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho; CNCS, 2022, p. C).
Ciberespaço	Ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho; CNCS, 2022, p. C).
Ciberespionagem	Ameaça geralmente direcionado aos setores industriais, as infraestruturas críticas e estratégicas em todo o mundo, incluindo entidades governamentais, transportes, provedores de telecomunicações, empresas de energia, hospitais e bancos. Foca-se na geopolítica, no roubo de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos (ENISA, 2018; CNCS, 2022, p. C).
Cibersegurança	Medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem (Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho; CNCS, 2022, p. C).

Ciberterrorismo	Existe uma maior convergência entre terrorismo e ciberespaço. Motivados para a realização de ciberataques, os 'ciberterroristas' têm por objetivos o recrutamento e a monetarização. Não obstante o uso instrumental do ciberespaço, o principal objetivo deste agente de ameaças, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas (ENISA, 2018; CNCS, 2022, p. C).
Comunicação do Risco	Consciencializar os grupos de utilizadores de sistemas de comunicação e informação para os riscos, informar as autoridades de aprovação desses riscos e reportá-los às autoridades operacionais (Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013; CNCS, 2022, p. C).
Crime Informático	Atos criminosos cometidos *online* utilizando redes de comunicação eletrónicas e sistemas de informação (CNCS, 2022, p. C).
Dark Web	Conteúdos publicamente acessíveis que estão hospedados em sites cujo endereço IP está oculto, mas ao qual qualquer um pode aceder, desde que conheça o endereço. Inclui conteúdos privados trocados numa rede fechada de computadores para partilha de arquivos (Paganini, 2017; CNCS, 2022, p. D).
DDoS	Ataques Distribuídos de Negação de Serviço (*Distributed denial of service*) ocorrem quando os utilizadores de um sistema ou serviço, não conseguem aceder a informações relevantes, serviços ou outros recursos. Isto acontece ao esgotar o serviço ou sobrecarregando a infraestrutura de rede (CNCS, 2022, p. D).
Deepfakes	Falsificações profundas, vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática. (CNCS, 2022, p. D; EUROPOL, 2022d).
Desinformação	É uma "uma informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente a população, e que é suscetível de causar um prejuízo público" (Comissão Europeia, 2018, p. 4; Comissão Europeia, 2020a). "(…) É uma informação falsa ou imprecisa cuja intenção deliberada é enganar" (OPAS, 2020, p. 2). Outra definição explicita-a como a "(…) informação

	comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público, o qual abrange ameaças aos processos políticos democráticos e aos processos de elaboração de políticas, bem como a bens públicos, tais como a proteção da saúde dos cidadãos da UE, o ambiente ou a segurança. A desinformação não abrange erros na comunicação de informações, sátiras, paródias ou notícias e comentários claramente identificados como partidários, nem a opinião escrita ou oral, salvo se esta servir para ampliar uma desinformação (informação comprovadamente falsa)" (ERC, 2019, p. 65).
Domínio	Grupo de computadores e dispositivos de uma rede, em particular da *internet*, que são administrados como uma unidade, com regras e procedimentos comuns, e que partilham um nome comum (nome do domínio) (CNCS, 2022, p. D).
Engenharia Social	O ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança (Paulsen & Byers, 2019; CNCS, 2022, p. E).
Espionagem Informática	Ciberataques dirigidos contra a confidencialidade de um sistema de tecnologias da informação (CNCS, 2022, p. E).
Fake News (Notícias Falsas)	Inicialmente utilizada para denegrir o trabalho dos meios de comunicação social, a expressão é enganadora. Uma notícia, por definição, não é falsa. Falsas são as narrativas que, embora anunciadas como notícias e contendo partes de textos copiados de jornais ou de sites do mesmo género, integram conteúdos ou informações falsas, imprecisas, enganadoras, concebidas, apresentadas e promovidas para intencionalmente causar dano público ou obter lucro (ERC, 2019; CNCS, 2022, p. F).
Geopolítica	Conceito contestado e em permanente evolução, a geopolítica pode ser definida como o método de análise ou perspetiva que refere a política e as dinâmicas de poder – isto é, os discursos e as práticas

	inventariadas com a aquisição e o uso do poder, o exercício de poder, as relações de poder e a estrutura de poder para certos fins – em função de e num determinado espaço, seja ao livel local ou a uma escala mais ampla, como uma região ou o mundo (Correia, 2012; Tomé, 2014, p. 190). Em suma, a geopolítica analisa os comportamentos e dinâmicas de poder em função de e num determinado espaço (informação verbal, apresentada por Luís Tomé no 'Seminário sobre Geopolítica Mundial e Segurança Internacional (SSGMSI)' – 3.º Ciclo de Estudos em Relações Internacionais: Geopolítica e Geoeconomia, da Universidade Autónoma de Lisboa (UAL), em Lisboa, em janeiro de 2021).
Grooming	É o processo pelo qual um indivíduo faz amizade com um jovem para contato sexual *online*, às vezes com o envolvimento de *webcams* que podem permitir a partilha da exploração entre redes de abusadores de crianças e, às vezes, levando a uma reunião física para cometer relações de abusos sexuais (CNCS, 2022, p. G).
Hacktivistas	Agentes de ameaças orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais (ENISA, 2018; CNCS, 2022, p. H).
IA	A 'inteligência artificial' é a "(…) subárea da Ciência da Computação responsável por pesquisar e propor a elaboração de dispositivos computacionais capazes de simular aspetos do intelecto humano, ao modo da capacidade de raciocinar, perceber, tomar decisões e resolver problemas" (Silva, 2013, p. 1). A aprendizagem automática, um subcampo da IA, recorre a modelos matemáticos para facultar aos computadores a capacidade de aprender a partir de dados, sem necessidade de programação explícita para a execução de tarefas específicas. Esta capacidade de aprendizagem é crucial para o desenvolvimento de sistemas inteligentes genéricos que ambicionam replicar ou exceder as capacidades humanas numa vasta gama de atividades. A conjugação da aprendizagem automática com a analítica tem possibilitado progressos notáveis na interpretação de grandes volumes de dados, facilitando a identificação de padrões,

	tendências e perceções anteriormente inacessíveis. Esta sinergia revela-se particularmente eficaz na previsão de comportamentos, na otimização de processos e no aprimoramento da tomada de decisão. Revolucionada pela incorporação da aprendizagem automática e da IA, a automação tem possibilitado o desenvolvimento de sistemas capazes de executar tarefas complexas e repetitivas com precisão e eficiência superiores. A automação inteligente, resultante da fusão entre IA e automação, criou oportunidades ao automatizar tarefas rotineiras. Ao libertar recursos humanos para atividades de maior valor agregado, impulsionou a produtividade e a inovação. A realidade aumentada e estendida (metaverso), a mudança de serviços para *clouds* e a 'sensorização' de sistemas IoT têm promovido mudanças estruturais. A longo prazo, a IA genérica, que visa desenvolver sistemas capazes de realizar qualquer tarefa cognitiva humana, representa o ápice desses avanços. Os avanços na aprendizagem automática e na automação estão a abrir o caminho para sistemas cada vez mais sofisticados e versáteis. A habilidade de aprender e adaptar-se a novas tarefas e ambientes constitui um pilar fundamental neste processo (Oliveira, 2018).
Incidente	Evento com um efeito adverso real na segurança das redes e dos sistemas de informação. São ações tomadas, através da utilização de uma rede de computadores, que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada (Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016; CNCS, 2022, p. I).
Infodemia	Apesar dos estudos que introduzem o conceito de infodemiologia remontarem a meados da década de 1990, a expressão foi consolidada em 2020 por Gunther Eysenbach, (Eysenbach, 2020). A infodemiologia é compreendida como a "ciência da distribuição e dos determinantes da informação em meio eletrónico, especificamente a *internet*, ou na população, com o objetivo final de informar sobre saúde pública e política pública" (Mavragani, 2020, p. 3). A

	expressão infodemia resulta da junção de 'informação' com 'epidemia'. Refere-se à rápida disseminação de informação, quer exata, como incorreta, sobre um determinado tópico. A disseminação em larga escala de desinformação encaixa nesta combinação (Rothkopf, 2003; Zarocostas, 2020).
Infoguerra	É "(…) um conflito relacionado com a informação a um grande nível, entre estados ou sociedades. Significa tentar desarticular, danificar ou modificar o que uma população 'sabe', ou pensa que sabe, sobre ela própria e o mundo à sua volta. A infoguerra pode focalizar-se na opinião pública, ou na elite, ou em ambas. Pode envolver medidas de diplomacia pública, propaganda e campanhas psicológicas, subversão cultural e política, induzir em engano ou interferir com os média locais, ou infiltrações em redes de computadores e bases de dados e esforços para promover movimentos dissidentes e de oposição através das redes de computadores. Assim, conceber uma estratégia para a guerra de informação significa reunir em conjunto, sob uma nova perspetiva, um conjunto de medidas que já foram usadas anteriormente, mas eram vistas de forma separada. Por outras palavras, a guerra de informação representa uma nova entrada no espectro do conflito que abrange formas de 'guerra' económica, política, social e militar. Em contraste com guerras económicas que têm como alvo a produção e a distribuição de bens, e as guerras políticas que têm como alvo a liderança e as instituições do governo, as guerras de informação distinguir-se-ão por procurarem atingir a informação e comunicação. Apesar de maioritariamente não militares, as infoguerras poderão ter dimensões que se justapõem à guerra militar" (Arquilla & Ronfeldt, 1993, p. 28).
Informação	Conhecimento que pode ser comunicado sob qualquer forma. São dados que foram interpretados ou organizados de forma coerente e posteriormente comunicados sendo então possível tirar conclusões do seu significado (Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016; CNCS, 2022, p. I).

Informática	Ramo da ciência e da tecnologia que trata do processamento automático de informação efetuado por meio de computadores (CNCS, 2022, p. I).
INFOSEC	A aplicação de medidas de segurança para proteger a informação processada, armazenada ou transmitida em Sistemas de Tecnologia da Informação e Comunicações contra a perda de confidencialidade, integridade ou disponibilidade, acidental ou intencional, e para prevenir a perda de integridade ou disponibilidade dos sistemas (CNCS, 2022, p. I).
Infraestrutura Crítica da Informação	Refere-se a quaisquer sistemas de tecnologias da informação que suportem ativos fundamentais e serviços das infraestruturas nacionais (Maurer & Morgus, 2014; CNCS, 2022, p. I).
Infraestrutura Crítica Europeia	A infraestrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado membro da União Europeia, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas (Decreto-Lei n.º 62/2011, de 9 de maio; CNCS, 2022, p. I).
Infraestrutura Crítica Nacional	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 (Decreto-Lei n.º 62/2011, de 9 de maio; CNCS, 2022, p. I).
Infraestrutura da Informação e da Comunicação	Conjunto de sistemas (*hardware* e *software*) e serviços que oferecem a base para a organização e comunicação de dados entre dois ou mais sistemas de computadores (CNCS, 2022, p. I).
Integridade	Garantia de que os dados ou a informação não sejam alterados de modo não autorizado (CNCS, 2022, p. I).
Interceção	O ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros (CNCS, 2022, p. I).

Internet	Rede de área alargada que é uma confederação de redes de computadores das universidades e de centros de pesquisa, do Governo, do comércio e da indústria, com base no protocolo TCP/IP. Proporciona acesso a sítios *Web*, correio eletrónico, bases de dados, fóruns de discussão, etc. (CNCS, 2022, p. I).
Internet das Coisas (IoT)	A extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores (CNCS, 2022, p. I).
Intranet	Rede corporativa baseada no protocolo TCP/IP e acessível apenas aos membros ou colaboradores de uma organização, ou a outros desde que autorizados (CNCS, 2022, p. I).
Malware (*Software* malicioso)	Programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima (Paulsen & Byers, 2019; CNCS, 2022, p. M).
Meme	Resultante da fusão do vocábulo grego *mimeme* (imitação) e da palavra inglesa *gene* (gene), os memes tornaram-se uma forma essencial de comunicação visual. Consciente da ameaça representada pela desinformação multimédia e pela superficialidade, a comunidade científica está a multiplicar esforços no desenvolvimento de sistemas sofisticados de IA para detetar e remover automaticamente conteúdos prejudiciais nos meios de comunicação, seja o falso sofisticado (*deepfakes*) ou o falso superficial. Enquanto os *deepfakes* buscam o realismo, os memes exploram o ridículo e o distópico, ajuntando reações e brincando com as emoções e crenças das pessoas (Yankoski, Scheirer, & Weninger, 2021; EUROPOL, 2022d).
Pharming	Uso de meios técnicos para redirecionar os utilizadores para páginas *Web* falsas, disfarçadas de páginas legítimas, de modo que esses utilizadores partilhem os seus dados pessoais (Tracy, *et al.*, 2007; CNCS, 2022, p. P).

Phishing	Mecanismo de criação de mensagens através de técnicas de engenharia social com a finalidade de ludibriar o alvo, 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *e-mails* ou mensagens de *phishing* para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas, façam transferências de dinheiro, etc. (CNCS, 2022, p. P).
Pirata Informático (*Hacker*)	Pessoa que explora as falhas da segurança de um sistema com o intuito de violar a sua integridade, destruindo ou alterando a informação ali residente, ou ainda de copiar fraudulentamente os seus ficheiros (CNCS, 2022, p. P).
Plataforma Eletrónica	A infraestrutura tecnológica constituída por um conjunto de aplicações, meios e serviços informáticos necessários ao funcionamento dos procedimentos eletrónicos de contratação pública nacional, sobre a qual se desenrolam os referidos procedimentos (Lei n.º 96/2015, de 17 de agosto; CNCS, 2022, p. P).
Política de Informação	Conjunto de orientações ou diretrizes relativas à utilização ou divulgação de informação, tais como as respeitantes à privacidade, aos direitos de cópia e à propriedade intelectual. A sua aplicação ao meio digital coloca novos desafios, tanto ao nível da redefinição da política como da sua aplicabilidade e do seu controlo (CNCS, 2022, p. P).
Política de Privacidade	Conjunto das medidas administrativas, técnicas e físicas destinadas a impedir as intrusões na vida privada das pessoas ou nos negócios privados das organizações (CNCS, 2022, p. P).
Portabilidade	No caso de um programa informático, capacidade do programa poder ser executado em diferentes computadores com nenhumas ou poucas alterações (CNCS, 2022, p. P).
Post	Mensagem ou conteúdo publicado numa rede social, num fórum ou num blogue (CNCS, 2022, p. P).
Privacidade de Dados	Característica de segurança de um sistema de informação que permite definir quais os dados que podem, ou não, ser acedidos por terceiros (CNCS, 2022, p. P).

Processo de Gestão do Risco de Segurança	Todo o processo de identificação, controlo e minimização de eventos incertos que tenham a potencialidade de afetar os recursos do sistema. São os processos aplicados para monitorizar, reduzir, eliminar, evitar ou aceitar riscos. Outra definição, explica-o como 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 (CNCS, 2022, p. P).
Proteção de Dados Pessoais	Implementação de medidas para proteger dados pessoais e sensíveis de acessos públicos não autorizados, e para controlar o fluxo desses dados (CNCS, 2022, p. P).
Quishing	É um tipo de ataque de *phishing* que utiliza códigos QR para recolher informação sensível, ao solicitar que se realize um *scan* do código QR disponibilizado por *e-mail*, o qual redireciona as potenciais vítimas para um *website* malicioso, onde estas são induzidas a partilhar dados ou a instalar *software* malicioso. *Quishing* é a contração dos termos QR e *phishing* (CNCS, 2022, p. Q).
Ransomware	Representa um tipo de *malware* (vírus, *trojans*, etc.) que infecta os sistemas informáticos dos utilizadores e manipulam o sistema de forma que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos (CNCS, 2022, p. R).
Rede	Conjunto formado por entidades e as suas interconexões. Em topologia de rede ou numa estrutura abstrata, as entidades interconectadas são pontos e as interconexões são linhas num esquema; numa rede de computadores, as entidades interconectadas são computadores ou equipamentos de comunicação de dados e as interconexões são ligações de dados (CNCS, 2022, p. R).

Rede e Sistemas de Informação	Uma rede de comunicações eletrónicas, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), pode ser explicado como um dispositivo ou um grupo de dispositivos interligados ou associados, um ou mais dos quais efetuam o tratamento automático de dados digitais com base num programa. Por fim, os dados digitais armazenados, tratados, obtidos ou transmitidos por elementos acima indicados, tendo em vista a sua exploração, utilização, proteção e manutenção (Artigo 2.º, alínea a), da Diretiva n.º 2002/21/CE, do Parlamento Europeu e do Conselho, de 7 de março de 2002; CNCS, 2022, p. R).
Redes Sociais	São plataformas usadas para criar ligações sociais entre pessoas que partilham interesses ou atividades similares. Este sistema *Web* providencia uma variedade de meios para que os utilizadores interajam, tais como *chat*, mensagem, *e-mail*, vídeo, *chat* de voz, partilha de ficheiros, *blogging*, grupos de discussão, etc. (Richardson, Milovidov, & Schmalzried, 2017; CNCS, 2022, p. R).
Resiliência	Capacidade de adaptação rápida e/ou recuperação de qualquer tipo de disrupção, para permitir a continuidade das operações a um nível aceitável tendo por base os objetivos de missão e o impacto na segurança (CNCS, 2022, p. R).
Risco	Possibilidade de uma ameaça específica explorar as vulnerabilidades internas e externas de uma organização ou de um dos sistemas por ela utilizados, causando assim danos à organização e respetivos ativos corpóreos ou incorpóreos. Mede-se pela combinação entre a probabilidade de as ameaças ocorrerem e o respetivo impacto. Pode ser compreendido como uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação (Decisão do Conselho n.º 2013/488/EU, de 23 de setembro de 2013; Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016; CNCS, 2022, p. R).

Roubo de Identidade	Fraude cometida através do roubo da informação de identificação pessoal, reforçada pela digitalização massiva dos dados pessoais dos indivíduos, o que, grande parte das vezes, inclui informação relacionada com aspetos legais e civis (CNCS, 2022, p. R).
Scanning	Envio de pacotes ou solicitações a outros sistemas de forma a obter informação para ser usada em ataque subsequente (CNCS, 2022, p. S).
Script Kiddies	Indivíduos com poucas competências na realização de ciberataques que, ainda assim, os conseguem realizar através da aquisição de ferramentas de *hacking* fáceis de adquirir e usar. Estas ferramentas podem tornar-se meios com muito alcance nas mãos de grupos com poucas capacidades. Além disso, quando se tenta quantificar o conhecimento disponível e poder de ataque dos *script kiddies*, consegue-se ter um vislumbre de um dos desafios de cibersegurança: jovens com alguma orientação podem tornar-se muito eficientes em ações de *hacking* (ENISA, 2018; CNCS, 2022, p. S).
Segurança das Redes dos Sistemas de Informação	A capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles (Diretiva (UE) n.º 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016; CNCS, 2022, p. S).
Segurança de Redes	Conjunto de regras que devem ser respeitadas no acesso a redes de comunicação, na navegação na *Web*, no uso de palavras-passe e de chaves criptográficas, e nos ficheiros anexados a mensagens de correio eletrónico. Geralmente são integradas num documento que expõe a arquitetura do ambiente de segurança da empresa (CNCS, 2022, p. S).
Segurança Informática	Tomada de um conjunto de medidas de segurança (físicas, lógicas e administrativas) e de medidas de urgência em caso de situações imprevistas, de forma a assegurar a proteção dos bens informáticos

	de uma organização (*hardware*, *software* e dados), assim como a continuidade do serviço. Segurança informática é o conjunto de confidencialidade, integridade e disponibilidade (CNCS, 2022, p. S).
Sistema de Informação	Dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção (Diretiva n.º 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013; CNCS, 2022, p. S).
Sistema Informático	Significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado de dados. Outra definição, explica-o como qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção (CNCS, 2022, p. S).
Smishing	Combinação das palavras SMS e *phishing*, tratando-se da tentativa de adquirir informações pessoais, financeiras ou de segurança por texto mensagem (CNCS, 2022, p. S).
Software Malicioso	Programas informáticos destinados a perturbar, alterar ou destruir todos ou parte dos módulos indispensáveis ao bom funcionamento de um sistema informático. Exemplos: vírus, vermes, cavalos de Tróia (CNCS, 2022, p. S).
Spam	Mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que, para além do incómodo

	provocado aos utilizadores do correio, podem comprometer o bom funcionamento dos sistemas informáticos (CNCS, 2022, p. S).
Spin Doctors	Criadores de narrativas, através da distorção de factos. São assessores/consultores com um perfil político muito vincado e que recorrem a técnicas de indução de notícias muito sofisticadas, extravasando o âmbito das relações-públicas. A atuação destes atores é de tal forma "(…) sibilina e manipuladora que, não raras vezes, roça a amoralidade e até a ilegalidade" (Ribeiro, 2015, p. 249).
Spoofing	Mistificação IP (IP *spoofing*), que consiste na utilização do endereço IP de outro utilizador; mistificação do domínio (*domain spoofing*), que significa a utilização de um nome de domínio pertencente a outrem; mistificação do endereço eletrónico (*e-mail spoofing*), que é a utilização de outro endereço eletrónico que não o próprio do utilizador (CNCS, 2022, p. S).
Tecnologias de Informação e de Comunicação (TIC)	Integração de métodos, processos de produção, *hardware* e *software*, com o objetivo de proporcionar a recolha, o processamento, a disseminação, a visualização e a utilização de informação, no interesse dos seus utilizadores (CNCS, 2022, p. T).
Violação de Dados Pessoais	Uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público (Lei n.º 46/2012, de 29 de agosto; CNCS, 2022, p. V).
Vírus	Classe de *software* malicioso que tem a capacidade de se auto-replicar e infetar partes do sistema operativo ou de outros programas, com o intuito de causar a perda ou alteração da informação (CNCS, 2022, p. V).
Vishing	Uso de mensagens de voz ou de chamadas telefónicas, para roubar identidades e recursos financeiros. O termo resulta da combinação de *voice* e *phishing* (CNCS, 2022, p. V).
Vulnerabilidade	Insuficiência, independentemente da natureza, que possa ser explorada por uma ou mais ameaças. A vulnerabilidade pode consistir

numa omissão ou estar relacionada com uma insuficiência dos controlos no que se refere ao rigor, coerência ou exaustividade destes últimos, podendo ser de natureza técnica, processual, material, organizativa ou operacional. Fraqueza de um sistema informático, revelada por um exame à sua segurança (por exemplo, devido a falhas na análise, conceção, implementação ou operação), que se traduz por uma incapacidade de fazer frente às ameaças informáticas que pesam sobre ele (CNCS, 2022, p. V).

1. INTRODUÇÃO

> "O nosso planeta está em perigo. (...) As guerras estão a aumentar em número e ferocidade. E a confiança escasseia. (...) Juntos, temos de nos erguer contra a discriminação e o ódio que estão a envenenar as relações entre países e comunidades. E temos de garantir que as novas tecnologias, como a inteligência artificial, sejam uma força para o bem (...)" (Guterres, 2023, p. 1).

Ao longo da História, a antropogénese tem desencadeado uma série de volubilidades compósitas e intercruzadas que sobressaem como instigações existenciais para as sociedades da época (Crutzen & Stoermer, 2000). A pestilência do SARS-CoV-2 (Covid-19) e o morticínio, sem precedentes, provocado à escala planetária atestam esta asserção, cujas ressonâncias subsistem aos dias de hoje[1] (Elias, 1939; Beck, 1992; Mecklin, 2021). Fazendo uso da sua prevalência mundial, as Nações Unidas (NU) perseveram em comover a comunidade internacional para a escalada dos riscos pós-pandémicos e as transformações estruturais geradas na Humanidade. A desconfiança e a perda de credibilidade institucional, a par do caos e da desarrumação global germinadas pela pandemia[2], polarizaram as relações entre cidadãos, comunidades, sociedades e países, desbravando espaço fértil para o aparecimento de multiplicadores de ameaças (Moreira, *et al*., 2018; *WEF*, 2024a).

A crise dos nossos tempos tem por principais componentes a sua dimensão planetária, a irreversibilidade aparente, a aceleração cumulativa, a crescente agitação sociopolítica e cultural, o risco de conflitos armados (intraestatais ou e/ou internacionais) e o confronto entre a entropia e a complexidade no domínio da cultura e da informação (Soromenho-Marques, 2019; Rosner & Brown Jr., 2021). Segundo a projeção de centenas de especialistas e académicos auscultados pela plataforma *Statista*, o agravamento das alterações climáticas[3], a desinformação[4], a polarização social e/ou política e a insegurança cibernética ressaltam

[1] Em 2018, a Organização Mundial de Saúde (OMS) referenciou um elenco de doenças em relação às quais deveria existir uma estratégia mundial de prontidão, adequada à imediata ativação de mecanismos durante epidemias, nomeadamente através da aceleração de testes, vacinas e medicamentos eficazes para salvar vidas e evitar crises em grande escala. Para além da Covid-19, a listagem incluía a febre hemorrágica da Crimeia-Congo e as febres de Lassa, de Rift Valley e Zika; os vírus ébola e Marburg; as síndromes respiratórias Sars e Mers; a doença X e de nifa, entre outras. No caso da doença X, a mesma compreende o conhecimento de que uma epidemia internacional grave possa ser despoletada por patogénicos desconhecidos, adequados a provocar doenças nos seres humanos (Alves, 2024).

[2] *Vide* figura 1, em anexo.

[3] Distinguido como o ano mais quente de que há registo, 2023 assinalou inumeráveis incêndios florestais, inundações e outras devastações naturais associadas com condições meteorológicas extremas, afetando milhões de pessoas em todo o mundo (*vide* figura 2, em anexo).

[4] 'Desinformação' é toda a "(…) informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público" (CNCS, 2022, p. D). *Vide* Glossário em anexo.

como algumas das principais preocupações globais[5] para 2024 (Lewandowsky, *et al*., 2012; Richter, 2024; Dyvik, 2024).

> "O mundo está assolado por um duo de crises perigosas: clima e conflito. Tensões geopolíticas subjacentes, combinadas com o surgimento de hostilidades ativas em múltiplas regiões, estão contribuindo para uma ordem global instável caracterizada por narrativas polarizantes, pela erosão da confiança e insegurança" (Zahidi, 2024, p. 4).

A conflitualidade parece cadenciar o pulsar da contemporaneidade, como atestam as guerras de atrito israelo-palestiniana (desde 1948) e russo-ucraniana (desde 2014) às portas da Europa[6], ensombrando o ideal pacifista da *Declaração de Schuman*[7] (1950). Tendo entrado no seu terceiro ano, a invasão militar russa na Ucrânia (2022) – a pior crise de segurança desde a Segunda Guerra Mundial (1939-1945) –, a corrida armamentista e a proliferação nuclear[8], a revolução digital e a sofisticação dos ciberataques, a globalização do (ciber)terrorismo e a competição geoeconómica entre a América e a China[9], entre outros fatores, adensam as tensões geopolíticas[10] e reconfiguram a ordem internacional liberal, tal como a compreendíamos[11] (Eaves, 2021; Oledan, *et al*., 2021; Squassoni, 2021; Gill & Goolsby, 2022; Cohen, *et al*., 2023; Fernandes, 2024b). A "parceria abrangente" e a "cooperação estratégica" entre a Rússia e a China, decursivas de uma relação "sem limites", prometem traçar uma nova disposição sino-cêntrica (Ribeiro, 2013; Costa, 2020; Tomé, 2020 e 2023). Para o presidente chinês, Xi Jinping, a "(…) China está disposta a (…) alcançar conjuntamente o desenvolvimento e o rejuvenescimento dos (…) respetivos países e trabalhar em conjunto para defender a equidade e a justiça no mundo" (Redação Exame,

[5] *The Cornell Alliance for Science* classificou as principais criticidades para a sociedade global em 2024. 53 % dos inquiridos elegeram a desinformação gerada por inteligência artificial (IA) e 46 % dos inquiridos escolheram a polarização social e/ou política (Dyvik, 2024). *Vide* figura 3, em anexo.

[6] O mundo tornou-se menos pacífico nos últimos 17 anos, com aumentos substanciais da instabilidade política, do número de mortes em consequência de conflitos e manifestações violentas. O conflito em Gaza e a guerra Rússia-Ucrânia foram os principais fatores da diminuição da paz em 2024 (IEP, 2024, pp. 2-7).

[7] O Dia da Europa é comemorado anualmente a 9 de maio, assinalando a célebre proposta de Robert Schuman para uma nova forma de cooperação política na Europa, apta a favorecer a paz e a unidade europeia.

[8] Como retrata a figura 4, em anexo.

[9] Em 2016, George Friedman preanunciava mudanças nas dinâmicas de poder global. Apesar da manutenção da hegemonia de poder norte-americana, antecipou a ascensão desafiadora da China e da Rússia. Afirmava, então, que o mundo experimentaria eventos geopolíticos e conflitos significativos, como uma potencial luta entre a China e os EUA (Friedman, 2016).

[10] Originalmente concebida por Rudolf Kjellén, a 'geopolítica' é, antes de tudo, uma maneira de pensar e perceber o mundo (Kjellén, 1924; Dodds, 2007). *Vide* Glossário apenso.

[11] "(…) A Rússia considera que a ordem mundial internacional pós-Guerra Fria, baseada em regras liberais, é uma criação dos Estados Unidos e dos seus aliados europeus e um meio de os Estados Unidos manterem o seu domínio político, económico e mesmo cultural a nível mundial" (Radin & Reach, 2017, p. 22). O Kremlin pretende, assim, formar uma *post-West order*, ou seja, uma ordem mundial e internacional alternativa, de âmbito iliberal e enfoque russófono (Stent, 2014; Boyle, 2016; Kanet, 2018). A multipolaridade parece ser o seu propósito estratégico, em manifesta oposição à hegemonia de poder norte-americano.

2024, p. 1). O provável regresso de Trump à Casa Branca – o maior incitador da desinformação – atemoriza os mercados financeiros e o globo com a sua visão de "soma zero" (Evanega, *et al*., 2020b; Fernandes, 2022a). A desintegração da *velha ordem* é observável por todo o lado (*The Economist*, 2024a). "(…) As divisões geopolíticas estão a impedir-nos de nos unirmos em torno de soluções globais para os desafios globais" (Guterres, 2024, p. 2). As criticidades contemporâneas, quando associadas à galvanização disruptiva das ciências da vida e das tecnologias emergentes, perigam a supervivência da sociedade moderna e das democracias ocidentais[12] (Richter, 2024). Segundo Emmanuel Macron: "(…) Temos de ser claros quanto ao facto de que, hoje, a nossa Europa é mortal. (…) Pode morrer, e tudo depende das nossas escolhas" (Macron, 2024, p. 3). Todos estes dinamismos constituem forças estruturais globais em relação às quais importa criar mecanismos coletivos de resposta transfronteiriça, estratégias localizadase esforços inovadores e coordenados (*WEF*, 2024a; Mecklin, 2024).

Amplificada pelos progressos tecnológicos e pela inteligência artificial (IA), a "infoguerra"[13] manifestou-se como uma portentosa vulnerabilidade para a segurança global, ameaçando a arrumação internacional e os equilíbrios estabelecidos[14] (Libicki, 2009; Fernandes, 2012). "(…) Não é um exagero dizer que os Estados modernos são Estados informativos: Estados que reconhecem e resolvem problemas de governação através da recolha, análise e distribuição de informação" (Balkin, 2012, p. 4). Disputando o ciberespaço e o ecossistema de informação como territórios geopolíticos, a infoguerra e a desinformação[15] exploram as assimetrias da literacia digital das comunidades

[12] O *World Economic Forum* identificou as dez tecnologias emergentes com o potencial para reconfigurar o mundo em 2024, a saber: IA para a descoberta científica; tecnologias de reforço da privacidade; superfícies inteligentes reconfiguráveis; estações de plataforma de alta altitude; deteção e comunicação integradas; tecnologia imersiva para o mundo construído; elastocalórica; micróbios captadores de carbono; alimentos alternativos para animais; e genómica para transplantes (*WEF*, 2024b). Em 2024, cerca de 76 países e quase metade da população mundial vai a eleições, num exercício de democracia que, paradoxalmente, defronta uma conjunção de múltiplas ameaças, particularmente as tecnologias de IA generativa (Zovatto, 2022; Buchholz, 2024). As eleições na América, Europa, Índia, Indonésia ou Venezuela desvelam o poder dos números em jogo (*International IDEA*, 2023).

[13] Entende-se por 'infoguerra', ou guerra de informação, "um conflito relacionado com a informação a um grande nível, entre estados ou sociedades" (Arquilla & Ronfeldt, 1993, p. 28). *Vide* Glossário anexo.

[14] Friedman preadivinhou a essencialidade da tecnologia na modelação do futuro, com avanços em áreas como robótica, IA e exploração espacial impactando na política global, na economia e na guerra (Friedman, 2016).

[15] É essencial diferenciar os diferentes fenómenos que são erroneamente designados por 'desinformação' a fim de conceber respostas adequadas. 'Informação incorreta' é o conteúdo falso ou enganador, partilhado sem intenção de prejudicar, mas cujos efeitos podem causar danos, por exemplo quando as pessoas partilham informações falsas com amigos e familiares de boa-fé. 'Tentativas de exercer influência sobre a informação' são esforços coordenados desenvolvidos por intervenientes internos ou externos com o objetivo de influenciar uma audiência-alvo através de vários meios enganadores, incluindo a supressão de fontes de informação independentes em combinação com a desinformação. Por fim, a 'interferência estrangeira no espaço de

interconectadas, moldando conteúdos e influenciando a construção da opinião pública (Libicki, 2009; Lewandowsky, *et al*., 2012; informação verbal[16]). Usufruindo da diminuta regulamentação e ausência de controlo efetivo, vários atores globais utilizaram o potencial disruptivo do envolvente digital para explorar as inclinações, atitudes adversas e vulnerabilidades inerentes à natureza e condição humana (Douglas, *et al*., 2019). O isolacionismo típico das comunidades cibernéticas intensifica o autismo informacional, a falta de capacidade crítica e o discurso dicotómico, deliberadamente emotivo (Jesus, 2020; Barrinha, 2020). A empatia e a adscrição do usuário proliferam em relação a alegorias desvirtuadas da realidade, num género de distopia digital (Zaval & Cornwell, 2016). O condicionamento cognitivo compromete o discernimento epistemológico e evoca a predominância de instintos primários e pouco reflexivos, dando lugar à intolerância, discriminação, radicalismo e violência[17] (Arendt, 1963; Bodenhausen, Sheppard, & Kramer, 1994; Goel & Vartanian, 2011). Uma vez inseminada no ventre globalizado da informação, a disrupção infodémica, associada ao negacionismo científico[18] e à incredulidade generalizada quanto aos reguladores tradicionais, catalisou a propagação da desinformação

informação', realizada frequentemente no âmbito de uma operação híbrida mais vasta, pode ser entendida como os esforços desenvolvidos por um interveniente estatal estrangeiro ou pelos seus agentes para corromper a livre formação e expressão da vontade política dos indivíduos, utilizando meios coercivos e enganadores (Comissão Europeia, 2020a, p. 21). Este racional é refletido no 'Relatório Especial Desinformação na UE: fenómeno combatido, mas não controlado' (União Europeia, 2021).

[16] Comunicação de Pedro Matos, do Centro Nacional da Cibersegurança (CNCS), na Conferência 'A nova geopolítica da Segurança: Ciberespaço e dimensões disruptivas', de 19 de abril de 2023, no ISCPSI.

[17] De acordo com Arendt, a trivialização da violência está relacionada com a falta de pensamento crítico, resultando na instalação da banalidade do mal. De forma análoga, no ecossistema de informação corrompido a polarização está ligada a uma dinâmica cognitiva opaca, vazia e agressiva, especialmente propícia à generalização e à banalização da infodemia (Goel & Vartanian, 2011).

[18] Os negacionismos nucleares e ambientais estão intrincadamente relacionados à infoguerra e ao seu exagero nos circuitos digitais (Elsasser & Dunlap, 2013; Alam, *et al*., 2020). Em jogo estão vários mecanismos psicológicos e preconceitos cognitivos recrutados para mitigar esta problemática, tais como a disponibilidade heurística (Zaval & Cornwell, 2016); a substituição de atributos (Kahneman & Frederick, 2002); a aversão às perdas, na qual se valorizam mais as carências do que os ganhos de igual valor; e o enviesamento otimista, que sugere a generalização da probabilidade de ocorrência de um acontecimento negativo como algo de natureza excecional, numa lógica de que só acontece aos outros (Lin, 2019). O financiamento de campanhas de desinformação por conglomerados negacionistas para ofuscar a verdade científica sobre determinado interesse é uma realidade insofismável (Goel & Vartanian, 2011; Oreskes & Conway, 2011; Goldenberg, 2013).

multimédia ("memes"[19]), teorias de conspiração[20] e *fake news* (notícias falsas)[21], sobretudo através de influenciadores digitais e figuras políticas de proa (Goldenberg, 2013; Gelfert, 2018; Douglas, *et al*., 2019; Keeley, 1999; Roxburgh, *et al*., 2019; Jesus, 2020; Scott, 2020a e 2020b; Cerulus, 2021; Rottweiler & Gill, 2021; Wendling, 2021). Pervertendo o postulado *hobbesiano* de que *scientia potentia est*[22], a desinformação, otimizada por sobrecargas massivas de dados desordenados, mergulhou a sociedade coeva numa crise profunda (Hobbes, 1651; Lewandowsky, *et al*., 2012; Soromenho-Marques & Magalhães, 2024).

"Toda a guerra se baseia no engano" (Sun Tzu, 2023, p. 17). A massificação do compartilhamento desorganizado de retóricas inflamadas, especulativas e acríticas[23] que culpabilizam grupos específicos, *i.e*., "bodes expiatórios", e incitam à desordem social, nuclearizou a eficácia das respostas dos sistemas públicos e minou a confiança na informação (Keeley, 1999; Pfeffer, Zorbach, & Carley, 2014; Douglas, *et al*., 2019; Rottweiler & Gill, 2021). A "infodemia" pode ser definida como "(…) um excesso de informações, algumas precisas e outras não, que tornam difícil encontrar fontes idóneas e orientações confiáveis quando se precisa" (Zarocostas, 2020, p. 676). O vocábulo refere-se ao invulgar aumento do volume de informações relacionadas com um tema específico e que se multiplica exponencialmente em pouco tempo, por força de um catalisador específico. Numa sociedade interconectada digitalmente, as plataformas de comunicação social aceleram a difusão indiferenciada e o consumo acrítico de rumores, informações maliciosas ou manipuladas, como se de um vírus se tratasse[24] (Cadwalladr, 2019). Enquanto acelerador

[19] Criada em 1976 por Richard Dawkins, a expressão 'meme' visa explicar como os artefactos culturais evoluem ao longo do tempo e à medida que se difundem pela sociedade, replicando-se através de atos imitativos. *Vide* Glossário anexo.

[20] A *QAnon* consiste numa teoria da conspiração da extrema-direita norte-americana que alega haver uma cabala secreta da esquerda, formada por adoradores de Satanás, pedófilos e canibais, que dirige uma rede global de tráfico sexual infantil e que conspirou contra o mandato de Donald Trump. Vulgarizada durante as eleições presidenciais norte-americanas de 2016, esta e outras teorias, como a *Pizzagate*, foram profusamente compartilhadas nas redes digitais e sociais. Apesar de contestadas por diversas organizações e entidades, tais conjeturas foram assimiladas por milhares de cibernautas, redefinindo as idiossincrasias conspiratórias (McConnachie & Tudge, 2008; Amarasingam & Argentino, 2020).

[21] Trump, enquanto presidente norte-americano (2017-2021), quando confrontado com posições contrárias ou informações negativas, refutava-as amplamente nas redes sociais, classificando-as de *fake news*, de 'factos alternativos' ou mesmo de hipérbole da verdade (Gelfert, 2018; Keeley, 1999). A associação de Trump a informações falsas propaladas nos *media* foi de tal grandeza (38%) que foi considerado o maior impulsionador da infodemia sobre a Covid-19 (Evanega, *et al.*, 2020a; Soares, 2020).

[22] "Conhecimento [ou Informação] é poder" (Hobbes (1651). Leviatã: Ou A Matéria, Forma e Poder de uma República Eclesiástica e Civil, traduzida por João Paulo Monteiro, Maria Beatriz Nizza da Silva, Cláudia Berliner, 2019. São Paulo: Martins Fontes).

[23] Kahneman (2011) sustenta que os julgamentos rápidos, precipitados e intuitivos têm, as mais das vezes, precedência sobre o pensamento analítico, mais exigente e demorado.

[24] Gigantescos conglomerados económicos, como a *Google*, *Meta*, *Microsoft*, *TikTok*, *Amazon*, *Tesla* e *Youtube*, capitalizam financeiramente os dados pessoais dos utilizadores, hoje mais valiosos do que o petróleo. Estas

de ameaças híbridas[25] que transcendem fronteiras e autoridades, a infodemia ameaça tudo, em todo o lado e ao mesmo tempo, perigando a estabilidade das democracias e apadrinhando a consolidação das autocracias[26] (Hyvönen, 2018; Scott, 2020b; Alam, *et al*., 2020; Smith, Cubbon, & Wardle, 2020; Cerulus, 2021; Oledan, *et al*., 2021; Stover, 2021).

Confrontado com um ambiente cosmopolita, volátil e compósito, o policiamento complexificou-se e estendeu-se às sofisticações de interdependência securitária entre os Estados. Intervindo muito para além dos contornos típicos da segurança interna pátria, a atuação policial moderna assenta, em boa medida, em políticas de cooperação transfronteiriça convencionadas entre aliados, membros de subsistemas regionais de segurança e organizações internacionais (Elias, 2013). Geográfica e politicamente comprometido com o projeto da União Europeia (UE), Portugal, através dos Ministérios dos Negócios Estrangeiros (MNE), Justiça (MJ) e Administração Interna (MAI), projeta, desde a década de 1990, recursos policiais especializados para missões e estruturas de cooperação internacional, nomeadamente da UE, NU e Organização Internacional de Polícia Criminal (INTERPOL). Integrando redes multinacionais agregadoras de parceiros estratégicos da segurança internacional, de entre os quais se destaca a Agência da UE para a Cooperação Policial (EUROPOL), o país contribui para o policiamento pan-europeu através da

cleptocracias digitais monitorizam e armazenam anonimamente todas as interações digitais, utilizando sofisticadas ferramentas de IA para analisar as informações e criar perfis de personalidade. Com base nestes perfis, desenvolvem estratégias de persuasão infodémica, criando conteúdos personalizados que são disseminados globalmente. Os utilizadores mais suscetíveis a estímulos emotivos, como medo, ódio e vaidade, são alvos preferenciais. Esta capacidade tecnológica é vista como uma arma psicológica numa infoguerra global, capaz de moldar comportamentos e ameaçar a autodeterminação individual. A falta de regulação e supervisão desses conglomerados tecnológicos representa uma ameaça às democracias. Alguns defensores dos direitos civis propõem considerar os direitos aos dados pessoais como novos Direitos Humanos (informação verbal, apresentada por Carole Cadwalladr, em abril de 2019, no âmbito da Conferência *TED talk*, sob a égide: 'O papel do Facebook no Brexit e a ameaça à democracia'; informação verbal, apresentada no documentário da *Netflix*, intitulado 'Nada é privado: O escândalo da *Cambridge Analytica*', de 24 de julho de 2019, realizado por Karim Amer e Jehane Noujaim; Arquilla & Ronfeldt, 1993).

[25] Entende-se por 'ameaças híbridas' a "(…) a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada. Em geral, a tónica incide na exploração das vulnerabilidades do alvo e na criação de ambiguidade para entravar o processo de tomada de decisões" (Comissão Europeia, 2016a, p. 2). *Vide* Glossário anexo. O conceito de 'guerra híbrida russa' ganhou grande projeção nos debates sobre os conflitos modernos (Clark, 2020).

[26] Atenda-se, exemplificativamente, como a manipulação disruptiva da opinião e da perceção pública em momentos cruciais da política eleitoral de diversos Estados alterou, de modo significativo, os contornos geopolíticos de poder em várias regiões do globo terrestre. Disso são exemplo o ocorrido na Tailândia (1997), em Trindade e Tobago (2009), na Índia (2010), em Itália (2021), no Quénia e na Malásia (2013), na Argentina (2015), nos EUA (2016) e no referendo de 2016 que redundou no processo de saída do Reino Unido da UE (*Brexit*). Um outro caso, particularmente alarmante, refere-se à rede social *Facebook* e ao condicionamento que infligiu na instigação das etnias predominantes em Myanmar contra a comunidade Rohingya, desencadeando uma profunda crise humanitária (*The New York Times*, 2018). Rememore-se o assalto ao Capitólio norte-americano por uma turba de manifestantes, animada por teorias conspiracionistas e negacionistas pró-Trump, provocando a morte de 5 pessoas (Wendling, 2021; Simon, 2021; Wu Ming 1, 2022).

mobilização de oficiais de ligação do MJ (OLMJ), oriundos da Polícia Judiciária (PJ), e, desde 2021, do MAI (OLMAI), provenientes da Guarda Nacional Republicana (GNR) e da Polícia de Segurança Pública (PSP). Colmatando lacunas e construindo alianças, os OLMJ e os OLMAI estabeleceram-se como interlocutores favorecidos da diplomacia policial portuguesa em prol da segurança europeia (Fernandes, 2024a e 2024b).

Circunscrevendo a investigação aos OLMAI destacados na EUROPOL, certificamos que estes agentes diplomáticos policiais, acreditados no aparato diplomático-cooperativo, desempenham missões capitais, de âmbito estratégico e operacional, no estabelecimento de relações de proximidade, reciprocidade e confiança junto de estruturas policiais análogas. A sua integração em redes, fóruns, grupos de trabalho e círculos reservados, anteriormente exclusivos a políticos e diplomatas de carreira, proporciona-lhes o acesso privilegiado a produtos analíticos, informações estratégicas e sistemas sofisticados interagências que os habilitam a influenciar dossiês e políticas de segurança de impacto transnacional, em alinhamento com as Políticas Externas e de Segurança Interna (Fernandes, 2022b).

As repercussões da pandemia de Covid-19 nas dinâmicas de poder das relações internacionais, a beligerância russo-ucraniana[27] e a emergência de táticas não convencionais ligadas à dimensão infodémica[28] instigaram-nos a desenvolver uma análise atualizada (SSI, 2023). A nossa investigação aborda os impactos da proliferação da infodemia na segurança europeia, com enfoque na catalisação disruptiva da Federação da Rússia para confrontar e destabilizar o Ocidente (GEC, 2020; Sanger, Perlroth, & Schmitt, 2020; Finnin & Roozenbeek, 2022). A garantia da paz e a confiança da comunidade parecem depender da adaptação eficaz a estas mudanças vertiginosas, de modo a reverter a tendência *lose-lose* decursiva da última Conferência de Segurança de Munique[29] (Bunde, Eisentraut, & Schütte,

[27] Numa breve referência ao 'segredo de Fátima', recorde-se que o mesmo consistiu numa série de visões que três crianças afirmaram ter recebido da Virgem Maria, em Fátima, Portugal, no ano de 1917. Uma parte do segredo preanunciava a Rússia a espalhar os seus "erros" pelo mundo, no que foi considerado uma alusão à disseminação do comunismo consequente da Revolução Russa (1917) e da subida ao poder de Vladimir Ilyich Ulianov, conhecido por Lenine. A relação do segredo com a invasão russa à Ucrânia – o celeiro da Europa – e a exacerbação da insegurança alimentar global é interpretativa e especulativa, inexistindo consenso entre a conexão das visões de Fátima com os eventos geopolíticos coevos no Médio Oriente e Norte de África.

[28] Criada em 2015, no rescaldo na anexação da Crimeia pela Rússia, a plataforma *EUvsDisinfo* visa prever, analisar, expor, gerir e responder às campanhas de desinformação (incluindo, refutação *fact-checking*) do Kremlin, consciencializando (comunicação do risco) os cidadãos europeus sobre essas operações e capacitando-os para identificarem e resistirem à manipulação da informação digital e dos *mass media* (Xavier, 2023). O projeto destaca a sinalização de quase 500 casos de desinformação pró-Kremlin sobre a Covid-19. A mesma fonte identificou ainda mais de 10000 exemplos de desinformação russófona. O Serviço Europeu para a Ação Externa (SEAE), através de diferentes forças-tarefa, tem conferido atenção aos Estados hostis no seu relatório analítico anual, com destaque para a Rússia (*EUvsDisinfo*, 2020; Comissão Europeia, 2020a, p. 22).

[29] A *Munich Security Conference* (MSC), ou *Wehrkundetagung*, é um fórum anual, realizado desde 1963, onde políticos, diplomatas, estrategas, cientistas, militares e industriais abordam os desafios atuais e futuros da

2024). O policiamento proficiente a estes fenómenos transnacionais exige novas capacidades, técnicas, recursos e abordagens colaborativas e pluridisciplinares, envolvendo parcerias das polícias nacionais e internacionais com os diferentes setores (públicos e privados) da sociedade, incluindo governos, organizações não governamentais (ONG), conglomerados económicos, entre outros (Comissão Europeia, 2020a).

Partindo do reconhecimento desta problemática a nossa contribuição estruturou-se em seis secções. Começando por explicitar o advento do "polícia científico" na "era digital", correlacionamos a conflitualidade pós-pandémica e os seus refluxos infodémicos na corrupção do ecossistema da informação global com a resposta fornecida pelo policiamento transnacional coevo, personificada *in casu* pela EUROPOL e pelos OLMAI ali destacados (Fortin, 2009). Através de uma análise dedutiva, centrípeta às Ciências Policiais[30] e arrolada com a Ciência das Relações Internacionais[31], o estudo procura responder à questão: Como é que o policiamento pan-europeu, assente nas novas tecnologias digitais, contribui para superar os desafios securitários apresentados pela infodemia pró-russa? Circunscrevendo as variáveis do presente estudo para melhor responder à pergunta principal, incluímos as seguintes questões derivadas: a) Quais as tecnologias e produtos analíticos desenvolvidos pela EUROPOL aproveitam a estratégia anti-infodémica? b) Em que medida a cooperação interagências contribui para mitigar aquelas ameaças híbridas no contexto europeu? c) Quais as prudências tidas pela EUROPOL na implementação da estratégia anti-infodémica? d) Quais as linhas de ação para a PSP neste campo concreto?

Na decorrência de uma análise documental baseada em fontes narrativas, em registos públicos ou privados, na imprensa e vários estudos e relatórios, explicitaremos os ecos da

política externa, defesa e segurança internacional (Vandenhoeck & Ruprecht, 2014; *Munich Security Conference Foundation*, 2024).

[30] De acordo com o Artigo 5.º do Decreto-Lei n.º 13/2022, de 12 de janeiro, as Ciências Policiais compõem um "(…) acervo organizado e sistematizado de conhecimentos científicos sobre a organização policial, enquanto instituição, e sobre a ação policial, enquanto processo, cujo estudo científico aplicado contribui para a edificação de padrões de atuação dos organismos policiais e dos seus profissionais, tendo por referência os direitos fundamentais dos cidadãos, a defesa da legalidade democrática e a garantia da segurança interna". Segundo Jack R. Greene, a "(…) ciência policial ocupa-se do policiamento no seu sentido mais lato, desde o policiamento como um conjunto de comportamentos individuais até às interconexões do policiamento em todo o mundo. A ciência policial situa-se na intersecção do direito, das ciências físicas (no caso da ciência forense), psicologia, psicologia social, sociologia, políticas públicas, história, economia, métodos de avaliação e análise estatística, bem como a criminologia e a administração da justiça. A variedade é considerável nos domínios de conhecimento que informam a nossa compreensão do policiamento" (Greene, 2007, pp. xix-xx).

[31] As Relações Internacionais constituem uma disciplina científica centrada no estudo sistemático das relações e interações políticas, económicas, jurídicas, estratégicas, sociais, ideológicas e culturais, conflituosas e cooperativas, que os agentes sociais realizam através das fronteiras dos Estados. Trata-se de um campo interdisciplinar que se caracteriza por três conjuntos distintos de perspetivas: "conflito, segurança e guerra; cooperação e condições para a paz; equidade, justiça e fontes de desigualdade internacional" (Silva & Gonçalves, 2010, pp. 244-246).

"era digital" no policiamento europeu, interligando-os com as complexidades apresentadas pela infodemia na desorganização do mapeamento informacional e mediático (Sarmento, 2013). Examinando o ecossistema de propaganda e desinformação fabricado pela Rússia, demonstraremos a relevância da EUROPOL na promoção da integridade da informação e na proteção democrata contra as ameaças híbridas russófonas (*гибридная война*). Enunciado este argumentário e afloradas as dimensões implícitas, buscar-se-á apresentar o contributo da cientificização da atividade policial e do potencial patenteado pela cooperação internacional na partilha de tecnologias digitais e informações fidedignas entre a comunidade policial (Vollmer, 1930; Zarocostas, 2020). A estratégia anti-infodémica refere-se, portanto, à concertação de esforços europeus para combater a desinformação por via da promoção de informação rigorosa e de confiança, favorecendo as capacidades de pensamento crítico e implementando medidas para contrariar a difusão massiva de informações falsas nos canais noticiosos e nas multiplataformas. A intercessão promovida pelos OLMAI, destacados na EUROPOL, num ambiente cooperativo complexo, multinível e multilátero, com acesso partilhado a avançados sistemas de informação, parece surgir como um sinal de esperança na conciliação de esforços internacionais em benefício do bem-comum (EUROPOL, 2022a).

2. A ERA DIGITAL E O 'POLÍCIA CIENTÍFICO'

> "É um erro capital teorizar antes de se dispor de todas as provas. Enviesa o julgamento" (Doyle, 1887).

A expressão "era digital" surge do desenvolvimento histórico que culminou no período tecnológico atual e na sua democratização. À frente do seu tempo, Alan Turing (1950) questionou-se se seria "(…) teoricamente possível que um computador digital de estados finitos, equipado com uma tabela de instruções grande, mas finita, ou programa, forneça respostas a questões que levem um interrogador desconhecedor a pensar que é um ser humano?" (Turing *apud* Santo, 2019, p. 38). Desde então, este dilema foi amplamente discutido e inspirou uma classe de teorias funcionalistas coetâneas (Putnam, 1960; Gödel, 1990). A "máquina de Turing universal" corresponde ao que designamos por computador digital (Santo, 2019, p. 16). "(…) O trabalho da computação digital é semelhante a contar pelos dedos" (Peters, 2016, p. 104). A computação (ou "teste de Turing")[32] é apreciada como a pedra angular da teoria da IA que tanto seduz e inquieta a sociedade coeva (Rothbaum, *et*

[32] Segundo Arlindo Oliveira, o pressuposto fundamental da IA baseia-se no "teste de Turing", o qual sugere que qualquer computação realizável num computador pode ser realizada noutro, levantando a possibilidade de que o cérebro humano, sendo um "tipo de computador", possa ter suas funções replicadas por máquinas (Oliveira, 2018, p. 4).

al., 1997). O aprofundamento da investigação científica, a globalização e os progressos tecnológicos dos últimos quarenta anos consagraram a dimensão digital como algo indissociável das atividades quotidianas, caraterizadas pela hiperligação a múltiplas redes, serviços e tecnologias digitais, às quais o policiamento não é alheio (Arquilla & Ronfeldt, 2001). Foram necessários contributos de matemáticos, filósofos, inventores, cientistas, empresários e programadores para conceber, preparar e substantificar a era digital[33].

> "(…) Os processos dominantes na era da informação estão cada vez mais organizados em torno de redes. Redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura. (…) Redes são estruturas abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmos códigos de comunicação (…)" (Castells, 1999 [1942], p. 565).

Numa contemporaneidade vincada pela capilaridade digital e informacional importa distinguir os conceitos de "digitização" (*digitisation*) e digitalização" (*digitalisation*) (Nogala, 2023, p. 7). A "digitização" respeita ao processo de converter informações de um formato físico para digital (*v.g*., textos, imagens, sons, etc.); enquanto que a "digitalização" envolve a utilização de dados digitais para aprimorar processos de perceção, comunicação e interação, crescentemente assistidos pela IA, como *bodycams*, drones, sistemas automatizados de deteção de tiros, identificação de placas de veículos e de videovigilância, soluções biométricas de identificação de impressões digitais[34], reconhecimento facial[35] e análise preditiva, sistemas de posicionamento global, entre outros (Brennen & Kreiss, 2016). A digitalização apoia-se, como vimos, numa infraestrutura tecnológica construída ao longo de séculos, com progressos em variadíssimas áreas do Saber (Nogala, 2023).

A era digital abrange a interligação compreensiva entre computadores, informações, redes e outras inovações tecnológicas, redundando em alterações significativas nas práticas sociais e costumes desde a disponibilização massiva dos computadores. Esta época distingue-se pela hiperconexão e a capacidade em processar tecnologicamente quantidades

[33] De acordo com Arlindo Oliveira, as contribuições históricas de figuras como Thomas Hobbes, Charles Babbage, Ada Lovelace e Alan Turing pavimentaram a rota para o desenvolvimento da IA. Todavia, ainda há um caminho a percorrer para alcançar sistemas com inteligência equivalente à humana (Oliveira, 2018).
[34] Como o *Automated Fingerprint Identification System* (AFIS).
[35] O reconhecimento facial é uma tecnologia que tem ganho destaque, mas também enfrenta desafios significativos (Almeida, 2022, p. 276). Estudos desenvolvidos no Reino Unido, indicam que, em média, 95% das correspondências feitas por reconhecimento facial resultaram na identificação incorreta de pessoas inocentes. As forças policiais armazenaram as fotografias das pessoas incorretamente identificadas pelos sistemas de reconhecimento facial automatizado, ficando na posse indevida de milhares de fotos biométricas de cidadãos comuns (BBW, 2018, p. 3). Este contexto concorre para o reconhecimento das implicações éticas e sociais do uso de ferramentas digitais na aplicação da lei, sobretudo ao nível das limitações de dados, viés de automação, impactos sociais, etc. (Bigo, 2006).

elevadas de dados. Nas décadas de 1970 e 1980, o desenvolvimento e acesso universal a equipamentos informáticos transverteu as relações comerciais e as trocas informações nas sociedades industriais avançadas (Alvin, 1980). Como sustentado por Detlef Nogala, foram necessários "(…) pelo menos oito séculos do ponto de vista europeu (…)" para edificar tecnicamente a infraestrutura digital que está na base do processo de digitalização hodierno (Nogala, 2023, p. 9). A era digital representa um período de informatização e desterritorialização da informação através das redes universais descritas por Castells (1999). O poder e o vazio de poder são calculados em função do acesso a redes e do controlo dos seus fluxos de recursos financeiros ou informacionais. "As redes são portas de acesso onde se sucedem oportunidades. Fora das redes, a sobrevivência é cada vez mais difícil" (Elias, 2022, p. 339). Os computadores atuais são um produto intermédio de uma sequência gradual de inovações e melhorias técnicas. Atuando como ferramentas complexas e interconectadas, capazes de processar quantidades de dados anteriormente inimagináveis, as modernas "máquinas de Turing universal" desencadearam transformações profundas. Se considerarmos que a criação, utilização, distribuição, manipulação e integração da informação são características típicas de uma "sociedade da informação", então uma "sociedade digital" é aquela em que a adoção e incorporação de tecnologias avançadas nos processos sociais e culturais são proeminentes. A *internet*, por exemplo, seria inconcebível sem a informatização e a tecnologia das redes globais, juntamente com as digitalizações subjacentes (Arquilla & Ronfeldt, 2001; Castells, 2003).

Contudo, a transferência sistémica das rotinas diárias para apresentou-nos ao "(…) lado negro do mundo digital" (Guterres, 2020, p. 2). Desregulado, sem fronteiras e desprovido de curadoria, o ambiente digital desvelou áreas de negócio e oportunidades para a expansão da criminalidade organizada local, nacional, regional e internacional, frequentemente associadas a abusos e iniquidades cibernéticas, como vírus informáticos, ciberassédio, *cyberbullying*, ataques *Distributed Denial-of-Service* (DDoS), *hackers*, *malware*, fraude em linha, *ransomware*, *phishing*, *spam*, técnicas de *spoofing*, desinformação, entre tantos outros incidentes digitais. Os crimes digitais, as *cyberwars* e as *netwars* são a "moeda de troca" pelas comodidades e benefícios modernos (Beck, 1992, p. 19; Arquilla & Ronfeldt, 1993 e 2001; Libicki, 2009). O crime organizado transnacional (COT) da época digital apresenta maior fluidez, complexidade e uma natureza multifacetada, sendo moldado por uma infinidade de forças, oportunidades e mudanças estruturais no sistema internacional. Envolve bens e serviços, pessoas e dinheiro, tecnologia e poder, território e capacidade de adaptação permanente às oportunidades estruturais económicas,

tecnológicas, legais, sociais e políticas (Bastrup-Birk, *et al.*, 2023). A cibercriminalidade é uma realidade incontrovertível que não reconhece soberanias, merecendo a mais atenta vigilância, análise e repressão das forças policiais[36] (Marion & Twede, 2020).

> "No seu início, o policiamento era bastante acientífico, ou seja, não estava bem ligado ao conhecimento científico. Os rápidos avanços da ciência ao longo do século XX alteraram a necessidade de proficiência científica da polícia. (…) O papel da investigação e do inquérito científicos expandiu-se e é provável que continue a expandir-se com os progressos das ciências forenses" (Greene, 2007, p. xxiv).

O sucesso do policiamento e da aplicação da lei dependem do apetrechamento de instrumentos e procedimentos atualizados aos sinais dos tempos. Com maior expressão a partir de 1950, a profissionalização do policiamento introduziu progressivamente técnicas, táticas, equipamentos, armamento e outros acessórios ajustados ao eficaz cumprimento da missão (*Seaskate Inc*., 1998). Personalidades como Hans Gross (1847-1915), Edmond Locard (1877-1966), August Vollmer (1876-1955), Paul Kirk (1902-1970), Marvin Wolfgang (1924-1998), entre outros, revolucionaram o amadorismo do policiamento tradicional, modernizando-o segundo as prioridades sócio criminais e com recurso a aproximações da Ciência (como a criminologia, psicologia, sociologia, etc.). "(…) A polícia se apresenta numa grande variedade de formas" (Bayley, 2001, p. 19). A multidimensionalidade da atividade policial acelerou as transformações internas. A formação, o conhecimento da lei, a ética e a tecnicidade passaram a fazer parte do âmago policial, apesar das diferentes velocidades de desenvolvimento associadas à industrialização e à dedicação financeira dos países à segurança, mormente na conjunção da Europa (com os modelos britânicos, franceses, mediterrânicos ou nórdicos) e da América do Norte. Em 1920, a polícia berlinense instalou um sistema de rádio inédito para as comunicações dedicadas (Nogala, 2023). Em 1935, a INTERPOL[37] – que recentemente celebrou um século de existência –, lançou a primeira rede-rádio internacional, fornecendo uma rede de telecomunicações independente e exclusiva para utilização das autoridades policiais nacionais agregadas (INTERPOL, s.d.). A partir da década de 1970, os Estados Unidos da América (EUA) e a Alemanha introduziram os primeiros sistemas informáticos para o processamento de dados criminais no serviço policial, posteriormente estendidos aos países mais desenvolvidos e às polícias de combate ao crime transfronteiriço (Bergien, 2017). Em

[36] Em 2018, Portugal era o 8.º país europeu mais vulnerável ao cibercrime (Watts, 2018). *Vide* figura 7.
[37] Criada em 1923, a INTERPOL tem acolhido continuamente as novas tecnologias. Desde os códigos telegráficos à rede policial segura I-24/7 ou das impressões digitais ao reconhecimento facial, a inovação tecnológica tem sido utilizada no apoio técnico aos 195 Países-Membros na debelação do COT. No atual momento de perturbação global, animado pela digitalização e pelos fluxos geopolíticos, a cooperação policial internacional é mais necessária do que nunca.

1975, a PSP portuguesa era responsável pelo auxílio a vítimas de acidentes na via pública, sendo alertada através de uma rede de avisadores de estrada e de uma linha telefónica de emergência – o célebre 115, posteriormente alterado para o 112 (Martins, 2017). O potencial da revolução técnica e informática nas organizações policiais desvelava as capacidades de recolha, processamento e análise da informação, tendência paulatinamente consolidada.

> "Na década de 1990, a tecnologia da informação começou a permear mais claramente as fronteiras das organizações policiais, e as práticas e a linguagem da "responsabilização" começaram a alimentar o uso de tal tecnologia à medida que sistemas mais sofisticados de gestão de registos, tecnologia de chamadas para serviço e a análise criminal nas suas muitas variedades entraram em linha. (…) A informação assumiu uma postura mais estratégica e o seu carácter passou de uma perspetiva individual para a da organização, ou pelo menos de partes maiores da organização. (…) Atualmente, a polícia recolhe, processa e utiliza muito mais informação do que no passado e, neste sentido, aderiu verdadeiramente à era da informação" (Greene, 2007, p. xxii).

Com a afirmação ulterior das Ciências Policiais, o *scientific policeman*, proposto por Vollmer, passou de ficção a realidade (Vollmer, 1930). Progressivamente, universalizou-se o recurso a ferramentas digitais para efeitos de aplicação da lei. Os *big data*, o *software* analítico, a IA[38] e as técnicas preditivas, baseadas em algoritmos, são cada vez mais utilizadas pelos serviços policiais (Coldren, Huntoon, & Medaris, 2013; EUROPOL, 2022c).

> "A IA é uma tecnologia relativamente nova no contexto do policiamento e está em vias de se tornar um ativo crítico para a eficácia e eficiência da comunidade de segurança interna, incluindo a aplicação da lei e o sector da justiça. O desafio para os profissionais de segurança interna envolvidos na aplicação da lei e (…) da justiça consiste em determinar como capitalizar as oportunidades oferecidas pela IA para melhorar a forma como os agentes de patrulha, os procuradores, os juízes ou os guardas de fronteira cumprem a sua missão de fazer justiça e manter os cidadãos seguros, salvaguardando e demonstrando ao mesmo tempo a verdadeira responsabilidade da utilização da IA perante a sociedade" (EUROPOL, 2022c, p. 6).

Produto de uma inovação tecnológica insólita, a IA evoluiu vertiginosamente. Explorando os prismas da excelência, da confiança e dos valores europeus, o 'Livro Branco' sobre a IA é um guia estratégico para a Europa enfrentar os desafios e aproveitar as oportunidades dessa tecnologia, em constante evolução (Comissão Europeia, 2020b). Em 9

[38] Os cidadãos reconhecem enorme potencial na aplicação da IA e das tecnologias emergentes para proteger grupos vulneráveis e a sociedade em geral. No âmbito da sua estratégia digital, a UE está comprometida em regulamentar a IA para garantir melhores condições para o desenvolvimento e a utilização desta tecnologia inovadora, sob os auspícios de princípios éticos e valores fundamentais. A IA pode ser aplicada em sistemas virtuais, como assistentes de voz, análise de imagens e reconhecimento facial, bem como em dispositivos físicos, como robôs avançados e veículos autónomos. Um projeto-piloto bem-sucedido no Reino Unido utilizou a IA para apoiar os operadores das chamadas de violência doméstica. Segundo o estudo publicado pela *Policing Insight*, a tecnologia de IA aumentou a segurança dos polícias e do público, melhorando a recolha de provas e reduzindo o stress do pessoal (Gibbons, 2024). É fundamental envolver a sociedade civil nas decisões relacionadas a estas tecnologias, garantindo que as mesmas sejam usadas de modo responsável (Elias, 2023). Segundo Luís Elias, é importante que "(…) a Polícia esteja atenta aos desafios securitários emergentes e desenvolva a sua ação de forma adaptativa" (Elias, 2024, p. 476).

de dezembro de 2023, o Parlamento Europeu e o Conselho chegaram a acordo político sobre o Regulamento de IA da UE, o primeiro quadro jurídico neste domínio[39].

Num primeiro momento os avanços tecnológicos iludiram as comunidades policiais e de inteligência, levando-os a crer que a priorização do processamento da informação digital e a inteligência de fonte aberta (OSINT) alcançariam resultados imediatos e melhores. Esta quimera reivindica um olhar atento sobre a problemática, conciliando estratégias policiais eficazes com a indispensável interação cidadã. A abordagem integrada entre a inteligência humana (HUMINT) e tecnológica (TECHINT) afigura-se determinante para compreender as singularidades das comunidades e avigorar a relação *peeliana* entre a polícia e o público, mormente junto das franjas mais vulneráveis (*Parliament of the United Kingdom*, 1829; Elias, 2023). Antes de tudo, a polícia tem de ser uma organização de pessoas e ao serviço das pessoas[40]. Através da investigação, desenvolvimento e inovação (ID&I) previne-se e combate-se riscos coletivos (Moreira, *et al*., 2018). O policiamento na era digital consiste num exercício combinado, baseado no conhecimento e em competências comunitárias de proximidade, acordado numa formação técnico-operacional aprofundada e em saberes analíticos e contextuais resultantes da aplicação dos sistemas computacionais (Turing, 1950; Elias, 2023; Nogala, 2023 e 2024).

Apesar de moroso, intrincado e repleto de arduidades, o processo de inovação na polícia reverberou positivamente no dinamismo e eficácia do policiamento transnacional. Não olvidemos que a enorme velocidade da digitalização é acompanhada por ciclos rápidos de inovação tecnológica e por réplicas, igualmente aceleradas, de obsolescência (Brennen & Kreiss, 2016; Schwab, 2018). A necessidade de constante adaptação das organizações policiais acarreta desafios financeiros, organizacionais, formativos e gestionários (humanos e materiais). Contrariando estas compressões, as polícias investiram na sua capacitação digital e modernização tecnológica, constituindo bases de dados essenciais para uma segurança interpenetrada que se fixa, crescentemente, para além das fronteiras nacionais (Hoogenboom, Schoneveld, & Meiboom, 1997). A cooperação transfronteiriça impulsionou a modernização digital, a partilha de recursos e a interconexão dos serviços de aplicação da lei, de que são bons exemplos a EUROPOL, a Agência Europeia da Guarda de Fronteiras e Costeira (FRONTEX) e a Agência da União Europeia para a Gestão Operacional de Sistemas

[39] Arlindo Oliveira categoriza a IA em três grandes áreas: a) a substituição de funções humanas por sistemas automatizados; b) a possibilidade de desenvolver sistemas com inteligência equivalente à humana; e c) a aplicação de técnicas de IA em diversos campos (Oliveira, 2018).
[40] "Uma Polícia das pessoas e para as pessoas: segurança, igualdade, respeito e confiança" (PSP, 2024).

de Tecnologia em Grande Escala na Área da Liberdade, Segurança e Justiça (eu-LISA). Os investimentos na digitalização dos conjuntos de equipamentos técnicos são dispendiosos, mas imprescindíveis. Acresce que tais sistemas carecem de ser operados por recursos humanos especializados, cada vez menos abundantes. É fundamental promover a formação, educação, treino e adaptação dos polícias às novas tecnologias e métodos desta "era das redes" e em rápida transformação (Bayley & Shearing, 1996; Castells, 1999 [1942]; Arquilla & Ronfeldt, 2001). A aposta no digital não substitui, como referido, a necessária mobilização de polícias, de carne-e-osso, em abordagens locais e preventivas, orientadas para a visibilidade e proximidade comunitária (Elias, 2023; Nogala, 2024).

3. INFODEMIA: A EPIDEMIA DE INFORMAÇÃO DESORDENADA

> (…) Manchetes desanimadoras são transfronteiriças, compartilhadas regular e amplamente, e o sentimento de frustração com o *status quo* é cada vez mais palpável. Juntos, isso deixa espaço para que os riscos acelerados – como a informação incorreta e a desinformação –, se propaguem em sociedades que já foram política e economicamente enfraquecidas nos últimos anos." (Zahidi, 2024, p. 4).

A sociedade da informação coetânea carateriza-se pelo uso intensivo de tecnologias de informação e comunicação (Elias, 2022). Na era digital assiste-se a "(…) uma desterritorialização das ameaças e dos riscos, o que faz das redes digitais uma nova dimensão para a expansão das redes criminosas e para a justiça e a polícia" (Elias, 2023, p. 27). A sofisticação dos agentes do crime e das suas estratégias de encobrimento da atividade em linha mascara a circulação de fluxos ilícitos (monetários, pessoas e bens, etc.), dificultando a atuação policial (EUROPOL, 2021). A emergência destas ameaças híbridas, nomeadamente da desinformação[41], representam uma parcela da complexidade do policiamento na era digital (Lewandowsky, *et al*., 2012).

Em 2015, a desinformação russa passou a constar da agenda da UE (Conselho Europeu, 2015). Criando riscos significativos para a saúde pessoal e coletiva, gestão eficaz de crises, economia e coesão social, esta virulência informacional precipitou a aprovação de uma resolução sobre comunicação estratégica (Parlamento Europeu, 2016). Seguiu-se a adoção de um 'Código de Conduta sobre Desinformação', em 2018, e a publicação de

[41] A informação incorreta (*i.e*., errónea, mas sem intenção de prejudicar) e a desinformação (deliberadamente concebida e disseminada com o objetivo de enganar) obstaculizam a tomada de decisões informadas. A produção e a difusão veloz de conteúdos enganosos, incluindo produtos áudio e audiovisuais falsificados (*deepfakes*), tem sido magnificada pelas tecnologias emergentes. Segundo os dados difundidos pelo *Think Tank* do Parlamento Europeu cerca de 85% da população mundial está inquieta com o impacto da desinformação nos seus concidadãos; 87% acreditam que a desinformação já afetou o ambiente político do seu país; e 38% dos cidadãos da UE consideram as informações falsas e/ou enganosas uma ameaça à democracia (*Ipsos European Public Affairs* & UNESCO, 2023; *European Union*, 2023; Bentzen, 2024).

orientações relativas ao reforço desse mesmo diploma, em 2021 (*European Commission*, 2018c; Comissão Europeia, 2021). Foi, então, formada a *East StratCom Task Force* (ESCTF), integrada na Divisão de Comunicações Estratégicas e Análise de Informação (*StratCom*)[42] do Serviço Europeu de Ação Externa (SEAE). O seu objetivo era identificar e monitorizar campanhas de desinformação levadas a cabo por Moscovo.

Em março de 2020, a OMS classificou a epidemia da Covid-19 como uma pandemia. O surto pandémico e as alterações substanciais que advieram no modo de vida europeu, ao nível da comunicação, aprendizagem, trabalho e socialização, catapultaram a importância das tecnologias e do mercado digital, expandindo os riscos de exposição humana[43] (Postmes, *et al.*, 2001). Esta permeabilidade global, potenciada pela universalização do acesso à *internet* e a portabilidade dos *smartphones*, levou ao aparecimento de uma "infodemia" caracterizada pela acelerada divulgação de informações falsas, inexatas ou enganosas sobre a pandemia. A OMS descreveu-a como um excesso de informações, algumas precisas e outras não, que embaraça a identificação de fontes confiáveis e orientações seguras (*WHO*, 2020 e 2021). Assim, a Humanidade defrontou-se com duas epidemias de alcance e efeitos prolongados. Os consumidores digitais procuravam informações sobre um surto mortífero desconhecido, mas depararam-se com uma sobrecarga de informações baralhadas e imprecisas. Classificada como "o lado desagradável e problemático da digitalização" (Nogala, 2023, p. 11), esta "arma" não convencional atua através da disseminação de uma quantidade incomensurável de informações mediáticas, de tal modo desordenadas, sem avaliação ou curadoria adequada, que o consumidor tem dificuldades em discernir quais as fontes confiáveis[44], originando ceticismo generalizado e descrença política (Taber & Lodge, 2006; Libicki, 2009). A superfluidade de informações potencializa incertezas, ansiedades, preconceitos e dúvidas sobre a veracidade dos dados, o que, ainda assim, não obstaculiza o seu compartilhamento viral nas redes e ambientes digitais (Rothkopf, 2003; Oreskes &

[42] A *StratCom* organiza-se em duas áreas: uma relacionada com Política, Estratégia e Prioridade Global, que inclui estratégia e política, ameaças emergentes, e cooperação com as partes interessadas; outra ligada à Análise de Informação, Código Aberto e Estratégia de Dados, focada na análise e avaliação da informação, metodologia, e cooperação analítica (Xavier, 2023).

[43] O fenómeno levou à criação da 'Estratégia para o Mercado Único Digital na Europa' (Comissão Europeia, 2015 e 2016b) e à aprovação de uma Resolução do Parlamento Europeu sobre a comunicação estratégica da UE para combater a propaganda e as campanhas de desinformação em linha (Comissão Europeia, 2016a e 2018), posteriormente integradas na 'Estratégia Global de Segurança da UE'.

[44] A superdisseminação infodémica, artificialmente condicionada ou perfilhada por uma forte base popular, prospera com facilidade e sem oposição cabal neste macrossistema de informação. A sobrecarga dos nichos de formação da opinião digital pode, em algumas situações, precipitar a tomada de decisões, enquanto influencia negativamente a aptidão do público-alvo para distinguir a informação analisada das suas próprias fontes de informação e de dados não estabelecidos, provenientes em larga escala dos círculos tecnológicos.

Conway, 2011; Zarocostas, 2020). Vídeos, fotos, áudios, mensagens, *blogs* e redes sociais alimentam esta superabundância caótica de informação, estorvando a distinção entre o autêntico e o inexato (Hart, *et al.*, 2009). Assumindo consequências vastas e, potencialmente, mais dispendiosas do que a Covid-19, a infodemia, ou "epidemia de informação", influenciou e continua a afetar, de modo incontrolado, a vida de milhões de pessoas. Mesclando factos com especulação, rumores e receios, a infodemia maximiza a velocidade da transmissão de conteúdos adulterados ao nível mundial (Pfeffer, Zorbach, & Carley, 2014). Consideradas como um dos fenómenos mais virulentos conhecidos pelo Homem, as infodemias atravessam instantaneamente continentes, regimes, culturas, credos, ideologias, religiões e línguas (Rothkopf, 2003). A ultra imediatidade dos fluxos infodémicos exalta as convulsões na sociedade, na política, na segurança e nas economias em relação às realidades de base (Postmes, *et al.*, 2001). O prodígio infodémico causa e agrava a ineficiência económica, a perda de oportunidades e a expansão do populismo e da demagogia. Enquanto forma de persuasão e manipulação social, constrange os decisores políticos na gestão das exigências societais, afetando transversalmente todos os vetores da *Res publica*, desde a saúde pública à economia, da segurança interna aos assuntos internacionais (Heath, 2021).

A infodemia é, de facto, um fenómeno engenhoso e complexo resultante da maximização da interação entre os principais *mass media*, comunidades especializadas e os sítios da *internet* com os telemóveis, mensagens de texto, correio eletrónico, etc., na transmissão de uma certa combinação de factos, interpretações, intrigas e propaganda[45] adequadas a provocar o caos. Movendo-se livremente no fluxo aberto da informação, a infodemia enrola uma grande parte dos consumidores de informação, desde funcionários Estatais a cidadãos privados, com diferentes níveis de literacia e resiliência digital. Explorando as limitações da representação cognitiva humana e as capacidades inconstantes para analisar e organizar (a)criticamente o turbilhão informacional, a infodemia desconstrói,

[45] Um dos casos mais paradigmáticos das campanhas propagandistas de massas surgiu com a ascensão do regime nazi na Alemanha. A propósito da propaganda, Adolf Hitler enfatizou: "[O] seu objetivo deve ser ... atrair a atenção das massas e não, de forma alguma, dispensar instruções individuais àqueles que já têm uma opinião instruída sobre as coisas ou que desejam formar tal opinião com base num estudo objetivo - porque esse não é o objetivo da propaganda, deve apelar aos sentimentos do público e não aos seus poderes de raciocínio. [...] A arte da propaganda consiste precisamente em ser capaz de despertar a imaginação do público através de um apelo aos seus sentimentos, em encontrar a forma psicológica apropriada que prenda a atenção e o apelo ao coração das massas nacionais. [...] Os poderes recetivos das massas são muito limitados, e a sua compreensão é débil (…)" (Hitler, 1925, pp. 155-156). Se transportarmos o paradigma da propaganda nazi para as sociedades contemporâneas, interconectadas e permeáveis a incontáveis estímulos tecnológicos que ampliaram desproporcionalmente o volume e a velocidade da informação disponível em linha, concluímos que estamos, mais do que nunca, especialmente vulneráveis à infoguerra por parte de um inimigo invisível. De facto, esta contenda desigual, entre a galopante infodemia *versus* a capacidade cognitiva do ser humano – finita e razoavelmente inalterada ao longo dos tempos – afigura-se ter um vencedor predestinado.

confunde e adormenta a estrutura de pensamento lógico do cidadão comum, reduzindo-o à pulsão e à emoção do momento[46] (Bodenhausen, Sheppard, & Kramer, 1994). Introduzindo categorias de sofisticação variável sobre o que fazer ou como interpretar a informação que é apresentada ao público, ela diminui as oportunidades de autenticação ante uma contextura difusa (Rothkopf, 2003). O resultado é a distorção, a confusão e, por vezes, uma profunda incongruência entre os factos subjacentes e as suas implicações reais.

Tal como outras enfermidades e vírus, a infodemia apresenta sintomas identificáveis, uma epidemiologia própria, portadores conhecidos e até terapêuticas simples. Devemos lidar com ela do mesmo modo que fazemos com as doenças (Rothkopf, 2003). Daqui advém a necessidade de suster os seus avanços e gerir adequadamente os seus efeitos. O que alimenta as infodemias pode ser mobilizado para a construção de melhores sistemas de alerta precoce e a preparação de contramedidas, acompanhadas da indispensável monitorização dos resultados. É vital que os órgãos regulares dos *mass media* orientem a sua política editorial na publicação de artigos úteis e fidedignos, informando o que foi feito e o que terá de ser feito na sua mitigação. Os *media* têm de se assumir como membros de uma *entente* de integridade e transparência de informação (Asai, 2023). Ao fazê-lo, os cidadãos poderão beneficiar de informação credível e das *lessons learned* para controlar eficazmente futuras epidemias (Rigues, 2021; Willett, 2021). A credibilidade e a confiança poderão imunizar os cidadãos, empresas e países inteiros contra a infodemia (Fernandes, 2022a). Se a desinformação é a doença, o conhecimento é a cura (Rothkopf, 2003). As orientações da Comissão Europeia (2021) e os ensinamentos retirados da crise da pandémica e da guerra de agressão russo-ucraniana contribuíram o revigoramento do 'Código de Conduta sobre a Desinformação', republicado a 16 de junho de 2022 (Xavier, 2023). Juntamente com o 'Regulamento dos Serviços Digitais', a 'Declaração Europeia sobre os Direitos e Princípios Digitais' e a legislação proposta no quadro de transparência e direcionamento da propaganda política, o reforçado 'Código de Conduta'[47] constitui o instrumento central no combate à

[46] A metáfora de Albert Camus (2011 [1947]) descreve o perigo das ameaças adormecidas: "(…) Sabia o que esta multidão eufórica ignorava, que o bacilo da peste não morre nem desaparece nunca, que pode ficar adormecido durante décadas nos móveis ou entre a roupa, que aguarda pacientemente nos quartos, nas caves, nas malas, nos lenços e na papelada, e que, possivelmente, viria um dia em que, para infelicidade e ensinamento dos homens, a peste acordaria os seus ratos e enviá-los-ia para morrerem numa cidade feliz" (Camus *apud* Ferreira, 2013, p. 45).

[47] O Código visa ampliar a participação de grandes plataformas e intervenientes para mitigar a propagação da desinformação, eliminando os incentivos financeiros à sua propagação e garantindo que os seus transmissores não beneficiem de receitas publicitárias. Complementarmente, identifica novos comportamentos manipuladores, como contas falsas, robôs digitais ou falsificações profundas maliciosas, e capacita os utilizadores com novas ferramentas para reconhecer, compreender e denunciar a desinformação. Neste

desinformação na UE (*European Commission*, 2022). O Conselho da EU, a Comissão Europeia e os 14 Centros de Combate à Desinformação formam uma frente comum para detetar e analisar campanhas de desinformação, promover a literacia mediática e apoiar a resiliência digital na defesa dos Direitos Humanos e da democracia (*European Commission*, 2020; APCD, 2022). Neste âmbito, destacam-se quatro plataformas emblemáticas de combate multidisciplinar à "(…) desinformação russa, uma ameaça já bem estabelecida e reconhecida" (União Europeia, 2021, p. 28), a saber: a *EUvsDisinfo* (*StratCom*/SEAE); o *Social Observatory for Disinformation and Social Media Analysis* (SOMA); o *European Digital Media Observatory* (EDMO); e o Centro Europeu para Transparência dos Algoritmos (ECAT).

É crucial compreender como a desinformação é apresentada à população, como irradia, o que acelera a sua difusão, quais são os seus efeitos e que surtos podem ser contidos. Isto significa gerir proficientemente cada evento infodémico e apresentar os factos de modo completo, claro e rápido às audiências, reforçando as suas capacidades críticas[48] (Lewandowsky, *et al*., 2012). A monitorização da *internet* e dos meios de comunicação locais são fundamentais para a identificação precoce e interpretação coerente. As sociedades desfavorecidas têm infraestruturas mediáticas mais primitivas e menos sofisticadas, sendo mais vulneráveis. Por essa razão carecem de apoio e investimento urgente perante uma infodemia que se complexifica e se reconstrói vorazmente (Asai, 2023). O imediatismo dos acontecimentos e a volatilidade da informação resultam na amplificação das suas consequências, substancialmente diferentes da visão decorrente de bases analíticas sólidas, repercutindo significativamente nas operações policiais de manutenção da paz social (Rothkopf, 2003; Zarocostas, 2020; Asai, 2023). A volumosa propagação de informações falsas pode confundir e manipular a opinião pública, levando a distúrbios civis, pânico e desordens[49]. Em situações de crise, acidentes graves, catástrofes ou emergências, a infodemia pode interferir no planeamento e gestão dos incidentes, comprometendo a eficácia

particular, urge aclarar que a desinformação pode "(…) não ser só informação completamente falsa, mas também informação que seja deliberadamente produzida, instrumentalizando a comunicação digital para criar disrupção (*trolling*) e/ou dissimular a proveniência de mensagens de movimentos políticos alegadamente legítimos (*astroturfing* ou *grassrooting*) e/ou fazer circular, partilhar e comentar informação dirigida (*tweeting* e *retweeting*)" (Xavier, 2023, p. 226).

[48] É essencial verificar o conteúdo, o órgão de comunicação, o autor, as fontes e as imagens. Depois é importante pensar antes de partilhar, questionando os próprios preconceitos e estereótipos (Kunda & Sinclair, 1999). Estas precauções, associadas ao conhecimento das técnicas de desinformação e à denúncia das notícias falsas, podem ajudar a combater a desinformação, melhorar a literacia digital e aumentar a resiliência coletiva (Bentzen, 2024).

[49] A tentativa de homicídio do primeiro-ministro da Eslováquia, Robert Fico, em maio de 2024, terá resultado da polarização política sentida no país (Avó, 2024).

da atuação policial[50]. Além disso, a desinformação infodémica erode a confiança do público nas instituições públicas, entorpecendo a cooperação entre a comunidade e a polícia. As instituições que resguardavam o sistema internacional estão defuntas ou a perder a credibilidade[51], tendência que urge inverter (Wendling, 2021; *The Economist*, 2024a).

Na dinâmica geopolítica coetânea, em que os regimes autoritários recorrem a tecnologias sofisticadas para diminuir a democracia e a liberdade, Antony Blinken evidenciou a necessidade de garantir que a tecnologia apoie os valores e normas democráticas (Salvador, 2024). A construção de um ambiente de informação mais resiliente é uma prioridade para a diplomacia e constitui um interesse vital para a segurança nacional (Collier, 2003; Salvador, 2024). Tanto as redes sociais, como a IA, são aceleradores da infodemia (Simon & Mahoney, 2022). O presidente sul-coreano, Yoon Suk Yeol, enfatizou que as *fake news* e a desinformação, com base na IA e na tecnologia digital, violam a liberdade individual e os Direitos Humanos, constituindo uma ameaça aos sistemas democráticos (Gelfert, 2018; Salvador, 2024). Aquele que dominar a IA vai dominar a economia do planeta (Oliveira *apud* Dias, 2023).

4. A ROLETA-RUSSA DE DESINFORMAÇÃO E PROPAGANDA

> "Uma mentira dita uma vez continua uma mentira, mas uma mentira dita mil vezes torna-se verdade." (Goebbels *apud* Harari, 2018b, p. 254).

A guerra no século XXI está a mudar em resultado de duas grandes tendências: as mudanças na tecnologia militar e a crescente concorrência geopolítica[52] (IEP, 2024). Na

[50] Em 2012, Portugal assistiu a manifestações violentas anti Troika que provocaram graves alterações da ordem pública, obrigando à intervenção da PSP. Vários agentes da desinformação alegaram que havia "polícias à paisana infiltrados entre os manifestantes a agirem como agentes provocadores", situação prontamente refutada pela governação (Público, 2012). Em agosto de 2024, os incêndios que assolaram a Ilha da Madeira geraram forte contestação mediática e popular contras as autoridades regionais. Declarações imprecisas dos responsáveis pelo serviço regional de proteção civil e pela Associação Nacional de Conservação da Natureza (QUERCUS) imputaram erroneamente responsabilidades à PSP quanto ao licenciamento de queimas e queimadas, atribuições essas legalmente conferidas à Direção Regional de Florestas e das Câmaras Municipais. A desinformação centrou a atenção do público na PSP e alimentou polémica (Rodrigues, 2024).

[51] A Organização Mundial do Comércio (OMC) aparenta estar estagnada, sobretudo devido à negligência americana. O Fundo Monetário Internacional (FMI) atravessa uma crise de identidade, preso entre uma agenda ecológica e a garantia da estabilidade financeira. O Conselho de Segurança das NU está paralisado. Os tribunais supranacionais, como o Tribunal Internacional de Justiça (TIJ), são cada vez mais instrumentalizados pelas partes beligerantes. Em abril de 2024, alguns políticos norte-americanos, incluindo o líder dos republicanos no Senado, Mitch McConnell, ameaçaram o TIJ com sanções caso emitisse mandados de captura para os dirigentes de Israel, acusados de genocídio pela África do Sul (*The Economist*, 2024a).

[52] Os conflitos regionais, como a guerra russo-ucraniana, ilustram a complexidade da guerra moderna e o seu custo humano devastador: só na Ucrânia registaram-se mais de 2.000 mortes por mês, durante quase todos os meses dos últimos dois anos, sem ganhos significativos. Estes conflitos são exemplos de "guerras eternas", em que a violência prolongada se torna aparentemente interminável, sem resoluções claras, exacerbada por apoio militar externo, pela guerra assimétrica e por rivalidades geopolíticas (IEP, 2024).

ressaca do momento atual de instabilidade generalizada, a razão, a lógica e a realidade, enquanto pilares fundamentais do discurso civilizado, enfrentam desafios significativos num ambiente labiríntico, difuso e autorreferencial das suas próprias (micro) realidades informativas. A conflitualidade digital e a incessante vulgarização infodémica alimentam estratagemas, sistemas inteligentes e métodos avançados de persuasão destinados a subverter os alicerces da coerência racional, a verdade e a perceção do mundo real, substituindo-os por narrativas fictícias, logros, dúvidas, negacionismos, indignações e receios[53] (Petty & Cacioppo, 1986; Elsasser & Dunlap, 2013). Ao invés de orientar a razão, a comunicação e a informação desordenada, ampliadas pela infodemia, exacerbam emoções e preconceitos, explorando perversamente as vulnerabilidades das arquiteturas cognitivas humanas (Bodenhausen, Sheppard, & Kramer, 1994). "(…) Se o pensamento corrompe a linguagem, a linguagem também pode corromper o pensamento" (Orwell, 1946, p. 4). A proliferação desta estratégia de infoguerra na arena geopolítica global, mormente pela Rússia[54], tem desvirtuado os processos cognitivos internos dos cidadãos comuns, enquanto enfraquece os sistemas institucionais, políticos e jurídicos externos[55].

"Na guerra, pratique a dissimulação e será bem-sucedido" (Sun Tzu, 2023, p. 61). A degradação intencional da biogeocenose informativa ocorre de maneira progressiva, intensa e muitas vezes encoberta (GEC, 2020). Mais do que nunca, é crucial a adesão ao postulado iluminista *sapere aude*[56] (Kant, 1784) para discernir a verdade dos factos da falsidade encoberta. Condicionada pela distorção infodémica, a ordem internacional inclina-se para uma reconfiguração forçada e multipolar, mais antagónica e menos consensual. Assuntos anteriormente situados na *low politics* contrapõem potências e atores rivais da mesma forma que na *high level politics* (Arquilla & Ronfeldt, 1993; Von der Leyen, 2019a; Borrell, 2020; Tomé, 2021). A *realpolitik* cedeu lugar à *netpolitik*, cujo *soft power* foi corrompido pelo *dark power* da "militarização" da infodemia (Collier, 2003). A desinformação é uma das armas mais relevantes e de longo alcance da Rússia. Operacionalizando o conceito da "competição adversária perpétua" no ambiente da informação, os serviços de inteligência militar russos –

[53] Técnica conhecida por "Pirataria de Crescimento" (informação verbal, apresentada no documentário da *Netflix*, intitulado 'O dilema das Redes Sociais', realizado por Jeff Orlowski, de 9 de setembro de 2020).
[54] Ao longo dos últimos vinte anos, o aparelho de desinformação da Rússia tem divulgado, antecipadamente, as bases para várias ações internas e externas do regime. Os *mass media* russos, controlados pelo Estado (como a RT – antiga "*Russia Today*" – e as redes *Sputnik*), divulgam pistas para decifrar os objetivos encobertos do Kremlin no estrangeiro, desde a interferência eleitoral até às invasões militares da Ucrânia (Harlow, 2024).
[55] A interferência russa nas eleições de 2016, nos EUA, é paradigmática da disrupção destes avanços da tecnologia (MacFarquhar, 2018; *U.S. Senate Select Committee on Intelligence*, 2020; Schick, 2020; *The White House*, 2021; Sanger & Kramer, 2021; Observador, 2021).
[56] "Atreva-se a conhecer" ou "ouse saber" (Kant, [1784] 1990).

encabeçados pela Diretoria Principal de Inteligência ou *Glavnoye razvedyvatel'noye upravleniye* (doravante, GRU)[57] – edificaram um ecossistema de desinformação global, propaganda computacional e ciberataques, alicerçado na engenharia social (Gill & Goolsby, 2022; *U. S. Department of State*, 2024; Fleck, 2024)

> "Há verdades e há mentiras. Mentiras contadas para obter poder e lucro. E cada um de nós tem um dever e uma responsabilidade como cidadãos (…) e, especialmente, como líderes (…) de defender a verdade e derrotar as mentiras" (Biden, Jr. *apud U. S. Department of State*, 2024, p. 1).

A infodemia do regime de Putin suplanta os meios tradicionais de controlo de qualidade da informação para abrir as comportas da desinformação e inundar o público com mentiras e "complotismos"[58] (Clark, 2020; Simon & Mahoney, 2022; *EUvsDisinfo*, 2024). O desequilíbrio no arranjo de poder manifesta-se de modo veemente no ciberespaço, um território infindável, sem regulação clara e onde vários atores globais buscam consolidar posições dominantes na nova geopolítica digital (Borrell, 2020). Potências autocráticas, grupos extremistas[59] e movimentos terroristas[60] recorrem a sofisticadas campanhas de

[57] Criada em 1942, a GRU é responsável pela condução de operações de informação legais (sob proteção diplomática) e ilegais/oficiosas (sem cobertura oficial) no estrangeiro, maioritariamente focadas na "avaliação de capacidades militares estratégicas", a obtenção de tecnologia ocidental e outras informações militarmente pertinentes (Garthoff, 2015, pp. 13-15, 46). Maximizando as múltiplas unidades *Spetsnaz* e brigadas *Razvedchiki* em operações de reconhecimento, sabotagem e guerrilha, a GRU desenvolve "ações de recolha [e análise] de informações estrangeiras", tecnologicamente avançadas e com recurso a variados métodos e fontes (*v.g*., informações humanas, cibernéticas, por sinais e satélite), relacionando-se com as várias agências de inteligência russófonas (Bowen, 2020, p. 5). Destaque para a Unidade 26165, subdividida na APT 28 (*Fancy Bear*) e na APT 29 (*Cozy Bear*), responsáveis pela criptografia dos serviços secretos militares e pelas operações digitais; Unidade 74455 (*Sandworm*), dedicada às capacidades cibernéticas; e a Unidade 54777 (72º Centro de Serviço Especial) operações psicológicas (Lilly & Cheravitch, 2020). A sua vasta experiência na gestão de 'forças de procuração' foi especialmente relevante na invasão da Crimeia e do leste da Ucrânia, em 2014 (Bartles & McDermott, 2014; Galeotti, 2014; Lavrov, 2015).

[58] Os relatórios do Centro de Engajamento Global sintetizam as evidências da desinformação russa. Destacam-se 'Explorando medos primários', de 13 de janeiro de 2022; 'Deturpando fatos sobre o assassinato de Nemtsov e as tentativas de assassinato de Navalny e Skripal', de 4 de outubro de 2021; 'Os objetivos e as principais táticas da desinformação da Rússia', de 23 de agosto de 2021; e 'O extraordinário alcance e amplitude da propaganda e da desinformação russas', de 1 de dezembro de 2020 (*U. S. Department of State*, 2024).

[59] A Europa coeva posiciona-se, cada vez mais, à direita (Cardoso, Paola, & Moreira, 2023). Entre os casos mais sonantes, conta-se o *Fidesz*, na Hungria; o *Prawo i Sprawiedliwość*, na Polónia; o *Rassemblement National*, em França; o Partido da Liberdade (PVV), nos Países Baixos; o Irmãos de Itália, em Itália; o *Vox*, em Espanha; e o Chega, em Portugal. No Reino Unido, o ultranacionalismo ganhou notoriedade através de grupos organizados como *The London Forum* ou o *Millennial Woes*, de Colin Robertson. Na América do Norte, a extrema-direita está associada ao movimento *alt-right* (*alternative right*), de Daniel Friberg, Jason Jorjani e Richard Spencer. O *North West Forum* e o *True Cascadia*, também com forte implantação. Rentabilizando o ativismo de baixo custo e o acesso a um grande público, os supremacistas digitais defendem mudanças sociais pelo uso da força. Apostando na propaganda ideológica, promovem o compartilhamento viral nas redes sociais, com recurso à abundância de memes caóticos e satíricos. Através do ambiente digital, normalizam fervorosos discursos de ódio (Hyvönen, 2018) contra judeus, muçulmanos, afro-americanos, mulheres liberais e todos os que defendam a igualdade entre os povos. Advogam a criação de estados étnicos e o fascismo, opondo-se a uma humanidade homogeneizada (Harari, 2018a; informação verbal, apresentada no documentário da RTP2, intitulado 'O extremo da extrema-direita' (versão portuguesa), de 17 de fevereiro de 2021).

[60] Em 2018, a Grã-Bretanha expôs o patrocínio russo e gestão *proxy* do *Cyber Califado* (PRP Channel, 2018).

recrutamento, propaganda e terror[61], desinformação e conspiração em diversas regiões e continentes, numa estratégia irredentista de conquista de poder[62] (McConnachie & Tudge, 2008; AFP, 2017; IEP, 2020; SSI, 2023).

A assertividade da desinformação russa destaca-se em numerosas frentes, em especial contra a Ucrânia e o "Ocidente plural" (Douglas, *et al*., 2019; Guterres, 2020; Duarte, 2020). Para o efeito, Moscovo concebeu uma rede internacional de atores humanos e de IA para espalhar desinformação (PRP Channel, 2018; informação verbal[63]). Inumeráveis *script kiddies*, plataformas de *pharming* e "fábricas de trollagem" pró-Kremlin empolam sistematicamente as tensões sócio estruturais para fortalecer teorias conspiratórias antiocidentais, negacionismos e ofensivas cibernéticas. Espalhando retóricas enviesadas, sentimentos de ódio (homofobia, antissemitismo, islamofobia, xenofobia, etc.) e discursos inflamados e retorcidos, redes de *hactivistas*, hordas de *trolls*[64] e *botnets* assoberbaram os *social media*, favorecendo a multipolarização social (Hyvönen, 2018; Douglas, *et al*., 2019; Marx, *et al*., 2020). Jessikka Aro denunciou as redes de "trollagem institucionalizada" e as operações híbridas[65] de desinformação de Putin, expondo como a infoguerra russa investe

[61] Para Arendt (1973), a propaganda e do terror são determinantes para a construção do mundo totalitário. Quando relacionados com o isolamento e solidão dos indivíduos em relação à sociedade, a propaganda e o terror são uma pré-condição para o domínio absoluto daquela forma de governação autoritária.

[62]Como a Rússia, China, Irão e Coreia do Norte – o "Eixo dos Autoritários" (Sanner, 2024). Os sucessivos ciberataques russos contra a Alemanha, a República Checa, a Lituânia, a Polónia, a Eslováquia e a Suécia levaram, no polo oposto, a novas alianças das democracias (Tek/Lusa, 2024a e 2024b). *Vide* figura 6, em anexo.

[63] Informação verbal extraída do 'O poder da infodemia em guerras como a Ucrânia-Rússia', publicado a 21 de março de 2022 pelo canal noticioso Voa Português.

[64] Gigantescas redes de *trolls* russos tentam condicionar apoio dos EUA à Ucrânia através da multiplicação de campanhas de desinformação. Estas ações híbridas, orquestradas por *spin doctors* de Moscovo e políticos antissistema populistas, abrangem linhas de esforço alargado que acicatam tensões raciais e económicas, bem como criam receios sobre a segurança fronteiriça (Ribeiro, 2015; Neto, 2023; Belton & Menn, 2024).

[65] Moscovo está a travar uma guerra híbrida contra Washington, os seus aliados europeus e Kyiv. A conceptualização russa de guerra híbrida é ampla e compreende a utilização de conflitos, de forças convencionais e não convencionais, divergindo da noção ocidental. É percebida, de modo coerente e preciso, como um tipo de guerra não convencional, rápida e multimodal, ao invés de um conjunto de meios para conduzir a política do Estado. Envolve todos meios, instrumentos, atores e áreas da concorrência, incluindo os componentes subversivo, tecnológico, ambiental e de lazer, a informação e os meios diplomáticos, bem como o emprego de forças militares (com destaque para as brigadas especiais da *Spetsnaz*), empresas militares privadas e/ou organismos paramilitares (como o Grupo Wagner (*Группа Вагнера*)), unidades de mercenários e *hackers* de aluguer, entre outros. A Rússia desenvolveu múltiplas estratégias para adaptar, modernizar e aumentar as suas capacidades político-militares de modo a conduzir eficazmente as operações. Entre as principais medidas, destaca-se a centralização de todos os órgãos de decisão, sejam eles civis, militares, mediáticos ou económicos, para coordenar os esforços governamentais de maneira unificada. A proliferação de campanhas massivas de informação junto de toda a sociedade visa reforçar a consciência patriótica, considerada essencial neste tipo de conflito. As doutrinas militares tradicionais foram modeladas e as capacidades expedicionárias convencionais foram aprimoradas para facilitar a mobilização e deslocação para o exterior. Complementarmente, o Kremlin utiliza companhias militares privadas e outras 'forças de procuração' de poder (*proxy forces*) que podem ser negadas oficialmente. O planeamento e a execução das operações cinéticas subordinam-se às operações de informação (inteligência), refletindo uma mudança de paradigma na natureza da guerra, mais eficaz, coordenada e disruptiva (Clark, 2020, pp. 8-15).

em formas complexas, massivas e confusas de fabricação de realidades alternativas[66]. Um dos centros nevrálgicos desta máquina de desinformação é a *Internet Research Agency*. Segundo a autora, a obscuridade das operações de manipulação da informação em linha pelo Kremlin condiciona a vida das pessoas e a saúde das democracias. A série de ciberataques à Estónia, em 2007 e 2022, são paradigmáticos (Público, 2007; Novais, 2022; Fernandes, 2024b). A estratégia da "trollagem" explora habilmente os interstícios da legalidade e os circuitos mediáticos (MacFarquhar, 2018). A amplitude destas operações fora da Rússia vitimiza indistintamente cidadãos privados (políticos, diplomatas, jornalistas, empresários, etc.), empresas multinacionais e organizações internacionais, sujeitando-os a pressões psicológicas, chantagens, subornos, exposições públicas, violações da privacidade, insultos, abusos, perseguições e ameaças nas redes sociais[67] (Aro, 2022; Vaidišová, 2022). A infoguerra, a desinformação, a ciberespionagem e a corrupção influenciam-se mutuamente.

Neste contexto, o conflito russo-ucraniano demanda uma referência dedicada. Iniciado em 2014, com a controversa anexação da Crimeia e os subsequentes envolvimentos militares da Federação Russa no leste da Ucrânia, a tensão escalou em 2022. Após a *Mauerfall* de Berlim (1989), a dissolução da União Soviética (1991) e os ataques terroristas ao *World Trade Center* e ao Pentágono nos EUA (2001), a "operação militar especial" do Kremlin em território ucraniano foi o evento internacional que mais desafiou a ordem convencionada desde 1945. O neoimperialismo moscovita contra Kyiv constitui uma grave violação do Direito Internacional e dos princípios fundamentais da Carta das NU, perigando a segurança internacional e, sobretudo, a estabilidade europeia, fitada como um "espelho partido" (Cassese, 2012; Soromenho-Marques & Magalhães, 2024). Ao desafiar o *status quo* da ordem internacional liberal, Vladimir Putin recondicionou a sua preponderância nos cálculos de poder mundial. O liberalismo multilátero está a desmoronar-se lentamente e o seu colapso pode ser intempestivo e irreversível (*The Economist*, 2024a). Um número preocupante de fatores pode acelerar a anarquia. O poder é *la raison d'être* e a guerra volta a ser o recurso das potências expansionistas. Como proclamou Dmitri Medvedev, a "Mãe

[66] *Vide* figura 5, em anexo.

[67] Nos finais de maio de 2024 e a poucas semanas das eleições europeias, as polícias belga e francesa, coordenadas pela Agência da UE para a Cooperação Judiciária Penal (EUROJUST), realizaram buscas na casa e no escritório de Guillaume Pradoura, um funcionário do Parlamento Europeu, num caso de ingerência, corrupção passiva e participação numa organização criminosa. Vários eurodeputados de partidos de extrema-direita e eurocéticos terão sido aliciados e subornados para promoverem propaganda e desinformação pró-Kremlin através do sítio de notícias *Voice of Europe* e de outros meios de comunicação russos, entretanto banidos (Carvalho, 2024; Lopatka & Hovet, 2024; Blenkinsop, 2024). Os objetivos da rede passavam por influenciar a "cooperação" entre políticos pró-Kremlin dentro do órgão legislativo da UE. Recorde-se que, em 26 de abril de 2024, o Parlamento Europeu aprovou uma resolução contra a interferência estrangeira, alertando para as tentativas de ingerência e desinformação da Rússia e da China (Agência Lusa, 2024a).

Rússia" invoca o direito de usar armas atómicas para vencer a guerra e recuperar a grandeza do *RussKiy mir* ("mundo russo") (Diário de Notícias/AFP, 2022). As implicações geopolíticas são profundas e comprovam a profunda frangibilidade das relações internacionais contemporâneas.

Empenhado em justificar uma guerra injustificável e manipular narrativa histórica[68], o *Leviathan* infodémico de Putin envolve um conjunto de intrincadas táticas de desinformação, propaganda computacional e estratégias de engenharia psicossocial contra a Ucrânia, a UE, a Organização para a Segurança e Cooperação na Europa (OSCE), a Organização do Tratado do Atlântico Norte (OTAN) e os EUA (*Recorded Future*, 2024a). A proteção da comunidade russófona e a "desnazificação" ucraniana foram os primeiros argumentos para a narrativa revisionista do Kremlin (Barreto, 2022).

> "O coro de enganos de Putin inundar-nos-á com mensagens destinadas a semear confusão e dúvida suficientes para que alguns comecem a reinterpretar o significado da invasão que ele lançou (…). A causa da paz e da segurança dependerá em parte da nossa capacidade de manter a clareza moral e intelectual no meio do nevoeiro espesso de uma guerra de informação" (Finnin & Roozenbeek, 2022, p. 3).

A Rússia tem revigorado as operações de propaganda e desinformação como parte de uma segunda frente de combate que, segundo diplomatas ocidentais, se tem tornado quase tão importante como a campanha militar na Ucrânia (Belton & Menn, 2024). Apesar da magnitude infodémica pró-russa, a coesão ocidental e ucraniana "(...) não pode ser rompida por mentiras ou intimidação, informações falsas ou teorias da conspiração" (Zelensky *apud* GEC, 2023). Visando a demagogia e a "censura através do ruído", o complexo russo abrange os *media* tradicionais (televisão, rádio, imprensa, etc.) e os *outlets* oficiais e clandestinos (como as banidas *Sputnik* e a RT[69]), incluindo fontes "por procuração" e não atribuídas, cooptadas na criação e amplificação de abordagens variadas, sobrepostas e que se autorreforçam em narrativas falsas e adaptadas a diferentes públicos-alvo (Simon & Mahoney, 2022). Este mecanismo disruptivo exagerado pela IA generativa baseia-se nas teses e comunicações oficiais do governo russo (cujo rosto visível tem sido Maria

[68] "Quem controla o passado, controla o futuro. Quem controla o presente, controla o passado" (Orwell, 2012, p. 38).

[69] A crise ucraniana é marcada por uma infoguerra, coroada pela manipulação de informações (Arquilla & Ronfeldt, 1993). Os meios de comunicação russos, predominantemente estatais, estão envolvidos numa sofisticada campanha de desinformação. O canal de notícias multilíngue RT é o principal veículo global da narrativa do Kremlin. Na Rússia, a maioria das pessoas aceita acriticamente a versão dos eventos veiculada pelos *media*. Todavia, apesar da RT ter uma grande audiência internacional, a imagem da Rússia tem se deteriorado desde o início da guerra com a Ucrânia. Para combater a desinformação russa, a UE propõe-se a aumentar o financiamento para os meios de comunicação ocidentais que transmitem em russo, como o Serviço Mundial da BBC, bem como a criar órgãos de comunicação social, como um canal de televisão em língua russa que ofereça notícias e entretenimento (Bentzen & Russell, 2015; Bentzen, 2024).

Zakharova); mensagens globais financiadas pelo Estado (e pela aliada China); falsas *personas* de *mass media*; e em robustas campanhas de desinformação digital[70], cuja escala e intensidade são exponenciadas pela infodemia[71] (*The Economist*, 2024b). A anarquia sistémica obscurece e confunde o ambiente de informação, sectorizando "bolhas" epistémicas de informação e câmaras de eco que acedem a conteúdos fechados e persuadem ao "monopensamento" (Petty & Cacioppo, 1986; Kruglanski & Thompson, 1999; Gill & Goolsby, 2022; Silveira, 2022).

As vigorosas campanhas de desinformação russas principiam pela infiltração num espaço de informação ou audiência, procurando influenciá-la com narrativas prejudiciais contra alvos específicos, como figuras públicas[72] e organizações políticas (CSCE, 2017). As táticas de desinformação do Kremlin são variadas, sincrónicas e interpenetradas. Entre elas, destacam-se a falácia do *tu quoque* ("tu também"), o *retconning* ("continuidade retroativa") e a projeção preditiva[73]. Estas "operações de influência" estão organizadas em quatro categorias de interferência[74] e visam o enfraquecimento das posições políticas, económicas, científicas, técnicas e militares dos adversários, bem como a manipulação de terceiros em favor do interesse russo. Por regra, implicam o descrédito, a divisão, o desarmamento e a desmoralização (GEC, 2021). O efeito multiplicador dos *media* e o compartilhamento

[70] Seguindo a tradição do *Komitet Gosudarstvennoy Bezopasnosti SSSR* (KGB), o *Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii* (FSB) e o *Sluzhba Vneshney Razvedki* (SVR) redobraram o investimento na estratégia infodémica contra o Ocidente. Robustecida pelos progressos tecnológicos, a infodemia pró-Kremlin assumiu um alcance planetário, apostando na adulteração de documentos genuínos e introduzindo acrescentos (*The Economist*, 2024b). Em março de 2024, a rede de sítios *Web* chamada *CopyCop* publicou uma série de histórias controversas, em inglês e francês, extraídas de meios noticiosos legítimos e modificadas através de grandes modelos linguísticos, em tudo semelhantes ao *ChatGPT* da *Openai*. Utilizando extensivamente a IA generativa e a "multimodalidade nativa" para traduzir, plagiar, editar e modificar conteúdos de fontes mediáticas legítimas, o *CopyCop* divulgou instruções para a corrupção de mensagens políticas com preconceitos específicos contra as políticas ocidentais, enquanto enfatizavam Trump, DeSantis e Putin como figuras positivas (*Recorded Future*, 2024b). Associada a plataformas de desinformação russófona, como a *DCWeekly*, *Doppelgänger*, *Portal Kombat*, *Foundation to Battle Injustice* e *InfoRos*, a *CopyCop* gerou automaticamente mais de 19000 artigos naquele período, posteriormente amplificados pelas plataformas referenciadas, num esforço coordenado. A sofisticação dos argumentos, concebidos para despertar sentimentos políticos específicos, dificulta o combate à rápida difusão destas falsas narrativas (*Recorded Future*, 2024c).

[71] A investida infodémica ocorrida na campanha presidencial de 2016, nos EUA, é exemplo do poder da desinformação russa. Através de uma quinta de *trolls* da *internet* e de *bots*, a máquina de Putin multiplicou a difusão de conteúdos falsos, fraturando o público americano (Galante, 2017; MacFarquhar, 2018).

[72] O Kremlin criou equipas específicas para divulgar *fake news* nas redes sociais a fim de dividir a Ucrânia e prejudicar a imagem pública e a confiança em Zelensky (Belton, 2024).

[73] O sofisma do *tu quoque* tenta desviar a atenção dos crimes de Putin, apontando para os atos dos "parceiros" ocidentais e pondo causa a base do próprio conceito de crime. No fundo, transforma as violações das regras numa oportunidade para sugerir que são irrelevantes. O *retconning* consiste em reescrever o passado para se adequar ao presente. O revisionismo das realidades de ontem serve para justificar os acontecimentos de hoje. A "desnazificação" e "desmilitarização" ucraniana ou as perspetivas de adesão da Ucrânia à OTAN são bons exemplos. Por fim, a projeção preditiva é uma narrativa de bandeira falsa que assenta na imputação de falsas intenções aos adversários para justificar as próprias ações e intenções.

[74] Elas são a manipulação de informações, a disrupção cibernética, o aliciamento político e a intervenção extrema (Xavier, 2023).

sistemático em grupos, redes e comunidades virtuais potenciam "tempestades de desinformação" que fragilizam a credibilidade e a união ocidental (GEC, 2020, p. 5). Esta dissimulação permite a negação de envolvimento oficial e a continuidade da beligerância através de *proxy wars* digitais[75], via *bots* automatizados, *hacktivistas* de aluguer e inumeráveis intermediários e multiplataformas como o *Facebook*, *X* (anterior *Twitter*), *YouTube*, *VKontakte*, entre outros., que ampliam conteúdos miméticos e transpõem narrativas (GEC, 2020; Marx, *et al*., 2020). "A guerra é paz. A liberdade é escravidão. Ignorância é força" (Orwell, 2012, p. 8).

5. A EUROPOL NA VANGUARDA DO POLICIAMENTO NA ERA DIGITAL

> "(…) Precisamos de baixar a temperatura e fazer recuar a polarização, que envenena praticamente tudo em que toca e impede a cooperação internacional" (*HDRO*, 2024, p. 7).

Como vimos, a era digital corresponde a um período consolidado, associado à otimização dos fluxos informacionais mundiais desde o final do século XX. A transição social, apressurada pelos avanços da tecnologia e a globalização, reconfigurou a sociedade, as suas interações e os seus modos de pensar, comunicar e laborar. As repercussões da transformação digital no campo da segurança coetânea – correlativa e partilhada – reivindicam a agudeza das organizações policiais. Embora em constante evolução e aperfeiçoamento, o policiamento internacional revelou-se um domínio descurado. *Igitur qui desiderat pacem, praeparet bellum* (*Vegetius apud* Milner, 2001).

Recentemente, o modo como as forças policiais operam, investigam crimes e interagem com a comunidade sofreu colossais desenvolvimentos consequentes dos enredamentos dos ambientes digitais, enquanto espaços – assimétricos e infindos – de interação social massiva e, como tal, propensos a desvios (Hoogenboom, Schoneveld, & Meiboom, 1997; Freire, 2023). A frenética virulência de ciberataques e cibercrimes estimulou o desenvolvimento de competências policiais específicas para investigar delitos *online*, como fraudes, roubo de identidade, *ciberbullyng*, *hacking*, *phishing*, *quishing*, *smishing*, *vishing*, *grooming*, *ransomware*, *cheap fake*, *deepfakes* e outros relacionados com

[75] Destacam-se os seguintes perfis de sites *proxy* que integram a rede de desinformação pró-Kremlin: *Strategic Culture Foundation*, *Global Research*, *New Eastern Outlook*, *SouthFront*, *News Front*, *Geopolitica.ru*, *Katehon*, Rede de Sincrética de Desinformação, *New Resistance*, *Fort Russ News*, Centro para Estudos Sincréticos, *Euromore*, entre muitos outros (GEC, 2020, pp. 9-15). A fundação, conhecida como Fundo para Apoio e Proteção dos Direitos dos Compatriotas que Vivem no Estrangeiro (*Pravfond*), foi identificada como fachada para operações de desinformação e influência russa em 48 países na Europa (Gonçalves, 2024).

a *deep web* e a *dark web*[76] (Schick, 2020). As capacidades de monitorização e patrulhamento social foram ampliadas pelo uso da videovigilância, a análise de dados concretos em tempo real e outras tecnologias emergentes. A eficiência da prevenção criminal parece ser favorecida pelo acesso e análise da "metainformação", através da qual são promovidas abordagens proativas, antecipando padrões criminais e otimizando os recursos penhorados na segurança (CNCS, 2023). A presença policial nas redes sociais e a interação com a comunidade em linha auxiliam a comunicação fluída com diferentes públicos, a rápida divulgação de informações verosímeis e a formalização de parcerias virtuais para questões securitárias prementes. O patrulhamento digital, a avaliação do risco e a sinalização precoce de ameaças são, hoje, imperatividades operacionais das forças da lei. O combate à infodemia envolve o policiamento digital de fontes abertas e os seus díspares ambientes, como o metaverso[77], para identificar tendências e, se possível, os seus mentores como parte do ciclo de produção de inteligência. Para corresponder a estes desideratos, as polícias carecem, desde logo, de formação, treino, capacitação tecnológica e uma "visão de futuro" (Kennedy, 1962, p. 2; Freire, 2023; Nogala, 2024).

A vulgarização da utilização de ferramentas digitais sofisticadas e de técnicas disruptivas desafiadoras – como os *deepfakes*[78], a tecnologia que lhes está subjacente e o potencial impacto na aplicação da lei e nos cidadãos–, inspiram a maior cooperação entre as polícias da UE e destas com os especialistas (públicos e privados) em segurança digital, diferentes sectores da governação e ONG (EUROPOL, 2022d). Para além dos *big data*, a atualização e a capitalização das boas práticas policiais englobam a IA, a aprendizagem

[76] *Deep web* representa a parte da *Web* que ainda não foi indexada pelos motores de busca comuns. *Dark web* é o conjunto de conteúdos acessíveis ao público que estão alojados em sítios *Web* cujo endereço IP está oculto, mas ao qual qualquer pessoa pode aceder, desde que conheça o endereço. Pode ser compreendida como o conjunto de conteúdos privados trocados numa rede fechada de computadores para partilha de ficheiros (Paganini, 2017). *Vide* Glossário apenso.

[77] A multidimensionalidade da realidade aumentada e os seus fundamentos obrigam à correlação da tecnologia que o impulsiona, o uso adverso e crimes praticados (incluindo identidade, crimes financeiros, assédio, terrorismo e desinformação), o impacto no mundo físico, a viabilidade de monitorização de evidências, o policiamento, o treino e as intervenções alternativas, etc., para compreender esse novo espaço e se adaptá-lo à aplicação da lei. O 'metaverso' consiste numa iteração hipotética da *internet* que esbate as fronteiras entre os mundos físico e virtual para criar uma experiência imersiva. As polícias necessitam de antecipar as mudanças trazidas por este território geopolítico e se preparar para sua ascensão. Desenvolvimentos recentes na Europa, como a plataforma *Horizon Worlds* da *Meta* e os investimentos significativos de conglomerados tecnológicos em tecnologia de metaverso, destacam a importância do tema para a agenda global. O seu impacto potencial na segurança global e dos cidadãos sublinha a urgência de se investir na investigação para nos adaptarmos a uma paisagem digital em apressurada evolução (EUROPOL, 2022b).

[78] Por exemplo, antes da segunda invasão russa à Ucrânia (2022), os EUA denunciaram a utilização de vídeos *deepfake* pelo Kremlin para justificar a operação militar (Sganga, 2022; EUROPOL, 2022d).

automática, a *Internet of Things* (IoT)[79], o *software* analítico e outras técnicas de previsão baseadas em algoritmos (Deloitte, 2019). O policiamento inteligente (*smart policing*) apresenta-se como um paradigma auspicioso, empenhando a ciência e a inovação na condução das operações policiais, mormente através da promoção de aplicações analíticas, tecnologias e práticas reticulares vanguardistas, de base científica (Coldren, Huntoon, & Medaris, 2013; Deloitte, 2019). Na senda do "polícia científico" *vollmeriano*, a cientificização do policiamento convenciona-se na ID&I e na utilização de metadados, colecionados, analisados, mensurados e processados por técnicas cientificamente comprováveis, ampliadas por parcerias público-privadas, multidisciplinares e multinacionais na prevenção e repressão do crime (Vollmer, 1930; Bayley & Shearing, 1996; Deloitte, 2019; Elias, 2024). Ainda assim, a atuação policial deve encarar a tecnologia como um "parceiro" no teatro de operações e não como um "substituto", atenta a importância da presença, interação e proximidade junto da população (Deloitte, 2019; SAS, 2021; Elias, 2023). A componente humana é a mais habilitada a beneficiar da digitalização do policiamento, constituindo, simultaneamente, a guardiã do equilíbrio entre a partilha de informações e a defesa da privacidade (Freire, 2023). O uso extensivo das tecnologias revolucionárias, numa lógica de vigilância omnipresente, suscita questões éticas, deontológicas e legais (EUROPOL, 2024b). A emergência e expansão da IA no domínio da segurança assomam uma dupla vertente: por um lado, auxiliam a missão de recolha, análise e armazenamento de dados; por outro lado, são potenciadoras de ameaças.

Beneficiando de uma posição proeminente na arquitetura da segurança europeia, a EUROPOL é um centro operacional de alta segurança que providencia um trabalho analítico de alta qualidade, empregando ferramentas tecnológicas aprimoradas para apoiar as investigações criminais realizadas pelas autoridades policiais e judiciárias da UE[80], bem como para proteger e fortificar um ecossistema anti-infodémico e de "contra-desinformação" coerente, fiável e seguro (EUROPOL, 2024b). Os sistemas especializados da EUROPOL oferecem capacidades rápidas e seguras de armazenamento, pesquisa, visualização e ligação de informações criminais. Desperta para as vulnerabilidades estruturais causadas pela

[79] A *Internet Society* define a IoT, em sentido lato, como "(…) a extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores". A IoT abrange todos os aparelhos e objetos habilitados a estarem permanentemente ligados à *internet*, sendo capazes de se referenciar na rede e de comunicar entre si. O seu estado pode ser alterado com ou sem o envolvimento ativo da ação humana e permite recolher uma ampla quantidade de informação sobre o que o rodeia (CNCS, s.d.).

[80] A Agência tem um papel central na descodificação de redes complexas ligadas ao COT. Um relatório recente identificou 821 redes criminosas ativas, integrando cerca de 25.000 membros (EUROPOL, 2024a, p. 5).

infodemia e pelo alcance global da desinformação, a Agência está empenhada em proteger as sociedades, os cidadãos e as liberdades democráticas, seguindo a linha europeísta (EUROPOL, 2020 e 2022d). Como sublinhado na 'Agenda Estratégica da União Europeia para 2019-2024', o reforço da cooperação é uma das prioridades da UE, envolvendo as várias partes interessadas numa abordagem multidisciplinar a fim de detetar, prevenir e melhorar as respostas aos ciberataques, e, simultaneamente, reforçar a resiliência através de diligências diplomáticas (Conselho Europeu, 2019). O fortalecimento dos grupos de trabalho da *StratCom*[81] do SEAE, a transformação digital, o reforço da literacia mediática e a implementação de medidas adicionais de integridade e transparência para as plataformas em linha sobressam da estratégia europeia contra a desinformação (*European Council*, 2015; *European Commission*, 2018a; Comissão Europeia, 2020a).

Funcionando como uma plataforma privilegiada de informações estratégicas e operacionais sobre atividades criminosas e terroristas transnacionais, a EUROPOL patrocina um apoio técnico e analítico às operações policiais no espaço europeu (Reid, 2013). A Agência emprega cerca de 100 analistas criminais, altamente qualificados, que, em conjunto, constituem uma das maiores convergências de capacidade analítica mundial (EUROPOL, 2024b). Neste arco, a EUROPOL dispõe de cinco centros altamente especializados e orientados para rechaçar ameaças específicas, a saber: *Operation and Analysis Centre*; *European Serious and Organised Crime Centre*; *European Cybercrime Centre*; *European Counter Terrorism Centre*; e o *European Financial and Economic Crime Centre*[82]. Os seus produtos estratégicos-analíticos incluem a 'Avaliação da Ameaça da Criminalidade Grave e Organizada' (SOCTA), que atualiza a comunidade policial europeia e os decisores políticos sobre a evolução do COT e as ameaças que representa para a Europa; a 'Avaliação da

[81] Como vimos as forças-tarefa da *StratCom* abrangem os Balcãs Ocidentais e a zona Sul (*i.e.*, região do Médio Oriente e Norte de África). Existe ainda uma equipa horizontal centrada nas ameaças emergentes, na análise de dados, no desenvolvimento de políticas e na cooperação internacional, incluindo o Sistema de Alerta Rápido da UE sobre Desinformação, uma plataforma digital ativada em 2019, para sinalizar em tempo real campanhas de desinformação (Agência Lusa, 2019; *EUvsDisinfo*, 2019).

[82] De acordo com Julia Viedma, o *Operation and Analysis Centre* opera nos bastidores para interligar as autoridades responsáveis pela aplicação da lei nos EM da UE e fornecer-lhes o melhor apoio operacional disponível para protegerem os seus cidadãos. Por sua vez, Jean-Philippe Lecouffe sobreleva que o *European Serious and Organised Crime Centre* se dedica a desmantelar redes da criminalidade grave e organizada, cada vez mais ágeis, sem fronteiras, controladoras e destrutivas. Para Edvardas Šileris, a ação do *European Cybercrime Centre* é determinante para debelar o crescendo da cibercriminalidade numa sociedade fortemente digitalizada. Anna Sjöberg enfatiza o papel do *European Counter Terrorism Centre* na construção de uma perspetiva global, concertada com uma abordagem proativa e tecnologicamente avançada, contra o terrorismo e o extremismo violento. Por fim, Burkhard Mühl sobressai como o *European Financial and Economic Crime Centre* está fortemente empenhado na investigação da criminalidade financeira e económica internacional e na recuperação de ativos criminosos (EUROPOL, 2024b, pp. 25-34).

Ameaça da Criminalidade Organizada na *Internet*' (IOCTA)[83], que ajuda os decisores políticos a escolher os domínios prioritários para combater a cibercriminalidade; o 'Relatório sobre a Situação e as Tendências do Terrorismo na EU' (TE-SAT), que fornece uma panorâmica dos atentados terroristas falhados, frustrados e consumados na UE, num espaço temporal; e, por fim, as notificações de alerta precoce de novas ameaças do COT[84].

Importa ainda uma referência particular à '*EUROPOL Strategy – Delivering Security in Partnership*', de 2023, a qual espelha as mudanças no cenário criminal e no contexto político europeu, respondendo a desenvolvimentos críticos, como a Covid-19 (e outras epidemias de *novo tipo*), a guerra russo-ucraniana ou a beligerância entre o *Hamas* e Israel. Este estratagema prospetivo é o resultado de amplas consultas junto dos Estados-Membros (EM) e dos parceiros operacionais, projetando a Agência em novos domínios e capacidades no apoio a investigações complexas, cooperação transfronteiriça, ação conjunta no campo da aplicação da lei, etc., abordando os desafios de segurança de maneira colaborativa e integrada[85] (EUROPOL, 2023; SSI, 2023).

Neste campo estratégico e analítico, os prolíficos canais de cooperação internacional mantidos pelas redes transnacionais de oficiais de ligação policial[86], especialmente as integradas pelos OLMAI junto da EUROPOL, representam uma vigorosa capacidade de

[83] Assinalando o décimo aniversário da criação deste instrumento pela EUROPOL, a publicação do *Internet Organised Crime Threat Assessment* (IOCTA) 2024 é particularmente relevante num momento crítico da evolução e crescente massificação das ameaças cibernéticas. Milhões de vítimas em toda a UE são atacadas e exploradas em linha diariamente. A *dark web* continua a ser um fator-chave para a cibercriminalidade, permitindo aos infratores a partilha de conhecimentos, ferramentas e serviços de uma forma mais dissimulada. O ciclo de vida dos sítios criminosos tornou-se mais curto e os sítios-espelho proliferam para contrariar os *takedowns* das autoridades (EUROPOL, 2024c).

[84] Através da equipa de *Scanning, Analysis and Notification* (SCAN/EUROPOL).

[85] As seis prioridades estratégicas da EUROPOL orientam a organização na realização dos seus principais objetivos e visão, bem como na prestação de um conjunto único de serviços operacionais à UE: a) ser o *hub* de informação criminal da UE, por via da centralização e facilitação do compartilhamento de informações sobre crimes entre os EM da UE, tornando-se o ponto de referência para a recolha, análise e disseminação de inteligência criminal; b) providenciar apoio operacional ágil e em tempo real às autoridades nacionais, ajudando na coordenação de operações transfronteiriças e na resposta a ameaças emergentes; c) assumir a vanguarda do suporte operacional, inovador e eficaz, às forças de segurança, com recurso à tecnologia de ponta e práticas recomendadas para melhorar a eficácia das operações policiais; d) fornecer uma plataforma de desenvolvimento e compartilhamento de soluções para o policiamento europeu; e) ser modelo de excelência em cooperação policial internacional, promovendo a colaboração eficaz entre os EM e com parceiros fora da UE; f) facilitar a cooperação e coordenação entre partes interessadas, incluindo agências de aplicação da lei, sector privado e organizações internacionais, para combater o COT de forma mais eficaz (EUROPOL, 2023 e 2024b). Estas prioridades decorrem dos resultados da Avaliação da Ameaça da Criminalidade Grave e Organizada (SOCTA), realizada quadrienalmente, e determinam o trabalho operacional efetuado no âmbito da *European Multidisciplinary Platform Against Criminal Threats* (EMPACT).

[86] A EUROPOL é composta por mais de 1700 profissionais de 54 países diferentes que abrangem uma vasta gama de domínios, incluindo uma rede de mais de 300 agentes de ligação dos EM da UE, bem como de países terceiros e organizações internacionais. Os agentes de ligação são funcionários responsáveis pela aplicação da lei destacados para a EUROPOL a partir do seu país de origem ou de organizações internacionais e que constroem diariamente fortes redes internacionais e facilitam a cooperação operacional, representando simultaneamente os interesses dos seus diferentes países (EUROPOL, 2024b).

debelação das avalanches infodémicas responsáveis pela degradação dos ecossistemas de informação. Segundo Ludo Block, os "agentes de ligação são um fator importante na cooperação policial" (Block, 2013, p. 107). As dimensões estratégicas e operacionais do policiamento prosseguido pelos OLMAI junto da Agência reforçam o capital de confiança e agilizam a cooperação policial internacional no quadro da UE, mas também junto de países terceiros e de organizações de espectro mundial, como as NU ou a INTERPOL (Fernandes, 2024b).

> "O agente de ligação da EUROPOL é geralmente considerado diferente do agente de ligação bilateral, baseado nas embaixadas dos Estados-Membros, em termos de papel, função e especialização. Trata-se de uma raça à parte" (Reid, 2013, p. 151).

Primeiramente, as funções dos OLMAI da GNR e da PSP na EUROPOL revestem uma dimensão estratégica na medida em que elaboram, periodicamente, relatórios e análises relevantes para a segurança interna europeia e nacional. Partilhados no círculo internacional, estes produtos informacionais são igualmente consumidos e permutados no plano doméstico. Ao participarem nas reuniões de alto nível da EUROPOL, vocacionadas ao enquadramento e análise dos principais fenómenos criminais na Europa, os oficiais de ligação envolvem-se e contribuem ativamente para a segurança da coletividade europeia. Por outro lado, os OLMAI desenvolvem ainda uma componente operacional ao processar pedidos de informação[87] no *Secure Information Exchange Network Application* (SIENA)[88], o sistema de intercâmbio, seguro e célere, de mensagens da EUROPOL para o seguimento das pesquisas e dos resultados encontrados no âmbito de processos-crime investigados pela PSP ou GNR (EUROPOL, 2022a). O SIENA assegura a conexão com o *Europol Information*

[87] Os pedidos e as mensagens dos serviços de aplicação da lei são analisados através de projetos de análise, numa dupla aceção: operacional e estratégica. Os projetos de análise centram-se em certos domínios da criminalidade numa perspetiva baseada em produtos de inteligência ou numa abordagem à rede criminosa. A informação resultante alimenta um ciclo de informação que pode conduzir à identificação de ameaças emergentes (EUROPOL, 2024b).

[88] O SIENA é uma plataforma de ponta que responde às necessidades de comunicação das autoridades policiais da EU, facilitando o intercâmbio de informações operacionais e estratégicas entre os agentes de ligação, analistas e peritos da EUROPOL; EM; e Estados Terceiros convencionados. Congregando mais de 3000 autoridades, o SIENA é, por excelência, o canal de intercâmbio de informações das unidades especializadas de aplicação da lei e de várias iniciativas, como os gabinetes de recuperação de bens, os centros de cooperação policial e aduaneira (CCPA), as unidades de informação sobre passageiros e de informação financeira (FIU), as equipas de busca ativa de fugitivos (ENFAST), as unidades táticas especiais (ATLAS), as unidades do grupo de trabalho conjunto para a ação contra a cibercriminalidade (J-CAT), as iniciativas transfronteiriças LO e *Lake of Constance*. A 'Estratégia 2020+' da EUROPOL promove o desenvolvimento da SIENA, através do avanço do arquétipo de gestão da informação da EUROPOL e da rápida adoção de métodos e tecnologias sofisticadas (EUROPOL, 2022a).

System (EIS)[89], a base de dados central de informações e registos criminais (EUROPOL, 2024b). Para além do SIENA e do EIS, importa ainda destacar a *Europol Platform For Experts* (EPE), uma plataforma *Web* segura e colaborativa para especialistas que operam numa variedade de áreas de aplicação da lei, com o objetivo de facilitar e apoiar a partilha de dados não pessoais sobre a criminalidade (*v.g*., disponibiliza ferramentas de gestão de conteúdos e de comunicação, tais como *wikis*, blogues, mensagens e partilha de ficheiros) entre mais de 22.000 especialistas e de 65 plataformas (EUROPOL, 2024b). Ademais, os OLMAI acompanham o planeamento operacional no quadro da iniciativa securitária *European Multidisciplinary Platform Against Criminal Threats* (EMPACT)[90] e das operações conjuntas entre as agências nacionais e as de outros EM e países terceiros[91].

É essencial trabalhar em rede com governos, parceiros e aliados, organizações da sociedade civil, *academia*, imprensa e o público internacional na definição de estratégias conjuntas[92] de aprofundamento das análises e de combate operacional à infodemia com vista a desmantelar redes de desinformação, responsabilizar os perpetradores e aumentar a

[89] Criado em 2005, o EIS encerra informações sobre crimes internacionais graves, pessoas suspeitas e condenadas, estruturas criminosas, infrações e meios utilizados para as cometer. Trata-se de um sistema primacial utilizado para certificar e correlacionar informações sobre uma determinada pessoa ou objeto de interesse no contexto das jurisdições nacionais ou organizacionais, permitindo o armazenamento e o controlo cruzado automático de dados biométricos (ADN) e de dados relacionados com a cibercriminalidade, construindo uma visão estruturada de um processo penal. O EIS é usado pelos funcionários da EUROPOL, pelos agentes de ligação dos EM, pelos peritos nacionais destacados na sede da EUROPOL, pelo pessoal das unidades nacionais da EUROPOL e pelas autoridades competentes.

[90] O atual ciclo do EMPACT privilegia o combate aos seguintes fenómenos criminógenos: redes criminosas de alto risco, ciberataques, tráfico de seres humanos, exploração sexual de crianças, contrabando de migrantes, tráfico de droga, fraude, crimes económicos e financeiros, criminalidade organizada contra o património, criminalidade ambiental e tráfico de armas de fogo.

[91] A EUROPOL tem capacidade de assistência *in locu* mediante o destacamento de analistas e especialistas para apoiar as operações em curso nos EM. Esta capacidade concretiza-se através de *Joint Action Days* (JADs), *i.e.*, iniciativas operacionais conjuntas baseadas em inteligência; *Operacional Task Force* (OTF), formadas para levar a cabo um projeto específico; *Joint Investigation Team* (JIT), instrumento de cooperação internacional criado para realizar investigações específicas e articuladas entre autoridades judiciárias e policiais; e de *Mobile Offices* no apoio a investigações em curso, grandes eventos desportivos, conferências internacionais e outras atividades numa base de *ad hoc* (EUROPOL, 2024b).

[92] No quadro da UE, ressaltamos cinco instrumentos estruturantes: a) 'Estratégia Europeia de Segurança – Uma Europa Segura num Mundo Melhor', de 12 de dezembro de 2003; b) Comunicação da Comissão, de 28 de abril de 2015, sobre a 'Agenda Europeia para a Segurança' (COM(2015)0185); c) Resolução do Parlamento Europeu, de 9 de julho de 2015, sobre a 'Agenda Europeia para a Segurança' (2015/2697(RSP)); d) Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, de 24 de julho de 2020, sobre a 'Estratégia da UE para a União da Segurança' (COM(2020) 605 final); e e) a 'Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais', do Conselho Europeu, de 21 de março de 2022 (7371/22). Este conjunto de diplomas estabeleceu as matrizes da promoção dos interesses da UE em matéria de segurança, com base no reforço da cooperação operacional, o intercâmbio de informações e o desenvolvimento de ações de apoio aos EM no combate à criminalidade transfronteiriça. O aparato estratégico é alçado pela 'Estratégia global para a política externa e segurança da EU', de 2016, que interliga as extensões da segurança interna com a política externa, procedendo à sua implementação.

resiliência coletiva (Gill & Goolsby, 2022). A maior capacitação e formação das autoridades nacionais é basilar para aperfeiçoar a deteção e debelação da infodemia, com base no respeito pelos direitos fundamentais e em defesa da infraestrutura crítica nacional e europeia (GEC, 2020; Simon & Mahoney, 2022; *HDRO*, 2024; Nogala, 2023 e 2024).

Concluímos que a sofisticação, coerência e profundidade dos produtos analíticos concebidos pelos especialistas da EUROPOL contribuem para a construção de conhecimento informado, congruente e crítico. A partilha segura e fluída de informações (INFOSEC) entre as forças policiais e outras agências fortalece respostas coerentes contra a corrupção infodémica (Andress, 2014). Contudo e apesar da EUROPOL contribuir para o combate supletivo da desinformação, *fake news* e infodemia, principalmente através da investigação de crimes conexos ou consequentes, confirmamos que o mandato da Agência não contempla, *de jure* ou de modo explícito, tais fenómenos[93]. Esta lacuna no seu mandato e no ordenamento jurídico-penal de alguns EM obstaculiza uma atuação anti-infodémica uniforme e assertiva. Assim, a EUROPOL restringe-se à investigação dos crimes previstos no Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016 (adiante, Regulamento EUROPOL)[94], ou, quando muito, das formas de criminalidade lesivas de um interesse comum protegido pela política da UE (EUROPOL, 2020 e 2022d).

6. CONCLUSÃO

6.1. Instigações geopolíticas ao policiamento moderno

> "A causa fundamental do problema é que, no mundo moderno, os estúpidos estão cheios de certezas enquanto os inteligentes estão cheios de dúvidas" (Russell, 1998, p. 28).

O policiamento pan-europeu sofreu uma profunda transformação nas últimas três décadas, sobretudo com a permeabilização das tecnologias de informação e comunicação em todos os aspetos da segurança societal (CNCS, 2023). A natureza transnacional da cooperação policial aumentou expressivamente as complexidades organizacionais e procedimentais. Incontáveis fenómenos transfronteiriços, incluindo ataques terroristas em todo o continente; a expansão e sofisticação do COT; o *crash* financeiro; os numerosos

[93] O mandato contempla as atividades de estupefacientes; tráfico de seres humanos; imigração clandestina organizada; cibercriminalidade; contrafação do euro; fraude em matéria de IVA; branqueamento de capitais e localização de bens; grupos móveis (itinerantes) de criminalidade organizada; criminalidade no domínio da propriedade intelectual; contrabando de cigarros; gangues de motociclistas fora-da-lei; e terrorismo (Regulamento EUROPOL).

[94] Cria a EUROPOL e substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53). Foi alterada pelo Regulamento (UE) 2022/991 do Parlamento Europeu e do Conselho, de 8 de junho de 2022.

conflitos militares nos confins da Europa e a instrumentalização de migrantes, deslocados e refugiados[95] sírios, afegãos, iranianos, ucranianos, palestinianos e subsarianos contra as fronteiras europeias circunjacentes à Bielorrússia, Sérvia, Turquia, Líbia e Marrocos – *weaponizing migration* (Greenhill, 2022) –; uma pandemia que parou o mundo; um *coup* russo em prol de uma ordem internacional alternativa; entre outras instigações, contribuíram para essas mudanças (Block, 2013; Deloitte, 2019; Santos, 2020).

> "A situação atual é potencialmente pior do que em 1939 ou 1965. Não é só o facto de uma guerra nuclear pôr em perigo centenas de milhões de pessoas em países neutros. A humanidade enfrenta também as ameaças existenciais adicionais das alterações climáticas e da IA fora de controlo" (Harari *apud The Economist*, 2024c, p. 1).

Nesta moldura geopolítica, várias inseguranças históricas, ilusões de grandeza e desejos de reconhecimento mundial relançaram Moscovo na *velha campanha* de conquista de poder global, cujos efeitos que continuam a modelar a atualidade (Oliker, 2015; Radchenko, 2024). "Tal como o [presidente] chinês Xi Jinping é comparado por alguns a Mao Zedong, Putin foi recentemente comparado a Estaline, que governou com paranoia, mão-de-ferro e um sistema orwelliano de desinformação" (Nagorski, 2024, p. 3). O modelo russo de propaganda infodémica – "mangueira de falsidade"[96] – representa uma ameaça significativa (Paul & Matthews, 2016; *European Commission*, 2018a). A verdade desarma o belicismo infodémico e a falácia da desinformação do poderoso *RussKiy medved* ("urso russo"). *Le mensonge n'a pas de pieds*[97]. A loquacidade do maquinismo da desinformação da Rússia e a sua perspetiva maniqueísta galvanizaram o complexo de (ciber)segurança internacional, exigindo a criação de mecanismos de "defesa híbrida" que visem a autenticidade da informação (Gill & Goolsby, 2022). "Nem tudo o que é confrontado pode ser mudado, mas nada pode ser mudado até ser confrontado" (Baldwin, 1962).

[95] Mais de 95 milhões de pessoas estão atualmente refugiadas ou foram deslocadas internamente devido a conflitos violentos (IEP, 2024).
[96] Segundo a investigação de Paul & Matthews (2016), o modelo contemporâneo da propaganda russa apresenta as seguintes características distintivas: a) alto volume e multicanal (apresenta uma variedade de fontes, em número e quantidade, que são semelhantes ao destinatário da mensagem); b) rápido, contínuo e repetitivo (considerando que as primeiras impressões são muito resistentes, o aparelho infodémico russo insiste na repetição, a qual leva à familiaridade e depois à aceitação); c) falta de compromisso com a realidade objetiva (a sobrecarga de informação leva as pessoas a atalhar o juízo de fiabilidade das mensagens, mesmo que falsas; a familiaridade de temas apelativos, sustentados por provas (falsas), aumenta a probabilidade de serem aceites; e a aparência de objetividade pode aumentar a credibilidade da propaganda); e d) ausência de compromisso com a consistência (a incoerência tem um efeito deletério na persuasão, embora as audiências ignorem as contradições em determinadas circunstâncias, como uma razão válida para uma mudança de opinião).
[97] Provérbio francês que pode traduzir-se como "a mentira tem perna curta".

6.2. Dinamismos da cooperação policial transfronteiriça

A intensidade das contaminações infodémicas justifica o estudo periódico da cooperação internacional – em declínio desde 2016 e agravada abruptamente em 2020 –, das correspondências entre as polícias europeias e das consequências que geram na ordem convencionada, ainda que imperfeita (Bertolin, 2015; *WEF*, 2024c). Os triunfos e fiascos do policiamento transnacional são mais notórios do que nunca, especialmente no contexto das mudanças sísmicas ocorridas na UE (SSI, 2023). A segurança interna e as polícias têm sido desafiadas a partilhar informações e a participar no esforço de "policiamento coletivo" (Greene, 2007, p. xxiv). A nossa investigação, necessariamente incompleta, apresenta-se como precursora de outros estudos comparativos e analíticos dos mecanismos estratégicos, diplomáticos e operacionais do policiamento pan-europeu, em especial do desempenho da EUROPOL e dos seus elos de ligação aos EM, organizações e países terceiros.

Na verdade, o policiamento moderno atravessa uma metamorfose multinível que entrecruza o plano global, nacional, regional, sub-regional e local. A velocidade potencial da era digital modificou as práticas policiais, impondo uma abordagem glocal, proativa e tecnologicamente avançada quanto aos desafios e oportunidades supervenientes[98]. "(…) O policiamento mudou, tal como a sociedade que é policiada" (Elias, 2023, p. 33). Os avanços tecnológicos coetâneos testemunham um ciclo de produção aberta e de inovações sem precedentes. A tecnologia integra os perigos e as respostas transnacionais. Apoiadas na digitalização e em produtos de inteligência partilhados, as autoridades policiais e judiciárias projetam cenários para analisar e compreender as ameaças vindouras, formular contramedidas inovadoras e, se necessário, questionar os "modelos de negócio" estabelecidos, a fim de introduzir mudanças organizacionais ajustadas ao ritmo da evolução conjuntural (Deloitte, 2019). A exaltação do progresso tecnológico resulta da sua convergência com aplicações inovadoras e as instigações colocadas aos quadros jurídicos vigentes. Concebemos como vital uma abordagem estratégica à desinformação e às ameaças impulsionadas pela IA (Fitz-Gerald & Padalko, 2024). Ao tirar partido da sua diversidade para desenvolver sistemas inclusivos de IA e que beneficiem todos os segmentos da sociedade, o policiamento da era digital pode avalizar que a ID&I neste domínio espelhe

[98] Em 2020, a Direção Nacional da PSP encarregou o Centro de Investigação (ICPOL – *Police Research Center*) do ISCPSI de promover a realização do 'Inquérito Nacional de Avaliação da Satisfação sobre a Polícia de Segurança Pública 2021'. Esta investigação para a ação, inédita em Portugal, abrangeu o continente e as regiões autónomas, traçando uma impressão fidedigna da perceção pública quando ao desempenho da polícia urbana e à qualidade do serviço público prestado, essenciais para a adequação da atividade securitária às exigências e necessidades dos cidadãos (Fernandes & Machado, 2021, p. 20).

uma vasta gama de perspetivas e necessidades, tal como já acontece ao nível da defesa com a recente revisitação da estratégia da OTAN para a IA (NATO, 2024). Assim, o policiamento moderno deve explorar o potencial tecnológico emergente – como a IA, computação quântica, 5G, redes e tecnologias de informação e de comunicação (TIC) descentralizadas e alternativas, a cripto moeda, a impressão 3D, biotecnologia, etc. –, enquanto lida com revelações criminosas crescentemente modificadas[99] (Silva & Guerreiro, 2020; Bolle, 2020). A desterritorialização colocou o envolvente cibernético sob a atenção da justiça e assuntos internos (Elias, 2022 e 2023). É capital que o território digital crie ambientes seguros e ecossistemas inteligentes, tornando a digitalização um fator legítimo de democratização e qualidade de vida, ao invés de ser uma causa de dissensão ou exclusão social (Covas, 2020). A unidade e a capacidade de adaptação assumem dimensões críticas à medida que enfrentamos conflitos geopolíticos voláteis e multidimensionais (Gill & Goolsby, 2022). A cooperação policial internacional e a segurança interdependente são cruciais[100] (SSI, 2023).

Deste reexame da cooperação policial internacional parece ressaltar uma abordagem compreensiva às variabilidades que constrangem o desenvolvimento humano, o progresso social e a sustentabilidade global. A cosmopolização de uma cultura de cooperação plural é essencial para promover a confiança e inverter as desigualdades no acesso aos recursos, à tecnologia e às oportunidades (Fernandes, no prelo). Uma ação coletiva, solidária e interpenetrada contra a infodemia propende a desconstruir especulações tendenciosas, manipulações polarizadoras e perceções erradas sobre a realidade (Gill & Goolsby, 2022). Importa envolver e capacitar os cidadãos a influenciarem as tomadas de decisões, tornando-os "coproprietários" dos seus destinos, com base em informação confiável e rigorosa. Urge recentrar as instituições nas pessoas e estreitar as distâncias. A empatia, a confiança interpessoal e a comunhão das identidades mostram-se fulcrais na construção de compromissos entre o que as divide. A colaboração interagências empodera a partilha de conhecimentos, tecnologias e recursos, bem como o desenvolvimento de soluções práticas, céleres, eficazes e consensuais. Somente uma arquitetura de segurança partilhada enfrentará eficazmente os desafios interligados que o mundo enfrenta. Para tal há que criar mecanismos

[99] Segundo Didier Jacobs, a cooptação e utilização responsável de tecnologias revolucionárias e inovadoras, como a IA e outros desafios digitais, revestem uma importância fundamental para a proteção dos valores sociais e da segurança pública, apesar da persistência de inúmeros desafios digitais, como a transformação da nuvem e a futura computação quântica (EUROPOL, 2024b).

[100] A 'Estratégia da PSP 2024/2026' procura contribuir para o esforço de segurança internacional, investindo no alargamento estratégico das redes policiais de cooperação transfronteiriça (PSP, 2024).

e espaços de deliberação seguros e esclarecidos, onde se corrijam perceções enviesadas sobre as preferências e motivações de terceiros e se acertem visões informadas (*HDRO*, 2024).

6.3. Uma União em defesa da informação fidedigna

> "Mais de 80% dos cidadãos da União Europeia acreditam que a desinformação é uma ameaça à democracia. Numa era de *fake news* e pós-verdades, Bruxelas procura regular os gigantes tecnológicos como forma de proteger os cidadãos e a democracia" (Paiva & Gómez, 2021, p. 1).

O aprofundamento da interação multidisciplinar nos círculos informacionais privilegiados afigura-se-nos indispensável para atualizar o conhecimento da preparação da UE para a era digital e os seus efeitos caleidoscópicos (Comissão Europeia, 2024). A UE tem estado *avant-garde* no combate à desinformação, adotando várias recomendações estruturais e defendendo o respeito à liberdade de expressão e a proibição de censura de discursos críticos, divergentes, epigramáticos ou impressionantes (Comissão Europeia, 2018; *European Commission*, 2018b; Silveira, 2022). Sujeito a permanente escrutínio democrático[101], o policiamento da era digital desenvolve-se unicamente no espaço de atuação legalmente positivado e na observância estrita da dimensão ética e dos Direitos Humanos, não podendo atuar fora desse quadro sob pena de recair na vigilância *orwelliana* ou na censura dos inflamados *451 Fahrenheit* características das autocracias, regimes iliberais e conglomerados marginais[102] (Orwell, 2012; Snowden, 2019; Bradbury, 2020 [1953]). O balanceamento entre o exercício da autoridade e a proteção das liberdades individuais constituem a pedra-de-toque do policiamento democrático na produção de segurança coletiva. A estratégia europeia para a "desminagem" infodémica passa, assim, pelo reforço dos primados humano e tecnológico, na lógica multidimensional da Segurança Humana (informação verbal[103]). Só assim se fortalecerá a credibilidade dos órgãos institucionais e seus representantes, bem como dos *media*, enquanto verificadores de

[101] Não descuremos que a transferência de poder dos Estados para os seus representantes policiais e o próprio exercício da autoridade coerciva dos Estados é objeto de uma positivação exaustiva e de fiscalização permanente por parte de *integrity warriors*, domésticos e internacionais (De Sousa, Hindess, & Larmour, 2009).
[102] Em 2013, Edward Snowden, funcionário demissionário da Agência Central de Inteligência (CIA) norte-americana, expôs os programas *Fairview* e o *PRISM* assimilados no sistema de vigilância global da Agência de Segurança Nacional (NSA). Denunciando a participação da Austrália, do Canadá, da Nova Zelândia e do Reino Unido, bem como de conglomerados como a *Microsoft*, *Google*, *Facebook*, *Yahoo!*, *Apple*, *Youtube*, *Dropbox*, *AOL*, *Paltalk*, *Skype*, *Verizon*, *Cisco*, *Oracle*, *Intel*, *Qwest*, *EDS*, *AT&T*, *IBM*, *Qualcomm*, entre outras, Snowden chocou o mundo (informação verbal, apresentada no documentário norte-americano, intitulado '*Citizenfour*', de 24 de outubro de 2014, realizado por Laura Poitras; Snowden, 2019; Pandey, 2021).
[103] Informação verbal extraída da conferência '*Clearing the Path to Growth: Ukraine's Tech-Driven Strategy for Humanitarian Demining*', promovida pelo IEP, em 16 de janeiro de 2024.

factos[104], com recurso a dados empíricos e consolidados (Fernandes, 2022a e 2024a). A rede europeia para combater a desinformação e os ciberataques integra três dezenas de países voluntários, entre os quais Portugal (Diário de Notícias/Agência Lusa, 2024). A estratégia anti-infodémica dos 27 EM da UE e das 57 nações da OSCE deve aperfeiçoar as formas de identificação precoce e de desaceleração das campanhas de desinformação em tempo real, bem como aprimorar mecanismos para supervisionar, regular, punir, degradar, perturbar e expor manobras de infodemia ou outros estratagemas insidiosos de terceiros, conhecidos ou anónimos, singulares ou coletivos. A educação e formação dos membros de uma "sociedade de conhecimento intensivo" são elementares para habilitar a empregar a razão, a lógica, a ética e a análise crítica perante a exposição à polémica infodémica – literacia mediática e resiliência digital (Fernandes & Júnior, 1896; Poiares, 2019; Marques & Santos, 2020; Guterres, 2020; Almeida, 2021). A UE terá, incontornavelmente, de robustecer a sua capacidade vigilância e controlo do espaço digital por entidades reguladoras internacionais que disciplinem o ambiente cibernético e que estejam dotadas de mecanismos eficazes de supervisão e correção, em particular contra a utilização desviante do ciberespaço e a corrupção da informação (Paiva & Gómez, 2021; Gill & Goolsby, 2022).

6.4. A singularidade dos subsídios da EUROPOL

> "Aproveitando a marca EUROPOL e tirando o máximo partido das suas bases de dados e produtos e serviços analíticos, os agentes de ligação da EUROPOL podem prestar um serviço muito atrativo para os respetivos serviços responsáveis pela aplicação da lei" (Reid, 2013, p. 150).

A EUROPOL tem encimado a modernização do policiamento pan-europeu, adaptando as respostas às necessidades, máxime através de métodos, técnicas e ciências aplicadas, materializadas em produtos analíticos e de inteligência policial credíveis, fundamentados e partilhados (EUROPOL, 2024b). No presente, como no passado, dependemos de informação verosímil para tomar decisões informadas quanto a temas importantes do quotidiano (Lin, 2019). Conseguintemente, precisamos de conhecer,

[104] Alinhada com o esforço geoestratégico de digitalização europeia, a 'Agenda Estratégica da União Europeia para 2019-2024' prioriza o combate à desinformação e às interferências externas através de plataformas digitais (Von der Leyen, 2019b). A ESCTF e a iniciativa *Verified* das NU convergem nesse propósito (Guterres, 2020; Valenza, 2021). Desde 1941, a agência Reuters perfilha os 'Princípios de confiança' que defendem a integridade, independência e isenção de preconceitos (Reuters, 1941). Muitos outros *integrity warriors* informacionais, como a *NewsGuard* ou o *First Draft*, juntaram-se à causa anti-infodémica. O Observador, o Público e o Polígrafo integram a rede mundial de *fact-checkers* independentes (Oliveira, 2020). O "*ContraFake*", resultante do consórcio da Agência Lusa, o Inesc-ID do Instituto Superior Técnico, o CNCS e a empresa tecnológica *in:know*, é um projeto de agregação de informação e desenvolvimento de recursos computacionais e ferramentas tecnológicas, baseadas em IA, para proteção e apoio aos profissionais de comunicação, cidadãos e instituições contra ações de desinformação divulgadas através das redes sociais e de outras fontes de informação digital (Agência Lusa, 2024c).

combinar e estruturar informações variadas, pensar criticamente sobre os seus benefícios e desvantagens na proteção dos próprios interesses. A informação contextualizada e confiável reveste uma importância decisiva para o pensamento crítico e a organização dos cidadãos, da sociedade, do Estado e da coletividade de Estados. As iniciativas europeias, unificadas em esforços colaborativos de sistemas de "sentinela" e mecanismos de deteção precoce, bem como na interoperabilidade de dados, capacidades analíticas e distribuição de informações congruentes sobre anomalias criminais ou geopolíticas, podem ser instrumentais na atenuação de ameaças potenciais e, concretamente, da infodemia (Fernandes, 2022a; Mecklin, 2023).

Satisfazendo a questão central da nossa investigação, o sistema SIENA, o repositório EIS e a plataforma EPE compõem as principais componentes tecnológicas, credíveis e seguras para as interações informacionais e investigatórias das polícias europeias e de países terceiros reunidas na EUROPOL. Alinhados com a '*EUROPOL Strategy – Delivering Security in Partnership*', os relatórios e produtos de análise – especificamente o SOCTA, IOCTA e o TE-SAT –, acrescentam dimensão, valor e vanguardismo à estratégia anti-infodémica europeia. A capacidade de análise e avaliação do ambiente de informação deve contar com pessoal bem formado, com os conhecimentos científicos adequados e apoiado pela tecnologia certa (Nogala, 2024). Para navegar neste plano extraordinariamente complexo será fulcral desenvolver estratégias de comunicação proativas e orientadas para objetivos, reagindo eficazmente ao volume crescente de ataques informáticos às instituições ocidentais (Gill & Goolsby, 2022). O diálogo e a proximidade, a permutação interagências e a negociação diplomática entre EM são fundamentais para preservar a segurança coletiva e mitigar as ameaças híbridas e não convencionais, cada vez mais complexas (*HDRO*, 2024). No arco da cooperação policial promovida pela EUROPOL, os OLMJ/OLMAI apresentam-se como os *custodes* da simetria entre a partilha de informações estratégicas, a promoção dos interesses (multi)nacionais e a proteção das liberdades pessoais.

> "O nível de cooperação alcançado e realizável não tem precedentes e é limitado apenas pelas disposições legislativas nacionais individuais em matéria de cooperação internacional no domínio da aplicação da lei e da informação criminal" (Reid, 2013, p. 137).

A prospeção estratégica sobre tecnologias disruptivas realizada pelo *Europol Innovation Lab* informa, como estratégias inovadoras de policiamento da UE, a necessidade de os quadros jurídico-penais dos EM reprimirem as ameaças da desinformação e da fenomenologia infodémica, incluindo tecnologia *deepfakes* e a IA, ante as múltiplas

dimensões de dano que contemplam para uma democracia pluralista, plena e informada (EUROPOL, 2022d). A debelação eficaz destes prodígios depende do aperfeiçoamento da regulamentação da UE e da sua positivação no ordenamento penal dos vários EM, introduzindo normas que criminalizem expressamente a desinformação, as *fake news* e a infodemia. Neste sentido, países como a França[105] e a Grécia[106] adotaram iniciativas legislativas pioneiras.

Outrossim, em sede da revisão do mandato da EUROPOL, é essencial introduzir competências expressas neste domínio concreto, mobilizando a enorme capacitação prospetiva, analítica e investigatória da Agência contra este constructo disruptivo que tanto impacta na UE e ameaça a democracia. No entanto, as medidas regulatórias e os instrumentos de criminalização ora aventados poderão gerar controvérsia na medida em que podem contender com direitos fundamentais, nomeadamente a liberdade de expressão e informação, de dignidade Constitucional, o que importa acautelar, a todo o tempo (Silveira, 2022).

6.5. Complexidades da criminalização da desinformação em Portugal

O quadro jurídico português vigente é omisso na previsão de uma norma que sancione especificamente o tipo de atuação que a desinformação pode suscitar, mormente quando esta não se enquadre nos tipos legais de crime tradicionais[107]. Logo, reputamos como

[105] Através da Lei n.º 2018-1202, de 22 de dezembro de 2010, a França criminalizou as *fake news*, definindo-as como "alegações ou imputações inexatas ou notícias que falsamente reportam factos com o intuído de mudar a veracidade de um escrutínio", excluindo opiniões e comentários satíricos ou humorísticos.

[106] A 11 de novembro de 2021, o Parlamento grego aprovou uma alteração legislativa que criminalizou a divulgação pública, ou através da *internet*, de *fake news* que possam causar preocupação ou medo ao público ou minar a confiança do público na economia nacional, na capacidade de defesa do país ou na saúde pública, sancionando-as com pena de multa e pena de prisão até 5 anos.

[107] "(…) [Q]uando a desinformação representar uma ameaça, difamação ou provocação de atos de violência contra pessoa ou grupos de pessoas em razão da sua raça, cor, origem étnica ou nacional, religião, sexo, orientação sexual ou identidade de género ou constituir uma instigação ou apologia pública de um crime, tal conduta está prevista e punida nos tipos legais correspondentes, apesar de haver sempre a hipótese de os elementos do tipo do crime não abrangerem necessariamente o que se considera como desinformação" (Silveira, 2022, pp. 42-43). Verifica-se que, apesar da falta de regulação específica, existem situações de desinformação suscetíveis de integrar tipos legais de crime já existentes. Contudo, a questão agrava-se quando o tipo ou conteúdo de desinformação não se enquadra na legislação vigente. Nesta última situação e no que tange à regulação e supervisão da atividade da comunicação social, Portugal conta com a sentinela da Entidade Reguladora para a Comunicação Social (ERC). Para além da ERC, o Artigo 6.º da Lei n.º 27/2021, de 17 de maio – Carta Portuguesa de Direitos Humanos na Era Digital –, introduziu o direito à proteção contra a desinformação e firmou o compromissos do Estado português a assegurar o cumprimento do 'Plano Europeu de Ação contra a Desinformação' (*European Commission*, 2018a), nos termos da Resolução da Assembleia da República n.º 50/2019, por forma a proteger a sociedade contra pessoas singulares ou coletivas, *de jure ou de facto*, que produzam, reproduzam ou difundam narrativa considerada desinformação. O Artigo 2.º do Lei n.º 15/2022, de 11 de agosto, simplificou o regime de proteção contra a desinformação, revogando os números 2 a 6 do Artigo 6.º da Lei n.º 27/2021, de 17 de maio. O Centro Internet Segura (CIS) promove a utilização segura, saudável e consciente da *internet*, contribuindo para o desenvolvimento de competências que potenciem uma cidadania digital informada e inclusiva. O projeto resulta de um consórcio do CNCS com a Direção-Geral da Educação, Instituto Português do Desporto e Juventude, Fundação para a Ciência e a Tecnologia, Associação Portuguesa de Apoio à Vítima, a Fundação *Altice* e a *Microsoft* Portugal (CIS|CNCS, s.d.).

fundamental fixar: a) um consenso internacional em torno do conceito e definição da desinformação, de modo a não cair no perigo da censura à liberdade de expressão e imprensa; b) um catálogo específico dos tipos de condutas e comportamentos que possam integrar o respetivo tipo legal de crime, tarefa esta dificultada pela complexidade inerente a este fenómeno transfronteiriço[108]; c) a diversificação de *alavancas de ação* (*e.g.*, literacia mediática, autorregulação (realizada por agentes privados) e corregulação (efetuada por privados e pelo Estado) das plataformas, mecanismos de *fact-checking*, etc.) para mitigar a desinformação disseminada com a finalidade de perturbar a ordem pública[109] ou constranger o regular funcionamento das instituições democráticas (Haciyakupoglu, Hui, Leong, & Rahman, 2018; *European Commission*, 2018b). O enfreamento da desinformação não poderá deixar de ser realizado, ainda que perpasse pela delineação criteriosa da liberdade de expressão – um direito constitucionalmente consagrado.

> "Se a liberdade de expressão é sagrada, ela não pode ser sinónimo de impunidade: certos discursos não podem ser proferidos e devem ser punidos, já estando estabelecidos limites à mesma, (…) através, por exemplo, dos crimes contra a honra e crimes de incitamento ao ódio e à violência" (Silveira, 2022, pp. 9-10).

Concludentemente, está em causa um equilíbrio muito fino. Os direitos fundamentais, quando exercidos corretamente, salvaguardam o bom funcionamento das sociedades. Porém, o seu exercício abusivo, a pretensamente coberto da liberdade de expressão, é merecedor da correspondente repreensão legal, já que não se sobrepõe aos demais direitos protegidos e de igual dignidade (*v.g.*, direito da imagem, bom nome, honra, etc.). A criminalização da desinformação – dolosa, manipulada[110] e lesiva[111] –, devidamente comprovada pelo processo judicial, pode conferir a proteção adequada aos excessos descritos. A delimitação da liberdade de expressão parece ser indispensável para depurar a superabundância da desinformação moderna. Por outro lado, o potencial de aproveitamento abusivo dos limites à liberdade de expressão para fins de censura arbitrária e repressão estatal

[108] A urgência do combate à desinformação influencia a premência de revisão das políticas criminais e, consequentemente, a necessidade de atualização dos Códigos Penais relativamente aos crimes virtuais e às práticas de engenharia social. Estas e outras preocupações têm sido objeto de várias reflexões científicas e estudos internacionais (Bayer, 2016; de Melo Nascimento, Santos, & Edler, 2022).
[109] Como aconteceu em agosto de 2024, em Southport, no Reino Unido, onde centenas de manifestantes de extrema-direita, instigados por desinformação *online* (de que o alegado homicida de três crianças era um imigrante e radical islâmico), entraram em confrontos violentos com a polícia (Alhinho & Reuters, 2024).
[110] Em agosto de 2024, a PSP denunciou publicamente uma publicação falsa, amplamente partilhada nas redes sociais, que ficcionava o testemunho de um pai que teria sido alvo de agressões ao impedir que a filha fosse sequestrada por três homens indostânicos, em Loures (Rodrigues Alves, 2024).
[111] A manipulação da informação não só provoca danos ao indivíduo, à sua integridade pessoal, reputação e segurança pessoal, como também à própria sociedade, lesando a liberdade do comércio, o processo democrático, a saúde, ordem, segurança e tranquilidade públicas (Chesney & Citron, 2019).

constitui uma preocupação latente, sobretudo quando relacionada com a natureza estrutural dos Estados, *i.e.*, democracias[112] ou autocracias[113] (Matsuoka, 2021; Silveira, 2022; Yuzefovich, 2024).

6.6. Prospetivas de ação para a PSP

Aqui chegados, todos os envolvidos, especialmente as forças de segurança e a *longa manus* exercida pelos oficiais de ligação policial na EUROPOL, devem desenvolver estratégias para precaver eventuais contingências futuras com uma razoabilidade temporal (INTERPOL, 2020 e 2022b). A proatividade deve substituir a tradicional reatividade na resposta aos problemas potencialmente impactantes na sociedade[114]. Enquanto atores essenciais do policiamento da era digital, os oficiais de ligação das polícias dos EM na EUROPOL "(…) formam uma teia azul em todo o mundo (…)" que compõe a linha da frente do combate às ameaças transnacionais emergentes, designadamente contra a infodemia e a desinformação (den Boer & Block, 2013, p. 189). É prioritário multiplicar o dinamismo e sofisticação desta rede de largo espectro com recursos humanos e tecnológicos, legal e tecnicamente habilitados e em número suficiente (Elias, 2023; Nogala, 2023 e 2024).

Mais do que isso, consideramos essencial partilhar tais predicados com as principais forças de segurança do *corpus* da Segurança Interna portuguesa – mormente a PSP, GNR e PJ – mobilizando-as na luta anti-infodémica da UE, mediante a indispensável atualização do arquétipo jurídico-penal nacional. À luz de um *insight* prospetivo, recomendamos o reforço

[112] Há registo de várias condenações judiciais por crimes de desinformação e *fake news* em países democráticos que criminalizaram essas condutas. Exemplificativamente, notamos uma decisão judicial, em 2022, que condenou um homem espanhol a 15 meses de prisão por divulgar um vídeo na *internet* que sugeria que um imigrante menor de idade seria o autor de uma agressão, a qual, na verdade, tinha ocorrido na China (Diário de Notícias/Agência Lusa, 2022). Em 2023, Rudolph Giuliani foi condenado pelos crimes de difamação, conspiração e imposição de sofrimento emocional a duas mulheres, acusadas pelo advogado de Trump de terem interferido nas eleições presidenciais de 2020 (Redação O Antagonista, 2023).

[113] Também o regime de Putin tem usado o sistema judicial para reprimir a desinformação, de acordo com a sua narrativa política. Em 2022, a justiça russa condenou, pela primeira vez, um cidadão por "falsificar" documentos do Ministério de Defesa e publicar vídeos numa rede social (Soares, 2022). Já em agosto de 2024, o administrador do *Moscow Calling* da *Telegram*, Andrei Kurshin, foi condenado a seis anos e meio de prisão por divulgar "notícias falsas" sobre o Exército russo na Ucrânia (Agência Lusa, 2024b). Não obstante, assiste-se a uma resistência cautelosa da comunidade literária russa – inclusive dos leitores – em relação à censura do Kremlin contra o "ativismo público", o que reforça a esperança no poder crítico da literacia mediática. Esta nova estratégia, a que James C. Scott chamou de "as armas dos fracos", traduz-se em práticas que evitam o confronto direto e frugal com o bloco opressor em favor de uma dissidência habilmente camuflada, embora deliberadamente percetível (Yuzefovich, 2024).

[114] Apesar do grande esforço desenvolvido pela UE para debelar as operações agressivas e de alto risco da Rússia, as estratégias *name and shame* revelam-se pouco impactantes. É urgente uma resposta coordenada entre os aliados ocidentais que aumente a eficácia das sanções e de outras opções políticas que insulem a Rússia e contenham a disrupção provocada pelo seu aparelho de inteligência. A purga alargada de diplomatas russos e dos seus agentes de inteligência, a par das parcerias do sector público com o privado, mormente no ambiente cibernético, renovam a esperança na luta contra as "operações ativas", nomeadamente as atividades de ciberespionagem, desinformação e propaganda russa (Bowen, 2020).

iminente da capacitação a PSP contra a desinformação, especialmente em tempos de crise[115]. A mudança de paradigma principiará ao nível da própria estrutura orgânica da PSP e da melhoria da flexibilização dos fluxos comunicacionais internos, de modo a maximizar a elaboração de réplicas integradas pelos Departamentos de Informações Policiais, Investigação Criminal, Sistemas de Informação e Comunicações, de Formação e pelo Gabinete de Imprensa e Relações Públicas. A capacitação anti-infodémica da PSP deve assentar em oito postulados estratégicos: a) revisão dos procedimentos internos e especialização[116]; b) formação contínua em literacia digital e ética[117]; c) atualização e integração tecnológica[118]; d) parcerias com instituições de *fact-checking*[119]; e) cooperação internacional[120]; f) apoio psicológico[121]; g) desenvolvimento competências comunicacionais[122]; e h) campanhas de sensibilização para o público interno e externo[123].

A escolha destas precedências estratégicas é inteiramente nossa. "(…) Ao olharmos para o futuro, asseguremo-nos de escolher sabiamente" (Guterres, 2020, p. 8).

Omnes omnibus

[115] Como manifestações violentas e alterações da ordem, desastres naturais, acidentes graves e pandemias.
[116] Esta visão de futuro passa por criar protocolos ou planos de ação específicos para lidar com a infodemia que incluam a monitorização de redes sociais e outras plataformas digitais. Para o efeito, sugere-se a criação de uma unidade multidisciplinar especializada na monitorização e combate à desinformação.
[117] Um combate anti-infodémico eficaz passa por oferecer formações regulares – cursos de literacia digital, ética e Direitos Humanos – sobre como identificar, verificar e combater desinformação *online*, incluindo o uso de ferramentas de *fact-checking*, com observância dos direitos, liberdades e garantias dos cidadãos. Esta componente deve ser reforçada com a implementação sistemática de simulações que reproduzam cenários críticos e em relação aos quais seja necessário identificar e neutralizar fontes de *fake news*.
[118] Impõe-se um investimento nas tecnologias emergentes e em ferramentas de IA que ajudem na identificação precoce de padrões de desinformação. A implementação de sistemas de alerta rápido sobre a propagação de boatos ou informações falsas permitirão uma resposta tempestiva, proficiente e coordenada.
[119] Afigura-se crucial o estabelecimento de parcerias e colaborações ativas com organizações especializadas em *fact-checking* e literacia mediática, como *The International Fact-Checking Network* (IFCN), associada ao *Poynter Institute*, a *European Fact-Checking Standards Network* (EFCSN) e outras entidades nacionais, como a ERC. O empenho dos *mass media* é crucial (*Meta*, 2024). É prioritário facilitar o acesso a ferramentas e bases de dados de verificação de informação.
[120] A participação em grupos de trabalho internacionais e a troca de experiências entre agências neste domínio são fundamentais. A CEPOL, EUROPOL, FRONTEX e INTERPOL destacam-se como principais ativos na promoção transversal de programas de formação específicos.
[121] Entrevemos como determinante providenciar apoio psicológico aos polícias que trabalham diretamente com a desinformação, uma vez que essa função pode revelar-se emocionalmente desgastante e stressante.
[122] A corrupção do ecossistema de informação exige o aprimoramento das competências comunicacionais. Para o efeito, é urgente formar os polícias em técnicas de comunicação e gestão de crises para lidar com o público e com os *media*, assegurando a transmissão tempestiva de informações corretas e confiáveis. É necessário explorar as várias plataformas eletrónicas e aumentar o patrulhamento digital.
[123] Partindo da capacitação interna, alicerçada literacia digital e conduta ética, importa intensificar e alargar a campanha educativa junto da comunidade, sensibilizando a população através de ações de policiamento de proximidade e de esclarecimentos públicos. Neste sentido e apenas no espaço de duas semanas, a PSP "desconstruiu" seis notícias falsas, confirmado que a infodemia tem aumentado, inclusive, em território nacional. Frequentemente, os agentes anónimos da desinformação reportam, através das redes sociais, "(…) factos que não ocorreram ou altera a versão original dos mesmos, tornando-os exacerbados, e potenciam o alarme social, gerando um sentimento de insegurança na população" (Firmino *apud* Henriques, 2024).

Referências

AFP. (8 de fevereiro de 2017). Estado Islâmico aposta em "ciber-marionetes" para se espalhar. *Exame*. Obtido em 10 de fevereiro de 2021, de https://exame.com/mundo/estado-islamico-aposta-em-ciber-marionetes/

Agência Lusa. (15 de março de 2019). Fake news. Sistema de alerta rápido sobre desinformação na UE lançado na 2.ª feira. *Observador*. Obtido em 24 de maio de 2024, de https://observador.pt/2019/03/15/fake-news-sistema-de-alerta-rapido-sobre-desinformacao-na-ue-lancado-na-2-a-feira/?cache_bust=1716536150161

Agência Lusa. (26 de abril de 2024a). Parlamento Europeu aprova resolução contra ingerência estrangeira e pede transparência nas contas. *Observador*. Obtido em 29 de maio de 2024, de https://observador.pt/2024/04/26/parlamento-europeu-aprova-resolucao-contra-ingerencia-estrangeira-e-pede-transparencia-nas-contas/

Agência Lusa. (7 de agosto de 2024b). 'Blogger' russo condenado a 6 anos por notícias falsas sobre guerra na Ucrânia. *Mundo ao Minuto*. Obtido em 8 de agosto de 2024, de https://www.noticiasaominuto.com/mundo/2611870/blogger-russo-condenado-a-6-anos-por-noticias-falsas-sobre-guerra-na-ucrania

Agência Lusa. (2024c). Verificadores em Portugal. *Combate às Fake News - Uma Questão Democrática*. Obtido em 22 de agosto de 2024, de https://combatefakenews.lusa.pt/verificadores-em-portugal/

Alam, F., Dalvi, F., Shaar, S., Durrani, N., Mubarak, H., Nikolov, A., . . . Nakov, P. (2020). Fighting the COVID-19 Infodemic in Social Media: A Holistic Perspective and a Call to Arms. Obtido em 2 de fevereiro de 2021, de https://arxiv.org/pdf/2007.07996.pdf

Alhinho, L., & Reuters. (31 de julho de 2024). Ataque em Southport: manifestantes envolvem-se em confrontos no centro de Londres. *Público*. Obtido em 6 de agosto de 2024, de https://www.publico.pt/2024/07/31/mundo/noticia/ataque-southport-manifestantes-envolvemse-confrontos-centro-londres-2099490

Almeida, E. C. (fev/mar de 2022). Os Grandes Irmãos: O uso de tecnologias de reconhecimento facial para persecução penal. *Revista Brasileira de Segurança Pública, 16*(2), pp. 264-283. Obtido em 7 de março de 2024, de https://revista.forumseguranca.org.br/index.php/rbsp/article/download/1377/548/6492

Almeida, S. J. (11 de março de 2021). Governo nomeia task force de cientistas comportamentais. *Público*. Obtido em 11 de março de 2021, de https://www.publico.pt/2021/03/11/politica/noticia/nomeada-taske-force-cientistas-comportamentais-1953872

Alves, A. (16 de janeiro de 2024). O que é a "Doença X" que pode ser 20 vezes mais mortal do que a Covid e será discutida em Davos? *Observador*. Obtido em 17 de janeiro de 2024, de https://observador.pt/2024/01/16/o-que-e-a-doenca-x-que-pode-ser-20-vezes-mais-mortal-do-que-a-covid-e-sera-discutida-em-davos/

Alvin, T. (1980). *The Third Wave (A Terceira Onda)* (4.ª ed.). (J. Tavora, Trad.) Rio de Janeiro: RJ, Record.

Amarasingam, A., & Argentino, M. A. (julho de 2020). The QAnon conspiracy theory: A security threat in the making. *CTC Sentinel, 7*(13), pp. 37-44. Obtido em 3 de maio de 2024, de https://ctc.westpoint.edu/wp-content/uploads/2020/07/CTC-SENTINEL-072020.pdf

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice* (2.ª ed.). Oxford: Syngress. Obtido em 3 de junho de 2024, de https://books.google.com.br/books?hl=pt-PT&lr=&id=9NI0AwAAQBAJ&oi=fnd&pg=PP1&dq=infosec&ots=Gs9kk_bs4w&sig=psJGQGHbyOjtNKjJO3IALwpmM4A

APCD. (2022). *Europa tem seis novos centros de combate à desinformação*. (Associação Portuguesa para o Desenvolvimento das Comunicações (APDC)) Obtido em 20 de maio de 2024, de www.apdc.pt: https://www.apdc.pt/noticias/atualidade-internacional/europa-tem-seis-novos-centros-de-combate-a-desinformacao

Arendt, H. (1963). *Eichmann em Jerusalém - Uma reportagem sobre a banalidade do mal.* (e. d. 2017, Ed., & A. C. Silva, Trad.) Lisboa: Ítaca.

Arendt, H. (1973). *As origens do totalitarismo, 8.ª edição, 2018.* (R. Raposo, Trad.) D. Quixote.

Aro, J. (2022). *Putin's Trolls: On the Frontlines of Russia's Information War Against the World.* New York: Ig Publishing.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), p. 28.

Arquilla, J., & Ronfeldt, D. (Edits.). (2001). *Networks and netwars: The future of terror, crime, and militancy.* Santa Monica: RAND. Obtido em 12 de abril de 2024, de https://www.rand.org/pubs/monograph_reports/MR1382.html

Asai, T. (2023). Pandemic and infodemic: the role of academic journals and preprints. *Journal of Anesthesia, 2*(37), pp. 173-176. Obtido em 7 de março de 2024, de https://doi.org/10.1007/s00540-022-03149-1

Avó, C. (15 de maio de 2024). Robert Fico, instigador e vítima da polarização política na Eslováquia. *Diário de Notícias*. Obtido em 15 de maio de 2024, de https://www.dn.pt/2862072215/robert-fico-instigador-e-vitima-da-polarizacao-politica-na-eslovaquia/

Baldwin, J. (14 de janeiro de 1962). As much truth as one can bear. *The New York Times*.

Balkin, J. M. (2012). *The First Amendment Is an Information Policy.* Obtido de https://scholarlycommons.law.hofstra.edu/hlr/vol41/iss1/2

Barreto, R. d. (22 de março de 2022). The other side of War: disinformation. *UNIO – EU Law Journal*. Obtido em 3 de agosto de 2024, de https://officialblogofunio.com/2022/03/22/the-other-side-of-war-disinformation/#more-5593

Barrinha, A. (9 de julho de 2020). Cibersegurança em Tempos de Pandemia. *Cibersegurança e Ciberdefesa em Tempos de Pandemia - IDN brief*(32). Obtido em 16 de fevereiro de 2021, de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20julho%202020%2

Bartles, C. K., & McDermott, R. N. (2014). Russia's Military Operation in Crimea: Road Testing Rapid Reaction Capabilities. *Problems of Post-Communism*, pp. 46-63.

Bastrup-Birk, J., Frinking, E., Arentze, L., Jong, E. d., & Bekkers, F. (2023). *Next Generation Organised Crime. Systemic change and the evolving character of modern transnational organised crime.* The Hague: The Hague Centre for Strategic Studies (HCSS). Obtido em 20 de maio de 2024, de https://hcss.nl/wp-content/uploads/2023/05/Next-Generation-Organised-Crime-HCSS-2023.pdf

Bayer, D. A. (2016). Meios de comunicação na era da desinformação, a reprodução do medo e sua influência na política criminal. *Ratio Juris, 11*(22), pp. 117-141.

Bayley, D. H. (2001). *Padrões de Policiamento: Uma Análise Internacional Comparativa* (Vol. 1). São Paulo: Edusp.

Bayley, D. H., & Shearing, C. D. (1996). The Future of Policing. *Law and Society Review, 3*(30), pp. 585-606.

BBW. (2018). *Face Off: the lawless growth of facial recognition in UK policing.* Londres: Big Brother Watch (BBW). Obtido em 8 de março de 2024, de https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

Beck, U. (1992). *Risk Society. Towards a New Society* (2nd ed.). (M. Ritter, Trad.) London: Sage Publications. Obtido em 8 de março de 2024, de http://www.riversimulator.org/Resources/Anthropology/RiskSociety/RiskSocietyTowardsAnewModernity1992Beck.pdf

Belton, C. (22 de fevereiro de 2024). A campanha de desinformação que o Kremlin montou contra Zelensky. *Público*. Obtido em 30 de maio de 2024, de https://www.publico.pt/2024/02/22/mundo/noticia/campanha-desinformacao-kremlin-montou-zelensky-2081148

Belton, C., & Menn, J. (9 de abril de 2024). Trolls russos tentam condicionar apoio norte-americano à Ucrânia, mostram documentos do Kremlin. *Público*. Obtido em 30 de maio de 2024, de https://www.publico.pt/2024/04/09/mundo/noticia/trolls-russos-tentam-condicionar-apoio-norteamericano-ucrania-mostram-documentos-kremlin-2086393

Bentzen, N. (2024). *Bússola de verificação de factos: como detetar a manipulação de informação.* Think Tank do Parlamento Europeu, EPRS | Serviço de Estudos de Apoio aos Deputados. União Europeia. Obtido em 1 de agosto de 2024, de https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/762355/EPRS_ATA(2024)762355_PT.pdf

Bentzen, N., & Russell, M. (2015). *Russia's disinformation on Ukraine and the EU's response.* European Parliament Think Tank, EPRS | European Parliamentary Research Service. European Union. Obtido em 1 de agosto de 2024, de https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571339/EPRS_BRI(2015)571339_EN.pdf

Bergien, R. (2017). »Big Data« als Vision. Em *Computereinführung und Organisationswandel in BKA und Staatssicherheit (1967–1989). Zeithistorische Forschungen/Studies in Contemporary History.* Obtido em 7 de março de 2024, de https://doi.org/10.14765/ZZF

Bertolin, G. (2015). Conceptualizing Russian Information Operations: Info-War and Infiltration in the Context of Hybrid Warfare. *IO Sphere*, p. 10.

Bigo, D. (2006). Security, Exception, Ban and Surveillance. Em L. D., *Theorizing Surveillance. The Panopticon and beyond. Reino Unido* (pp. 46-68). Reino Unido: Wilan.

Blenkinsop, P. (29 de maio de 2024). Belgium raids EU lawmaker aide's home, offices on Russia propaganda suspicions. *Reuters*. Obtido em 5 de junho de 2024, de https://www.reuters.com/world/europe/belgium-raids-eu-lawmaker-aides-home-offices-russia-propaganda-suspicions-2024-05-29/?utm_source=Pol%C3%ADgrafo+Europa&utm_campaign=cd871f1590-EMAIL_CAMPAIGN_2023_12_05_02_33_COPY_01&utm_medium=email&utm_term=0_-8c5b48

Block, L. (2013). EU Policy-making on Liaison Officers. Em M. den Boer, & L. Block (Edits.), *Liaison Officers: Essential Actors in Transnational Policing* (pp. 103-118). The Hague: Eleven International Publishing. Obtido em 29 de maio de 2024, de https://www.researchgate.net/profile/Ludo-Block/publication/327200714_Liaison_Officers_Essential_Actors_in_Transnational_Policing/links/5db7e024299bf1a47bfa36ef/Liaison-Officers-Essential-Actors-in-Transnational-Policing.pdf

Bodenhausen, G. V., Sheppard, L. A., & Kramer, P. G. (1994). Negative Affect and Social Judgment: The Differential Impact of Anger and Sadness. *European Journal of Social Psychology 24 (1)*, pp. 45–62. doi:10.1002/ejsp.2420240104.

Bolle, C. d. (2020). The Role of Europol in International Interdisciplinary European Cooperation. *European Law Enforcement Research Bulletin*(19), pp. 17-24.

Borrell, J. (2020). Embracing Europe's Power. *Project Syndicate*. Obtido em 16 de fevereiro de 2021, de https://www.project-syndicate.org/commentary/embracing-europe-s-power-by-josep-borrell-2020-02

Bowen, A. S. (2020). *Russian Military Intelligence: Background and Issues for Congress.* Washington D. C.: Congressional Research Service (CRS). Obtido em 1 de agosto de 2024, de https://crsreports.congress.gov

Boyle, M. J. (2016). The Coming Illiberal Order. *Survival, 58*(2), pp. 35–66. Obtido em 6 de junho de 2024, de https://www.gmfus.org/sites/default/files/Coalition%2520Building%2520in%2520a%2520Post-Western%2520World%2520edited.pdf

Bradbury, R. (2020 [1953]). *Fahrenheit 451.* (C. d. Piedade, Trad.) Porto Salvo: Edições Saída de Emergência.

Brennen, J., & Kreiss, D. (2016). Digitalization. Em K. J. al. (Ed.), *The International Encyclopedia of Communication Theory and Philosophy.* New York: John Wiley & Sons. Obtido em 7 de março de 2024, de https://doi.org/10.1002/9781118766804.wbiect111

Bunde, T., Eisentraut, S., & Schütte, L. (2024). Munich Security Report 2024: Lose-Lose? Em T. Bunde, S. Eisentraut, & L. Schütte (Ed.), *Munich Security Conference, February 2024* (p. 9). Munich: MSC Publications. doi:10.47342/BMQK9457

Cadwalladr, C. (abril de 2019). *O papel do Facebook no Brexit e a ameaça à democracia.* Obtido em 24 de março de 2021, de TED talk: https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=pt

Camus, A. (2011 [1947]). *La Peste.* Ebooks libres et gratuits.

Cardoso, J., Paola, E., & Moreira, M. (23 de julho de 2023). Direita pode reforçar hegemonia na Europa com eleições na Espanha. *Poder360*. Obtido em 25 de janeiro de 2024, de https://www.poder360.com.br/internacional/direita-pode-reforcar-hegemonia-na-europa-com-eleicoes-na-espanha/

Carvalho, C. (29 de maio de 2024). Parlamento Europeu alvo de buscas por suspeita de ingerência russa. *Observador*. Obtido em 29 de maio de 2024, de https://observador.pt/2024/05/29/parlamento-europeu-alvo-de-buscas-por-suspeita-de-ingerencia-russa/

Cassese, A. (2012). Gathering Up the Main Thread. Em A. Cassese, *Realizing Utopia: The Future of International Law* (pp. 645, 672). Oxford: Oxford University Press.

Castells, M. (1999 [1942]). *A Sociedade em Rede* (6.ª ed.). (R. V. Majer, & K. B. Gerhardt, Trads.) São Paulo: Paz e Terra.

Castells, M. (2003). *A Galáxia da Internet: reflexões sobre a internet, a sociedade e os negócios.* Rio de Janeiro: Zahar.

Cerulus, L. (15 de janeiro de 2021). Hackers behind EU medicines agency attack sought to sow distrust in vaccines. *Politico*. Obtido em 10 de fevereiro de 2021, de https://www.politico.eu/article/hackers-of-eu-medicines-agency-sought-to-sow-distrust-in-vaccines/

Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review,, 107*.

CIS|CNCS. (s.d.). *www.internetsegura.pt*. (Centro Nacional de Cibersegurança) Obtido em 28 de agosto de 2024, de Centro Internet Segura (CIS) | Centro Nacional de Cibersegurança (CNCS): https://www.internetsegura.pt/cis/missao-e-objetivos

Clark, M. (2020). *Russian Hybrid Warfare.* Washington D. C.: Institute for the Study of War (ISW). Obtido em 31 de julho de 2024, de https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

CNCS. (26 de setembro de 2022). *Glossário*. Obtido em 1 de junho de 2024, de CNCS - Centro Nacional de Cibersegurança: https://www.cncs.gov.pt/pt/glossario/

CNCS. (2023). *Relatório Tecnologias Emergentes.* Centro Nacional de Cibersegurança (CNCS). Obtido em 16 de maio de 2024, de https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cncs.pdf

CNCS. (s.d.). *www.cncs.gov.pt*. Obtido em 08 de fevereiro de 2021, de Centro Nacional de Cibersegurança (CNCS): https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/

Coldren, J. R., Huntoon, A., & Medaris, M. (2013). Introducing Smart Policing: Foundations, Principles, and Practice. *Police Quarterly, 3*(16), pp. 275-286. Obtido de https://doi.org/10.1177/1098611113497042

Collier, D. (2003). The rise of netpolitik: how the internet is changing international politics and diplomacy. *A report of the Eleventh Annual Aspen Institute Roundtable on Information Technology.* Washington D. C.: Aspen Institute - Communications and Society Program.

Comissão Europeia. (2015). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia para o Mercado Único Digital na Europa.* Bruxelas: Comissão Europeia. Obtido em 31 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&fro

Comissão Europeia. (2016a). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho – Quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia.* Bruxelas: Comissão Europeia. Obtido em 3 de junho de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Comissão Europeia. (2016b). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: As plataformas em linha e o mercado único digital: Oportunidades e desafios para a Europa.* Bruxelas: Comissão Europeia. Obtido em 31 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016DC0288&fr

Comissão Europeia. (2018). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Combater a desinformação em linha: uma estratégia europeia.* Bruxelas: Comissão Europeia. Obtido em 30 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0236&fro

Comissão Europeia. (2020a). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre o plano de ação para a democracia europeia.* Bruxelas. Obtido em 6 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0790

Comissão Europeia. (2020b). *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança.* Bruxelas: Comissão Europeia. Obtido em 21 de março de 2024, de https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_pt.pdf

Comissão Europeia. (2021). *Orientações da Comissão Europeia relativas ao reforço do Código de Conduta sobre Desinformação.* Bruxelas: Comissão Europeia. Obtido em 21 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52021DC0262

Comissão Europeia. (2024). *Uma Europa preparada para a era digital.* Obtido em 16 de maio de 2024, de https://commission.europa.eu/: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_pt

Conselho Europeu. (2015). *Reunião do Conselho Europeu (19 e 20 de março de 2015) - Conclusões.* Bruxelas: Conselho Europeu. Obtido em 30 de maio de 2024, de https://www.consilium.europa.eu/media/21889/st00011pt15.pdf

Conselho Europeu. (2019). *Agenda Estratégica da União Europeia para 2019-2024.* Bruxelas: Conselho Europeu. Obtido em 6 de maio de 2024, de https://www.consilium.europa.eu/media/39965/a-new-strategic-agenda-2019-2024-pt.pdf

Correia, P. d. (2012). Geopolítica e Geoestratégia. *Revista Nação e Defesa*(131 - 5.ª série), pp. 229-246. Obtido em 23 de janeiro de 2024, de https://comum.rcaap.pt/bitstream/10400.26/7670/1/NeD131_PedroPezaratCorreia.pdf

Costa, C. (14 de julho de 2020). *Uma nova guerra mundial por causa da tecnologia*. Obtido em 7 de abril de 2021, de www.maistecnologia.com: https://www.maistecnologia.com/uma-nova-guerra-mundial-por-causa-da-tecnologia/?amp

Covas, A. (20 de dezembro de 2020). Transição digital e inteligência coletiva territorial. *Observador*. Obtido em 18 de fevereiro de 2021, de https://observador.pt/opiniao/transicao-digital-e-inteligencia-coletiva-territorial/

Crutzen, P., & Stoermer, E. (2000). The Anthropocene. *Global Change Newsletter*(41), pp. 17- 18.

CSCE. (2017). *The scourge of Russian disinformation.* Commission on Security and Cooperation in Europe (CSCE). Washington D. C.: U. S. Government Publishing Office. Obtido em 22 de maio de 2024, de https://www.csce.gov/wp-content/uploads/2018/01/RussianDisinformation.pdf

de Melo Nascimento, G. A., Santos, J. N., & Edler, G. O. (novembro de 2022). A Importância do Combate à Desinformação e a atualização do Código Penal para Crimes Virtuais de Engenharia Social/Phishing. *Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE), 8*(11), pp. 2225-2233. doi:doi.org/10.51891/rease.v8i11.7809

De Sousa, L., Hindess, B., & Larmour, P. (2009). *Governments, NGOs and Anti-Corruption: The New Integrity Warriors.* Londres/Nova Iorque: Routledge.

Deloitte. (2019). Smart Policing: Top Five Policing Innovations Shaping the Future. *Deloitte US*. Obtido em 17 de janeiro de 2024, de https://www2.deloitte.com/us/en/pages/public-sector/articles/future-of-policing-and-law-enforcement-technology-innovations.html?id=us:2em:3cc:4dcom_share:5awa:6dcom:public_sector

den Boer, M., & Block, L. (Edits.). (2013). *Liaison Officers: Essential Actors in Transnational Policing.* The Hague: Eleven International Publishing.

Diário de Notícias/AFP. (27 de setembro de 2022). Rússia reitera ameaça nuclear no último dia de referendos nos territórios que quer anexar. *Diário de Notícias*. Obtido em 6 de fevereiro de 2023, de https://www.dn.pt/internacional/russia-reitera-ameaca-nuclear-no-ultimo-dia-de-referendos-nos-territorios-que-quer-anexar-15203381.html

Diário de Notícias/Agência Lusa. (8 de novembro de 2022). Homem condenado a 15 meses de prisão em Espanha por divulgação de fake news na internet. *Diário de Notícias*. Obtido em 8 de agosto de 2024, de https://www.dn.pt/internacional/homem-condenado-a-15-meses-de-prisao-em-espanha-por-divulgacao-de-fake-news-na-internet-15330116.html/

Diário de Notícias/Agência Lusa. (18 de julho de 2024). Macron anuncia rede europeia de peritos para combate à desinformação. *Diário de Notícias*. Obtido em 3 de agosto de 2024, de https://www-dn-pt.cdn.ampproject.org/v/s/www.dn.pt/4857385918/macron-anuncia-rede-europeia-de-peritos-para-combate-a-desinformacao/amp/?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=De%20%251%24s&aoh=17226839121723&referrer=https%3A%2F%2Fwww.go

Dias, S. S. (26 de janeiro de 2023). Arlindo Oliveira: "Quem dominar a inteligência artificial vai dominar a economia do planeta". *Jornal de Negócios*. Obtido em 20 de março de 2044, de https://www.jornaldenegocios.pt/sustentabilidade/governacao/detalhe/arlindo-oliveira-quem-dominar-a-inteligencia-artificial-vai-dominar-a-economia-do-planeta

Dodds, K. (2007). *Geopolitics : a very short introduction.* Oxford: Oxford University Press.

Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019). *Understanding Conspiracy Theories.* North Carolina, USA: International Society of Political Psychology.

Doyle, A. C. (1887). The Lauriston Garden Mystery. Em A. C. Doyle, & O. D. Edwards, *Sherlock Holmes - A Study In Scarlet.* Oxford University Press.

Duarte, F. P. (2020). Non-kinetic hybrid threats in Europe – The Portuguese case study (2017-18). *Emerald Publishing; Transforming Government: People, Process and Policy*. doi:10.1108/TG-01-2020-001

Dyvik, E. H. (8 de fevereiro de 2024). Biggest perceived threats to global society 2024, by event. *Statista*. Obtido em 26 de fevereiro de 2024, de https://www.statista.com/statistics/1207693/biggest-perceived-threats-to-global-society-by-event/

Eaves, E. (8 de fevereiro de 2021). Why is America getting a new $100 billion nuclear weapon? *Bulletin of the Atomic Scientists*. Obtido em 11 de fevereiro de 2021, de https://thebulletin.org/2021/02/why-is-america-getting-a-new-100-billion-nuclear-weapon/?utm_source=Newsletter&utm_medium=Emai

Elias, L. (2013). A Externalização da Segurança Interna: as dimensões global, europeia e lusófona. *Relações Internacionais*(40), pp. 009-029. Obtido em 12 de agosto de 2021, de http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri40/n40a02.pdf

Elias, L. (2022). *Ciências Policiais e Segurança Interna: Desafios e Prospetiva* (revista e atualizada, 2.ª ed.). Lisboa: Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

Elias, L. (2023). Policing in a Digital Age. *European Law Enforcement Research Bulletin, 6*, pp. 27-36. Obtido em 17 de janeiro de 2024, de https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/534

Elias, L. (2024). A Emergência e a Afirmação das Ciências Policiais. Em R. N. Fernandes, & P. Machado (Edits.), *40 anos das Ciências Policiais em Portugal* (1.ª ed., p. 609). Lisboa, Portugal: Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI). Obtido em 25 de julho de 2024, de http://hdl.handle.net/10400.26/51336

Elias, N. (1939). *O Processo Civilizacional* (abril de 2006, 2.ª ed.). (L. C. Rodrigues, Trad.) Lisboa: D. Quixote.

Elsasser, S. W., & Dunlap, R. E. (2013). Leading Voices in the Denier Choir: Conservative Columnists' Dismissal of Global Warming and Denigration of Climate Science. *American Behavioral Scientist, 6*(57), pp. 754–776.

ENISA. (2018). *ENISA Threat Landscape Report.* European Union Agency For Network and Information Security (ENISA). Heraklion: European Union. Obtido em 3 de junho de 2024, de https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/@@download/fullReport

ERC. (2019). *A Desinformação: Contexto nacional e europeu.* Lisboa: ERC - Entidade Reguladora para a Comunicação Social.

European Commission. (2018a). *Action Plan against Disinformation.* European Commission and the High Representative. Brussels: European Commission. Obtido em 6 de maio de 2024, de https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

European Commission. (2018b). *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation.* Directorate-General for Communications Networks, Content and Technology. Publications Office. Obtido em 5 de agosto de 2024, de https://data.europa.eu/doi/10.2759/739290

European Commission. (2018c). *EU Code of Practice on Disinformation.* Brussels: European Commission. Obtido em 30 de maio de 2024, de https://ec.europa.eu/newsroom/dae/redirection/document/87534

European Commission. (2020). *Roadmap - EU Action Plan on Human Rights and Democracy 2020-2024.* European External Action Service, Human Rights Division. European Commission. Obtido em 31 de maio de 2024, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0790

European Commission. (2022). *The Strengthened Code of Practice on Disinformation.* European Commission. Obtido em 21 de maio de 2024, de https://ec.europa.eu/newsroom/dae/redirection/document/87585

European Council. (2015). *European Council meeting (19 and 20 March 2015).* Brussels: European Council. Obtido em 6 de maio de 2024, de https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Union. (2023). *Flash Eurobarometer 522 Democracy – March 2023.* Ipsos European Public Affairs, European Commission, Secretariat-General; Directorate-General for Communication. European Commission. Obtido em 1 de agosto de 2024, de https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=90042

EUROPOL. (2020). *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic.* European Union Agency for Law Enforcement Cooperation (EUROPOL). Luxembourg: Publications Office of the European Union. Obtido em 20 de maio de 2024, de https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf

EUROPOL. (2021). *Internet Organised Crime Threat Assessment (IOCTA).* European Union Agency for Law Enforcement Cooperation (Europol). Luxembourg: Publications Office of the European Union. Obtido em 8 de março de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

EUROPOL. (2022a). Europol Information System (EIS). *European Union Agency for Law Enforcement Cooperation*. Obtido em 5 de fevereiro de 2024, de https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system

EUROPOL. (2022b). *Policing in the Metaverse - What Law Enforcement Needs to Know.* EUROPOL, EUROPOL Innovation Lab. Luxembourg: Publications Office of the European Union. Obtido em 18 de março de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf

EUROPOL. (2022c). *Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain AP4AI.* Luxembourg: Europol Innovation Lab & CENTRIC (Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research). Obtido em 8 de março de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf

EUROPOL. (2022d). *Facing reality? Law enforcement and the challenge of deepfakes.* European Union Agency for Law Enforcement Cooperation (EUROPOL), Observatory Report from the Europol Innovation Lab. Luxembourg: Publications Office of the European Union. Obtido em 20 de maio de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

EUROPOL. (2023). *Europol Strategy - 'Delivering Security in Partnership'.* The Hague: Europol Public Information. Obtido em 1 de março de 2024, de

https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Strategy%20-%20Delivering%20Security%20in%20Partnership%20%28EN%29.pdf

EUROPOL. (2024a). *Decoding the EU's most threatening criminal networks.* European Union Agency for Law Enforcement Cooperation (EUROPOL). Luxembourg: Publications Office of the European Union. Obtido em 20 de maio de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf

EUROPOL. (2024b). *The European Union Agency for Law Enforcement Cooperation: In Brief.* European Union Agency for Law Enforcement Cooperation (EUROPOL). Luxembourg: Publications Office of the European Union. doi:10.2813/5905

EUROPOL. (2024c). *Internet Organised Crime Threat Assessment (IOCTA).* European Union Agency for Law Enforcement Cooperation (EUROPOL). Luxembourg: Publications Office of the European Union. Obtido em 30 de julho de 2024, de https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

EUvsDisinfo. (2019). *Rapid Alert System.* European External Action Service (EEAS). The Strategic Communications division (StratCom). Obtido em 31 de maio de 2024, de https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf

EUvsDisinfo. (2020). *COVID-19 DISINFORMATION.* East Stratcom Task Force. EEAS Strategic Communications and Information Analysis Division. Obtido em 9 de maio de 2024, de https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/

EUvsDisinfo. (31 de maio de 2024). Elections are battlefields for the Kremlin: Flooding the information space. *EUvsDisinfo*. Obtido em 3 de junho de 2024, de https://euvsdisinfo.eu/elections-are-battlefields-for-the-kremlin-flooding-the-information-space/

Evanega, S., Lynas, M., Adams, J., & Smolenyak, K. (2020a). *Corona virus misinformation: quantifying sources and themes in the COVID-19 infodemic.* Ithaca: The Cornell Alliance for Science, Department of Global Development, Cornell University.

Evanega, S., Lynas, M., Adams, J., & Smolenyak, K. (2020b). *CORONAVIRUS MISINFORMATION: Quantifying sources and themes in the COVID-19 'infodemic'.* Cornell University, Department of Global Development. New York: The Cornell Alliance for Science. Obtido em 23 de fevereiro de 2024, de https://allianceforscience.org/wp-content/uploads/2020/09/Evanega-et-al-Coronavirus-misinformationFINAL.pdf

Eysenbach, G. (2020). How to fight an infodemic: the four pillars of infodemic management. *Journal of medical Internet research, 22*(6). doi:10.2196/21820

Fernandes, E., & Júnior, J. S. (1896). *História da Criminologia Contemporanea: sob o ponto de vista descriptivo e scientifico* (Vol. I). (A. Palhares, Ed.) Lisboa: Typographia da Papelaria Palhares.

Fernandes, J. P. (março de 2012). A ciberguerra como nova dimensão dos conflitos do século XXI. *Revista Relações Internacionais*. Obtido em 30 de março de 2021, de http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri33/n33a05.pdf

Fernandes, R. N. (2022a). O mavorcismo infodémico anti-imigração nos Estados Unidos da América. (R. N. Fernandes, & P. Machado, Edits.) *Politeia - Revista Portuguesa de Ciências Policiais*(XIX). Obtido em 29 de janeiro de 2024, de https://politeia-online.pt/wp-content/uploads/2022/07/Revista-POLITEIA-XIX-2022_O-mavorcismo-infodemico.pdf

Fernandes, R. N. (2022b). Le Réseau D'officiers De Liaison Du Portugal : La Mondialisation De La Diplomatie Policière. *Lettre d'information sur les Risques et les Crises (LIREC)*(67), pp. 26-30. Obtido de https://comum.rcaap.pt/handle/10400.26/42705

Fernandes, R. N. (2024a). A Mundialização da Diplomacia Policial Portuguesa. *Janus 2023*. Obtido de https://lnkd.in/dPSB_sqT

Fernandes, R. N. (2024b). The Police Diplomat Network as a response to Modern Challenges: A Portuguese Perspective. *Security Spectrum: Journal of Advanced Security Research*(23), pp. 48-74.

Fernandes, R. N. (no prelo). A diplomacia policial na produção de inteligência. Em H. H. Hamada, & R. P. Moreira (Edits.), *Teoria e Práticas de Inteligência de Segurança Pública.* Brasil: Instituto Brasileiro de Segurança Pública (IBSP) & Editora Parabellum.

Fernandes, R. N., & Machado, P. (2021). *Relatório de Atividades do ICPOL - Centro de Investigação do ISCPSI | 2021.* Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Obtido em 8 de março de 2024, de https://comum.rcaap.pt/bitstream/10400.26/44847/1/RA%20ICPOL%202021.pdf

Ferreira, A. M. (2013). *O essencial sobre Albert Camus.* Lisboa: Imprensa Nacional - casa da Moeda.

Finnin, R., & Roozenbeek, J. (22 de março de 2022). The Real Goal of Kremlin Disinformation Isn't What You Think. Disinformation is designed to sow apathy as well as confusion. Here's how that works. *Politico*. Obtido em 15 de maio de 2024, de https://www.politico.com/news/magazine/2022/03/22/putin-disinformation-apathy-00018974

Fitz-Gerald, A. M., & Padalko, H. (25 de julho de 2024). The Need for a Strategic Approach to Disinformation and AI-Driven Threats. *Commentary*. Obtido em 30 de julho de 2024, de https://www.rusi.org/explore-our-research/publications/commentary/need-strategic-approach-disinformation-and-ai-driven-threats

Fleck, A. (23 de fevereiro de 2024). Who's behind cyber attacks? *Statista*. Obtido em 1 de abril de 2024, de https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

Fortin, M. F. (2009). *Fundamentos e etapas do processo de investigação.* Loures: Lusociência.

Freire, S. P. (2023). *Revisão sistemática sobre cooperação policial internacional como dimensão a explorar na pesquisa de informações.* Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

Friedman, G. (2016). *Os Próximos 100 Anos.* Alfragide: D. Quixote.

Galante, L. (abril de 2017). *Como e porquê a Rússia interveio nas eleições dos EUA.* Obtido em 24 de março de 2021, de TED talk: https://www.ted.com/talks/laura_galante_how_and_why_russia_hacked_the_us_election

Galeotti, M. (2014). Putin's Secret Weapon. Em M. Kofman, & e. al., *Lessons From Russia's Operations in Crimea and Eastern Ukraine.* RAND.

Garthoff, R. L. (2015). *Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War.* Washington D. C.: Georgetown University Press.

GEC. (2020). *Pilares do Ecossistema de Desinformação e Propaganda da Rússia.* Departamento de Estado dos EUA. Estados Unidos: Global Engagement Center (GEC). Obtido em 8 de maio de 2024, de https://www.state.gov/wp-content/uploads/2020/10/Pillars-of-Russias-Disinformation-and-Propaganda-Ecosystem_Port_High.pdf

GEC. (2021). *The Goals and Main Tactics of Russia's Disinformation.* U. S. Department of State. Washington D. C.: Global Engagement Center (GEC). Obtido em 18 de maio de 2024, de https://e.america.gov/t/ViewEmail/i/CD46E76EEAD07F9E2540EF23F30FEDED

GEC. (22 de fevereiro de 2023). *Roleta da desinformação: o ano das mentiras do Kremlin para justificar uma guerra injustificável.* U. S. Department of State. Estados Unidos: Global Engagement Center (GEC). Obtido em 12 de maio de 2024

Gelfert, A. (15 de março de 2018). Fake News: A Definition. *Informal Logic, 38 (1), 84–117, Department of Philosophy, Literature, History of Science and Technology Technical University of Berlin*. Berlin, Alemanha. doi:10.22329/il.v38i1.5068

Gibbons, S. (23 de agosto de 2024). Humberside AI project supporting call handlers in DA cases could be rolled out nationally across more crime types. *Policing Insight*. Obtido em 28 de agosto de 2024, de https://policinginsight.com/feature/innovation/humberside-ai-project-supporting-call-handlers-in-da-cases-could-be-rolled-out-nationally-across-more-crime-types/

Gill, R., & Goolsby, R. (Edits.). (2022). *COVID-19 Disinformation: A Multi-National, Whole of Society Perspective.* Switzerland: Springer. doi:https://doi.org/10.1007/978-3-030-94825-2

Gödel, K. (1990). *Collected Works - Publications 1938-1974* (Vol. II). (S. Feferman, Ed.) New York: Oxford University Press. Obtido em 7 de março de 2024, de https://monoskop.org/images/b/b7/Kurt_Godel_Collected_Works_Volume_II_1989.pdf

Goel, V., & Vartanian, O. (2011). Negative Emotions Can Attenuate the Influence of Beliefs on Logical Reasoning. *Cognition and Emotion 25 (1)*, pp. 121–131. doi:10.1080/02699931003593942

Goldenberg, S. (2013). Secret Funding Helped Build Vast Network of Climate Denial Thinktanks. *The Guardian*.

Gonçalves, P. Z. (3 de junho de 2024). Fundação russa ligada ao Kremlin é 'fachada' para operações em 48 países na Europa, revela investigação. *Executive Digest*. Obtido em 3 de

junho de 2024, de https://executivedigest.sapo.pt/noticias/fundacao-russa-ligada-ao-kremlin-e-fachada-para-operacoes-em-48-paises-na-europa-revela-investigacao/

Greene, J. R. (2007). *The Encyclopedia of Police Science* (3.ª ed.). (J. R. Greene, Ed.) New York: Routledge. Obtido em 9 de junho de 2024, de https://doi.org/10.4324/9780203943175

Greenhill, K. M. (22 de fevereiro de 2022). When migrants become weapons. *Foreign Affairs*. Obtido em 30 de maio de 2024, de https://www.foreignaffairs.com/articles/europe/2022-02-22/when-migrants-become-weapons

Guterres, A. (22 de setembro de 2020). COVID-19 Dress Rehearsal for World of Challenges to Come. *United Nations Secretary-General, António Guterres, address to the General Assembly*. New York, United States of América. Obtido em 15 de maio de 2024, de https://www.un.org/sg/en/content/sg/statement/2020-09-22/secretary-generals-address-the-opening-of-the-general-debate-of-the-75th-session-of-the-general-assembly

Guterres, A. (28 de dezembro de 2023). Secretary-General's video message for New Year 2024. Obtido em 22 de janeiro de 2024, de https://www.un.org/sg/en/content/sg/statement/2023-12-28/secretary-generals-video-message-for-new-year-2024-scroll-down-for-french-version?_gl=1*1x1d9dj*_ga*MTA4NTE4MDQwNi4xNzA1ODQ5NjIw*_ga_TK9BQL5X7Z*MTcwNTg0OTYxOS4xLjAuMTcwNTg0OTYxOS4wLjAuMA..*_ga_S5EKZ

Guterres, A. (25 de janeiro de 2024). Davos 2024: Here's the impact on-ground across AI, climate, growth and global security. *World Economic Forum*. Obtido em 4 de março de 2024, de https://www.weforum.org/agenda/2024/01/davos-2024-insights-ai-climate-growth-and-global-security/

Haciyakupoglu, G., Hui, J. Y., Leong, D., & Rahman, M. F. (7 de março de 2018). *Countering Fake News: A Survey of Recent Global Initiatives.* Nanyang Technological University. Singapore: The S. Rajaratnam School of International Studies (RSIS). Obtido em 5 de agosto de 2024, de https://www.rsis.edu.sg/wp-content/uploads/2018/03/PR180416_Countering-Fake-News.pdf

Harari, Y. N. (abril de 2018a). *Porque é que o fascismo é tão sedutor e como as nossas informações o podem alimentar.* Obtido em 24 de março de 2021, de TED talk: https://www.ted.com/talks/yuval_noah_harari_why_fascism_is_so_tempting_and_how_your_data_could_power_it?language=pt

Harari, Y. N. (2018b). *21 lições para o século 21.* (P. Geiger, Trad.) Companhia das Letras. Obtido em 13 de maio de 2024, de https://edisciplinas.usp.br/pluginfile.php/8074338/mod_resource/content/3/21-Li%C3%A7%C3%B5es-Para-o-S%C3%A9culo-21-by-Yuval-Noah-Harari.pdf

Harlow, B. (2024). Book Review: In Their Own Words: How Russian Propagandists Reveal Putin's Intentions. Em J. Davis, *In Their Own Words: How Russian Propagandists Reveal Putin's Intentions* (Ukrainian Voices ed., p. 460). ibidem Press. Obtido em 8 de agosto de 2024, de https://www.thecipherbrief.com/book-review/making-sense-out-of-russias-propagandists

Hart, W., Albarracín, D., Eagly, I. B., Lindberg, M. J., & Merrill, L. (2009). Feeling Validated versus Being Correct: A Meta-Analysis of Selective Exposure to Information. *Psychological Bulletin 135 (4)*, pp. 555–588. doi:10.1037/a0015701

HDRO. (2024). *Breaking the gridlock. Reimagining cooperation in a polarized world.* New York: Human Development Report Office (HDRO) of the United Nations Development Programme (UNDP). Obtido em 15 de maio de 2024, de https://hdr.undp.org/system/files/documents

Heath, B. (15 de fevereiro de 2021). SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. (H. Timmons, & P. Cooney, Edits.) *Reuters*. Obtido em 8 de março de 2021, de https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2

Henriques, J. G. (28 de agosto de 2024). Em duas semanas, PSP "desconstruiu" seis notícias: desinformação tem aumentado. *Público*. Obtido em 28 de agosto de 2024, de https://www.publico.pt/2024/08/28/sociedade/noticia/duas-semanas-psp-desconstruiu-seis-noticias-desinformacao-aumentado-2101981

Hitler, A. (1925). *Mein Kampf. Murphy, James (trans.). 155-156.* Obtido de http://www.greatwar.nl/books/meinkampf/meinkampf.pdf

Hobbes, T. (1651). *Leviatã: Ou A Matéria, Forma e Poder de uma República Eclesiástica e Civil, Richard Tuck (Editor), João Paulo Monteiro (Tradutor), Maria Beatriz Nizza da Silva (Tradutor), Claudia Berliner (Tradutor), 30 setembro 2019.* São Paulo: Martins Fontes.

Hoogenboom, A. B., Schoneveld, D. C., & Meiboom, M. J. (1997). *Policing the Future* (1.ª ed.). Brill | Nijhoff.

Hyvönen, A.-E. (1 de outubro de 2018). Careless Speech: Conceptualizing Post-Truth Politics 1. *26*, pp. 31-55. Obtido em 8 de março de 2021, de https://doi.org/10.1177/2336825X1802600303

IEP. (novembro de 2020). *Global Terrorism Index 2020: Measuring the Impact of Terrorism.* Sydney: Institute for Economics and Peace (IEP). Obtido de http://visionofhumanity.org/reports

IEP. (2024). *Global Peace Index 2024: Measuring Peace in a Complex World.* Sydney: Institute for Economics & Peace (IEP). Obtido em 11 de junho de 2024, de http://visionofhumanity.org/resources

International IDEA. (2023). *The Global State of Democracy 2023 - The New Checks and Balances.* Stockholm: International Institute for Democracy and Electoral Assistance (IDEA). Obtido em 22 de fevereiro de 2024, de https://cdn.sanity.io/files/2e5hi812/production/f7b6fb692e1475af3927aff774dbc93f50771ba9.pdf

INTERPOL. (2020). *Global Horizon Scan.* INTERPOL , INTERPOL Global Complex for Innovation, Singapore. Obtido em 27 de fevereiro de 2024, de https://www.interpol.int/es/content/download/15121/file/20COM0201-04%20-

%20Innovation%20Center_Global%20Horizon%20Scan_project%20sheet_%202020-03_SP.pdf

INTERPOL. (2022). *Scanning for the Future(s) of Policing: First steps towards a new global paradigma.* INTERPOL Innovation Centre. Obtido em 16 de maio de 2024, de https://www.interpol.int/content/download/18111/file/INTERPOL%20Working%20Paper%20on%20the%20Future%20of%20Policing-EN-22062022.pdf

INTERPOL. (s.d.). *How our history started* . Obtido em 7 de março de 2024, de www.interpol.int: https://www.interpol.int/en/Who-we-are/Our-history/How-our-history-started

Ipsos European Public Affairs & UNESCO. (2023). *Survey on the impact of online disinformation and hate speech.* Ipsos European Public Affairs – UNESCO. Obtido em 1 de agosto de 2024, de https://www.unesco.org/sites/default/files/medias/fichiers/2023/11/unesco_ipsos_survey.pdf

Jesus, H. F. (9 de julho de 2020). Ciberespaço e Mundo Físico – As Duas Faces da Mesma Moeda. *Cibersegurança e Ciberdefesa em Tempos de Pandemia - IDN brief*(32). Obtido em 16 de fevereiro de 2021, de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20julho%202020%204ªversão.pdf

Kahneman, D. (2011). *Thinking, Fast and Slow.* New York: Farrar: Straus and Giroux.

Kahneman, D., & Frederick, S. (2002). Representativeness Revisited: Attribute Substitution in Intuitive Judgment. (T. Gilovich, D. Griffin, & D. Kahneman, Edits.) *Heuristics and Biases: The Psychology of Intuitive Judgment.*, pp. 49–81.

Kanet, R. (2018). Russia and global governance: The challenge to the existing liberal order. *International Politics, 55*(2), pp. 177–188. doi:10.1057/s41311-017-0075-3

Kant, I. ([1784] 1990). Resposta à pergunta: O que é o Iluminismo. Em I. Kant, *A paz perpétua e outros opúsculos.* Lisboa: Edições 70.

Kant, I. (1784). Resposta à pergunta: O que é o Iluminismo. *A paz perpétua e outros opúsculos (1990), Lisboa, Edições 70*.

Keeley, B. L. (março de 1999). Of Conspiracy Theories. *The Journal of Philosophy, Vol. 96, No. 3.*, pp. 109-126.

Kennedy, R. F. (7 de agosto de 1962). *Adress by Attorney General Robert F. Kennedy Seattle World's Fair, August 7, 1962.* Seattle: US Department of Justice. Obtido em 29 de fevereiro de 2024, de https://www.justice.gov/sites/default/files/ag/legacy/2011/01/20/08-07-1962.pdf

Kjellén, R. (1924). *Der Staat als Lebensform.* Berlim: Kurt Vowinckel Verlag.

Kruglanski, A. W., & Thompson, E. P. (1999). Persuasion by A Single Route: A View from the Unimodel. *Psychological Inquiry 10 (2)*, pp. 83–109. doi:10.1207/S15327965PL100201

Kunda, Z., & Sinclair, L. (1999). Motivated Reasoning with Stereotypes: Activation, Application, and Inhibition. *Psychological Inquiry 10 (1)*, pp. 12–22. doi:10.1207/s15327965pli1001_2

Lavrov, A. (2015). Russian Again: The Military Operation for Crimea. Em C. Howard, & R. Pukhov (Edits.), *Brothers Armed: Military Aspects of the Crisis in Ukraine* (Vol. 2, pp. 157-186). Minneapolis: East View Press.

Lewandowsky, S., Ullrich, K. H., Ecker, C. M., Seifert, N. S., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest 13 (3)*, pp. 106–131. doi:10.1177/1529100612451018

Libicki, M. (2009). Cyberdeterrence and Cyberwar. *Rand Corporation, 2009, pp. 3 4. Disponível em: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf*, pp. 3-4. Obtido em 30 de março de 2021, de http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

Lilly, B., & Cheravitch, J. (2020). Past, Present, and Future of Russia's Cyber Strategy and Forces. *12th International Conference on Cyber Conflict (CyCon). 1300*, pp. 145-146. IEEE.

Lin, H. (28 de junho de 2019). The existential threat from cyber-enabled information. *Bulletin of the Atomic Scientists, 75*, pp. 187-196.

Lopatka, J., & Hovet, J. (27 de maio de 2024). EU imposes sanctions on Voice of Europe, businessmen over Russian 'disinformation'. *Reuters*. Obtido em 5 de junho de 2024, de https://www.reuters.com/world/europe/eu-sanctions-voice-europe-related-businessmen-czech-ministry-says-2024-05-27/?utm_source=Pol%C3%ADgrafo+Europa&utm_campaign=cd871f1590-EMAIL_CAMPAIGN_2023_12_05_02_33_COPY_01&utm_medium=email&utm_term=0_-8c5b48202d-%5B

MacFarquhar, N. (2018). Inside the Russian Troll Factory: Zombies and a Breakneck Pace. *The New York Times, October 15*. Obtido em 7 de fevereiro de 2021, de https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html

Macron, E. (26 de abril de 2024). Emmanuel Macron's speech on 'Europe - it Can Die. A New Paradigm' at The Sorbonne. *Groupe d'études géopolitiques*. Obtido em 6 de maio de 2024, de https://geopolitique.eu/en/2024/04/26/macron-europe-it-can-die-a-new-paradigm-at-the-sorbonne/

Marion, N., & Twede, J. (2020). Cybercrime. Em *An Encyclopedia of Digital Crime.* Santa Barbara: ABC-CLIO.

Marques, A. G., & Santos, L. (9 de julho de 2020). Resiliência Física versus Resiliência Digital. *Cibersegurança e Ciberdefesa em Tempos de Pandemia - IDN brief* (32). Obtido em 16 de fevereiro de 2021, de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020

Martins, C. M. (2017). *O modelo de funcionamento do serviço 112 em Portugal.* Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna. Obtido em 8 de março de 2024, de https://comum.rcaap.pt/bitstream/10400.26/35123/1/O%20modelo%20de%20funcionamento%20do%20servi%C3%A7o%20112%20em%20Portugal.pdf

Marx, J., Brünker, F., Mirbabaie, M., & Hochstrate, E. (2020). Conspiracy Machines - The Role of Social Bots during the COVID-19 Infodemic. Nova Zelândia. Obtido em 14 de janeiro de 2021, de https://arxiv.org/ftp/arxiv/papers/2012/2012.09536.pdf

Matsuoka, J. S. (2021). *Os limites da liberdade de expressão: os efeitos da desinformação na exponenciação dos crimes contra a honra.* Escola de Direito e Relações Internacionais . Goiânia: Pontifícia Universidade Católica de Goiás. Obtido em 8 de agosto de 2024, de https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1932/1/JANAINA%20SILVA%20MATSUOKA.pdf

Maurer, T., & Morgus, R. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions.* New America Foundation. New America . Obtido em 3 de junho de 2024, de https://static.newamerica.org/attachments/175-compilation-of-existing-cybersecurity-and-information-security-related-definitions/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions_Updated122015.pdf

Mavragani, A. (28 de abril de 2020). Infodemiology and infoveillance: scoping review. *Journal of medical internet research, 22*(4). doi:10.2196/16206.

McConnachie, J., & Tudge, R. (2008). *The Rough Guide to Conspiracy Theories. 3rd Edition.* London: Rough Guides Limited.

Mecklin, J. (27 de janeiro de 2021). This is your COVID wake-up call: It is 100 seconds to midnight. *Bulletin of the Atomic Scientists, 2021 Doomsday Clock Statement, Science and Security Board Bulletin of the Atomic Scientists*.

Mecklin, J. (11 de setembro de 2023). Introduction: The Hype, Peril, and Promise of Artificial Intelligence. *Bulletin of the Atomic Scientists*. Obtido em 17 de janeiro de 2024, de https://thebulletin.org/premium/2023-09/introduction-the-hype-peril-and-promise-of-artificial-intelligence/

Mecklin, J. (23 de janeiro de 2024). A moment of historic danger: It is still 90 seconds to midnight. *Bulletin of the Atomic Scientists*. Obtido em 23 de janeiro de 2024, de https://thebulletin.org/doomsday-clock/current-time/

Meta. (11 de maio de 2024). How the International Fact-Checking Network Is Bringing Organizations Together to Fight COVID-19 Misinformation. *Meta Journalism Project*. Obtido em 22 de agosto de 2024, de https://www.facebook.com/journalismproject/ifcn-fighting-misinformation?locale=pt_BR

Milner, N. P. (2001). *Vegetius: Epitome of Military Science (Translated Texts for Historians - LUP)* (2.ª ed., Vol. 16). (M. P. Milner, Trad.) Liverpool: Liverpool University Press. Obtido em 15 de fevereiro de 2021, de https://books.google.pt/books?id=aPK7xjchZFUC&printsec=frontcover&dq=renatus&hl=en&ei=zhgtTfKeGoGosQPIzcH8Bg&sa=X&oi=book_result&ct=result&redir_esc=y#v=onepage&q&f=false

Moreira, A. R., Quefflec, C., Pereira, D. M., Rodrigues, E., Carvalho, J., Elias, L. M., . . . Fernandes, S. H. (2018). *Segurança Interna | Desafios na Sociedade de Risco Mundial.* (N.

Poiares, & R. Marta, Edits.) Lisboa: Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna.

Nagorski, T. (30 de julho de 2024). Book review: To Run the World: The Kremlin's Cold War Bid for Global Power (1.ª ed.). Radchenko, S. (2024). Cambridge : Cambridge University Press. *The Cipher Daily Brief*. Obtido em 30 de julho de 2024, de https://www.thecipherbrief.com/book-review/from-stalin-to-putin-a-push-to-run-the-world?utm_source=The+Cipher+Daily+Brief+Newsletter&utm_campaign=60b780d1ca-EMAIL_CAMPAIGN_2024_07_30_01_27&utm_medium=email&utm_term=0_-60b780d1ca-%5BLIST_EMAIL_ID%5D&mc_cid

NATO. (10 de julho de 2024). Summary of NATO's revised Artificial Intelligence (AI) strategy. *Newsroom: Official texts*. Obtido em 30 de julho de 2024, de https://www.nato.int/cps/en/natohq/official_texts_227237.htm

Netflix. (24 de julho de 2019). Nada é privado: O escândalo da Cambridge Analytica. (Karim Amer; Jehane Noujaim). Obtido em 23 de março de 2021

Netflix. (9 de setembro de 2020). O dilema das Redes Sociais. (Jeff Orlowski).

Neto, I. (15 de janeiro de 2023). Trolls, propaganda e muito frio. Como a Rússia quer "minar" a opinião pública no Inverno. *Público*. Obtido em 30 de maio de 2024, de https://www.publico.pt/2023/01/15/mundo/noticia/trolls-propaganda-frio-russia-quer-minar-opiniao-publica-inverno-2034635

Nogala, D. (2023). Preparing Law Enforcement for the Digital Age – editor's reflection. (E. U. (CEPOL), Ed.) *European Law Enforcement Research Bulletin - Special Conference Edition*(6).

Nogala, D. (2024). Mehr Zusammenarbeit erfordert bessere Ausbildung. (J. B. von S. Anastasiadis, & J. Grutzpalk, Edits.) *Polizei. Wissen. Themen polizeilicher Bildung - Wissensmanagement für die Polizei*(8).

Novais, V. (18 de agosto de 2022). Estónia alvo de maior ciberataque desde 2007. Grupo russo reinvindica ataque. *Observador*. Obtido em 24 de maio de 2024, de https://observador.pt/2022/08/18/estonia-alvo-de-maior-ciberataque-desde-2007-grupo-russo-reinvindica-ataque/

Observador. (17 de março de 2021). Biden promete que Putin "vai pagar" por ter autorizado operações para o prejudicar na campanha eleitoral. *Observador*. Obtido em 17 de março de 2021, de https://observador.pt/2021/03/17/putin-autorizou-operacoes-para-prejudicar-biden-durante-a-campanha-eleitoral-nos-eua-tamb

Oledan, J., Bariletto, N., Salihudin, S., Sitepu, M., & Shapiro, J. N. (25 de janeiro de 2021). Politics, race, and religion: Pandemic misinformation courses through the Southeast Asian internet. *Bulletin of the Atomic Scientists*. Obtido em 11 de fevereiro de 2021, de https://thebulletin.org/2021/01/politics-race-and-religion-pandemic-misinformation-courses-through-the-southeast-asian-internet/?utm_source=Newsletter&utm_medium=Email&utm_campaign=ThursdayNewsletter01282021&utm_content=

Oliker, O. (15 de janeiro de 2015). Russia's New Military Doctrine: Same as the Old Doctrine, Mostly. *Washington Post*.

Oliveira, A. (2018). Inteligência Artificial: oportunidades e desafios. *Inteligência Artificial: disrupção e oportunidade.* Lisboa: Instituto Miguel Galvão Teles. Obtido em 20 de março de 2024, de https://www.mlgts.pt/xms/files/v1/IMGT/IMGT_Inteligencia_Artificial_Arlindo_Oliveira.pdf

Oliveira, F. A. (2020). *Fazer Fact-Checking em Portugal: Análise ao Observador e ao Polígrafo.* Universidade da Beira Anterior. Obtido em 22 de agosto de 2024, de https://ubibliorum.ubi.pt/bitstream/10400.6/11042/1/7578_16046.pdf

OPAS. (2020). *Factsheet: Entenda a infodemia e a desinformação na luta contra a COVID-19.* Organização Pan-Americana da Saúde (OPAS). Obtido em 26 de fevereiro de 2024, de https://iris.paho.org/bitstream/handle/10665.2/52054/Factsheet-Infodemic_por.pdf

Oreskes, N., & Conway, E. M. (2011). Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming.

Orwell, G. (1946). *Politics and the English Language.* Peterborough: Broadview Press. Obtido em 12 de fevereiro de 2021, de https://www.orwell.ru/library/essays/politics/english/e_polit/

Orwell, G. (2012). *1984.* (A. L. Faria, Trad.) Lisboa: Antígona.

Paganini, P. (2017). *Digging into the Dark Web.* Rome: European Union Agency for Cybersecurity (ENISA) . Obtido em 3 de junho de 2024, de https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/digging-into-the-dark-web/@@download/file/Digging%20into%20the%20Dark%20web%20Paganini.pdf

Paiva, R. P., & Gómez, G. (21 de junho de 2021). O que pode a União Europeia fazer para salvar a democracia e travar a desinformação? *Público*. Obtido em 28 de agosto de 2024, de https://www.publico.pt/2021/06/21/infografia/uniao-europeia-salvar-democracia-travar-desinformacao-603

Pandey, S. (16 de abril de 2021). Tribunal na Austrália conclui que Google enganou usuários sobre coleta de dados. Obtido em 13 de maio de 2021, de https://www.uol.com.br/tilt/noticias/reuters/2021/04/16/tribunal-na-australia-conclui-que-google-enganou-usuarios-sobre-coleta-de-dados.htm?cmpid=copiaecola

Parlamento Europeu. (2016). *Resolução do Parlamento Europeu, de 23 de novembro de 2016, sobre a Comunicação estratégica da UE para enfrentar a propaganda dirigida contra ela por terceiros.* Estrasburgo: Parlamento Europeu. Obtido em 30 de maio de 2024, de https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_PT.html

Parliament of the United Kingdom. (19 de junho de 1829). *Metropolitan Police Act.* Obtido em 6 de fevereiro de 2024, de https://www.legislation.gov.uk/ukpga/Geo4/10/44/data.pdf

Paul, C., & Matthews, M. (11 de julho de 2026). The Russian "Firehose of Falsehood" Propaganda Model. Why It Might Work and Options to Counter It. *RAND*. Obtido em 30 de julho de 2024, de https://www.rand.org/pubs/perspectives/PE198.html

Paulsen, C., & Byers, R. (2019). *Glossary of Key Information Security Terms.* U. S. Department of Commerce. Gaithersburg: National Institute of Standards and Technology. Obtido em 3 de junho de 2024, de https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf

Pereira, J. (2018). As Ameaças híbridas – Uma Abordagem Conceptual no quadro da OTAN e da EU. *CEDIS Working Papers – Direito, Segurança e Democracia, ISSN 2184-0776, Nº 60, URL: http://cedis.fd.unl.pt/wp-content/uploads/2018/10/CEDIS_working-paper_DSD_As-*.

Peters, B. (2016). Digital. Em B. Peters (Ed.), *Digital Keywords – A Vocabulary of Information Society and Culture.* Princeton, N.J.

Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. (L. Berkowitz, Ed.) *Advances in Experimental Social Psychology, 19*, pp. 123–205. doi:10.1016/S0065-2601(08)60214-2

Pfeffer, J., Zorbach, T., & Carley, K. M. (2014). Understanding Online Firestorms: Negative Word-of-Mouth Dynamics in Social Media Networks. *Journal of Marketing Communications, 20* ((1–2)), pp. 117–128. doi:10.1080/13527266.2013.797778

Poiares, N. (2019). Cibersegurança, literacia e resiliência digital dos idosos. *Anuário Janus 2018-2019: A dimensão externa da segurança interna*(19), pp. 118-119. Obtido em 15 de fevereiro de 2021, de http://janusonline.pt/images/anuario2018_2019/

Postmes, T., Spears, R., Sakhel, K., & Daphne, D. G. (2001). Social Influence in Computer-Mediated Communication: The Effects of Anonymity on Group Behavior. *Personality and Social Psychology Bulletin 27 (10)*, pp. 1243–1254. doi:10.1177/01461672012710001

PRP Channel. (6 de outubro de 2018). Grã-Bretanha: o Cyber Califado gerenciado pelo governo russo. *PRP Channel*. Obtido em 10 de fevereiro de 2021, de https://www.prpchannel.com/pt/gran-bretagna-il-cyber-caliphate-gestito-dal-governo-russo/

PSP. (2024). *Estratégia da PSP 2024/2026.* PSP. Obtido em 6 de fevereiro de 2024, de https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Documentos%20Estrat%C3%A9gicos/Estrat%C3%A9gia%20da%20PSP%20-%202024-2026.pdf?lang=pt

Público. (18 de maio de 2007). Rússia acusada de ciberguerra à Estónia. *Público*. Obtido em 30 de março de 2021, de http://www.publico.pt/2007/05/18/jornal/russia-acusada-de-ciberguerra-a-estonia-215151

Público. (14 de novembro de 2012). Sete detidos e 48 feridos nos confrontos junto ao Parlamento, segundo a PSP. *Público*. Obtido em 6 de agosto de 2024, de https://www.publico.pt/2012/11/14/economia/noticia/greve-ao-minuto-1572391

Putnam, H. (1960). *Minds and machines.* (S. Hook, Ed.) New York: New York University Press. Obtido em 7 de março de 2024, de https://philpapers.org/archive/PUTMAM.pdf

Radchenko, S. (2024). *To Run the World: The Kremlin's Cold War Bid for Global Power* (1.ª ed.). Cambridge : Cambridge University Press.

Radin, A., & Reach, C. (2017). *Russian Views of the International Order.* California: RAND Corporation.

Recorded Future. (24 de março de 2024a). *Russian State-Sponsored Amplification of Bio Lab Disinformation Amid War in Ukraine.* Insikt Group. Obtido em 12 de maio de 2024, de https://go.recordedfuture.com/hubfs/reports/cta-2022-0324.pdf

Recorded Future. (9 de maio de 2024b). Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale. *Research (Insikt)*. Obtido em 12 de maio de 2024, de https://www.recordedfuture.com/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale

Recorded Future. (2024c). *Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale.* Insikt Group. Obtido em 12 de maio de 2024, de https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf

Redação Exame. (16 de maio de 2024). O que esperar de Putin na China — e por que os países estão tão próximos agora. *Exame*. Obtido em 16 de maio de 2024, de https://exame.com/mundo/o-que-esperar-de-putin-na-china-e-por-que-os-paises-estao-mais-proximos-do-que-nunca/

Redação O Antagonista. (15 de dezembro de 2023). Rudolph Giuliani é condenado por fake news em eleições de 2020. *O Antagonista*. Obtido em 8 de agosto de 2024, de https://oantagonista.com.br/mundo/rudolph-giuliani-e-condenado-por-fake-news-em-eleicoes-de-2020/

Reid, J. (2013). The Europol Liaison Officer: A Breed Apart. Em M. den Boer, & L. Block (Edits.), *Liaison Officers: Essential Actors in Transnational Policing* (pp. 137-153). The Hague: Eleven International Publishing. Obtido em 29 de maio de 2024, de https://www.researchgate.net/profile/Ludo-Block/publication/327200714_Liaison_Officers_Essential_Actors_in_Transnational_Policing/links/5db7e024299bf1a47bfa36ef/Liaison-Officers-Essential-Actors-in-Transnational-Policing.pdf

Reuters, T. (1941). The Trust Principles. *The five Trust Principles*. Obtido em 5 de junho de 2024, de https://www.thomsonreuters.com/en/about-us/trust-principles.html

Ribeiro, J. F. (junho de 2013). O reposicionamento da China: geoeconomia, geopolítica e estratégia. *Relações Internacionais, 38*, pp. 035-043.

Ribeiro, V. (2015). O spin doctoringem Portugal: Perspectivas de governantes, jornalistas e assessores de comunicação que operam na Assembleia da República. *Observatorio (OBS*) Journal, 9*(2), pp. 225-256. Obtido em 3 de junho de 2024, de https://obs.obercom.pt/index.php/obs/article/view/823/721

Richardson, J., Milovidov, E., & Schmalzried, M. (2017). *Internet Literacy Handbook - Supporting users in the online world.* Council of Europe. Strasbourg: Council of Europe Publishing. Obtido em 3 de junho de 2024, de https://rm.coe.int/internet-literacy-handbook/1680766c85

Richter, F. (11 de janeiro de 2024). The Largest Risks Faced by the World. *Statista News*. Obtido em 29 de janeiro de 2024, de https://www.statista.com/chart/29197/the-most-severe-global-risks-over-the-next-2-and-10-years/

Rigues, R. (15 de dezembro de 2021). SolarWinds: ataque foi o "maior e mais sofisticado" já visto. *Olhar Digital*. Obtido em 8 de março de 2021, de https://olhardigital.com.br/2021/02/15/noticias/solarwinds-ataque-foi-o-maior-e-mais-sofisticado-que-o-mundo-ja-viu/

Rodrigues Alves, T. (22 de agosto de 2024). PSP denuncia publicação falsa sobre alegado rapto de criança por imigrantes. *Jornal de Notícias*. Obtido em 26 de agosto de 2024, de https://www.jn.pt/4093014671/psp-denuncia-publicacao-falsa-sobre-alegado-rapto-de-crianca-por-imigrantes/amp/

Rodrigues, C. (24 de agosto de 2024). Machico queima hoje os 'Fachos' envoltos em grande polémica. *Diário de Notícias da Madeira*. Obtido em 25 de agosto de 2024, de https://www.dnoticias.pt/2024/8/24/417270-machico-queima-hoje-os-fachos-envoltos-em-grande-polemica/

Rosner, R., & Brown Jr., E. G. (27 de janeiro de 2021). The most dangerous situation humanity has ever faced. *CNN*. Obtido em 10 de fevereiro de 2021, de https://edition.cnn.com/2021/01/27/opinions/doomsday-clock-dangerous-situation-brown-rosner/index.html

Rothbaum, B. O., Hodges, L. F., Kooper, R., Opdyke, D., Williford, J. S., & North, M. (1997). Virtual reality exposure therapy. *Journal of Psychotherapy Practice and Research*(6), pp. 291-296. Obtido em 7 de março de 2024, de https://www.researchgate.net/profile/Barbara-Rothbaum/publication/14033965_Virtual_reality_exposure_therapy/links/540cc7990cf2f2b29a3822d8/Virtual-reality-exposure-therapy.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9

Rothkopf, D. J. (11 de maio de 2003). When the Buzz Bites Back. *Washington Post*. Obtido em 7 de março de 2024, de https://www.washingtonpost.com/archive/opinions/2003/05/11/when-the-buzz-bites-back/bc8cd84f-cab6-4648-bf58-0277261af6cd/

Rottweiler, B., & Gill, P. (22 de janeiro de 2021). Zoom Webinar. *The Relationship of Conspiracy Beliefs and Violent Extremism*. ERC-funded Grievance project https://www.grievance-erc.com., Cambridge, United Kingdom: Violence Research Centre, Institute of Criminology, University of Cambridge.

Roxburgh, N., Guan, D., Shin, K. J., Rand, W., Managi, S., Lovelace, R., & Meng, J. (2019). Characterising Climate Change Discourse on Social Media during Extreme Weather Events. *Global Environmental Change 54*, pp. 50–60. doi:10.1016/j.gloenvcha.2018.11.004

RTP2. (17 de fevereiro de 2021). O extremo da extrema-direita; (versão portuguesa). Obtido em 20 de fevereiro de 2021, de https://www.rtp.pt/play/p8495/o-extremo-da-extrema-direita

Russell, B. (1998). The Triumph of Stupidity. Em H. Ruja (Ed.), *Mortals and Others. American Essays 1931-1935 Bertrand Russell* (Vol. I, p. 28). London: Routledge.

Salvador, S. (18 de março de 2024). Blinken e Yoon alertam para riscos da desinformação e da IA para a democracia. *Diário de Notícias*. Obtido em 20 de março de 2024, de

https://www.dn.pt/4711206555/blinken-e-yoon-alertam-para-riscos-da-desinformacao-e-da-ia-para-a-democracia/

Sanger, D. E., & Kramer, A. E. (15 de abril de 2021). U.S. Imposes Stiff Sanctions on Russia, Blaming It for Major Hacking Operation. *The New York Times*. Obtido em 19 de abril de 2021, de https://www.nytimes.com/2021/04/15/world/europe/us-russia-sanctions.html

Sanger, D. E., Perlroth, N., & Schmitt, E. (14 de dezembro de 2020). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. *The New York Times*. Obtido em 19 de abril de 2021, de https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Sanner, B. (4 de agosto de 2024). Dealing with 'Axis of Authoritarians' Requires Greater U.S. Policy Risk. *The Cipher Brief*. Obtido em 10 de agosto de 2024, de https://thecipherbrief.us10.list-manage.com/track/click?u=9775ab595d580738d839f9d01&id=a7ed996d5d&e=0b3d1478cd

Santo, J. C. (Ed.). (2019). *Alan Turing, Cientista Universal.* Braga: UMinho Editora. Obtido em 7 de março de 2024, de https://repositorium.sdum.uminho.pt/bitstream/1822/70108/1/AlanTuring_ebook.pdf

Santos, D. (9 de julho de 2020). A Pandemia de COVID-19 e os Ciberataques em Portugal. *Cibersegurança e Ciberdefesa em Tempos de Pandemia - IDN brief*(32). Obtido em 16 de fevereiro de 2021, de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%

Sarmento, M. (2013). *Guia Prático sobre Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses de Doutoramento, Dissertações de Mestrado e Trabalhos de Investigação Aplicada.* Lisboa: Universidade Lusíada Editora.

SAS. (2021). *Procedural justice and analytics.* SAS Institute Inc. Obtido de https://www.sas.com/content/dam/SAS/documents/partner-collateral/en/procedural-justice-analytics-112191.pdf

Schick, N. (6 de agosto de 2020). *Deep Fakes and the Infocalypse.* United Kingdom: Monoray.

Schwab, K. M. (2018). *A Quarta Revolução Industrial.* Levoir.

Scott, M. (1 de abril de 2020a). Russia and China push 'fake news' aimed at weakening Europe: report. *Politico*. Obtido em 10 de fevereiro de 2021, de https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/

Scott, M. (29 de dezembro de 2020b). In 2021, coronavirus will reshape digital rules. *Politico*. Obtido em 10 de fevereiro de 2021, de https://www.politico.eu/article/tech-predictions-2021-covid19/

Seaskate Inc. (1998). *The Evolution and Development of Police Technology – A Technical Report prepared for The National Committee on Criminal Justice Technology.* Washington D. C.: National Institute of Justice. Obtido em 8 de março de 2024, de https://www.ojp.gov/pdffiles1/Digitization/173179NCJRS.pdf

Sganga, N. (4 de fevereiro de 2022). U.S. reveals Russian plot to use fake video as pretense for Ukraine invasion. *CBS News*. Obtido em 20 de maio de 2024, de https://www.cbsnews.com/news/russia-disinformation-video-ukraine-invasion-united-states/

Silva, C. C. (28 de abril de 2017). O que é, afinal, o jogo suicidário Baleia Azul? *Público*. Obtido em 12 de fevereiro de 2021, de https://www.publico.pt/2017/04/28/sociedade/perguntaserespostas/perguntas--respostas-sobre-o-jogo-suicidario-baleia-azul-1770413

Silva, G. A., & Gonçalves, W. (2010). *Dicionário de Relações Internacionais* (2.ª (revista e ampliada) ed.). São Paulo: Manole. Obtido em 21 de maio de 2024, de https://geovest.wordpress.com/wp-content/uploads/2021/05/dicionario-de-ri-varios-autores.pdf

Silva, M. M., & Guerreiro, J. (26 de outubro de 2020). On the 5G and Beyond. *MDPI Applied Sciences, 10, 7091*. Obtido em 30 de março de 2021, de https://www.mdpi.com/2076-3417/10/20/7091

Silva, R. (13 de janeiro de 2013). Inteligência Artificial. (A. d. Editares, Ed.) *Enciclopédia da Conscienciologia*. Obtido em 3 de junho de 2024, de http://reposicons.org/jspui/bitstream/123456789/3737/1/Inteligencia-Artificial.pdf

Silveira, R. S. (2022). *A Repressão Jurídico-Penal da Desinformação.* Lisboa: Universidade Catolica Portuguesa. Obtido em 3 de agosto de 2024, de https://repositorio.ucp.pt/bitstream/10400.14/39087/1/203060873.pdf

Simon, J., & Mahoney, R. (2022). *The Infodemic. How Censorship and Lies Made the World Sicker and Less Free.* New York: Columbia Global Reports.

Simon, S. (11 de fevereiro de 2021). Trump's Insurrection and America's Year of Living Dangerously, The Survival Editors' Blog. *Survival, 63*(1), pp. 7-16. doi:https://doi.org/10.1080/00396338.2021.1881247

Smith, R., Cubbon, S., & Wardle, C. (12 de novembro de 2020). Under the surface: Covid-19 vaccine narratives, misinformation and data deficits on social media. *First Draft*. Obtido em 4 de março de 2021, de https://firstdraftnews.org/wp-content/uploads/2020/11/FirstDraft_Underthesurface_Fullre

Snowden, E. (24 de outubro de 2014). Citizenfour. (L. Poitras, Ed.) Obtido em 24 de março de 2021, de https://upload.wikimedia.org/wikipedia/commons/c/cd/CITIZENFOUR_%282014%29_trailer.webm

Snowden, E. (2019). *Vigilância massiva - Registo Permanente* (2.ª ed.). (M. D. Correia, Trad.) Lisboa: Grupo Planeta.

Soares, M. R. (1 de outubro de 2020). Trump foi maior incitador à desinformação sobre Covid-19, revela estudo. *RTP*. Obtido em 4 de março de 2021, de https://www.rtp.pt/noticias/mundo/trump-foi-maior-incitador-a-desinformacao-sobre-covid-19-revela-estudo_n1263507

Soares, T. (1 de junho de 2022). Justiça russa condena primeiro cidadão por "espalhar fake news" sobre a guerra na Ucrânia. *Expresso*. Obtido em 8 de agosto de 2024, de https://expresso.pt/internacional/guerra-na-ucrania/2022-06-01-Justica-russa-condena-primeiro-cidadao-por-espalhar-fake-news-sobre-a-guerra-na-Ucrania-38b393ab

Soromenho-Marques, V. (2019). 'Human security' and the reshaping of contemporary thinking on peace and war. Em T. Rodrigues, & A. Inácio (Edits.), *Security at a crossroad. New tools for new challenges* (pp. 3-19). Nova lorque: Nova Science Publishers.

Soromenho-Marques, V., & Magalhães, P. (2024). Pensar a Segurança e o Direito Internacional na Época Antropoceno. Em T. Rodrigues, & J. Estevens, *Preparar o Futuro: A transição digital na segurança e defesa* (p. 420). Fronteira do Caos.

Squassoni, S. (30 de março de 2021). How the Biden administration can secure real gains in nuclear arms control. *Bulletin of the Atomic Scientists*. Obtido em 7 de abril de 2021, de https://thebulletin.org/2021/03/how-the-biden-administration-can-secure-real-gains-in-nuclear-arms-control/?utm_source=Newsletter&utm_medium=Email&utm_campaign=ThursdayNewsletter04012021&utm_content=NuclearRisk_ArmsControlGains_03302021

SSI. (2023). *Relatório Anual de Segurança Interna.* Gabinete do Secretário-Geral do Sistema de Segurança Interna. Lisboa: Ministério da Administração Interna. Obtido em 4 de junho de 2024, de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDEyNgEApqka1wUAAAA%3d

Stent, A. E. (2014). *The limits of partnership: U.S.-Russian relations in the twenty-first century.* Princeton: Princeton University Press.

Stover, D. (25 de fevereiro de 2021). The quest to rid Facebook of vaccine misinformation. *Bulletin of the Atomic Scientists*. Obtido em 4 de março de 2021, de Bulletin of the Atomic Scientists: https://thebulletin.org/2021/02/the-quest-to-rid-facebook-of-vaccine-misinformation/

Sun Tzu. (2023). *A Arte da Guerra.* (R. Castro, Trad.) Lisboa: Marcador.

Taber, C. S., & Lodge, M. (2006). Motivated Skepticism in the Evaluation of Political Beliefs. *American Journal of Political Science 50 (3)*, pp. 755–769. doi:10.1111/j.1540-5907.2006.00214.x

Tek/Lusa. (27 de fevereiro de 2024a). Países unem-se para desmontar desinformação orquestrada na sombra pela Rússia e pela China. *SAPOTEK*. Obtido em 30 de maio de 2024, de https://tek.sapo.pt/noticias/internet/artigos/paises-unem-se-para-desmontar-desinformacao-orquestrada-na-sombra-pela-russia-e-pela-china

Tek/Lusa. (3 de maio de 2024b). Rússia estará na origem de onda de ciberataques na Europa. Estados Unidos já condenaram as ações. *SAPOTEK*. Obtido em 30 de maio de 2024, de https://tek.sapo.pt/noticias/computadores/artigos/russia-estara-na-origem-de-onda-de-ciberataques-na-europa-estados-unidos-ja-condenaram-as-acoes

The Economist. (9 de maio de 2024a). *The new economic order. The liberal international order is slowly coming apart.* The Economist Group. Obtido em 11 de maio de 2024, de https://www.economist.com/leaders/2024/05/09/the-liberal-international-order-is-slowly-coming-apart

The Economist. (10 de maio de 2024b). A Russia-linked network uses AI to rewrite real news stories – CopyCop churned out 19,000 deceptive posts in a month. *The Economist: Science and technology*. Obtido em 12 de maio de 2024, de https://www.economist.com/science-and-technology/2024/05/10/a-russia-linked-network-uses-ai-to-rewrite-real-news-stories

The Economist. (3 de junho de 2024c). Yuval Noah Harari on how to prevent a new age of imperialism. *The Economist*. Obtido em 5 de junho de 2024, de https://www.economist.com/by-invitation/2024/06/03/yuval-noah-harari-on-how-to-prevent-a-new-age-of-imperialism?utm_campaign=later-linkinbio-theeconomist&utm_content=later-43415174&utm_medium=social&utm_source=linkin.bio

The New York Times. (6 de novembro de 2018). Facebook Admits It Was Used to Incite Violence in Myanmar. *The New York Times*. Obtido em 17 de maio de 2021, de https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html

The White House. (15 de abril de 2021). Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government. Washington D. C.: The White House. Obtido em 15 de abril de 2021, de https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Tomé, L. (2014). Geopolítica e Estratégia. *Estudos de Homenagem a Abel Cabral Couto*, p. 173. Obtido em 13 de janeiro de 2021, de https://repositorio.ual.pt/bitstream/11144/1768/1/Geopolitica%20e%20Geo-Estrat%c3%a9gia%2c%20cap.livro%20IESM%202014.pdf

Tomé, L. (10 de dezembro de 2020). A Ressurgência da China e a centralidade da Ásia no Século XXI. *Seminário online (via Zoom): Conflitos, crises e desafios do Mundo contemporâneo; Universidade de Évora*.

Tomé, L. (2022). The Impacts of the Pandemic Crisis on International Politics. Em S. Ş. Erçetin, N. Potas, & S. N. Açikalin (Edits.), *COVID-19 Beyond: Effects of Different Fields* (pp. 49-84). Springer/ World Scientific Publishing. doi:https://doi.org/10.1142/9781800611450_0004

Tomé, L. (dezembro de 2023). (Des)Ordem Mundial "com Características Chinesas" – um Mundo Seguro para a Autocracia. *Nação e Defesa*(166), pp. 83-116 . Obtido em 16 de maio de 2024, de https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD166/Nac%CC%A7a%CC%83o%20e%20Defesa_166_LuisTome.pdf

Tracy, M., Jansen, W., Scarfone, K., & Winograd, T. (2007). *Guidelines on Securing Public Web Servers - Recommendations of the National Institute of Standards and Technology.* U. S. Department of Commerce, Computer Security Division; Information Technology Laboratory. National Institute of Standards and Technology. Obtido em 3 de junho de 2024, de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-44ver2.pdf

Turing, A. M. (outubro de 1950). Computing Machinery and Intelligence. (O. U. Association, Ed.) *Mind, New Series, 59*(236), pp. 433-460. Obtido em 7 de março de 2024, de https://phil415.pbworks.com/f/TuringComputing.pdf

U. S. Department of State. (2024). *Desarmando a desinformação: nossa responsabilidade compartilhada*. Obtido em 18 de maio de 2024, de United with Ukraine : https://www.state.gov/desarmando-a-desinformacao/

U.S. Senate Select Committee on Intelligence. (2020). *Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election.* Washington D. C.: U.S. Senate Select Committee on Intelligence. Obtido em 18 de março de 2021, de https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

União Europeia. (2019). *Desafios à eficácia da política de cibersegurança da UE.* Tribunal de Contas Europeu. Luxemburgo: Serviços das Publicações da União Europeia. Obtido em 3 de junho de 2024, de https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf

União Europeia. (2021). *Desinformação na UE: fenómeno combatido, mas não controlado.* Tribunal de Contas Europeu. Luxemburgo: Serviço das Publicações da União Europeia. Obtido em 31 de maio de 2024, de https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_PT.pdf

Vaidišová, N. (2022). Book review on Jessikka Aro, Putin's Trolls: On the Frontlines of Russia's Information War Against the World. *Auc Studia Territorialia, 1*(22), pp. 93-96. doi:10.14712/23363231.2022.10

Valenza, D. (16 de março de 2021). The Trap of Geopolitics: Rethinking EU Strategic Communication. *College of Europe POlicy Brief (CEPOB)*(3.21). Obtido em 24 de junho de 2021, de https://www.coleurope.eu/system/tdf/research-paper/valenza_cepob_3_2021_final.pdf.pdf?file=1&type=node&id=62082&force=

Voa Português. (21 de março de 2022). *O poder da infodemia em guerras como a Ucrânia-Rússia*. Obtido em 12 de maio de 2024, de https://www.voaportugues.com/: https://www-voaportugues-com.cdn.ampproject.org/v/s/www.voaportugues.com/amp/o-poder-da-infodemia-em-guerras-como-a-ucr%C3%A2nia-russa-/6494359.html?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=De%20%251%24s&aoh=17155162359326&referrer=https%3

Vollmer, A. (janeiro-fevereiro de 1930). The Scientific Policeman. *The American Journal of Police Science, 1*(1), pp. 8-12. Obtido em 15 de janeiro de 2024, de https://doi.org/10.2307/1147252

Von der Leyen, U. (2019a). Europe must learn the language of power. *Deutsche Welle*. Obtido em 15 de fevereiro de 2021, de https://www.dw.com/en/von-der-leyen-europe-must-learn-the-language-of-power/a-51172902

Von der Leyen, Ursula. (2019b). A Union that Strives for More. My Agenda for Europe: Political Guidelines for the Next European Commission 2019-2024. Obtido em 16 de fevereiro de 2021, de https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en_0.pdf

Watts, T. (8 de novembro de 2018). Which EU Country Is Most Vulnerable To Cybercrime? *Website Builder Expert*. Obtido em 12 de março de 2024, de https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/

WEF. (2024a). *Global Risks Report 2024.* World Economic Forum (WEF). Obtido em 23 de janeiro de 2024, de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

WEF. (2024b). *Top 10 Emerging Technologies of 2024.* World Economic Forum (WEF). Obtido em 25 de julho de 2024, de https://www3.weforum.org/docs/WEF_Top_10_Emerging_Technologies_of_2024.pdf

WEF. (2024c). *The Global Cooperation Barometer.* World Economic Forum (WEF) & McKinsey & Company. Obtido em 22 de julho de 2024, de https://www3.weforum.org/docs/WEF_The_Global_Cooperation_Barometer_2024.pdf

Wendling, M. (7 de janeiro de 2021). QAnon: o que é e de onde veio o grupo que participou da invasão ao Congresso dos EUA. BBC News. Obtido em 13 de março de 2021, de https://www.bbc.com/portuguese/internacional-55577322

WHO. (2020). World Heath Organization Director-general speeches. *Munich Security Conference on 15th February 2020.* Munich. Obtido em 7 de março de 2024, de https://www.who.int/director-general/speeches/detail/munich-security-conference

WHO. (2021). *WHO Public Health Research Agenda for Managing Infodemics.* World Health Organization (WHO). Geneva, Switzerland: World Health Organization (WHO). Obtido em 16 de março de 2021, de https://apps.who.int/iris/rest/bitstreams/1330207/retrieve

Willett, M. (31 de março de 2021). Lessons of the SolarWinds hack; The Survival Editors' Blog. *The International Institute for Strategic Studies (IISS)*. Obtido em 16 de abril de 2021, de https://www.iiss.org/-/media/files/publications/survival/2021/aprmay/63-2-02-willett.pdf

Wu Ming 1. (2022). *Q comme qomplot: Comment les fantasmes de complots défendent le système.* (A. Echenoz, & S. Quadruppani, Trads.) Lux Editeur.

Xavier, A. I. (2023). O combate à Desinformação na União Europeia: Da pandemia Covid-19 à guerra de agressão na Ucrânia. Em S. S. Monteiro, C. M. Cebola, & E. Lucas (Edits.), *A União Europeia em tempos de crise. Direito e Políticas Públicas de 2020 a 2023* (pp. 219-238). Coimbra: Edições Almedina, S. A. Obtido em 30 de maio de 2024, de https://ijp.upt.pt/wp-content/uploads/2024/01/A-UE-em-tempos-de-crise_compressed.pdf#page=220

Yankoski, M., Scheirer, W., & Weninger, T. (13 de maio de 2021). Meme Warfare: AI countermeasures to disinformation should focus on popular, not perfect, fakes. *Bulletin of the Atomic Scientists*. Obtido em 17 de maio de 2021, de https://thebulletin.org/premium/2021-05/meme-warfare-ai-countermeasures-to-

disinformation-should-focus-on-popular-not-perfect-fakes/?utm_medium=socialmedia&utm_source=instagram&utm_campaign=meme+warfare

Yuzefovich, G. (8 de agosto de 2024). Weapons of the Weak: Fighting Literary Censorship in Contemporary Russia. *Carnegie Politika*. Obtido em 11 de agosto de 2024, de https://carnegieendowment.org/russia-eurasia/politika/2024/07/knizhnaya-cenzura?lang=en&center=russia-eurasia

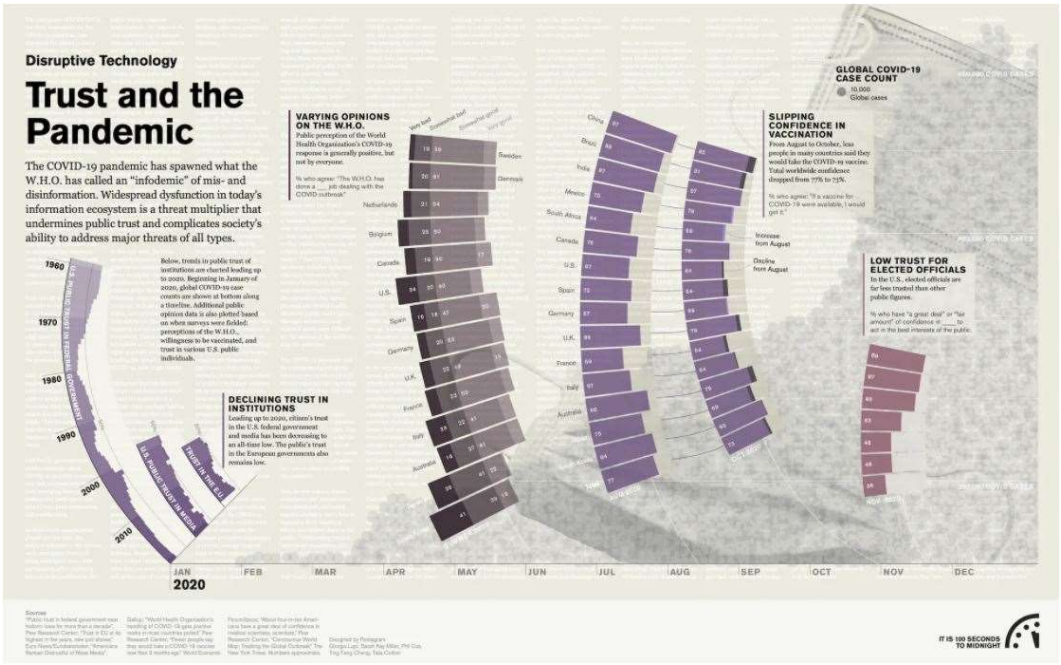
Zahidi, S. (2024). Global Risks Report 2024. Em WEF. World Economic Forum (WEF). Obtido em 13 de maio de 2024, de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Zarocostas, J. (20 de fevereiro de 2020). How to fight an infodemic. *The Lancet, 395(10225)*, p. 676. doi:https://doi.org/10.1016/S0140-6736(20)30461-X

Zaval, L., & Cornwell, J. F. (novembro de 2016). Cognitive Biases, Non-Rational Judgments, and Public Perceptions of Climate Change. doi:10.1093/acrefore/9780190228620.013.304

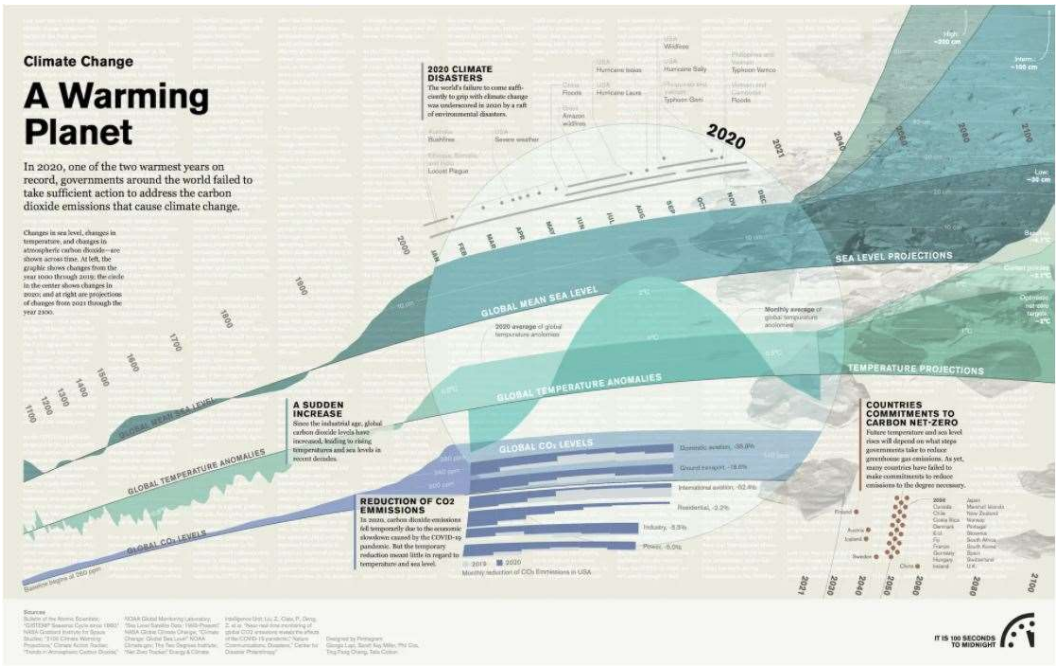
Anexos

Figura 1 – A confiança e a Pandemia.



Fonte: *Bulletin of the Atomic Scientists*, extraído de https://thebulletin.org/doomsday-clock/datavisualizations/ (consultado em 10 de fevereiro de 2024).

Figura 2 – Um planeta em aquecimento.

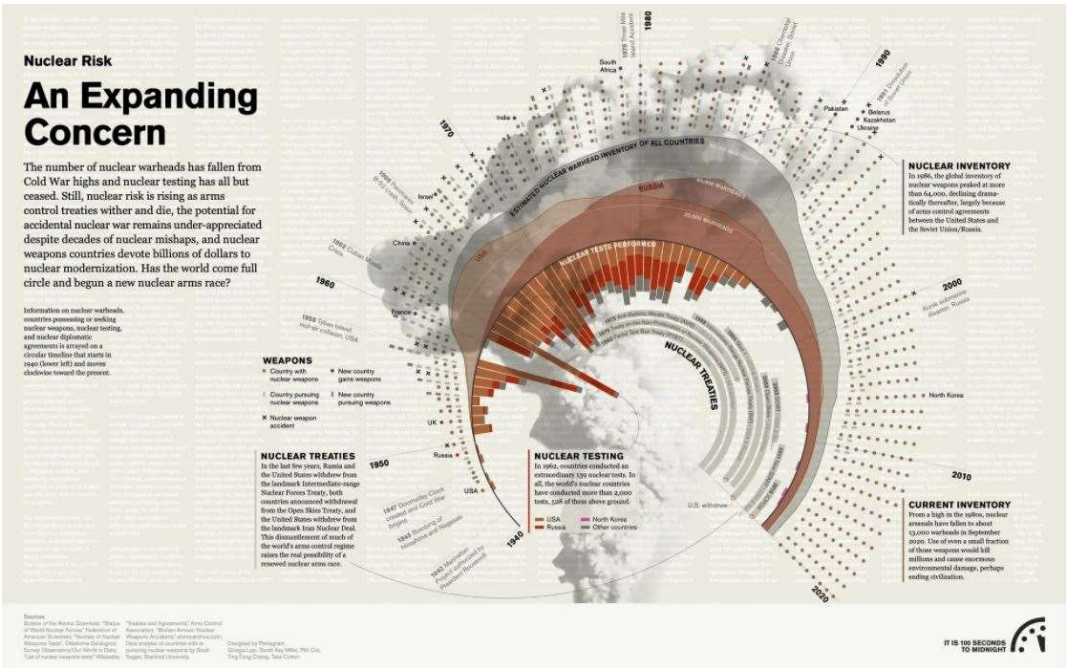


Fonte: *Bulletin of the Atomic Scientists*, extraído de https://thebulletin.org/doomsday-clock/datavisualizations/ (consultado em 10 de fevereiro de 2024).

Figura 3 – Os grandes desafios do próximo decénio.

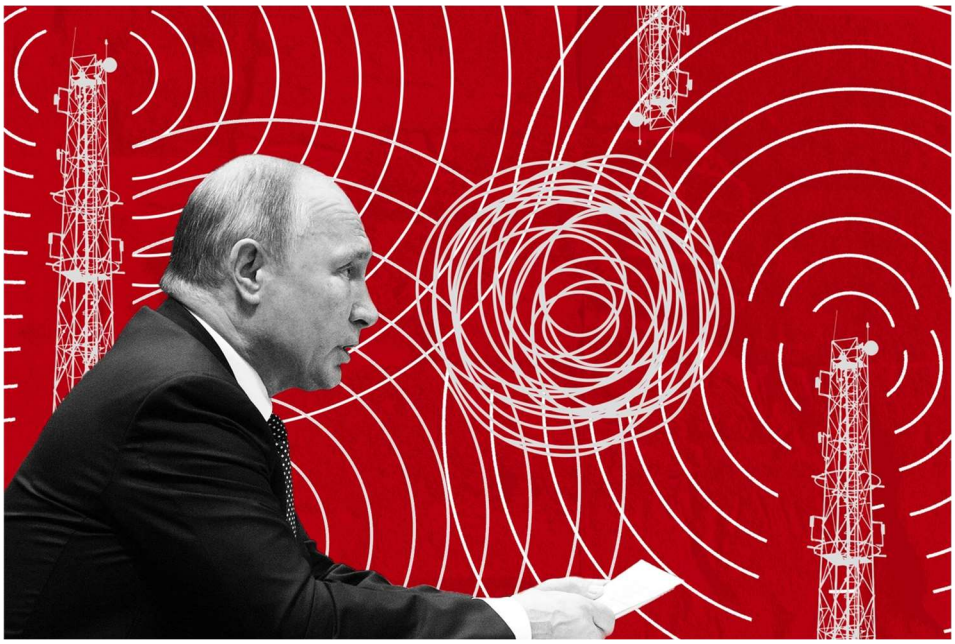
Fonte: *Statista*, extraído de https://www.statista.com/chart/29197/the-most-severe-global-risks-over-the-next-2-and-10-years/ (consultado em 23 de janeiro de 2024).

Figura 4 – A expansão dos riscos nucleares.



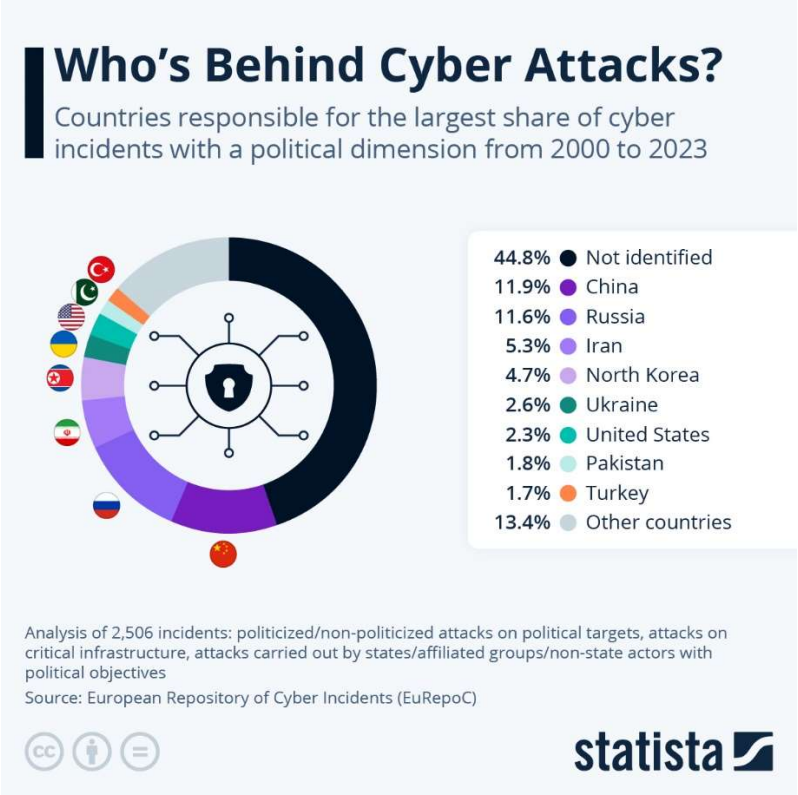
Fonte: *Bulletin of the Atomic Scientists*, extraído de https://thebulletin.org/doomsday-clock/datavisualizations/ (consultado em 10 de fevereiro de 2024).

Figura 5 – A infodemia de Putin.



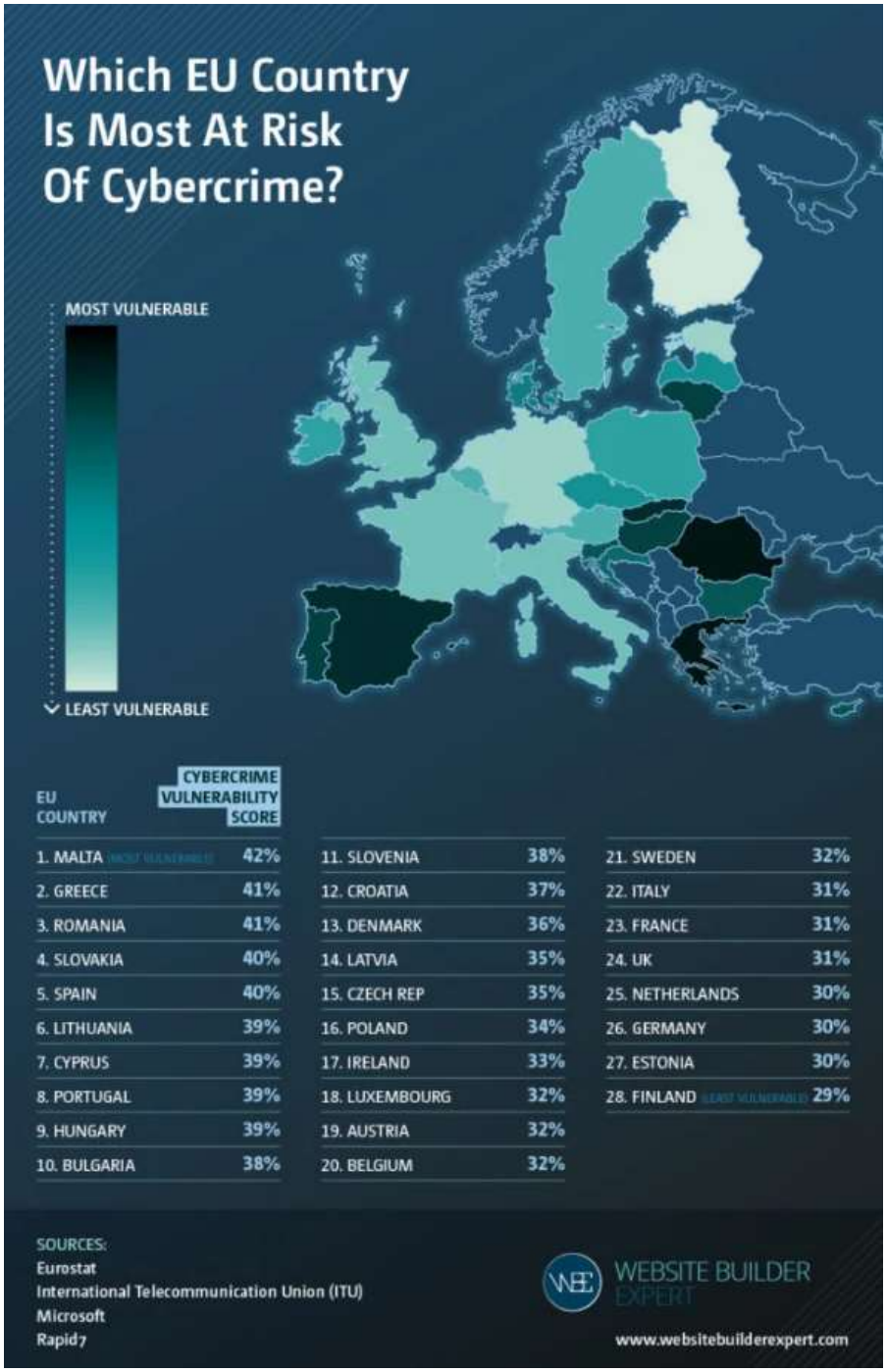
Fonte: *Politico*, extraído de https://www.politico.com/news/magazine/2022/03/22/putin-disinformation-apathy-00018974 (consultado em 15 de maio de 2024).

Figura 6 – Países responsáveis por ciberataques e outros incidentes conexos.



Fonte: *Statista*, extraído de https://cdn.statcdn.com/Infographic/images/normal/31805.jpeg (consultado em 15 de agosto de 2024).

Figura 7 – Países europeus mais vulneráveis ao cibercrime.



Fonte: *Website Builder Expert*, extraído de https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/ (consultado em 12 de agosto de 2024).