

2.º CICLO DE ESTUDOS

MESTRADO EM DIREITO, CIÊNCIAS JURÍDICO-POLÍTICAS

**A influência das redes sociais na política e a
regulamentação da União Europeia**

Pedro Daniel Pereira Vaz

M

2025



FACULDADE DE DIREITO

Dissertação apresenta à Faculdade de
Direito da Universidade do Porto para
obtenção do grau de mestre em Direito, na
menção de ciências Jurídico-Políticas sob a
orientação da científica da Senhora
Professora Doutora Maria da Graça
Jerónima Enes Ferreira

Agradecimentos

Chegar até aqui foi tudo menos um caminho solitário.

À minha orientadora, Professora Doutora **Graça Enes**, agradeço profundamente pela orientação exigente pela confiança que manteve mesmo em momentos que poderia não merecer.

Aos meus **pais**, este momento é, acima de tudo, vosso. Tudo o que sou, tudo o que alcancei, começa convosco. Ensinarão-me, com o exemplo, o que significa lutar com dignidade, viver com honestidade e amar sem condições. Sei que muitas vezes não vos digo isto em voz alta, mas nunca esqueço tudo o que fizeram – e continuam a fazer – por mim. Se hoje estou aqui, é porque vocês sempre estiveram aí

Ao meu **irmão**, és, de todas as certezas que tenho na vida, uma das mais seguras. A tua presença constante, o teu apoio discreto, a tua amizade incondicional, tornaram-me o Homem que sou hoje. Crescer contigo tornou tudo mais leve, mais verdadeiro, mais seguro.

Ao meu **afilhado**, que é, de tantas formas, a promessa do que há de vir. Talvez um dia leias isto, talvez não – mas ficam aqui para ti. Num tempo em que tantas coisas parecem frágeis, a tua existência dá sentido à necessidade de lutar por um futuro mais justo, mais livre, mais verdadeiro. No entanto, até lá, deixo-te estas palavras da canção *Father and Son*, de Yusuf/Cat Stevens: *“You're still young, that's your fault There's so much you have to know ... Look at me, I am old but I'm happy ... take your time, think a lot, think of everything you've got”*.

À **Rita**, obrigado por tudo o que foste ao longo deste percurso. És presença, és abrigo, és horizonte, és a família por opção. Obrigado por seres tanto. Esta etapa, como tantas outras na minha vida, tornou-se mais leve, mais verdadeira e mais feliz porque a vivi contigo. Não sei como teria atravessado este caminho sem ti – e, na verdade, não queria tê-lo feito de outra forma.

E aos **demais amigos e familiares**, pela presença discreta, mas sentida, deixo uma palavra de profunda gratidão.

Resumo

A ascensão das redes sociais digitais transformou profundamente o ecossistema político contemporâneo, reconfigurando as dinâmicas de comunicação, mobilização e influência no espaço público europeu. A capacidade de disseminação massiva e instantânea de informação, aliada à arquitetura algorítmica opaca destas plataformas, tornou-as simultaneamente espaços de participação democrática e vetores privilegiados de desinformação. Este novo cenário comunicacional, amplamente potenciado por interesses políticos, económicos e geoestratégicos, tem colocado desafios sem precedentes à integridade dos processos democráticos, à coesão social e à confiança nas instituições públicas.

Perante esta realidade, a União Europeia tem vindo a construir, de forma progressiva, um quadro normativo que visa equilibrar a proteção da liberdade de expressão com a necessidade de preservar a integridade do espaço informacional. Desde respostas iniciais centradas na autorregulação voluntária – como o Código de Conduta de 2018 – até à adoção de instrumentos jurídicos vinculativos – com destaque para o Regulamento dos Serviços Digitais e a sua articulação, ao abrigo do artigo 45.º, com o Código de Conduta Reforçado de 2022 –, a trajetória europeia revela uma crescente sofisticação institucional na abordagem ao fenómeno da desinformação.

A presente dissertação, analisa criticamente essa evolução, examinando os principais instrumentos normativos, os seus desafios operacionais e os riscos para os direitos fundamentais. A investigação enfatiza ainda a tensão entre moderação de conteúdos e liberdade de expressão, o papel das grandes plataformas digitais na conformidade regulatória e os limites práticos da governança digital no contexto europeu. Através desta análise, procura-se compreender em que medida a União Europeia está a conseguir estruturar uma resposta eficaz, coerente e proporcional à complexidade das ameaças híbridas no ambiente informacional digital da atualidade.

Palavras-Chave: Desinformação; Redes Sociais; Regulamentação da União Europeia; Código de Conduta sobre Desinformação

Abstract

The rise of digital social media has profoundly transformed the contemporary political ecosystem, reshaping the dynamics of communication, mobilization, and influence within the European public sphere. The capacity for massive and instantaneous dissemination of information, combined with the opaque algorithmic architecture of these platforms, has rendered them simultaneously spaces for democratic participation and privileged vectors of disinformation. This new communicational landscape – widely leveraged by political, economic, and geostrategic interests – has posed unprecedented challenges to the integrity of democratic processes, social cohesion, and public trust in institutions.

Faced with this reality, the European Union has progressively built a regulatory framework aimed at balancing the protection of freedom of expression with the need to preserve the integrity of the informational space. From early responses centred on voluntary self-regulation – such as the 2018 Code of Practice—to the adoption of binding legal instruments – most notably the Digital Services Act and its articulation, under Article 45, with the Strengthened Code of Practice of 2022—Europe’s trajectory reveals an increasing institutional sophistication in addressing the phenomenon of disinformation.

This dissertation critically analyses that evolution, examining the main regulatory instruments, their operational challenges, and the risks they pose to fundamental rights. The research further emphasizes the tension between content moderation and freedom of expression, the role of large digital platforms in regulatory compliance, and the practical limitations of digital governance in the European context. Through this analysis, the study seeks to understand to what extent the European Union is managing to structure an effective, coherent, and proportionate response to the complexity of hybrid threats in today’s digital informational environment.

Key-Words: Disinformation; Social Media; European Union Regulation; Code of Conduct on Disinformation

Índice

<i>Introdução</i>	4
<i>Entre o Erro e o Engano: Desinformação, Misinformation, Operações de Influência e Interferência Estrangeira</i>	7
<i>Regulamentação da União Europeia sobre Redes Sociais</i>	11
Evolução Legislativa da UE	14
Código de Conduta para o Combate à Desinformação	26
Compromissos do Código	27
Controlo de colocação de anúncios	28
Propaganda política e publicidade temática	28
Integridade dos Serviços	29
Capacitação dos Consumidores/Utilizadores	30
Capacitação da comunidade de investigação	30
Medição e monitorização da eficácia do código	31
Críticas ao Código de Conduta: Liberdade de Expressão e Limitações Estruturais	32
Código Reforçado de 2022: Uma Evolução na Governança Digital da UE	35
The EU Digital Services Package	42
<i>Críticas ao Regulamento dos Serviços Digitais (DSA): Limites, Ambiguidades e Riscos para os Direitos Fundamentais</i>	45
A ambiguidade terminológica e os riscos de sobreposição	46
A Falta de Harmonização no Mercado Interno: Riscos Sistémicos e Ameaças à Coerência Regulamentar Europeia	49
Obrigações de Diligência Devida: Entre a Proteção e a Censura Algorítmica	51
A Centralização do Poder Político na Governação Digital: Riscos para a Liberdade Informativa	52
O Dilema da Liberdade de Expressão e a Armadilha da Automação Algorítmica: Entre a Censura Preventiva e a Erosão Democrática	54
Conclusão	55
Bibliografia	57

Introdução

A democracia, o Estado de direito e os direitos fundamentais constituem os alicerces estruturantes da União Europeia (CHUNG, 2019), não apenas enquanto valores fundacionais, mas também como critérios essenciais de integração ao projeto europeu (Shehaj, 2015)¹. Estes princípios representam o núcleo identitário do espaço político europeu. Todavia, para que a democracia se manifeste enquanto prática efetiva e concreta, e não meramente proclamada, é imprescindível assegurar condições efetivas para uma participação cívica informada, crítica e plural². Tal só é possível num ambiente em que a liberdade de expressão e a liberdade de informação sejam plenamente respeitadas, em consonância com a Carta dos Direitos Fundamentais da União Europeia (A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation, 2018), e onde todos os atores – cidadãos, jornalistas, académicos e organizações da sociedade civil – possam contribuir, em liberdade, para o debate público (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 COM (2020) 790 final, 2020).

Num cenário político cada vez mais volátil, a democracia europeia enfrenta hoje múltiplas ameaças: a ascensão de discursos extremistas, a intensificação da polarização ideológica, a erosão progressiva da relação de confiança mútua entre eleitores e representantes (Pira, 2023) e, de forma particularmente insidiosa, a manipulação deliberada da informação no espaço público (Casero-Ripollés, Tuñón, & Bouza-García, The European approach to online disinformation: geopolitical and

¹ A democracia, o Estado de direito e os direitos fundamentais constituem os valores fundacionais da União Europeia, conforme consagrado no artigo 2.º do Tratado da União Europeia (TUE), que estabelece que a União assenta no respeito pela dignidade humana, liberdade, democracia, igualdade, Estado de direito e direitos humanos. Estes valores são também condição essencial de adesão à União, nos termos do artigo 49.º do TUE.

² Com vista a promover eleições europeias livres, transparentes e resilientes num contexto digital cada vez mais desafiante, a Comissão Europeia, em colaboração com o Instituto Internacional para a Democracia e a Assistência Eleitoral (International IDEA) e os partidos políticos europeus, adotou o Código de Conduta para as Eleições ao Parlamento Europeu de 2024. Este instrumento voluntário visa reforçar a integridade dos processos eleitorais, combatendo a desinformação, a manipulação através de conteúdos artificiais, o uso abusivo de dados e a interferência externa. Define princípios de transparência, ética no uso de tecnologias como a inteligência artificial e responsabilidade no financiamento e publicidade política. O documento completo encontra-se disponível em: https://commission.europa.eu/document/bebd9b72-fbb9-42f3-bcea-dbae7e0650f_en.

regulatory dissonance, 2023). A integridade dos processos eleitorais (Szakács & Bognár, 2021), a independência da comunicação social e a vitalidade do espaço democrático foram profundamente abaladas por um fenómeno que, embora não seja recente, atingiu proporções alarmantes na era digital – a desinformação³.

Neste contexto de reconfiguração acelerada do ecossistema informacional, o debate em torno da regulamentação do discurso político em ambiente digital ganhou uma importância crescente tanto nas esferas académicas como no plano institucional europeu (Borz, Francesco, Montgomerie, & Bellis, 2024). O crescimento exponencial do investimento partidário em campanhas digitais tem intensificado as exigências por mecanismos regulatórios mais eficazes. Esta necessidade (de regulamentação) tem sido ainda impulsionada por escândalos recentes, nomeadamente a utilização indevida de dados do Facebook pela Cambridge Analytica, com impacto direto no referendo do Brexit, bem como pela urgência de enfrentar o desafio global da interferência estrangeira em processos eleitorais. A emergência das redes sociais como principais canais de circulação de conteúdos e mobilização política transformou radicalmente as dinâmicas democráticas (Asimakopoulos, Antonopoulou, Giotopoulos, & Halkiopoulou, 2025). Assentes numa lógica algorítmica orientada para a maximização da atenção e do lucro (Narayanan, 2023), estas plataformas passaram a desempenhar um papel estratégico na construção – e, por vezes, na manipulação – da opinião pública (McKay & Tenove, 2021). A velocidade com que os conteúdos se propagam, aliada à opacidade na sua origem e à segmentação comportamental do público-alvo – recorrendo a técnicas como o micro direcionamento (Fraga-Kamas & Fernández-Caramés, 2020) – criou condições propícias à proliferação de narrativas falsas ou enganosas, dificultando a formação de uma vontade política verdadeiramente

³ Embora a desinformação seja frequentemente vista como um fenómeno contemporâneo associado ao ambiente digital, a sua existência remonta aos primórdios da história humana, tendo sido usada como instrumento estratégico de manipulação da perceção pública desde a Antiguidade. A emergência moderna do termo é frequentemente associada ao departamento soviético do KGB responsável pela chamada “propaganda negra” durante a Guerra Fria, onde a ocultação da origem da informação era uma técnica central. Exemplos notórios incluem campanhas fabricadas sobre a origem do vírus da SIDA e a alegada participação soviética na tentativa de assassinato do Papa João Paulo II – ambos amplamente difundidos antes da era digital. A desinformação distingue-se da propaganda tradicional por envolver a participação ativa dos recetores na disseminação de conteúdos falsos ou enganosos, o que a torna particularmente difícil de conter no ecossistema atual dominado pelas redes sociais. Como nota (O'SHAUGHNESSY, 2020), a desinformação nem sempre se baseia em mentiras absolutas, mas frequentemente em meias-verdades, o que lhe confere maior poder de penetração. Com a ascensão dos media digitais e das plataformas sociais, o fenómeno ganhou uma nova escala e complexidade, transformando-se num dos maiores desafios à integridade do debate democrático na atualidade (Ribeiro, 2021)

autónoma, livre e esclarecida (Romanishyn, 2024). As campanhas eleitorais já não se limitam aos meios tradicionais – decorrem agora, em grande medida, nas plataformas digitais (Contucci, Omicini, Pianini, & Sîrbu, 2019), o que, por um lado, abre novas possibilidades de participação, nomeadamente para os mais jovens (Asimakopoulos, Antonopoulou, Giotopoulos, & Halkiopoulos, 2025), mas, por outro, expõe os cidadãos a novos riscos de manipulação informacional (Woolley, 2022). É neste contexto de profundas reconfigurações da “arena” pública que se impõe refletir criticamente sobre a resposta da União Europeia à crescente influência das plataformas digitais nos processos democráticos.

A presente dissertação propõe-se, assim, analisar os principais instrumentos adotados pela UE com vista à regulamentação do ecossistema digital, com especial destaque para as estratégias desenvolvidas no combate à desinformação. Com o propósito de promover uma compreensão crítica e aprofundada do papel da União Europeia na regulamentação do ecossistema digital e na resposta ao fenómeno da desinformação, a presente dissertação organiza-se de forma progressiva, acompanhando a evolução dos instrumentos normativos e das estratégias políticas adotadas neste domínio. Numa primeira etapa, procede-se à delimitação conceptual dos termos desinformação, misinformation, operações de influência e interferência estrangeira. Posteriormente, será analisado o enquadramento jurídico e político da União Europeia, com especial atenção à sua trajetória evolutiva. No centro desta análise encontra-se o Código de Conduta para o Combate à Desinformação, concebido como um mecanismo de autorregulação em articulação com as principais plataformas digitais, visando conter a disseminação da desinformação. Será ainda analisado os seus compromissos, bem como as principais críticas que lhe foram dirigidas, nomeadamente quanto à sua eficácia, à transparência das métricas e os riscos que coloca à liberdade de expressão. A dissertação prosseguirá com a análise do Código Reforçado de 2022, enquanto tentativa de colmatar essas fragilidades, através de um reforço dos instrumentos de responsabilização, da cooperação institucional e do acompanhamento independente. A esta análise soma-se a reflexão em torno do Digital Services Act Package – que integra o Digital Services Act (DSA)⁴ e o Digital Markets Act (DMA)⁵ – enquanto pilares fundamentais da nova

⁴ O Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento

arquitetura regulatória das plataformas digitais. A articulação entre o Código e o Regulamento dos Serviços Digitais revela de forma clara a opção estratégica da União Europeia por um modelo de resposta “co-regulativa”, assente na lógica da responsabilização partilhada entre atores públicos e privados (Kachelmann & Reiners, 2023).

Entre o Erro e o Engano: Desinformação, Misinformation, Operações de Influência e Interferência Estrangeira

Neste novo ecossistema digital, a desinformação configura-se como uma ameaça estrutural à “saúde” das democracias (Kachelmann & Reiners, 2023) (Pamment, *The EU’s Role in Fighting Disinformation: Crafting A Disinformation Framework.*, 2020b). A sua difusão acelerada através das plataformas digitais colocou em evidência a necessidade urgente de compreender, de forma clara e diferenciada, os fenómenos que compõem o espectro mais amplo da manipulação informacional.

Para efeitos desta dissertação, adota-se a definição de **desinformação** acolhida pela União Europeia⁶ na sua (Europeia, 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 COM(2018) 236 final, 2018), onde esta é entendida como “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”. A mesma definição é

dos Serviços Digitais – Digital Services Act), pode ser consultado em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065>.

⁵ O Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais – Digital Markets Act), encontra-se disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925>.

⁶ Cumpre salientar que a própria Comissão Europeia percorreu um processo de maturação conceptual neste domínio. As primeiras respostas institucionais centravam-se no combate às denominadas fake news, como atesta a criação de um grupo de peritos de alto nível em 2017 (Commission, 2017). Foi apenas, em 2018, que a terminologia oficial passou a privilegiar o conceito de desinformação, mais preciso e operacional do ponto de vista jurídico e político (European Commission, 2018). Sendo entendida como um fenómeno que transcende a mera noção de “notícias falsas” (fake news). A definição europeia passou, assim, a distinguir cuidadosamente entre conteúdos ilícitos (como o discurso de ódio ou a difamação) e de outras distorções deliberadas, mas não enganosas, como a sátira ou a paródia (Directorate-General for Communications Networks, 2018).

reproduzida no Plano de Ação contra a Desinformação (JOIN (2018) 36 final) e no Código de Conduta contra a Desinformação (CoP)⁷ apresentada com pequenas diferenças no relatório (A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation., 2018, p. 3), aparecendo como: todas as formas de informações falsas, imprecisas ou enganosas concebidas, apresentadas e promovidas para causar intencionalmente danos públicos ou com fins lucrativos” (Santos & Lapa, 2022). Contudo, apesar da sua utilidade operacional, esta definição enfrenta importantes desafios conceptuais, nomeadamente no que se refere à delimitação entre desinformação e outros fenómenos conexos⁸ (Pamment, The EU’s Role in Fighting Disinformation: Taking Back the Initiative, 2020). O atual panorama informacional, caracterizado pela rápida circulação de conteúdos através de plataformas digitais, impõe à União Europeia o imperativo de distinguir e compreender, com rigor, as nuances entre os conceitos de misinformation⁹, desinformação, operações de influência e interferência estrangeira. Apesar de frequentemente utilizados de forma indistinta, estes termos possuem implicações distintas – tanto teóricas como práticas – que influenciam diretamente a formulação de políticas públicas eficazes.

Assim, importa, antes de mais, proceder à delimitação conceptual do fenómeno da **misinformation**, entendido como a partilha de informação falsa ou imprecisa desprovida de intenção deliberada de enganar (Kachelmann & Reiners, 2023). Trata-se, regra geral, de conteúdos que resultam de erros factuais,

⁷ O Código de Conduta contra a Desinformação, adotado pela primeira vez em 2018, encontra-se disponível no portal oficial da Comissão Europeia: <https://digital-strategy.ec.europa.eu/pt/library/2018-code-practice-disinformation>. A versão reforçada deste instrumento, revista em 2022, pode ser consultada em: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.

⁸ As empresas também recorrem a terminologias distintas de desinformação. No âmbito dos relatórios apresentados no contexto do Code of Practice on Disinformation, o Facebook recorreu ao conceito de comportamento inautêntico coordenado para designar campanhas organizadas que dissimulam a verdadeira identidade dos seus promotores (Facebook, 2019). A Google, por sua vez, adota terminologias como operações de influência e deturpação da identidade, evidenciando uma preocupação específica com práticas que visam distorcer a autenticidade da comunicação política (Google, 2019). Já o Twitter utiliza expressões como automação maliciosa, atividades inautênticas e operações informacionais, dando especial relevo ao papel dos bots, da desinformação automatizada e da instrumentalização do debate público (Twitter, 2019). Paralelamente, também os Estados-Membros da União Europeia adotam terminologias próprias, algumas das quais servem de base aos seus quadros legislativos nacionais, contribuindo para a heterogeneidade normativa no combate à desinformação no espaço europeu.

⁹ Optou-se por preservar o termo “misinformation” na sua forma original em inglês, por se tratar de uma expressão tecnicamente consolidada na literatura especializada e nas instituições europeias, cuja tradução direta para português não capta, com suficiente precisão, a especificidade do conceito.

interpretações errôneas ou da difusão de informação desatualizada ou não verificada (Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework., 2020b). Ao contrário da desinformação, a misinformation não assenta na manipulação intencional da realidade, mas sim na propagação involuntária de inverdades, frequentemente motivada pela confiança genuína na veracidade do conteúdo por parte do emissor¹⁰ (Jayakumar, Ang, & Anwar, 2020).

As **operações de influência** configuram-se como iniciativas estrategicamente coordenadas, orientadas para a moldagem da opinião pública, da conduta social ou dos próprios processos de tomada de decisão política (Tan, 2022). Tal como descritas por Pamment consistem em esforços coordenados para influenciar um público-alvo, utilizando um conjunto de meios ilegítimos e enganosos, em apoio aos objetivos de um adversário (Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework., 2020b). Estas operações assentam numa lógica de ação multidimensional, combinando instrumentos comunicacionais subtis e sofisticados, que vão desde a difusão seletiva de conteúdos verdadeiros e falsos até ao recurso a técnicas de propaganda, guerra psicológica e manipulação algorítmica nas redes sociais (A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation, 2018). A desinformação, neste contexto, surge não apenas como um componente recorrente, mas como elemento estruturante das operações de influência. No entanto, importa sublinhar que estas operações transcendem a mera disseminação de falsidades, englobando um conjunto mais amplo e articulado de práticas orientadas para a concretização de objetivos estratégicos precisos, frequentemente de natureza geopolítica, ideológica ou securitária. Trata-se, assim, de intervenções que visam desestabilizar sistemas democráticos, explorar clivagens internas e minar a confiança nas instituições (Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, 2020).

¹⁰ Uma intervenção legislativa de grande escala por parte da União Europeia relativamente ao fenómeno da misinformation revela-se, à luz dos riscos inerentes à restrição desproporcionada da liberdade de expressão, não apenas improvável, mas também juridicamente controversa (Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, 2020). No entanto, as plataformas digitais têm vindo a desenvolver políticas próprias para combater, em larga escala, a disseminação de conteúdos falsos ou enganosos, no âmbito dos respetivos termos de serviço. Nesse sentido, a UE deverá privilegiar uma abordagem não regulatória, promovendo um diálogo estruturado com essas plataformas, designadamente para estabelecer princípios orientadores que alinhem os seus termos de serviço com os direitos e liberdades fundamentais (Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework., 2020b).

Já a **interferência estrangeira** deve ser entendida como um conjunto de ações deliberadas empreendidas por Estados terceiros – ou pelos seus agentes – com o propósito de condicionar, manipular ou perturbar os assuntos internos de outro país soberano. Esta interferência pode assumir múltiplas formas, entre as quais se destacam-se, novamente, as campanhas de desinformação, os ciberataques dirigidos a infraestruturas críticas, a manipulação de processos eleitorais e o apoio a grupos extremistas que visam desestabilizar a ordem constitucional vigente (Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, 2020). Longe de se manifestar de forma isolada, a interferência estrangeira integra frequentemente operações de influência estrategicamente concebidas, funcionando como instrumento de projeção geopolítica e erosão democrática. O seu objetivo último não se esgota na criação de caos imediato, mas reside na fragilização progressiva da confiança pública nas instituições, na promoção de divisões internas e, sobretudo, no avanço silencioso dos interesses da potência interveniente. Trata-se, portanto, de uma ameaça difusa, persistente e adaptativa, cuja natureza híbrida exige respostas articuladas à altura da sofisticação dos métodos utilizados.

O reconhecimento por parte da União Europeia de que tem sido alvo de campanhas de desinformação dirigidas, em particular, a contextos eleitorais e políticos, reforça a urgência de desenhar respostas articuladas e diferenciadas¹¹. Compreender estas distinções conceptuais não constitui apenas um exercício de precisão teórica, trata-se de um imperativo estratégico com implicações diretas na conceção de medidas eficazes e proporcionais. Cada um destes fenómenos requer uma abordagem específica. A *misinformation* pode ser mitigada através da promoção da literacia mediática e digital, incentivando o pensamento crítico e a capacidade dos cidadãos para reconhecerem conteúdos potencialmente enganosos. Já a desinformação, pela sua natureza dolosa, exige uma resposta mais firme, incluindo a identificação e exposição de narrativas falsas, a colaboração com plataformas digitais para a sua remoção, e a aplicação de sanções a agentes que deliberadamente

¹¹ Por exemplo, a França tem sido recentemente alvo de uma campanha de desinformação sem precedentes, atribuída a redes de influência ligadas à Rússia, segundo concluiu uma investigação da secção de desinformação do Ministério das Forças Armadas francês. Ver: *Observador*, “França está a ser alvo de campanha de desinformação sem precedentes”, 18 de julho de 2025, disponível em: <https://observador.pt/2025/07/18/franca-esta-a-ser-alvo-de-campanha-de-desinformacao-sem-precendentes>.

promovam esse tipo de conteúdo¹². A distinção entre estes conceitos permite à União Europeia desenhar estratégias de comunicação e intervenção mais eficazes, sem abdicar dos princípios fundamentais da liberdade de expressão e do pluralismo democrático¹³.

Apesar das medidas já em curso – que incluem campanhas de sensibilização, programas de literacia digital, colaboração com plataformas tecnológicas e mecanismos de verificação de factos – a complexidade e sofisticação crescente das ameaças digitais têm colocado sob enorme tensão os instrumentos tradicionais de regulação e vigilância democrática (Neudert, 2020). Os mecanismos de financiamento das campanhas políticas, a proteção das infraestruturas eleitorais contra ciberataques, a salvaguarda da liberdade de imprensa e a responsabilização das plataformas digitais tornaram-se desafios centrais para a preservação de um espaço público democrático (Tenove, Buffie, McKay, & Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy*, 2018)¹⁴.

Regulamentação da União Europeia sobre Redes Sociais

¹² Distinguir entre operações de influência e interferência estrangeira é igualmente essencial, na medida em que permite identificar os autores das campanhas e adotar medidas adequadas, como sanções diplomáticas, ações judiciais ou mecanismos de pressão internacional.

¹³ Importa sublinhar que o direito à liberdade de expressão não se limita à proteção de opiniões amplamente aceites ou consideradas inofensivas. Pelo contrário, abrange igualmente as ideias e informações que possam ofender, chocar ou perturbar o Estado ou determinados sectores da população – tal como afirmado pelo Tribunal Europeu dos Direitos Humanos no emblemático acórdão *Handyside v. Reino Unido* (Kuczerawy, 2019). Ao definir com clareza os limites da desinformação, a União Europeia pode salvaguardar a liberdade de expressão, evitando práticas que possam ser interpretadas como censura e protegendo o direito dos cidadãos a exprimirem opiniões mesmo quando estas são controversas ou impopulares (Espaliú-Berdud, 2023).

¹⁴ A evolução recente do panorama político ilustra com particular clareza os riscos associados à desinformação em contextos eleitorais. De acordo com dados divulgados, entre as eleições europeias de 2024 e as legislativas nacionais (portuguesas) de 2025 verificou-se um aumento de 160% na disseminação de conteúdos desinformativos em Portugal. Estes dados sublinham a crescente instrumentalização das plataformas digitais para fins de manipulação política e demonstram a urgência de medidas regulatórias mais eficazes. Cfr. *Comunidade Cultura e Arte*, “Desinformação aumentou 160% entre as eleições europeias de 2024 e legislativas de 2025”, 17 de julho de 2025, disponível em: <https://comunidadeculturaearte.com/desinformacao-aumentou-160-entre-as-eleicoes-europeias-de-2024-e-legislativas-de-2025/>; *SIC Notícias*, “Chega foi o partido que mais divulgou desinformação nas legislativas, revela estudo”, 18 de julho de 2025 disponível em <https://sicnoticias.pt/pais/2025-07-18-chega-foi-o-partido-que-mais-divulgou-desinformacao-nas-legislativas-revela-estudo-3c6257ac>; *Público*, “Desinformação aumenta em Portugal e Chega contribui como principal fonte”, 29 de maio de 2025, disponível em: <https://www.publico.pt/2025/05/29/politica/noticia/desinformacao-aumenta-portugal-chega-partido-contribui-2134783>

Nas últimas décadas, as redes sociais emergiram como protagonistas centrais na arquitetura da esfera pública, revolucionando os paradigmas tradicionais de produção, difusão e consumo de informação em toda a União Europeia¹⁵. Esta metamorfose estrutural do ecossistema comunicacional – embora portadora de inegáveis oportunidades no que respeita à participação cívica, ao pluralismo e à inclusão digital – expôs, igualmente, fragilidades estruturais que hoje se manifestam de forma particularmente preocupante com a proliferação de conteúdos falsos, manipuladores ou enganosos¹⁶. Este fenómeno, insidioso por natureza e frequentemente orquestrado com intenções políticas, económicas ou geoestratégicas¹⁷, constitui uma ameaça real à integridade dos processos democráticos, corroendo a confiança nas instituições, distorcendo o debate público e fomentando a polarização social¹⁸. A sua propagação é facilitada pela exploração de falhas algorítmicas e, em parte, pela tendência humana para partilhar conteúdos sensacionalistas ou carregados de emoção (Schlag, 2023). A este cenário complexo junta-se o desenvolvimento

¹⁵ Conforme sublinhado pelo Tribunal Europeu dos Direitos Humanos no acórdão Yildirim, “a Internet tornou-se, atualmente, um dos principais meios através dos quais os indivíduos exercem o seu direito à liberdade de expressão e de informação, constituindo uma ferramenta essencial para a participação em atividades e debates relativos a questões políticas e a temas de interesse geral”.

¹⁶ Como advertiram (Kachelmann & Reiners, 2023, p. 35), “as maiores vagas de desinformação ainda estão por vir; por conseguinte, o modo como forem concebidas e aplicadas as estratégias de combate à desinformação online determinará, em larga medida, o próprio futuro da democracia”.

¹⁷ Nas últimas décadas, a desinformação consolidou-se como um instrumento geopolítico de elevado impacto, utilizado por atores estatais e não estatais com o propósito de desestabilizar instituições democráticas em Estados percecionados como adversários estratégicos ou rivais ideológicos, promovendo, em paralelo, agendas de influência que visam reforçar a sua projeção internacional e desafiar a ordem democrática global (Casero-Ripollés, Tuñón, & Bouza-García, *The European approach to online disinformation: geopolitical and regulatory dissonance*, 2023) (Hinš, 2021). Diversas análises identificam a Rússia e a China como protagonistas centrais neste campo, recorrendo a sofisticadas operações informacionais para minar a coesão interna da União Europeia e comprometer a sua credibilidade internacional (Legucka, 2020) (Belga, 2025) (Nagasako, 2020). A Federação Russa, em particular, recorre a uma rede complexa e coordenada de agentes estatais e paraestatais, incluindo meios de comunicação como a RT e a Sputnik (Rodrigues, 2024), utilizadas como veículos de disseminação sistemática de narrativas alinhadas com os seus objetivos geopolíticos. Um exemplo emblemático desta estratégia é a operação de desinformação conhecida como Doppelganger, através da qual são criados sites falsos que imitam graficamente meios de comunicação ocidentais credíveis, com o objetivo de disseminar conteúdos manipuladores e minar a credibilidade da imprensa livre. Esta campanha procura reforçar a narrativa do Kremlin, sobretudo visando enfraquecer o apoio ocidental à Ucrânia, e estrutura-se em torno de quatro eixos temáticos: (i) a alegada ineficácia das sanções impostas à Rússia; (ii) a suposta russofobia generalizada no Ocidente; (iii) a caracterização do exército ucraniano como bárbaro e composto por elementos neo-nazis; e (iv) a apresentação dos refugiados ucranianos como um fardo para os países europeus (What is the Doppelganger operation? List of resources, 2025).

¹⁸ Segundo o Eurobarómetro Flash n.º 522 (2023), dedicado à perceção dos cidadãos europeus sobre a democracia, 43 % dos inquiridos consideraram que a propaganda e/ou a disseminação de informações falsas ou enganosas por parte de fontes estrangeiras não democráticas, bem como a ingerência externa dissimulada na política e na economia do seu país, representam uma das mais graves ameaças à democracia. O relatório completo encontra-se disponível em: <https://europa.eu/eurobarometer/surveys/detail/2966>.

acelerado – e ainda amplamente não regulado¹⁹ - de tecnologias de inteligência artificial, como o ChatGPT e outras ferramentas generativas (Spitale, Biller-Andorno, & Germani, 2023)²⁰.

Neste novo contexto, a eficácia das medidas adotadas – tanto na prevenção como na mitigação dos efeitos da desinformação – tornar-se-ão, assim, determinantes para a preservação dos valores democráticos numa escala verdadeiramente global. Consciente da natureza transversal e transnacional desta ameaça, a União Europeia tem vindo a intensificar os seus esforços normativos, delineando um enquadramento jurídico e político que visa proteger o espaço digital europeu. O percurso da União Europeia no combate à desinformação não se traduziu numa resposta linear nem imediata. Pelo contrário, trata-se de um processo evolutivo, marcado por fases sucessivas de aprendizagem institucional, que foi sendo moldado por crises políticas e mediáticas cada vez mais sofisticadas. Longe de se tratar de uma resposta imediata ou linear, a evolução da UE nesta matéria traduz um processo de aprendizagem institucional que partiu de medidas essencialmente reativas e assentes na comunicação estratégica, até alcançar um enquadramento jurídico mais estruturado e ambicioso. Esta trajetória revela não apenas uma adaptação às novas dinâmicas

¹⁹ Apesar de se afirmar que o desenvolvimento da inteligência artificial decorre num contexto ainda amplamente não regulado, importa reconhecer que a União Europeia deu passos significativos no sentido da criação de um quadro normativo específico. Em junho de 2024, foi adotado o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, que estabelece regras harmonizadas em matéria de inteligência artificial, instituindo o primeiro regime jurídico abrangente para a IA no espaço europeu. Este diploma, conhecido como *Regulamento da Inteligência Artificial*, visa garantir que os sistemas de IA sejam seguros, transparentes, éticos e respeitadores dos direitos fundamentais. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>. Paralelamente, a Comissão Europeia promoveu o Código de Conduta para a Inteligência Artificial de Finalidade Geral, um instrumento de soft law que visa orientar os desenvolvimentos técnicos mais avançados no setor, em articulação com os princípios do Regulamento. Disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/contents-code-gpai>. No entanto, a sua eficácia enfrenta desafios relevantes, desde logo pela recusa de grandes plataformas – como a Meta – em subscrevê-lo. (ver: *ECO – Economia Online*, “Meta recusa assinar novo código de conduta para IA na Europa”, 18 de julho de 2025, disponível em: <https://eco.sapo.pt/2025/07/18/meta-recusa-assinar-novo-codigo-de-conduta-para-ia-na-europa/>).

²⁰ Um exemplo recente desta evolução tecnológica é o modelo Veo 3, desenvolvido pela Google, que permite a geração de vídeos com elevado realismo visual, ao ponto de se tornarem praticamente indistinguíveis de gravações autênticas. Estas capacidades aumentam exponencialmente o risco de proliferação de conteúdos manipulados, nomeadamente deepfakes, reforçando a complexidade do fenómeno da desinformação no espaço digital contemporâneo. O potencial impacto destas ferramentas na erosão da confiança pública e na manipulação de perceções coletivas tem vindo a suscitar crescente preocupação entre especialistas, reguladores e académicos, que alertam para a necessidade urgente de desenvolver mecanismos éticos, legais e técnicos de contenção e verificação. Para mais detalhes, ver: Google DeepMind, “Veo: A model for video generation,” 2024. Disponível em: <https://deepmind.google/technologies/veo>.

tecnológicas, mas também uma afirmação da desinformação como um desafio transversal à integridade democrática, à segurança coletiva e à coesão social europeia.

Evolução Legislativa da UE

A União Europeia tem vindo a posicionar-se como um dos principais atores globais na resposta institucional à desinformação²¹, assumindo progressivamente uma posição de vanguarda na construção de um enquadramento normativo e estratégico para a proteção do seu espaço digital. A sua atuação teve início no ano de 2015, quando o Conselho Europeu reconheceu formalmente o impacto das campanhas de desinformação russas no espaço europeu, particularmente após a anexação da Crimeia (Europeu C. , 2015)²². Nesse contexto, foi solicitado à Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança que desenvolvesse um plano de ação contra as ameaças híbridas (Europeia, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia JOIN (2016) 18 final, 2018), culminando na criação da East StratCom Task Force (ESTF) (no âmbito do Serviço Europeu para a Ação Externa (SEAE))^{23 24} (Pamment, *The EU's Role in Fighting Disinformation: Taking Back the Initiative*, 2020). O projeto emblemático do ESTF é o EUvsDisinfo. Tratou-se, inicialmente, de uma plataforma concebida para identificar, analisar e contrariar campanhas de desinformação, com especial enfoque

²¹ Apesar de a União Europeia se posicionar como uma das protagonistas globais na resposta institucional à desinformação, importa reconhecer que outros Estados democráticos têm igualmente desenvolvido estratégias ambiciosas e multifacetadas neste domínio. O Brasil destaca-se particularmente pelo conjunto de iniciativas legislativas, judiciais e institucionais implementadas nos últimos anos.

²² Na Reunião do Conselho Europeu (19 e 20 de março de 2015) – Conclusões: “O Conselho Europeu salientou a necessidade de reagir às atuais campanhas de desinformação lançadas pela Rússia e convidou a Alta Representante a preparar até junho, em cooperação com os Estados-Membros e as instituições da UE, um plano de ação para uma comunicação estratégica. A criação de uma equipa de comunicação constitui um primeiro passo nesse sentido.” (Europeu C. , 2015)

²³ O Serviço Europeu para a Ação Externa (SEAE) é o corpo diplomático da União Europeia, responsável por implementar a Política Externa e de Segurança Comum (PESC), coordenando a ação externa da UE em articulação com os Estados-Membros e outras instituições europeias. Para mais informações, consultar: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-external-action-service-eeas_pt.

²⁴ Inicialmente dependente de doações, a ESTF começou a receber financiamento do orçamento da UE em 2018. Entre as principais atividades da East StratCom Task Force (ESTF) destaca-se a conceção e implementação de campanhas de comunicação estratégica, bem como a produção semanal da EUvsDisinfo Disinformation Review – uma publicação que identifica e analisa narrativas desinformativas disseminadas no espaço europeu, disponível em <https://euvdisinfo.eu/disinformation-review/>. A ESTF tem ainda desenvolvido ações de formação dirigidas a instituições da União Europeia, Estados-Membros, jornalistas e organizações da sociedade civil.

nas narrativas promovidas por fontes pró-Kremlin. Através da construção de uma base de dados pública que compila exemplos de desinformação, bem como da publicação semanal da Disinformation Review, visa não apenas desmascarar conteúdos enganosos, mas também promover uma cidadania informada e resiliente às dinâmicas de manipulação informativa. Paralelamente, esta iniciativa contribui para o reforço da literacia mediática enquanto instrumento central da defesa democrática europeia, inscrevendo-se plenamente na estratégia mais alargada da UE para a salvaguarda do seu ecossistema digital e informacional. A constituição do ESTF, antes de qualquer iniciativa legislativa, demonstra o reconhecimento (precoce) da desinformação como uma ameaça estratégica e geopolítica – sobretudo na sua vertente externa, protagonizada por Estados terceiros (CARVALHO, et al., 2021). Esta resposta inicial centrou-se na construção de contra narrativas e na sensibilização pública, em vez de uma regulação direta das plataformas.

Em 2016, a UE reforçou a sua estratégia de segurança com o documento (Europeia, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia JOIN (2016) 18 final, 2016). Este documento/quadro definiu as ameaças híbridas como uma combinação sofisticada de atividades coercivas e subversivas, recorrendo a métodos tanto convencionais como não convencionais – incluindo instrumentos diplomáticos, militares, económicos e tecnológicos – utilizados de forma coordenada por atores estatais e não estatais com o intuito deliberado de desestabilizar os Estados e interferir nos seus processos políticos, sociais e económicos.

No mesmo ano, e no contexto de reforço da resiliência digital europeia – reconhecendo que a propagação de discursos de ódio e de conteúdos extremistas online constitui uma das formas mais insidiosas de desestabilização social e política – a Comissão Europeia lançou o Código de Conduta para a Luta contra os Discursos Ilegais de Incitação ao Ódio em Linha²⁵. Este código, desenvolvido em parceria com plataformas tecnológicas como Facebook, Twitter (agora X), YouTube e Microsoft, visava acelerar a deteção e remoção de conteúdos que incitem à violência ou à

²⁵ O Código de Conduta para a Luta contra os Discursos Ilegais de Incitação ao Ódio em Linha, promovido pela Comissão Europeia em cooperação com as principais plataformas digitais, está disponível na íntegra em: https://commission.europa.eu/document/download/551c44da-baac-4692-9e7d-52d20c04e0e2_pt.

discriminação, em conformidade com a Decisão-Quadro 2008/913/JAI²⁶. Através de sucessivas rondas de monitorização²⁷, coordenadas pela Comissão, foi possível observar uma melhoria na eficácia das plataformas: já em 2020, cerca de 90% dos conteúdos sinalizados como discurso de ódio eram analisados no prazo de 24 horas, e mais de 70% eram removidos quando considerados ilegais²⁸. Este Código, embora não seja juridicamente vinculativo, consolidou-se como um instrumento estratégico complementar no ecossistema europeu de regulação digital, antecipando práticas que seriam mais tarde reforçadas pelo DSA. A sua relevância reside também no facto de ter inspirado metodologias de autorregulação em áreas conexas, como a desinformação, e de ter demonstrado a viabilidade de modelos cooperativos entre instituições públicas e grandes plataformas tecnológicas. De igual modo, evidenciou os limites dessa abordagem: persistência de disparidades entre plataformas, variações nos critérios de remoção, tratamento diferenciado consoante a origem da denúncia (utilizador comum vs. trusted flagger) e ausência de padronização na transparência dos relatórios.

Com o intensificar das campanhas de desinformação – especialmente durante momentos eleitorais –, União Europeia reconheceu a necessidade de alargar o seu foco geoestratégico para além das suas fronteiras, passando a incluir regiões de crescente vulnerabilidade, como os Balcãs Ocidentais, o Médio Oriente e o Norte de África (Europeu T. d., 2021). Neste contexto foi instituído, em 2017, o Centro Europeu de Excelência para o Combate às Ameaças Híbridas (European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE), sediado em Helsínquia, como uma iniciativa conjunta da União Europeia e da Nato (Nagasako, 2020). O Hybrid CoE assume-se como uma plataforma intergovernamental de cooperação, análise e capacitação, concebida para reforçar a resiliência das democracias ocidentais perante a crescente sofisticação dos ataques híbridos – entendidas como a combinação

²⁶ Relativa à luta por via do direito penal contra certas formas e manifestações de racismo e xenofobia, criminalizando a incitação pública à violência ou ao ódio contra grupos de pessoas, ou um dos seus membros, definidos por referência à raça, cor, religião, ascendência ou origem nacional ou étnica. Texto integral disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32008F0913>.

²⁷ As diversas monitorizações podem ser encontradas https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

²⁸ Comissão Europeia. (2020). *Factsheet: Code of conduct on countering illegal hate speech online – 5th Monitoring round*. Disponível em: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

de métodos convencionais e não convencionais, militares e civis, empregues de forma coordenada para atingir objetivos estratégicos, sem recorrer a formas tradicionais de confronto armado. Tendo-se dedicado à investigação e desenvolvimento de estratégias de resposta a ataques que envolvem, entre outros, desinformação, ciberataques, pressão económica, influência política encoberta e instrumentalização de fluxos migratórios, promovendo assim um intercâmbio de boas práticas entre os seus Estados participantes. Um dos marcos do seu trabalho foi o relatório publicado em 2018, no qual, com base na análise da Alliance for Securing Democracy, do German Marshall Fund ²⁹, se concluiu que, desde 2004, o governo russo tem conduzido campanhas sistemáticas de interferência nos assuntos internos de, pelo menos, 27 países da Europa e da América do Norte, recorrendo a uma combinação de ciberataques, desinformação e influência financeira (Treverton, Thvedt, Chen, Lee, & McCue, 2018).

No final de 2017, face à crescente proliferação de desinformação online e a erosão da confiança pública nos ecossistemas informativos digitais, a Comissão Europeia criou um Grupo de Peritos de Alto Nível (High-Level Expert Group – HLEG) com a missão de formular recomendações estratégicas para a formulação de políticas públicas eficazes no combate às fake news e à desinformação. O relatório final do HLEG, publicado em março de 2018 sob o título “A multi-dimensional approach to disinformation” propôs uma abordagem multidimensional assente em cinco pilares interligados: “(1) Reforçar a transparência das notícias online, mediante uma partilha adequada de dados – em conformidade com as normas de privacidade – sobre os sistemas que possibilitam a sua disseminação digital; (2) Promover a literacia mediática e informacional como forma de contrariar a desinformação e auxiliar os utilizadores na navegação pelo ambiente mediático digital; (3) Desenvolver ferramentas que capacitem os utilizadores e os jornalistas no combate à desinformação, incentivando simultaneamente uma relação positiva com as tecnologias de informação em constante evolução; (4) Salvaguardar a diversidade e a

²⁹ A Alliance for Securing Democracy, iniciativa integrada no German Marshall Fund of the United States (GMF), tem desenvolvido análises aprofundadas sobre campanhas de desinformação, interferência estrangeira e ameaças híbridas, com especial destaque para as estratégias de influência levadas a cabo por regimes autoritários. A colaboração do Hybrid CoE com esta entidade tem permitido a consolidação de uma base empírica sólida para a compreensão dos vetores contemporâneos de desestabilização democrática. Mais informações disponíveis em: <https://securingdemocracy.gmfus.org/>

sustentabilidade do ecossistema europeu dos meios de comunicação social; (5) promover a investigação contínua sobre o impacto da desinformação na Europa, de modo a avaliar as medidas adotadas pelos diversos atores e a ajustar de forma dinâmica as respostas necessárias (A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation, 2018, pp. 5-6). O relatório foi claro ao afirmar que a desinformação é um problema multifacetado que não pode ser resolvido através de uma única medida e que, por conseguinte, exige uma abordagem global e multidimensional. Rejeitando categoricamente soluções simplista ou punitivas ao fenómeno, nomeadamente qualquer forma de censura – seja exercida pelo Estado ou por entidades privadas –, o HLEG advogou, em contrapartida, uma lógica de reforço da resiliência social e da capacitação cidadã. Recusando assim, o controlo vertical da informação e ao privilegiar uma lógica de corresponsabilização democrática. (A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation, 2018). Entre as principais recomendações, o HLEG apelou ainda à Comissão Europeia para que promovesse a criação de um Código de Práticas europeu, assente numa abordagem multilateral e na cooperação entre todas as partes interessadas (multi-stakeholder approach). Em resposta a este apelo, a Comissão Europeia publicou, em setembro de 2018, o primeiro Código de Conduta sobre a Desinformação (Kuczerawy, 2019).

Este relatório foi seguido pela Comunicação da Comissão intitulada (Combater a desinformação em linha: uma estratégia europeia COM (2018) 236 final), publicada em 26 de abril de 2018, que delineou a abordagem da UE para enfrentar o crescente desafio da desinformação em larga escala na Europa. Esta estratégia assentava em princípios como melhorar a transparência sobre a origem da informação, promover a diversidade de informação através do apoio ao jornalismo de qualidade e à literacia mediática, promover a credibilidade da informação com sinalizadores de confiança e rastreabilidade, e oferecer soluções inclusivas com o envolvimento de todas as partes interessadas. A Comissão instou as plataformas digitais a intensificarem os seus esforços no combate à desinformação, apoiando o desenvolvimento de um ambicioso Código de Conduta sobre a Desinformação.

Em dezembro do mesmo ano, a Comissão Europeia apresentou o (Plano de Ação contra a Desinformação JOIN (2018) 36 final), que assentava em quatro pilares fundamentais: (1) Melhorar as capacidades das instituições da União para detetar, analisar e denunciar a desinformação; (2) Reforçar a coordenação e as respostas comuns à desinformação, com a criação de Sistema de Alerta Rápido (SAR); (3) Mobilizar o setor privado para o combate à desinformação; (4) Sensibilizar as pessoas e reforçar a resiliência da sociedade, nomeadamente melhorar a literacia dos cidadãos, permitindo-lhes identificar e prevenir tentativas de desinformação (Plano de Ação contra a Desinformação JOIN (2018) 36 final). Entre as medidas propostas, destaca-se o SAR como um mecanismo inovador de cooperação interinstitucional e intergovernamental, concebido para permitir a partilha célere e eficaz de informações críticas entre a Comissão, o SEAE, os Estados-Membros e os seus pontos de contacto nacionais, nomeadamente em contextos de especial sensibilidade democrática, como períodos eleitorais (Europeu T. d., 2021). O seu principal objetivo é promover o diálogo, avaliar tendências e estruturar respostas coletivas, alertando rapidamente entidades como órgãos eleitorais ou serviços de informação em caso de campanhas de desinformação, particularmente em larga escala. A sua operação em tempo real é crucial para a identificação e neutralização rápida da desinformação, nomeadamente em períodos de vulnerabilidade democrática – como eleições. Para além da cooperação “intraeuropeia”, este sistema também promove a articulação com parceiros estratégicos, como o G7 e a NATO, consolidando a dimensão internacional da resposta europeia à desinformação e reforçando a sua capacidade de antecipação e resposta perante ameaças híbridas transnacionais (A Desinformação - Contexto Europeu e Nacional, 2019).

Paralelamente às iniciativas institucionais então em curso, a União Europeia deu um passo pioneiro no combate à desinformação com o lançamento, em setembro de 2018, do Código de Conduta sobre a Desinformação. Assinado voluntariamente por várias das principais plataformas tecnológicas, como a Google, a Meta (Facebook), o Twitter (atualmente designado por X) e a Mozilla, o Código materializou um compromisso inédito entre atores privados e entidades públicas na luta contra a desinformação e a manipulação da publicidade política. Tratou-se, de uma convergência entre os interesses da indústria e os objetivos políticos da União, na tentativa de instaurar um novo modelo de corresponsabilização para mitigar os riscos

informacionais emergentes (Kachelmann & Reiners, 2023). O Código visava, entre outros objetivos, controlo da colocação de anúncios; transparência da publicidade política e temática; integridade dos serviços; capacitação dos utilizadores; e apoio à comunidade de investigação. Importa, contudo, ressaltar que este mecanismo revelou desde cedo fragilidades estruturais e limitações práticas que comprometeram parte da sua eficácia. A análise crítica dessas limitações, bem como da evolução normativa que conduziu à adoção do Código Reforçado de 2022, será objeto de exploração detalhada em secção própria deste capítulo.

O período que antecedeu 2018 caracterizou-se pela confiança da UE em instrumentos de "soft law" e compromissos voluntários, refletindo uma preferência por uma autorregulação liderada pela indústria. Esta opção refletia uma tríplice motivação: a salvaguarda da liberdade de expressão, a complexidade técnica do ecossistema digital e o desejo político de privilegiar a cooperação institucional em detrimento da imposição regulatória. Embora funcional numa fase preliminar, esta abordagem revelou fragilidades significativas, sobretudo no que respeita à responsabilização das plataformas e à monitorização da eficácia das medidas implementadas. A irrupção da pandemia de COVID-19 veio acelerar esta consciencialização. Constituindo um ponto de reflexão na abordagem da União Europeia à desinformação. O contexto pandémico expôs brutalmente os riscos sistémicos associados à circulação massiva de conteúdos falsos ou manipuladores, desencadeando aquilo que a Organização Mundial da Saúde denominou de “infodemia”³⁰: uma avalanche de informação – muitas vezes contraditórias, alarmistas ou deliberadamente falsas – capazes de comprometer respostas sanitárias, pondo em causa a própria saúde das pessoas, basta recordar alguns dos exemplos mais caricatos – e perigosos – que circularam durante a pandemia: desde a ideia de que “beber lixívia mata o vírus”³¹, à versão portuguesa de que “um copo de bagaço mata o

³⁰ “O termo infodemia já foi utilizado e descrito pela OMS: trata-se da «quantidade excessiva de informação sobre um determinado problema, que dificulta a identificação de uma solução para o mesmo. Durante uma emergência sanitária pode ser divulgada informação enganosa ou desinformação, assim como lançados boatos. Uma infodemia pode impedir uma resposta eficaz em matéria de saúde pública e gerar confusão ou desconfiança entre as pessoas»: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4” (Europeia, Combater a desinformação sobre a COVID-19: repor a verdade dos factos JOIN(2020) 8 final, 2020)

³¹ Sobre a falsa alegação de que o consumo de lixívia poderia prevenir ou curar a COVID-19, ver: Representação da Comissão Europeia em Portugal, “*O consumo de lixívia pode ajudar a combater o coronavírus?*”, publicado em 3 de julho de 2020, disponível em:

bicho”, passando por teorias da conspiração que garantiam que as vacinas continham microchips para controlar a população^{32 33}. Estas narrativas, ainda que por vezes caricatas, minaram a confiança nas instituições públicas, e dessa forma dificultaram o esforço coletivo de contenção da pandemia, evidenciando a necessidade de uma resposta institucional mais robusta e coordenada ao fenómeno da desinformação. Face a este desafio sem precedentes, a Comissão Europeia respondeu com a comunicação (Europeia, Combater a desinformação sobre a COVID-19: repor a verdade dos factos JOIN(2020) 8 final, 2020), que instituiu um conjunto robusto de medidas, desenhadas para enfrentar os múltiplos níveis da ameaça. Entre as principais ações delineadas destacam-se: (i) o reforço da monitorização das plataformas digitais, no âmbito do Código de Conduta; (ii) a comunicação intensiva de informação fidedigna através de canais institucionais e colaborações com autoridades de saúde como a OMS; (iii) o estreitamento da cooperação com parceiros estratégicos, como o G7 e a NATO, nomeadamente através da ativação do Sistema de Alerta Rápido (SAR); (iv) o combate às burlas e fraudes online; e (v) a promoção da literacia mediática, capacitando os cidadãos com ferramentas críticas para reconhecer e rejeitar desinformação. A pandemia revelou mais uma vez a dimensão geopolítica do fenómeno, agora a nível da saúde física das pessoas, expondo campanhas de influência por parte de atores estatais e não estatais, com o intuito de semear a desconfiança e explorar divisões internas nos Estados-Membros.

A experiência com o Código de Conduta de 2018 – posto à prova durante a pandemia – tornou evidente a necessidade de um novo instrumento, mais “robusto”. Através do programa de monitorização lançado na sequência da referida

https://portugal.representation.ec.europa.eu/news/o-consumo-de-lixivia-pode-ajudar-combater-o-coronavirus-mito-2020-07-03_pt (consultado em julho de 2025).

³² Verificações independentes desmentiram reiteradamente a teoria da conspiração segundo a qual Bill Gates teria declarado que as vacinas contra a COVID-19 serviriam para controlar a população ou que incluíam chips de rastreamento. Cf. Observador, *Fact Check: Bill Gates disse que as vacinas contra a COVID-19 vão servir para controlar a humanidade?*, disponível em:

<https://observador.pt/factchecks/fact-check-bill-gates-disse-que-as-vacinas-contr-a-covid-19-vaoo-servir-para-controlar-a-humanidade>; e *Fact Check: Bill Gates confirmou que chips foram implantados nas vacinas?*, disponível em: <https://observador.pt/factchecks/fact-check-bill-gates-confirmou-que-chips-foram-implantados-nas-vacinas> (ambos consultados em julho de 2025).

³³ Durante os meses mais críticos da pandemia, o trabalho de plataformas de verificação de factos como o Polígrafo, da SIC, foi incansável. A desinformação multiplicava-se a um ritmo tão acelerado que, por vezes, parecia que a cada nova hora surgia uma nova teoria – desde remédios caseiros milagrosos a conspirações globais. As plataformas como o Polígrafo tornaram-se, por assim dizer, o “antivírus nacional da mentira”, esforçando-se por desmentir um número crescente de notícias falsas que circulavam velozmente pelas redes sociais e aplicações de mensagens.

comunicação³⁴, ficou demonstrado que, apesar de alguns avanços – como o reforço da visibilidade de fontes fidedignas, a introdução de ferramentas de sinalização de conteúdos enganosos e a limitação da publicidade enganosa –, persistiam fragilidades graves que comprometiam a eficácia e a abrangência da resposta europeia ao fenómeno da desinformação. Entre as fragilidades identificadas destacam-se: a (fraca) qualidade e uniformidade dos relatórios submetidos pelas plataformas; a insuficiência de granularidade nos dados, especialmente ao nível dos Estados-Membros e das línguas da UE; a ausência de um modelo padronizado de reporte; a necessidade de avaliação independente sobre a aplicação efetiva dos compromissos; lacunas na cobertura da verificação de factos, particularmente devido à ausência de um repositório centralizado; e, por fim, a persistente monetização de conteúdos desinformativos através de publicidade digital. Reconhecendo-as, a Comissão Europeia avançou, em maio de 2021, com a publicação de um conjunto de orientações estratégicas destinado ao reforço substancial do Código de Conduta (Europeia, Orientações da Comissão Europeia para o Reforço do Código de Conduta em Matéria de Desinformação COM (2021) 262 final). Estas Orientações não se limitaram a apresentar recomendações técnicas, assumiram-se como um verdadeiro apelo à ação, com a finalidade de transformar o Código num elemento central da arquitetura regulatória europeia no domínio da governação digital. Nomeadamente apelaram (i) ao reforço da responsabilização através do estabelecimento de indicadores de desempenho mensuráveis e de mecanismos de auditoria independentes; (ii) à necessidade de assegurar uma maior transparência dos sistemas algorítmicos e das práticas de moderação de conteúdos; (iii) ao aumento substancial do acesso a dados para investigadores, a fim de promover a compreensão científica do fenómeno; e (iv) ao desenvolvimento de medidas eficazes para a desmonetização de conteúdos desinformativos, quebrando os incentivos económicos à sua proliferação. Além destes eixos centrais, foi sublinhado o imperativo de assegurar a integridade dos serviços digitais, prevenindo práticas de manipulação computacional, como a proliferação de bots, contas falsas, técnicas de amplificação inorgânica e falsificações profundas (deepfakes). Paralelamente, a verificação de factos foi consagrada como um pilar essencial da resposta democrática à desinformação, sendo recomendada a sua expansão a todas as línguas oficiais da UE, a criação de repositórios comuns inter-

³⁴ Disponíveis em <https://digital-strategy.ec.europa.eu/pt/policies/covid-19-disinformation-monitoring>

plataforma e a integração automatizada dos conteúdos verificados nos serviços das plataformas. As orientações destacaram, ainda, a necessidade de resposta preventiva e educativa, sublinhando a importância de promover o empoderamento cívico dos utilizadores, através do reforço da literacia mediática, da disponibilização de instrumentos de sinalização e da facilitação do acesso a fontes de informação credíveis e verificadas. Este novo impulso político contribuiu para o alargamento do próprio universo de signatários, fomentando a participação de novas plataformas, serviços de mensagens, operadores do ecossistema publicitário e organizações especializadas, numa lógica de responsabilidade partilhada e corresponsabilização multissetorial³⁵.

Em 2022, fruto das críticas quanto à eficácia limitada do modelo original, a Comissão Europeia promoveu uma versão reforçada do Código, com um total de 44 compromissos, o dobro da versão de 2018 e, contou inicialmente com a adesão de 34 signatários, entre os quais se incluem as principais plataformas digitais (Meta, Google, Microsoft, TikTok e Vimeo), organizações da sociedade civil, empresas de tecnologia publicitária e entidades de verificação de factos³⁶. Entre as principais prioridades, destaca-se a eliminação dos incentivos económicos que alimentam a proliferação de conteúdos desinformativos, simultaneamente, visa-se alargar a resposta a comportamentos manipuladores emergentes, como a criação de contas falsas, a amplificação automatizada de conteúdos, a personificação e a difusão de deepfakes maliciosos. Paralelamente, o Código compromete-se a promover a literacia mediática e a capacitação dos utilizadores, disponibilizando ferramentas eficazes para que estes possam identificar e denunciar conteúdos desinformativos, bem como contestar decisões injustas. Reforça-se ainda a importância de expandir a verificação de factos a todas as línguas da União Europeia, garantindo a integração efetiva dos

³⁵ Oito novos potenciais signatários aderiram ao processo de revisão do Código de Conduta sobre Desinformação: Vimeo, Clubhouse, DoubleVerify, Avaaz, Globsec, Logically, NewsGuard e WhoTargetsMe. Disponível em: <https://eurocid.mne.gov.pt/cronologias/ue-na-luta-contra-desinformacao-principais-iniciativas>.

³⁶ Atualmente, o Código de Conduta Reforçado sobre Desinformação é subscrito por 41 entidades, que refletem a diversidade de atores envolvidos no combate à desinformação no espaço digital europeu. Entre os signatários encontram-se grandes plataformas tecnológicas (Meta, Google, Microsoft, TikTok, Twitch), empresas de publicidade e verificação de factos (Microsoft Advertising, DoubleVerify, NewsGuard, Maldita.es), organizações da sociedade civil e redes especializadas (Reporters Without Borders, Globsec, Democracy Reporting International), bem como iniciativas académicas e de transparência digital (AI Forensics, European Factchecking Standards Network, WhoTargetsMe). A lista completa dos signatários encontra-se disponível em: <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>

verificadores nos serviços digitais e assegurando a sua remuneração adequada. O acesso a dados para fins de investigação científica constitui outro pilar estruturante. Por fim, o Código consagra a criação de um quadro de monitorização robusto e transparente, com relatórios públicos periódicos e a constituição de uma Task Force permanente que integra a Comissão Europeia, o Serviço Europeu para a Ação Externa e o Observatório Europeu dos Media Digitais (EDMO), assegurando uma governação participada e eficaz no combate à desinformação.

Este percurso culminou, em 2022, na adoção do Digital Services Package – Digital Services Act (DSA) e do Digital Markets Act (DMA) – os quais introduziram novas obrigações às plataformas digitais, nomeadamente no que respeita à gestão de riscos sistémicos como a desinformação e à responsabilização algorítmica (JODANOVIC, 2024). Em particular, o DSA tornou-se o pilar central da resposta regulatória da UE à proliferação de riscos sistémicos no ambiente online, como a desinformação, a manipulação algorítmica, a publicidade opaca e a disseminação de conteúdos nocivos.

A entrada em vigor do Regulamento dos Serviços Digitais assinala um momento de viragem histórico na governança digital europeia, elevando o Código de Conduta sobre Desinformação, na sua versão reforçada de 2022, de um instrumento de autorregulação voluntária a um pilar fundamental de um regime co-regulativo vinculativo. Esta transição não é meramente formal, é uma consagração expressa (Recital 106), reconhecendo o Código como um instrumento passível de integração no novo Regulamento. A formalização desta integração, solenemente reconhecida pela Comissão Europeia e pelo Comité Europeu dos Serviços Digitais³⁷ em fevereiro de 2025³⁸, e com plena entrada em vigor a partir de 1 de julho de 2025, ao abrigo do Artigo 45.º do DSA, redefine o panorama da responsabilização das plataformas digitais (Sousa, 2025). A partir desse momento, VLOPs VLOSEs – os gigantes que moldam a nossa esfera digital – passam a ser submetidos a uma avaliação rigorosa do cumprimento dos compromissos assumidos no Código, no âmbito das auditorias

³⁷ Para mais informações sobre a constituição, composição e atividades do Comité Europeu dos Serviços Digitais (Digital Services Board), ver: Comissão Europeia, *Digital Services Board – Comité Europeu dos Serviços Digitais*, disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/dsa-board> (último acesso em julho de 2025).

³⁸ Sobre os Códigos de Conduta reconhecidos ao abrigo do Digital Regulamento dos Serviços Digitais, consultar: Comissão Europeia, *Digital Services Act – Codes of Conduct*, disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/dsa-codes-conduct> (último acesso em julho de 2025).

independentes e sistemáticas exigidas pelo DSA. Esta integração confere ao Código de Conduta um estatuto jurídico sem precedentes, permitindo que a sua adesão plena seja considerada como medida eficaz de mitigação de riscos sistémicos – nomeadamente no que toca à propagação de desinformação, conforme estipulado no artigo 34.º do DAS. Uma vez que a adesão e o cumprimento dos compromissos do Código podem ser considerados uma "medida de mitigação de riscos adequada" ao abrigo do Artigo 35.º do DSA. O que antes era uma simples adesão voluntária, passa agora a estar acompanhado por consequências legais concretas. E, talvez o mais impactante, a aparente ausência de sanções diretas no Código de Conduta é agora preenchida pela força coerciva do DSA. O incumprimento dos compromissos por parte das VLOPs e VLOSEs, outrora uma falha de "soft law", pode agora desencadear sanções severas ao abrigo do DSA, incluindo multas proporcionais à sua dimensão, que podem chegar até 6% do volume de negócios anual (artigo 52.º, n.º3). Esta ameaça de penalidades financeiras substanciais transforma a conformidade de uma aspiração numa imperiosa necessidade, conferindo ao DSA os "dentes" necessários para garantir a sua aplicação. (Gosztonyi, 2024). Adicionalmente, o sistema de relatórios do Código de Conduta, com os seus elementos qualitativos e indicadores de nível de serviço (SLIs e QREs), transcende a mera formalidade (Leiser, 2023), gera um fluxo contínuo dados adicionais que complementam as obrigações de transparência do DSA. Isto, além de aumentar responsabilização das plataformas, permite uma melhor compreensão das dinâmicas da desinformação.

A análise até aqui desenvolvida evidencia de forma inequívoca a evolução notável da União Europeia na construção de uma resposta (normativa) ao fenómeno da desinformação, refletindo um reconhecimento cada vez mais claro do fenómeno como uma ameaça sistémica aos processos democráticos, à saúde pública e à coesão social (Borz, Francesco, Montgomerie, & Bellis, 2024). Esta consciencialização conduziu à perceção de que as abordagens assentes exclusivamente na autorregulação e na soft law – como a East StratCom Task Force e o Código de Conduta de 2018 – eram insuficientes para lidar com a escala, complexidade e rapidez de propagação da desinformação no ecossistema digital contemporâneo. A experiência acumulada, em particular durante momentos críticos como a pandemia de COVID-19, revelou com clareza as limitações estruturais dos instrumentos de soft law, expondo a urgência de soluções mais eficazes e, juridicamente, vinculativas (Gosztonyi, 2024). Traduzindo-

se na adoção de instrumentos mais robustos e vinculativos, como o DSA e a integração do Código Reforçado, ao abrigo do artigo 45.º Neste percurso, e na sua resposta multifacetada, a União Europeia tem procurado equilibrar a necessidade de intervenção com a salvaguarda de princípios fundamentais como a liberdade de expressão, o pluralismo dos meios de comunicação³⁹ e a integridade do espaço público digital (Europeia, Proteção dos Direitos Fundamentais na Era Digital - Relatório Anual de 2021 sobre a Aplicação da Carta dos Direitos Fundamentais na UE, 2021). A sua estratégia distingue-se por privilegiar a transparência, a responsabilização e o empoderamento dos cidadãos (Buttaboni, Colangelo, & Floridi, 2025), recusando lógicas de censura e apostando antes numa governança cooperativa (Saurwein & Spencer-Smith, 2020). Iniciativas como o EDMO e a Rede Europeia de Normas de Verificação de Factos (EFCSN) assumem aqui um papel central no apoio à investigação independente e na verificação de factos, pilares essenciais de um ecossistema informativo resiliente e plural (Silva, 2025).

A batalha contra a desinformação é, contudo, uma maratona. A sua natureza dinâmica e adaptativa exige vigilância permanente, mecanismos de aplicação credíveis e um investimento contínuo na literacia mediática e no pensamento crítico dos cidadãos (D’Andrea, Fusacchia, & D’Ulizia, 2025). A persistência do fenómeno, apesar dos avanços regulatórios, recorda-nos que a legislação, por si só, é insuficiente sem uma implementação coerente e uma sociedade civil ativa e esclarecida.

Código de Conduta para o Combate à Desinformação

O Código de Conduta sobre Desinformação de 2018 representou uma das primeiras tentativas concretas da União Europeia de responder – ainda que por via não vinculativa – a crescente ameaça da desinformação em linha. Motivado pela

³⁹ Sobre os meios de comunicação é importante fazer referência ao Regulamento (UE) 2024/1083 do Parlamento Europeu e do Conselho, relativo à liberdade dos meios de comunicação social, que pretende garantir a independência editorial, o pluralismo mediático e a proteção dos jornalistas contra interferências políticas e económicas indevidas, constituindo um instrumento fundamental no reforço da integridade do espaço informacional europeu. Este regulamento visa também assegurar a transparência da propriedade dos media e do financiamento público aos órgãos de comunicação, contribuindo para um ecossistema mediático mais resiliente face à desinformação. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1083/oj/por>.

crescente evidência de campanhas de influência externas, manipulação algorítmica e estratégias coordenadas de disseminação de conteúdos falsos, o Código foi concebido como um mecanismo de autorregulação coordenada, na esperança de envolver diretamente os grandes intermediários digitais numa resposta cooperativa e voluntária.

Longe de se limitar a uma responsabilidade sectorial, este documento parte do reconhecimento de que a desinformação não é um fenómeno isolado, mas sim um problema sistémico que atravessa transversalmente todo o ecossistema informacional digital (Kuczerawy, 2019). É neste contexto que o Código procura delinear um conjunto de ações concretas a serem adotadas voluntariamente pelos signatários, com vista a enfrentar de forma coordenada e eficaz os desafios complexos colocados pela desinformação online. A ambição do Código consistia, assim, não apenas na mitigação da desinformação, mas na edificação de uma cultura de transparência, responsabilidade e pluralismo. Os objetivos centrais delineados no preâmbulo refletiam a vontade de agir sem comprometer os princípios fundamentais da liberdade de expressão e da diversidade informativa.

Compromissos do Código

O Código de Conduta sobre Desinformação de 2018 estrutura-se em torno de cinco domínios de ação prioritários, desenhados para articular uma resposta coordenada aos riscos crescentes da desinformação em linha. Os signatários – plataformas digitais, redes sociais, anunciantes e outros atores relevantes – comprometeram-se voluntariamente a adotar medidas nos seguintes eixos estratégicos: (1) controlo da colocação de anúncios; (2) transparência da publicidade política e temática; (3) integridade dos serviços; (4) capacitação dos utilizadores; e (5) apoio à comunidade de investigação. Esta arquitetura compromissória foi acompanhada de um mecanismo de monitorização periódico da sua implementação e eficácia.

Controlo de colocação de anúncios

O primeiro, centrado no controlo da colocação de anúncios, visava desincentivar a monetização da desinformação através da publicidade digital. O Código parte do pressuposto de que os incentivos económicos gerados pela publicidade online contribuem de forma significativa para comportamentos manipuladores, incluindo a falsificação de identidades ou a deturpação intencional dos propósitos de determinados espaços digitais. Como resposta, os signatários comprometeram-se a implementar políticas que preveniam a promoção ou financiamento de contas e sítios sistematicamente enganadores. Isso implica a adoção de medidas para deixar de promover, financiar ou apoiar, ainda que indiretamente, sites e contas cujo padrão de atividade seja sistematicamente enganoso. Recomendou-se, para o efeito, o uso de ferramentas de “segurança de marca” (brand safety tools) e sistemas de verificação de terceiros que permitissem maior rastreabilidade e responsabilidade. O Código sublinha ainda que todos os intervenientes no ecossistema publicitário – plataformas, anunciantes, agências e intermediários – devem colaborar para reforçar a transparência e a integridade do sistema como um todo. Tal colaboração exige o escrutínio rigoroso da colocação de anúncios, nomeadamente através da limitação da sua exibição em páginas associadas a conteúdos desinformativos. Acresce que os signatários são instados a realizar esforços comercialmente razoáveis para garantir que não recebem compensações financeiras, nem promovem ativamente entidades que persistentemente distorcem a realidade ou manipulam o seu posicionamento informativo. Por fim, o Código recomenda que se recorra a indicadores de fiabilidade (trustworthiness indicators) e a colaborações com organizações especializadas em verificação de factos, bem como com a rede independente de verificadores de factos criada sob a égide da Comissão Europeia (Código de Conduta da UE sobre Desinformação , 2018, pp. 4-5).

Propaganda política e publicidade temática

No que respeita à propaganda política e à publicidade temática, o Código sublinha a importância crucial da transparência como instrumento de reforço da integridade democrática e da confiança dos cidadãos no ecossistema informativo digital. Os signatários comprometeram-se, neste âmbito, a assegurar uma distinção clara e inequívoca entre conteúdos editoriais e conteúdos pagos, garantindo que todos

os anúncios sejam facilmente identificáveis como tal pelos utilizadores. Este compromisso implica, igualmente, a obrigação de tornar pública a identidade dos patrocinadores das campanhas publicitárias, bem como os montantes investidos na sua difusão, permitindo aos cidadãos compreender porque foram alvo de determinada mensagem e qual o seu enquadramento estratégico. Em particular, esta transparência deve estender-se também à publicidade temática (issue-based advertising), isto é, aquela que, embora não explicitamente partidária, visa influenciar o debate público sobre assuntos politicamente sensíveis ou divisivos. O Código apela ainda à adoção de esforços razoáveis por parte dos signatários para assegurar a divulgação pública destes conteúdos temáticos, sem, contudo, limitar ou inibir o jornalismo político, a liberdade de opinião ou a publicação de conteúdos editoriais de natureza crítica. Com efeito, reconhecendo as tensões inerentes entre a regulação da publicidade política e a salvaguarda da liberdade de expressão, o Código encoraja os signatários a colaborarem com peritos e partes interessadas – nomeadamente da sociedade civil, academia e setor da comunicação social – na definição de métodos que garantam simultaneamente a transparência e o respeito pelos direitos fundamentais consagrados nos instrumentos jurídicos europeus (Código de Conduta da UE sobre Desinformação , 2018, pp. 5-6).

Integridade dos Serviços

Relativamente à integridade dos serviços, foi estabelecida a necessidade de políticas explícitas contra a utilização abusiva de robôs e sistemas automatizados, bem como mecanismos para bloquear contas falsas, sobretudo aquelas cuja finalidade principal fosse a disseminação de desinformação. Este eixo era particularmente sensível, dado o imperativo de proteger o direito ao anonimato, essencial para diversos utilizadores em contextos repressivos. Os signatários comprometem-se, portanto, a implementar políticas claras sobre a identidade dos utilizadores e sobre a utilização indevida de robôs automatizados nas suas plataformas, bem como a aplicar essas políticas no espaço da União Europeia. Comprometem-se ainda a estabelecer normas que definam o que constitui uma utilização inadmissível de sistemas automatizados, tornando essas políticas publicamente acessíveis nas respetivas plataformas e disponíveis para os utilizadores da UE. No entanto, tais medidas não devem impedir a utilização anónima ou sob pseudónimo de contas e serviços, em

conformidade com o artigo 8.º da Convenção Europeia dos Direitos Humanos (Código de Conduta da UE sobre Desinformação , 2018, p. 6).

Capacitação dos Consumidores/Utilizadores

A capacitação dos utilizadores era considerada essencial para contrariar os efeitos corrosivos da desinformação. O Código defendia o investimento em ferramentas tecnológicas que priorizassem conteúdos credíveis, assim como a promoção de literacia mediática e pensamento crítico. Os signatários comprometeram-se a criar funcionalidades que facilitassem o acesso a perspetivas diversas, a melhorar a visibilidade de fontes fiáveis e a oferecer aos utilizadores mecanismos simples para denunciarem desinformação. Além disso, os utilizadores deveriam poder compreender as razões pelas quais foram alvo de determinada publicidade política ou temática, promovendo-se, assim, uma maior consciência sobre a arquitetura algorítmica da informação digital. Finalmente, o Código previa a cooperação com a sociedade civil, governos e instituições de ensino para reforçar as competências digitais e o espírito crítico dos cidadãos (Código de Conduta da UE sobre Desinformação , 2018, pp. 6-7).

Capacitação da comunidade de investigação

Reconhecendo o papel vital de investigações independentes, o Código apelava para que os signatários assumissem compromissos no sentido de apoiar a comunidade académica e os verificadores de factos, assegurando, sempre que possível, o acesso a dados relevantes e fomentando parcerias para a investigação independente do fenómeno da desinformação. Nesse sentido, os signatários comprometem-se a não proibir nem desencorajar a investigação de boa-fé sobre desinformação e publicidade política, antes pelo contrário, a promover ativamente o desenvolvimento deste tipo de estudos. Comprometem-se ainda a apoiar os esforços independentes, conduzidos de boa-fé, destinados a rastrear e compreender o impacto da desinformação, incluindo o trabalho da rede independente de verificadores de factos promovida pela Comissão Europeia. Este apoio poderá assumir diversas formas, nomeadamente o fornecimento de conjuntos de dados protegidos por regras de privacidade, a realização de projetos de investigação conjuntos ou a criação de parcerias com instituições académicas e organizações da sociedade civil. Os signatários comprometem-se igualmente a

organizar, com periodicidade anual, um evento destinado a fomentar o diálogo entre o meio académico, a comunidade de verificação de factos e outros intervenientes relevantes da cadeia de valor da informação digital (Código de Conduta da UE sobre Desinformação , 2018, pp. 7-8)

Medição e monitorização da eficácia do código

Por fim, o Código prevê a monitorização periódica da sua eficácia. Os signatários comprometem-se a elaborar, anualmente, um relatório de autoavaliação publicamente acessível, no qual prestem contas das medidas adotadas no combate à desinformação. Estes relatórios podem incluir detalhes sobre as ações concretas realizadas e os progressos alcançados em matéria de transparência no ecossistema digital informativo. Os relatórios deverão ser passíveis de revisão por terceiros independentes, escolhidos pelos próprios signatários. O papel dessas entidades externas é o de rever e avaliar, de forma objetiva, o grau de cumprimento dos compromissos assumidos pelos signatários no âmbito do Código. Além disso, os signatários devem colaborar com a Comissão Europeia e outros atores relevantes na identificação das abordagens mais eficazes para garantir a transparência da publicidade temática (“issue-based advertising”). Adicionalmente, os signatários comprometem-se a avaliar a eficácia do Código passados 12 meses da sua implementação. Durante esse primeiro período de avaliação, reuniram-se regularmente para analisar o progresso, a aplicação e o funcionamento do Código, bem como para discutir eventuais ações de seguimento. São igualmente instados a cooperar com a Comissão Europeia na avaliação dos relatórios relativos à implementação do Código (Código de Conduta da UE sobre Desinformação , 2018, pp. 8-9).

Contudo, apesar da amplitude dos compromissos e da aparente sofisticação das medidas, o modelo de autorregulação revelou-se estruturalmente limitado. A eficácia do Código assentava num mecanismo de monitorização essencialmente voluntário, no qual os próprios signatários apresentavam relatórios anuais de autoavaliação, muitas vezes desprovidos de dados granulares, harmonizados ou verificáveis por entidades externas. Embora o texto previsse a revisão dos relatórios por uma entidade terceira independente, tal supervisão nunca se consolidou de forma robusta. Acresce que os relatórios eram frequentemente incompletos, heterogéneos

entre plataformas e pouco transparentes, dificultando a comparação entre práticas e a avaliação do impacto real das medidas adotadas⁴⁰.

Críticas ao Código de Conduta: Liberdade de Expressão e Limitações Estruturais

Apesar de se apresentar como uma iniciativa consciente dos direitos fundamentais, o Código de 2018 tem sido alvo de críticas substanciais, nomeadamente quanto ao seu impacto na liberdade de expressão. Desde logo, embora o próprio Código reconheça, no seu preâmbulo, estar “consciente do direito fundamental à liberdade de expressão e a um ambiente digital aberto”, a sua aplicação prática revelou contradições estruturais que geraram fricções reais entre os objetivos declarados e os efeitos concretos da sua operacionalização (Kuczerawy, 2019). Na sua essência, o Código não visa substituir – nem pretende reinterpretar – o quadro jurídico europeu vigente, como a Carta dos Direitos Fundamentais da União Europeia ou a Convenção Europeia dos Direitos Humanos, mas o facto de não ter natureza vinculativa não o isenta de produzir efeitos práticos substanciais sobre o exercício da liberdade de expressão e o direito de acesso à informação.

Tal como consagrado no artigo 10.º da CEDH, a liberdade de expressão não protege apenas as ideias acolhidas de forma favorável, mas também aquelas que possam ofender, chocar ou perturbar o Estado ou qualquer setor da população (Kuczerawy, 2019). Ainda que tal proteção não seja absoluta, qualquer restrição deve respeitar três critérios fundamentais: estar prevista na lei, prosseguir um objetivo legítimo (como a proteção dos direitos de terceiros) e ser necessária numa sociedade democrática – ou seja, proporcional. As normas que regulam estas interferências foram concebidas para limitar o poder estatal, e não para disciplinar a atuação de entidades privadas. Todavia, o Código promove, de forma indireta, uma redistribuição do poder regulatório, encorajando as plataformas a interferirem com conteúdos lícitos considerados “falsos” (Kuczerawy, 2019). Esta interferência ocorre sobretudo por via da reconfiguração algorítmica da visibilidade desses conteúdos – prática que, embora

⁴⁰ Os relatórios de monitorização submetidos pelos signatários do Código de Conduta sobre Desinformação, bem como outros documentos relevantes sobre a sua implementação, encontram-se disponíveis para consulta no Centro de Transparência: <https://disinfocode.eu/reports>

não remova diretamente os conteúdos, compromete substancialmente a sua disseminação.

Embora esta abordagem evite tecnicamente a censura direta, não deixa de configurar uma forma de interferência restritiva⁴¹. Reduzir a exposição de determinado conteúdo no ecossistema digital é, em termos substanciais, limitar o seu alcance, contrariando o direito de todos os cidadãos a receberem e difundirem ideias e informações, como consagrado no artigo 11.º da Carta e no artigo 10.º da CEDH⁴². Como assinalado pelo Tribunal Europeu dos Direitos Humanos no caso *Yıldırım v. Turkey*, restringir o acesso à informação digital pode equivaler, em termos substanciais, a uma nova forma de censura.

O risco de arbitrariedade acentua-se perante a ausência de critérios objetivos e transparentes sobre quem classifica determinado conteúdo como “fidedigno”, “autêntico” ou “relevante”. A ausência de parâmetros objetivos e de mecanismos de recurso robustos aumenta o risco de decisões arbitrárias e suscetíveis de abuso. Este vácuo contribui para um cenário em que as gigantes tecnológicas, movidos por incentivos comerciais, reputacionais ou mesmo por pressões políticas, se tornam os novos árbitros da verdade no espaço público digital – sem responsabilidade pública direta e fora do alcance das salvaguardas dos direitos fundamentais. Importa aqui recordar a doutrina das obrigações positivas dos Estados que impõe aos poderes públicos não apenas a abstenção de interferências indevidas, mas também o dever de proteger os cidadãos contra interferências excessivas por parte de terceiros, incluindo empresas privadas. Esta exigência implica que, ao delegar a moderação de conteúdos em entidades privadas, os Estados devem garantir a existência de salvaguardas adequadas, mecanismos de supervisão e vias de recurso eficazes.

⁴¹ No acórdão *Murphy c. Irlanda*, o Tribunal Europeu dos Direitos Humanos sublinhou que a questão em causa dizia respeito essencialmente à exclusão do requerente da possibilidade de difundir um anúncio publicitário, tratando-se, assim, da regulação dos meios de expressão e não da sua profissão ou da manifestação da sua religião. O Tribunal recordou que o artigo 10.º da CEDH protege não apenas o conteúdo e a substância da informação, mas também os meios utilizados para a sua difusão, uma vez que qualquer restrição a esses meios interfere necessariamente com o direito de receber e transmitir informações (*Öztürk v. Turquia*, n.º 22479/93).

⁴² Com efeito, os utilizadores dedicam apenas uma quantidade limitada de tempo e atenção à procura de informação. Se determinado conteúdo for ocultado nos resultados mais distantes de pesquisa ou confinado a perfis que raramente emergem na navegação habitual, a probabilidade de esse conteúdo alcançar qualquer audiência torna-se extremamente reduzida.

Além das fragilidades substantivas relacionadas com os direitos fundamentais, o Código de 2018 revelou igualmente limitações estruturais profundas. As mesmas foram amplamente assinaladas por análises académicas e relatórios institucionais. (Pamment, *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission*, 2020), num estudo desenvolvido para a Carnegie Endowment for International Peace, sublinha que os signatários adotaram uma abordagem altamente desigual aos compromissos assumidos, com escassos indícios de impacto efetivo, ausência de responsabilização e opacidade quanto à forma como os algoritmos influenciam a disseminação de conteúdos. Da mesma forma, a própria Comissão Europeia, na sua avaliação publicada em 2020 (SWD(2020) 180 final), reconheceu deficiências graves na implementação do Código, apontando a falta de métricas comuns, o acesso insuficiente a dados por parte dos investigadores e a incapacidade de assegurar uma cooperação eficiente entre plataformas, verificadores e autoridades nacionais. Da mesma forma, a própria Comissão Europeia, na sua avaliação publicada em 2020 (SWD(2020) 180 final), reconheceu deficiências graves na implementação do Código, apontando a falta de métricas comuns, o acesso insuficiente a dados por parte dos investigadores e a incapacidade de assegurar uma cooperação eficiente entre plataformas, verificadores e autoridades nacionais. Esta avaliação crítica foi reiterada e aprofundada na *Comunicação COM(2021) 262 final*, onde a Comissão sublinhou que a aplicação do Código de 2018 permaneceu incoerente e incompleta, sendo limitada pela sua natureza meramente autorreguladora e pela ausência de mecanismos robustos de verificação e responsabilização. A “infodemia” funcionou como um verdadeiro teste de esforço ao Código, expondo as suas lacunas estruturais, como a escassa granularidade dos dados fornecidos pelas plataformas, a falta de um modelo de reporte comum, a fraca cobertura territorial das medidas comunicadas e a persistência da monetização da desinformação através da publicidade online. Em complemento, o Relatório sobre as Eleições Europeias de 2019 (SWD(2020) 113 final) acentuou os riscos políticos e democráticos resultantes da desinformação online e do frágil compromisso das plataformas em garantir integridade informacional, defendendo um reforço estrutural do quadro de regulação e cooperação.

Perante este quadro, emergiu a necessidade de uma abordagem mais exigente e articulada: um novo modelo de co-regulação, com obrigações reforçadas, mecanismos de verificação independentes e sanções proporcionais. Esta nova fase

culminou na adoção do Código de Conduta Reforçado de 2022, integrado numa lógica normativa mais robusta e articulada – posteriormente – com o Regulamento dos Serviços Digitais, orientado para a corresponsabilização, a transparência e a proteção efetiva dos direitos fundamentais no ambiente digital europeu.

Código Reforçado de 2022: Uma Evolução na Governança Digital da UE

A rápida e generalizada migração das interações humanas para o espaço digital, impulsionada em grande parte por eventos globais como a pandemia de COVID-19, amplificou significativamente os desafios associados à desinformação online (Sleibi, 2023). Em resposta a isso e, tal como estabelecido no Plano de Ação para a Democracia na Europa (COM(2020) 790 final, ponto 4.2), a Comissão Europeia publicou, em maio de 2021, diretrizes (COM(2021) 262 final) convidando os signatários a subscrever uma versão revista do Código de Conduta sobre Desinformação. Estas diretrizes, apelavam a compromissos mais fortes e personalizados, à sua implementação célere e eficaz e, a uma participação mais alargada de todas as partes interessadas, incluindo plataformas de menor dimensão e o ecossistema da publicidade. Em particular, a comunicação de 2021 sublinhou a necessidade premente de uma maior responsabilização de todos os signatários, a urgência de medidas mais estruturadas e coesas que superassem as limitações de uma abordagem meramente voluntária, bem como a definição de indicadores-chave de desempenho (KPIs) mais precisos, capazes de assegurar uma monitorização eficaz e uma avaliação independente. Continuaram ainda a destacar a importância de desmonetizar a desinformação, aumentar a transparência da publicidade política, capacitar os utilizadores e melhorar o acesso a dados para investigadores e verificadores de factos.

A experiência do Código de 2018 serviu, assim, como um catalisador crucial para o desenvolvimento do Código Reforçado de Conduta sobre Desinformação de 2022. A nova versão do Código emerge assim como um documento mais ambicioso, tecnicamente detalhado e politicamente exigente, estruturado em 44 compromissos e 128 medidas específicas. Diferentemente da versão anterior, cuja elaboração se

restringiu a um círculo mais limitado de intervenientes, o Código de 2022 nasce de um processo alargado de co-construção, envolvendo 34 signatários iniciais provenientes de uma pluralidade de sectores⁴³. Este leque alargado inclui não apenas as grandes plataformas digitais (como Google, Meta, Twitter/X e Microsoft), mas também pequenas plataformas, representantes da indústria publicitária, redes de verificadores de factos, organizações da sociedade civil e empresas especializadas no fornecimento de soluções tecnológicas para a mitigação de conteúdos nocivos. Mantém e expande os cinco domínios centrais do texto original, designadamente o controlo da colocação de anúncios; a transparência da publicidade política e temática; a integridade dos serviços; a capacitação dos utilizadores; e o apoio à comunidade de investigação. Entre as várias diferenças entre os dois códigos, destaca-se assim o objetivo de reforçar a colaboração com os verificadores de factos (fact-checkers) e com a comunidade académica, bem como a incorporação de tecnologias de ponta, como a inteligência artificial (IA), para enfrentar problemas emergentes.

A operacionalização do Código Reforçado de 2022 introduz um sistema significativamente mais estruturado de monitorização e responsabilização, procurando superar as fragilidades do modelo anterior de 2018. Nesse sentido, os signatários comprometem-se a apresentar relatórios de base (“baseline reports”), conforme estipulado no Compromisso 43, no prazo de seis meses após a adesão, sendo a atualização subsequente obrigatória semestralmente para as Plataformas de Muito Grande Dimensão (VLOPs) e anualmente para os demais intervenientes. Estes relatórios contemplam um total de 152 indicadores, repartidos entre 111 qualitativos (Qualitative Reporting Elements – QREs) e 42 quantitativos (Service Level Indicators – SLIs), permitindo uma análise mais rigorosa e comparável da implementação das medidas. Adicionalmente, o Código Reforçado estabelece que os provedores de VLOPs e VLOSEs se comprometem a ser "auditados às suas próprias custas, pela sua conformidade com os compromissos assumidos ao abrigo deste Código" (Strengthened Code of Practice on Disinformation, 2022, Compromisso 44). Essas auditorias devem ser realizadas por "organizações independentes e sem conflito de interesses" e com "comprovada experiência na área da desinformação, competência técnica e capacidades apropriadas, e objetividade e ética profissional comprovadas".

⁴³ Atualmente, a 13 de fevereiro de 2025, encontra-se com 42 signatários

Um dos avanços mais significativos foi a introdução dos chamados “Indicadores Estruturais” (Structural Indicators - SIs), concebidos em colaboração entre o Observatório Europeu dos Meios Digitais (EDMO), o Grupo Europeu de Reguladores para os Serviços de Comunicação Audiovisual (ERGA) e peritos independentes. Estes visam aferir os recursos, estratégias e processos organizacionais que as plataformas implementam para garantir a concretização efetiva do Código. O segundo relatório do EDMO (Nenadić, Brogi, Bleyer-Simon, & Reviglio, 2024) sublinha, entre outras dimensões cruciais, a importância de dados sobre a cooperação com verificadores de factos – nomeadamente no que toca ao financiamento e alcance das atividades de verificação —, os investimentos financeiros e humanos mobilizados para a execução do Código, e o impacto real das políticas adotadas no combate à desinformação, incluindo medidas de remoção de conteúdos, desmonetização e redução da visibilidade.

Contudo, persiste um conjunto de desafios estruturais relevantes: o EDMO identifica obstáculos na obtenção de dados, bem como uma resistência continuada por parte de algumas plataformas em partilhar informação detalhada sobre os seus processos internos. Limitando assim a monitorização independente e dificultando a transformação do compromisso voluntário numa verdadeira responsabilização pública. Ainda assim, a integração de indicadores estruturais representa um passo decisivo na transição de uma lógica meramente declarativa para um modelo centrado na implementação substantiva e na reforma das práticas de governança digital.

A Comissão Europeia continua a desempenhar um papel central na monitorização e avaliação do Código Reforçado. A Opinião de 13 de fevereiro de 2025 sobre a avaliação do Código de Práticas sobre Desinformação, reitera o seu compromisso em "monitorizar e avaliar regularmente a consecução dos objetivos do Código de Práticas sobre Desinformação" e "incentivar e facilitar a revisão e adaptação regulares desse código".

A mudança mais significativa em relação ao código anterior reside no facto de este ser integrado no DSA. A combinação entre o Código e o DSA permite estabelecer um equilíbrio entre obrigações vinculativas e métodos operacionais flexíveis, capazes de se adaptar às especificidades de cada plataforma, transitando para um modelo de co-regulação (Guedes, et al., 2025). Esta interconexão confere ao

Código um peso regulatório sem precedentes. O Artigo 45.º do DSA permite que a Comissão Europeia reconheça os códigos de conduta como o Código Reforçado como ferramentas para o cumprimento das obrigações do DSA, particularmente para as VLOPs e VLOSEs (BOARD, 2025). Esta vinculação significa que – para as plataformas designadas como VLOPs e VLOSEs – a adesão e o cumprimento dos compromissos do Código Reforçado não são meramente voluntários, mas podem ser considerados parte das suas obrigações de mitigação de riscos ao abrigo do DSA. A ameaça de sanções, que podem ascender a 6% do volume de negócios global anual da empresa em caso de incumprimento das obrigações do DSA, transforma fundamentalmente a dinâmica da conformidade, incentivando as plataformas a uma implementação mais robusta e menos simbólica das medidas (Comission, COMMISSION OPINION of 13.2.2025 on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065, 2025). A Comissão também indica que irá avaliar os "níveis de compromisso individuais dos provedores de VLOPs e VLOSEs signatários do Código, bem como a sua implementação", e, se necessário, "realizará diálogos regulatórios com esses provedores e decidirá sobre outras ações de acompanhamento apropriadas". As suas conclusões sobre o reconhecimento do Código de Conduta sobre Desinformação como um código de conduta nos termos do Artigo 45 do DSA fornecem uma avaliação crítica do progresso e apontam para áreas onde os signatários precisam melhorar, como a necessidade de aumentar o nível de adesão e de aplicar uma abordagem em várias camadas para a verificação de factos.

O Comité Europeu para os Serviços Digitais⁴⁴ também desempenha um papel crucial, fornecendo uma avaliação crítica do progresso e apontando áreas para melhoria, como a necessidade de aumentar o nível de adesão e de aplicar uma abordagem em várias camadas para a verificação de factos. Enfatiza a importância do escrutínio da colocação de anúncios e da desmonetização da desinformação como "áreas de importância chave para combater a desinformação de forma eficiente". Em

⁴⁴ O Comité Europeu dos Serviços Digitais é um órgão consultivo independente criado ao abrigo do Regulamento dos Serviços Digitais (Regulamento (UE) 2022/2065). É composto pelos Coordenadores dos Serviços Digitais de cada Estado-Membro da União Europeia e presidido pela Comissão Europeia. A sua principal missão consiste em garantir a aplicação coerente e eficaz do Regulamento em toda a União, promovendo a cooperação institucional, emitindo pareceres técnicos, coordenando grupos de trabalho especializados e apoiando a supervisão das plataformas e motores de busca de muito grande dimensão. Informação oficial disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/dsa-board> (consultado em 02 de junho de 2025).

conjunto, estes mecanismos de conformidade e responsabilização procuram garantir que o Código Reforçado não seja apenas uma declaração de boas intenções, mas um instrumento eficaz para promover um ambiente online mais seguro e transparente⁴⁵.

Apesar dos avanços teóricos e dos novos mecanismos de responsabilização introduzidos pelo Código Reforçado de 2022, a sua eficácia, na prática, é o verdadeiro teste da sua capacidade de combater a desinformação online. As primeiras avaliações, baseadas nos relatórios das plataformas e na análise de entidades independentes como o EDMO, revelam um quadro misto de progresso e desafios persistentes. A desmonetização de conteúdo de desinformação é um pilar central do Código Reforçado, visando cortar o fluxo de receitas que sustenta os disseminadores de conteúdo falso. O compromisso de "evitar a colocação de publicidade junto de conteúdo de desinformação" (Código de Conduta sobre Desinformação reforçado de 2022) é fundamental. No entanto, (Papadogiannakis, Papadopoulos, Kourtellis, & Markatos, 2023) apresentam uma análise crítica sobre este aspeto. A sua investigação – que se focou na extensão em que as redes de anúncios continuam a publicitar em sites de desinformação – concluiu que, embora possa parecer haver uma melhoria superficial, não há uma redução significativa na quantidade de relações de publicidade entre sites populares de desinformação e grandes redes de anúncios (Papadogiannakis, Papadopoulos, Kourtellis, & Markatos, 2023). Sugeriram que as redes de anúncios se retiraram principalmente de sites de desinformação impopulares com poucos visitantes, mas "ainda formam relações com sites altamente não confiáveis que representam a maioria da desinformação" (Papadogiannakis, Papadopoulos, Kourtellis, & Markatos, 2023, p. 1). Esta constatação sugere uma lacuna significativa na implementação efetiva da desmonetização, particularmente em relação aos maiores disseminadores de desinformação. Este tópico foi também

⁴⁵ Numa entrevista concedida a Zorloni (12 de setembro de 2024), Roberto Viola, diretora-geral da Direção-Geral Connect da Comissão Europeia, explicou que todos os regulamentos têm um ciclo de implementação que não dura apenas alguns meses. É necessário, no mínimo, um par de anos para os ativar plenamente. No caso do DSA, um elemento fundamental que ainda não está plenamente em vigor é a auditoria algorítmica – ou seja, um controlo externo dos algoritmos das plataformas, essencial para compreender como os dados são utilizados. Viola acrescentou: “Agora entramos nessa fase; o DSA implica uma auditoria aos sistemas de recomendação algorítmica por uma empresa independente.” As observações de Viola sugerem claramente que um processo de mudança radical exige tempo, sendo apenas através de esforços constantes e monitorização contínua que será possível avaliar a sua eficácia real e identificar eventuais fragilidades. Contudo, o DSA foi já testado nas eleições europeias de 2024, durante as quais não se registaram ataques sistémicos, nem foi necessário ativar quaisquer procedimentos de emergência por parte da Comissão. Segundo o Observatório Europeu dos Media Digitais (EDMO), tal poderá dever-se à rápida identificação de ameaças e à maior atenção dedicada ao fenómeno da desinformação (D’Andrea, Fusacchia, & D’Ulizia, 2025)

discutido (The recognition of the Code of Practice on Disinformation as a code of conduct pursuant to Article 45 of Regulation 2022/2065 (Digital Services Act or “DSA”), 2025) que destacou a importância do escrutínio da colocação de anúncios e da desmonetização como áreas de importância chave para combater a desinformação de forma eficiente.

A transparência na publicidade política é outra área-chave do Código Reforçado, com requisitos para “rotulagem” clara, repositórios de anúncios e acessos a dados via APIs (Código de Conduta sobre Desinformação reforçado de 2022, 2022, pp. 10-13)⁴⁶. Embora sejam avanços significativos, a qualidade dos dados e a utilidade das APIs para investigadores e a sociedade civil ainda são temas de discussão, e a aplicação consistente da rotulagem continua a ser um desafio. A qualidade e a granularidade dos dados disponibilizados nos repositórios podem variar entre as plataformas, e o acesso e a utilidade das APIs para investigadores e a sociedade civil ainda são temas de discussão. A garantia de que a identificação, de conteúdos desinformadores, é consistentemente aplicada e facilmente compreensível pelos utilizadores continua a ser um desafio.

Uma análise conduzida por (Borz, Francesco, Montgomerie, & Bellis, 2024) evidencia a persistente assimetria nas prioridades entre a UE e as empresas. Enquanto a UE assume como desígnio primordial a salvaguarda da democracia, a proteção dos direitos fundamentais e a integridade do espaço público digital, as plataformas tendem a privilegiar a preservação da sua reputação, a maximização do lucro e a mitigação de riscos jurídicos (Borz, Francesco, Montgomerie, & Bellis, 2024). Com efeito, embora muitas plataformas tenham manifestado um elevado – onsubstanciado em declarações de intenção e políticas internas —, a sua tradução prática em medidas concretas e o verdadeiro alinhamento com os valores democráticos (aquilo a que os autores designam por “compromisso simbólico”) têm-se revelado substancialmente mais ténues (Borz, Francesco, Montgomerie, & Bellis, 2024). Esta "conformidade simbólica" permitia às empresas sinalizar acordo sem necessariamente traduzi-lo em mudanças substantivas. Essa divergência de orientações traduziu-se numa subvalorização, por parte das plataformas, de compromissos relacionados com os direitos democráticos e a liberdade de expressão, em favor de áreas consideradas

⁴⁶ Estes compromissos visam aumentar a visibilidade de quem está a pagar por anúncios políticos, o seu público-alvo e o montante gasto, o que é crucial para a integridade eleitoral.

menos sensíveis ao seu modelo de negócio, como a integridade dos serviços, o empoderamento dos utilizadores e a responsabilidade partilhada (Borz, Francesco, Montgomerie, & Bellis, 2024). O Código Reforçado de 2022 procurou atenuar este desequilíbrio, impondo compromissos mais explícitos e articulados com o novo quadro jurídico europeu, nomeadamente através da sua interligação com o DSA. Resta saber, no entanto, se o potencial sancionatório previsto no DSA será suficiente para induzir uma verdadeira mudança comportamental nas plataformas, incentivando-as a dedicar atenção efetiva a todos os eixos do Código – e não apenas àqueles que melhor protegem os seus interesses comerciais. Neste sentido, tanto a Comissão Europeia como o Comité das Entidades para os Serviços Digitais manifestaram a intenção de intensificar o escrutínio e monitorizar atentamente a aplicação concreta dos compromissos assumidos por cada signatário, com especial foco na coerência, abrangência e efetividade das medidas implementadas.

Olhando para o futuro, a regulação da desinformação na UE enfrentará vários desafios. A rápida evolução tecnológica, incluindo a inteligência artificial – que pode criar desinformação de forma mais sofisticada e em escala – exigirá uma adaptação contínua do Código e do quadro regulatório. A aplicação consistente, garantindo uma aplicação consistente e eficaz das disposições do DSA e do Código Reforçado em todas as VLOPs e VLOSEs, será crucial. A natureza transfronteiriça da desinformação exige uma cooperação internacional contínua para evitar "paraísos" regulatórios e garantir uma abordagem global coordenada. Por fim, manter um equilíbrio cuidadoso entre a luta contra a desinformação e a proteção da liberdade de expressão, da privacidade e da inovação continuará a ser um imperativo central da abordagem da UE.

Em suma, o Código Reforçado de Conduta de 2022 representa um passo audacioso e necessário na jornada da UE para construir um espaço digital mais seguro e confiável. A sua eficácia será determinada não apenas pela sua letra, mas pela sua implementação rigorosa, pela capacidade de adaptação a um cenário tecnológico em constante mudança e pelo compromisso contínuo de todas as partes interessadas em defender a integridade do debate público e os valores democráticos na era digital.

The EU Digital Services Package

A transição da União Europeia para uma governação mais robusta e sistemática do espaço digital consubstancia-se, de forma paradigmática, no chamado Digital Services Package – composto essencialmente pelo Regulamento dos Serviços Digitais (DSA) e pelo Regulamento dos Mercados Digitais (DMA)⁴⁷. Este pacote legislativo marca o início do fim da era de “autorregulação quase absoluta” das plataformas digitais, que até então operavam sob os auspícios da Diretiva do Comércio Eletrónico (Diretiva 2000/31/CE), beneficiando de um quadro normativo flexível, mas desprovido de mecanismos eficazes de escrutínio e responsabilização⁴⁸ (Leiser, 2023). Na génese desta nova abordagem está o reconhecimento político e jurídico de que as plataformas digitais não são meros intermediários neutros, mas agentes estruturantes da esfera pública digital (Bartóki-Gönczy, 2021). Estas entidades detêm um poder considerável na definição das regras de visibilidade, acesso à informação e moldagem do discurso público (Balkin, 2017). Apesar disso, importa sublinhar que o DSA não revoga a e-Commerce Directive, antes a complementa. Nesse sentido, a abordagem da União Europeia à governação das plataformas continua a assentar em três princípios fundamentais, consagrados na Diretiva do Comércio Eletrónico: em primeiro lugar, o princípio do país de origem exige que as plataformas cumpram as leis do Estado-Membro onde estão estabelecidas (artigo 3.º); em segundo lugar, em determinadas condições, o princípio da responsabilidade limitada isenta as plataformas de qualquer responsabilidade relativamente aos conteúdos que alojam (artigos 12.º a 14.º da Diretiva), até que sejam notificadas da sua ilicitude; por fim, a proibição de qualquer obrigação geral de monitorização garante a proteção de direitos fundamentais como a liberdade de expressão, a

⁴⁷ O Regulamento (UE) 2022/1925, conhecido como *Digital Markets Act* (DMA), estabelece um conjunto de obrigações e proibições dirigidas às plataformas designadas como *gatekeepers*, isto é, entidades que detêm uma posição consolidada e duradoura de intermediação entre empresas e utilizadores finais no ecossistema digital. Entre as principais disposições destacam-se as constantes dos artigos 5.º a 7.º, que consagram práticas proibidas e obrigações ex ante, como a interoperabilidade entre serviços de comunicação (art. 7.º), a proibição de auto-preferenciação (art. 6.º, n.º 5) ou a partilha de dados com utilizadores empresariais (art. 6.º, n.º 10). A Comissão Europeia assume um papel central na aplicação do regulamento, podendo aplicar coimas até 10% do volume de negócios anual global (art. 30.º), realizar investigações de mercado (arts. 17.º a 20.º) e impor medidas corretivas estruturais (art. 18.º). Pela limitação de espaço e enfoque deste trabalho, o DMA não será aqui aprofundado, embora a sua articulação com o DSA constitua um pilar essencial da estratégia europeia de regulação do ambiente digital.

⁴⁸ Gerando perceções de arbitrariedade e falta de responsabilização, o que levou algumas, como o Facebook e a TikTok, a instituírem conselhos consultivos na tentativa de restaurar a confiança dos utilizadores (Leiser, 2023).

privacidade e a proteção de dados (artigo 15.º da Diretiva do Comércio Eletrónico) (Leiser, 2023). O "safe harbour" (artigo 14.º da ECD) e a proibição de monitorização geral (artigo 15.º) – confirmados por jurisprudência do Tribunal de Justiça da União Europeia (TJUE) – ⁴⁹, visaram proteger, respetivamente, o direito à liberdade de expressão e o direito à privacidade. Contudo, o DSA, embora mantendo este regime, estabelece limitações e exceções, condicionando a aplicação do "safe harbour" à não interferência ativa e reforçando a responsabilidade em caso de omissão dolosa ou negligente na remoção de conteúdo ilegal após notificação (JODANOVIC, 2024). Contudo, a arquitetura do regime anterior apresentava fragilidades significativas. A ausência de obrigações positivas de diligência e o foco nos mecanismos autorregulatórios de moderação favoreceram práticas opacas e inconsistentes, muitas vezes orientadas por critérios comerciais em detrimento da proteção dos direitos fundamentais (Leiser, 2023). A jurisprudência europeia procurou, pontualmente, colmatar essas lacunas, mas fê-lo de forma casuística, sem consolidar um quadro harmonizado e robusto.

Neste novo quadro a União Europeia consagra, de forma inequívoca, a necessidade de reconfigurar as responsabilidades das plataformas digitais, adotando um modelo normativo assente em obrigações assimétricas proporcionais à escala, influência e impacto dos diferentes operadores. A lógica subjacente a este regime é clara, quanto maior o poder de uma plataforma sobre o ecossistema informacional europeu, maiores devem ser os seus deveres de diligência e mitigação de riscos. É neste contexto que se destacam as obrigações específicas às Plataformas Online de Muito Grande Dimensão (Very Large Online Platforms – VLOPs) e aos Motores de Busca Online de Muito Grande Dimensão (Very Large Online Search Engines – VLOSEs, ou seja, entidades com mais de 45 milhões de utilizadores mensais na UE (artigo 33.º). As estas plataformas são impostas obrigações, incluindo avaliações periódicas de riscos sistémicos (artigo 34.º), auditorias independentes (artigo 37.º), transparência nos sistemas de recomendação (artigo 27.º) e adaptação das suas “interfaces” para prevenir padrões manipulativos (*dark patterns*) (artigo 25.º) (JODANOVIC, 2024). Este novo quadro não se limita, contudo, à definição de princípios éticos ou diretrizes técnicas, consagra um regime de responsabilização

⁴⁹ Nomeadamente nos casos Netlog e Eva Glawischnig-Piesczek v Facebook Ireland Ltd., que vedaram a imposição de filtros genéricos de conteúdo como medida desproporcionada.

efetiva, com a previsão de sanções financeiras severas que podem atingir até 6% do volume de negócios mundial da entidade infratora.

No âmbito do combate à desinformação, o DSA consagra igualmente medidas robustas, abordando-a como um risco sistémico com impacto potencial na saúde pública, nos processos eleitorais e na segurança pública (artigo 34.º, n.º 1, alínea b)). Neste domínio, destaca-se a articulação com o Código de Conduta Reforçado sobre Desinformação de 2022 – previamente referido. Embora este instrumento conserve um carácter voluntário, o seu cumprimento efetivo permite às plataformas signatárias invocar uma presunção de cumprimento das obrigações de mitigação de riscos previstas no artigo 35.º, beneficiando assim de uma presunção de diligência na adoção de medidas preventivas, uma vez serem signatários do Código. Tal mecanismo estabelece uma ponte entre soft law e hard law, numa lógica de *co-regulação* (Balázs, 2021).

O reforço do papel dos chamados *trusted flaggers* – entidades independentes acreditadas pelos Coordenadores de Serviços Digitais dos Estados-Membros (Art. 19.º) – constitui outra inovação central. Estas entidades devem cumprir critérios rigorosos de independência, transparência e competência, sendo sujeitas a escrutínio e podendo ver o seu estatuto revogado em caso de abuso (artigo 19.º, n.º 6).

Do ponto de vista da transparência informacional, o DSA dá especial ênfase à criação de repositórios públicos de publicidade, nomeadamente publicidade política e comportamental, especialmente quando dirigida a grupos específicos. O artigo 26.º impõe às plataformas a obrigação de identificar claramente os promotores e financiadores das campanhas, bem como os parâmetros utilizados para a segmentação dos anúncios.

Por outro lado, ainda que o DSA preserve, no artigo 7.º, a proibição de qualquer obrigação geral de monitorização, consagra um modelo que exige das plataformas uma atitude proativa na identificação e mitigação de riscos, através de medidas como a adaptação dos sistemas de recomendação, alterações aos termos de serviço, cooperação com verificadores de factos e medidas de literacia mediática.

Em síntese, o DSA constitui uma tentativa ambiciosa de transitar de um modelo autorregulatório e fragmentado para uma governação digital europeia

estruturada, centrada na responsabilidade proporcional das plataformas, na proteção de direitos fundamentais e na transparência dos processos. A sua eficácia dependerá, contudo, da capacidade de implementação efetiva, da articulação entre os diversos atores envolvidos – plataformas, sociedade civil, autoridades nacionais e Comissão Europeia – e da consolidação de uma cultura de responsabilidade partilhada no espaço digital europeu. Ambos os regulamentos (DSA e o DMA) assentam numa abordagem regulatória mista, que conjuga elementos de regulação tradicional ("command-and-control") (Dooley, 2024) com modelos de autorregulação e co-regulação, promovendo a participação dos próprios agentes regulados, bem como o envolvimento ativo da Comissão Europeia e das autoridades nacionais através da figura dos Coordenadores de Serviços Digitais (DSCs). Apesar de todos estes avanços, o DSA não escapa a críticas significativas – como se verá na secção seguinte – sobretudo no que respeita à vagueza dos conceitos jurídicos centrais - como “conteúdo ilegal”, “desinformação” ou “risco sistémico” – a ausência de uma harmonização eficaz no seio do mercado interno, as exigências excessivas ou irrealistas de diligência devida impostas às plataformas digitais, a centralização do poder político na governação do espaço digital europeu e, por fim, o dilema emergente entre liberdade de expressão e a automação algorítmica, que ainda que eficazes do ponto de vista técnico, suscita fundadas preocupações quanto a enviesamentos algorítmicos e falhas de contextualização, com potencial impacto na liberdade de expressão e outros direitos fundamentais dos utilizadores (Atzori, 2024). Ainda assim, a sua promulgação representa um passo decisivo na afirmação de um modelo europeu de regulação digital baseado nos valores fundamentais da União: dignidade humana, liberdade, pluralismo e responsabilidade democrática.

Críticas ao Regulamento dos Serviços Digitais (DSA): Limites, Ambiguidades e Riscos para os Direitos Fundamentais

O DSA representa um dos mais ambiciosos quadros normativos do Séc. XXI no que concerne à regulação do ambiente digital, visando estabelecer um ambiente mais seguro, transparente e responsável para utilizadores e empresas (Dooley, 2024). Surge como resposta ao crescente reconhecimento de que as plataformas digitais desempenham um papel significativo na formação do discurso público, na facilitação

do comércio e na disseminação de informação. Apesar de proclamar o propósito de garantir um espaço digital mais seguro, transparente e responsável, o DSA enfrenta o risco de se transformar num instrumento de repressão disfarçado, com potencial para comprometer gravemente a liberdade de expressão e o pluralismo democrático no seio da União Europeia (Atzori, 2024).

As críticas ao DSA incidem, em larga medida, sobre o modo como o regulamento articula os seus objetivos com os instrumentos que propõe. As suas formulações conceptuais ambíguas, as exigências desproporcionadas impostas às plataformas, a ausência de garantias processuais robustas para os utilizadores e a concentração de poderes em entidades administrativas com frágil legitimação democrática suscitam interrogações fundamentais sobre a coerência do quadro proposto com os valores fundacionais da União Europeia.

Neste capítulo, propõe-se uma análise crítica e sistematizada das principais fragilidades do DSA, com o objetivo de compreender até que ponto este novo regime regulatório responde de forma adequada aos desafios do mundo digital – ou se, paradoxalmente, contribui para os agravar. Ao fazê-lo, procura-se também contribuir para uma reflexão mais ampla sobre a necessidade de garantir que qualquer processo de regulação do “ciberespaço” seja ancorado em princípios claros de legalidade, proporcionalidade, transparência e responsabilidade democrática. Porque regular é, sim, necessário – mas é igualmente imperativo que essa regulação não se transforme num mecanismo de erosão das liberdades que define, em última instância, a identidade política e jurídica da União Europeia.

A ambiguidade terminológica e os riscos de sobreposição

Uma das críticas mais prementes ao DSA reside na sua linguagem potencialmente vaga e excessivamente ampla, que, embora pretenda ser “à prova de futuro” ao adotar uma abordagem baseada no risco, pode levar a interpretações inconsistentes e a uma aplicação desarmonizada em toda a União Europeia. Conceitos centrais como “conteúdo ilegal”, “risco sistémico”, “moderação de conteúdos” ou “desinformação” não se encontram suficientemente delimitados, conferindo um poder discricionário considerável às plataformas e às autoridades nacionais para interpretar e aplicar as disposições legais de forma desigual (Atzori, 2024). Esta indefinição pode

ser facilmente instrumentalizada para justificar a remoção de conteúdos legítimos, sobretudo quando os interesses políticos ou económicos assim o ditarem.

A imprecisão da noção de "conteúdo ilegal" (artigo 3.º e artigo 9.º do DSA)

O artigo 3.º, alínea h), do DSA define "conteúdo ilegal" como qualquer informação que, nos termos da legislação aplicável (nacional ou da União), seja considerada ilícita, incluindo, por exemplo, discurso de ódio, conteúdos terroristas, mensagens discriminatórias ou violações de direitos de propriedade intelectual. Esta formulação confere a cada Estado-Membro a faculdade de estabelecer, segundo os seus próprios critérios legislativos, o que deve ou não ser considerado ilegal. O artigo 9.º reforça esta possibilidade ao permitir que as autoridades nacionais imponham ordens para a remoção de conteúdos com base na sua própria legislação. Esta dualidade normativa – entre o direito da União e os ordenamentos jurídicos nacionais – compromete seriamente a harmonização pretendida pelo DSA, e, mais preocupante ainda, abre caminho a uma aplicação fragmentada e desigual da norma em todo o território europeu

Particularmente alarmante é a possibilidade, real e já verificada, de certos Estados-Membros criminalizarem a desinformação, equiparando-a a conteúdo ilegal – representando uma ameaça direta à liberdade de expressão (Atzori, 2024). Em países como Malta, França, Grécia ou Hungria⁵⁰, por exemplo, existem disposições penais que criminalizam a divulgação de "informações falsas", frequentemente com base em categorias vagas e suscetíveis de abuso. Esta realidade conduz à possibilidade de remoção de conteúdos legítimos sob o pretexto de combater a desinformação, sem garantias processuais adequadas para os utilizadores (Fathaigh, Helberger, & Appelman, The perils of legally defining disinformation, 2022). Bem como pode conduzir inevitavelmente a um “*chilling effect*”, inibindo os utilizadores de partilharem opiniões potencialmente controversas, mas legítimas – comprometendo a vitalidade dos debates públicos

⁵⁰ A Lituânia é, até à data, o único Estado-Membro da União Europeia que consagra explicitamente uma definição legal de “desinformação” e que proíbe a sua disseminação intencional no seu ordenamento jurídico interno, nos termos dos artigos 2.º e 19.º da *Lei sobre a Prestação de Informação ao Público* (Law on the Provision of Information to the Public).

A ambiguidade em torno do conceito de "desinformação" e os riscos para a liberdade de expressão

Outro problema grave é a indefinição do conceito de "desinformação". Esta ausência de rigor normativo transforma a desinformação numa categoria aberta, suscetível de ser usada politicamente como mecanismo de silenciamento da crítica, em especial em contextos de dissidência política, campanhas eleitorais ou crises sanitárias (Atzori, 2024). Tal como salientam (Fathaigh, Helberger, & Appelman, The perils of legally defining disinformation, 2022), esta ambiguidade foi amplamente explorada durante a pandemia de COVID-19, com medidas governamentais que resultaram na censura de opiniões dissidentes ou críticas às políticas públicas⁵¹. A este respeito, a Declaração Conjunta emitida pelo Relator Especial da ONU sobre a Liberdade de Opinião e Expressão (2017) alertou para a incompatibilidade entre proibições gerais baseadas em conceitos vagos como "notícias falsas" ou "informações não objetivas" e os padrões internacionais de proteção da liberdade de expressão. Em 2020, uma nova declaração reforçou esta advertência, recomendando explicitamente que os Estados se abstenham de adotar legislações que criminalizem a desinformação, dado o elevado risco de abuso e de silenciamento do discurso legítimo (Karanicolas, 2019).

Riscos sistémicos e o escopo excessivamente lato dos artigos 34.º e 35.º

A questão torna-se ainda mais sensível quando analisamos os artigos 34.º e 35.º do DSA, que impõem às plataformas de muito grande dimensão a obrigação de realizarem avaliações de risco, incluindo os "efeitos negativos previsíveis sobre o discurso cívico, os processos eleitorais, a segurança pública ou a saúde pública" e implementar medidas para mitigar esses impactos. Ainda que à primeira vista estas disposições possam parecer razoáveis, a sua formulação vaga e genérica revela-se problemática. Termos como "efeitos negativos" ou "integridade do discurso cívico" carecem de objetividade e podem abranger críticas legítimas às autoridades públicas,

⁵¹ Durante a pandemia de COVID-19, diversos Estados europeus adotaram medidas de controlo da informação que suscitaram preocupações quanto à censura de opiniões dissidentes. Exemplo disso são os casos da Roménia, onde sites foram bloqueados sem recurso judicial; da Grécia, com financiamento seletivo de meios de comunicação ("lista Petsas"); da Polónia, onde profissionais de saúde foram demitidos por questionar sobre as condições hospitalares, além disso, o Ministério da Saúde proibiu os consultores regionais de saúde de falarem publicamente sobre o Covid sem prévia aprovação estatal; e de Espanha, onde se verificaram restrições ao acesso de jornalistas e vigilância ativa sobre conteúdos online.

campanhas políticas de oposição ou debates controversos sobre políticas de saúde. Como observa (Barata, 2021), esta amplitude conceitual coloca em risco a deliberação democrática e pode legitimar a censura preventiva sob pretextos genéricos. Neste quadro, os operadores de plataformas veem-se forçados a adotar tecnologias automatizadas de moderação para cumprir exigências. Conforme advertido por (Atzori, 2024) e (Barata, 2021), estas tecnologias, são particularmente suscetíveis a enviesamentos sistemáticos, erros de classificação e interpretações desajustadas.

A arquitetura normativa do DSA, ao recorrer a conceitos vagos e excessivamente amplos e ao confiar às plataformas e às autoridades nacionais poderes praticamente discricionários, introduz um risco sistémico para a liberdade de expressão no espaço europeu. A ausência de salvaguardas claras, a possibilidade de criminalização da desinformação e a fragmentação regulatória resultante das diferentes interpretações nacionais do DSA podem transformar este instrumento legislativo, com intenções legítimas, num veículo de repressão digital e erosão dos direitos fundamentais.

A Falta de Harmonização no Mercado Interno: Riscos Sistémicos e Ameaças à Coerência Regulamentar Europeia

Apesar de o DSA enunciar, entre os seus objetivos fundamentais, o propósito de criar um conjunto de regras uniformes, eficazes e proporcionais para os prestadores de serviços intermediários na União Europeia – com vista a evitar a fragmentação do mercado interno e a garantir segurança jurídica (Recital 4) –, a sua arquitetura revela fragilidades significativas que, em vez de resolverem a dispersão existente, podem, agravá-la (Fathaigh, Helberger, & Appelman, The perils of legally defining disinformation, 2022).

O Artigo 9.º e os Efeitos nas Ordens Nacionais

Um dos principais catalisadores desta disfunção encontra-se no artigo 9.º do regulamento, que permite às autoridades nacionais emitirem ordens para agir contra conteúdos ilegais com base na legislação nacional – e com efeitos transfronteiriços. Este mecanismo comporta implicações alarmantes. Ao consagrar a possibilidade de um Estado-Membro “exportar” os seus padrões normativos restritivos, o artigo 9.º enfraquece os esforços de uniformização legislativa e colide frontalmente com

princípios fundamentais do direito internacional (Barata, 2021). Além disso, esta lógica regulatória poderá dar lugar a interpretações abusivas e politicamente motivadas, alimentando um terreno fértil para a censura indireta de conteúdos legítimos, como o discurso político, a sátira ou a investigação científica controversa. A margem de discricionariedade conferida às autoridades nacionais é particularmente problemática quando aplicada a categorias vagas como “discurso de ódio”, “extremismo” ou “desinformação”, cujo significado e alcance variam substancialmente de país para país (Fathaigh, Helberger, & Appelman, 2022). É certo que o próprio artigo 9.º estabelece salvaguardas formais, exigindo que as ordens nacionais sejam emitidas em conformidade com o direito da União, devidamente fundamentadas, proporcionais, territorialmente delimitadas e respeitadoras dos direitos fundamentais consagrados na Carta. Não se trata, portanto, de uma autorização genérica ou ilimitada para impor censura transfronteiriça – ainda que, na prática, o uso abusivo desta disposição possa levantar preocupações legítimas sobre harmonização normativa, proporcionalidade e risco de fragmentação jurídica, como apontado por diversos autores.

Fragmentação Normativa e Insegurança Jurídica

A manutenção, pelo DSA, da liberdade legislativa nacional em domínios sensíveis torna o sistema europeu vulnerável a uma aplicação desigual das regras. Esta fragmentação normativa afeta negativamente a previsibilidade jurídica exigida pelas plataformas, elevando os custos de conformidade regulatória e comprometendo a experiência dos utilizadores, que se veem submetidos a diferentes níveis de proteção de direitos consoante a jurisdição aplicável. O impacto desta inconsistência torna-se ainda mais crítico quando associado à questão da desinformação. Como demonstrado por (Fathaigh, Helberger, & Appelman, 2022), vários Estados-Membros possuem disposições penais que criminaliza a disseminação de “notícias falsas” ou “informações enganosas” – como acontece, por exemplo, na Lituânia, França, Hungria, Croácia ou Roménia. A ausência de uma definição clara e uniforme de “desinformação” no DSA significa que qualquer conteúdo classificado como tal poderá ser removido ou sancionado de acordo com normas internas mais restritivas, sem salvaguardas adequadas à liberdade de expressão, e, em muitos casos, em violação direta do artigo 19.º do Pacto Internacional sobre os Direitos Civis e

Políticos, do artigo 10.º da Convenção Europeia dos Direitos Humanos e do artigo 11.º da Carta dos Direitos Fundamentais da União Europeia.

Obrigações de Diligência Devida: Entre a Proteção e a Censura Algorítmica

O DSA impõe às plataformas – em especial às de muito grande dimensão – obrigações rigorosas e complexas de diligência devida, exigindo a adoção de medidas proativas de avaliação e mitigação de riscos sistémicos. Fundamentadas no objetivo de criar um espaço digital “seguro, previsível e de confiança (Recital 3) estas exigências visam garantir uma maior responsabilização das plataformas face à proliferação de conteúdos ilegais e à emergência de riscos sistémicos. No entanto, na prática, estas obrigações revelam-se, em muitos casos, desproporcionadas, vagamente definidas e dificilmente executáveis, especialmente para plataformas de menor escala ou com recursos limitados (Barata, 2021).

Novamente, a indefinição conceptual que caracteriza o DAS potencia desigualdades na aplicação das obrigações previstas, delegando de forma excessiva nas plataformas privadas a responsabilidade de identificar, classificar e remover esses conteúdos. Esta situação é particularmente visível no artigo 16.º do DSA, que estabelece os chamados mecanismos de “notificação e ação”. Através deste regime, basta a receção de uma denúncia por terceiros para que uma entidade privada tenha de tomar decisões sobre a licitude do conteúdo em causa – muitas vezes, sem acesso a critérios objetivos ou fundamentação jurídica clara. Paralelamente, os artigos 34.º e 35.º outorgam-lhes poderes vastos – mas mal definidos – para avaliar e mitigar “riscos sistémicos”, sem delimitar com precisão o seu conteúdo, alcance ou limites.

Este enquadramento normativo atribui às plataformas funções tipicamente reservadas ao poder público, como a ponderação de direitos fundamentais, a qualificação jurídica de condutas e a imposição de medidas restritivas – mas fá-lo sem os mecanismos essenciais de escrutínio democrático, imparcialidade institucional ou contraditório. Como sublinha (Barata, 2021), estas entidades comerciais são transformadas em pseudo-reguladores da esfera pública digital, sem a legitimidade, transparência ou responsabilidade que se exige à Administração Pública num Estado de Direito. E, dessa forma, obriga as plataformas a recorrer a filtros automáticos e algoritmos de deteção de conteúdos potencialmente ilegais ou danosos. Embora estas

ferramentas tecnológicas proporcionem uma resposta célere e escalável, a sua eficácia é limitada: algoritmos não compreendem contextos culturais, ironia, ambiguidade linguística ou intencionalidade comunicativa. Sob pressão de um quadro sancionatório severo e da ameaça de coimas, que podem atingir até 6% do volume de negócios global, muitas plataformas optam por adotar políticas internas de moderação excessivamente conservadoras. Este fenómeno, conhecido por *overcompliance*, resulta numa estratégia de remoção preventiva de conteúdos cuja legalidade não é clara, numa lógica de defesa regulatória que privilegia a segurança jurídica da empresa em detrimento da liberdade de expressão dos utilizadores. Esta prática induz um efeito de autocensura sistémico, fragilizando o pluralismo informativo e empobrecendo o espaço público digital.

O efeito cumulativo desta arquitetura é inquietante. Ao atribuir às plataformas o papel de árbitros algorítmicos da legalidade, sem garantias substanciais de transparência, proporcionalidade, o DSA corre o risco de comprometer os próprios valores que proclama defender. A situação é ainda mais preocupante quando se considera que, segundo as normas internacionais de direitos humanos, quaisquer restrições à liberdade de expressão devem ser claras, previsíveis e necessárias num Estado democrático (Karanicolas, 2019).

A Centralização do Poder Político na Governação Digital: Riscos para a Liberdade Informativa

Uma das transformações mais profundas introduzidas pelo Regulamento dos Serviços Digitais reside na sua nova arquitetura de governação do espaço digital europeu, que atribui às autoridades políticas – em especial à Comissão Europeia – um papel central e potencialmente excessivo na supervisão do discurso em linha. Para além dos amplos poderes já conferidos às autoridades nacionais na definição e remoção de “conteúdo ilegal” (arts. 3.º e 9.º), o DSA consagra um modelo de cooperação vertical entre plataformas digitais, coordenadores nacionais (art. 49.º), entidades certificadas como *trusted flaggers* (art. 22.º) e a própria Comissão Europeia, elevando esta última a um verdadeiro ator interventivo na moderação de conteúdos e no combate à desinformação (Barata, 2021).

Este modelo adquire contornos particularmente sensíveis através dos chamados “protocolos de crise”, previstos no artigo 48.º que facultam à Comissão o poder de impor medidas extraordinárias, nomeadamente alterações nos sistemas de moderação algorítmica ou a promoção de conteúdos considerados como “informação fiável”, em contextos de emergência pública. Contudo, a ausência de uma definição normativa precisa sobre o que configura uma “crise” ou o que constitui “informação fiável” confere à Comissão uma margem de discricionariedade excessiva, em dissonância com os princípios fundamentais da separação de poderes, imparcialidade e previsibilidade jurídica. Ainda que o próprio artigo 48.º, n.º4, alínea e), determine que estas medidas devem considerar os “efeitos negativos sobre os direitos fundamentais”, essa cláusula surge desprovida de força vinculativa real, sobretudo na ausência de mecanismos robustos de controlo jurisdicional e escrutínio parlamentar⁵².

O risco de transformar autoridades políticas em árbitros absolutos da verdade – com capacidade para silenciar vozes dissidentes sob o pretexto do combate à desinformação – é incompatível com os padrões internacionais de direitos humanos.

Como bem referem (Sartor & Loreggia, 2020) a liberdade de expressão deve ser protegida mesmo quando envolva opiniões falsas, injustificadas ou controversas, pois é precisamente essa pluralidade, e não a imposição de um discurso oficial, que sustenta o debate democrático. A concentração de poderes decisórios na Comissão Europeia – sem contrapesos judiciais ou parlamentares adequados – compromete não apenas o equilíbrio institucional europeu, mas também a própria integridade do espaço público digital. Apesar de o DSA prever mecanismos procedimentais para contestar decisões de moderação, a sua eficácia permanece altamente questionável. Como alertam (Dooley, 2024) e (Leiser, 2023) existe o risco de que, na prática, os utilizadores sejam confrontados com processos complexos e pouco transparentes para fazer valer os seus direitos.

Por fim, importa salientar que o modelo de conformidade imposto pelo DSA poderá reforçar a concentração de mercado nas mãos das grandes plataformas, penalizando desproporcionalmente os operadores de pequena e média dimensão. A

⁵² A título ilustrativo, declarações recentes de altos responsáveis da União Europeia – como a do Comissário Thierry Breton, admitindo o encerramento de plataformas em contexto de agitação social – suscitam legítimas preocupações quanto à tentação de instrumentalização política da regulação digital.

exigência de implementação de sistemas sofisticados de moderação, auditoria e transparência poderá exceder as capacidades financeiras e técnicas desses agentes, conduzindo, na prática, à exclusão do mercado digital ou à sua dependência de serviços oferecidos pelas plataformas dominantes (JODANOVIC, 2024)⁵³. Tal pode intensificar a concentração do mercado digital em torno das grandes plataformas, contrariando os objetivos de pluralismo e concorrência leal.

O Dilema da Liberdade de Expressão e a Armadilha da Automação Algorítmica: Entre a Censura Preventiva e a Erosão Democrática

Como já verificamos, ao mesmo tempo que proclama a defesa dos direitos fundamentais, o DSA impõe às plataformas – sobretudo às de muito grande dimensão – obrigações de diligência que, na prática, podem gerar efeitos colaterais preocupantes para a liberdade de expressão, carecendo de mecanismos concretos que a garantam eficazmente na prática (Barata, 2021). Abrindo caminho à remoção preventiva de conteúdos lícitos, na tentativa de evitar sanções severas – que podem atingir os 6% do volume de negócios global da empresa – promovendo assim um ambiente de *overcompliance* digital, onde o medo de represálias se sobrepõe à proteção da expressão livre e plural (Oliva, 2020).

Paralelamente, a moderação algorítmica, baseada em tecnologias de Inteligência Artificial e processamento de linguagem natural, é limitada na sua capacidade de compreender o contexto, a ironia, o tom ou as nuances culturais. Como tal, tende a produzir *falsos positivos*, eliminando conteúdos válidos, e *falsos negativos*, permitindo a persistência de conteúdos nocivos (Sartor & Loreggia, 2020). Os algoritmos – treinados com dados permeados por preconceitos sociais e

⁵³ Embora distinga formalmente entre plataformas de muito grande dimensão (VLOPs e VLOSEs) e operadores de menor escala, as obrigações impostas às plataformas pequenas e médias continuam a levantar sérias preocupações práticas de proporcionalidade. Estas entidades, ainda que isentas das obrigações mais gravosas previstas para os grandes operadores (como as avaliações de risco sistémico, auditorias independentes ou exigências de transparência algorítmica), permanecem vinculadas a deveres complexos, como os mecanismos de notificação e ação (art. 16.º), a cooperação com ordens judiciais e administrativas (arts. 9.º e 10.º), e a manutenção de pontos de contacto e representantes legais (arts. 11.º e 13.º). Na ausência de critérios operacionais claros que materializem a “proporcionalidade” consagrada no artigo 33.º do DSA, muitas pequenas plataformas enfrentam custos elevados de conformidade, riscos de sanções e tendência para o “sobrecumprimento” (*overcompliance*). Este quadro normativo pode contribuir para a exclusão de operadores mais frágeis do ecossistema digital europeu ou para a sua dependência tecnológica das grandes plataformas, contrariando os princípios de pluralismo e concorrência leal que o próprio regulamento afirma promover.

programados sem transparência – não são meras ferramentas técnicas, são verdadeiros dispositivos regulatórios que moldam o fluxo de informação, a visibilidade de ideias e até a percepção da realidade. Quando utilizados sem revisão humana, tornam-se instrumentos de censura tecnocrática, operando com eficácia matemática, mas legitimidade democrática questionável (Barata, 2021)

A ausência de salvaguardas vinculativas no DSA quanto ao uso destas tecnologias acentua o problema, transformando-se, como alertava (Rodotà, 2012), numa verdadeira “ditadura do algoritmo”. Apesar de o regulamento fazer alusão ao respeito pelos direitos fundamentais nos seus considerandos (nomeadamente no Recital 155), não consagra obrigações claras e operacionais que imponham limites concretos ao poder das plataformas. O resultado é uma privatização do poder de censura, transferido para sistemas algorítmicos opacos que funcionam fora dos mecanismos tradicionais de responsabilização legal e judicial. Se não forem corrigidas, estas falhas poderão transformar o DSA num instrumento de governação tecnocrática, onde os algoritmos ditam os termos do debate público e os direitos fundamentais se subordinam à eficiência regulatória. Tal cenário colocaria em risco a soberania digital dos cidadãos europeus e consolidaria um desequilíbrio de poder entre utilizadores e grandes plataformas privadas – muitas das quais sediadas fora do espaço europeu. Proteger a liberdade de expressão na era digital exige mais do que proclamações normativas: requer limites claros, supervisão independente e uma arquitetura regulatória que coloque os direitos humanos no centro da governação digital.

Conclusão

Num tempo em que o debate político e a formação da opinião pública se desenrolam cada vez mais nos espaços digitais, as redes sociais tornaram-se protagonistas centrais de uma nova ecologia comunicacional, simultaneamente promissora e vulnerável. Ao mesmo tempo que democratizam o acesso à informação e potenciam novas formas de mobilização cívica, essas mesmas plataformas expõem as sociedades a riscos inéditos: a manipulação algorítmica, a desinformação em larga

escala e as campanhas coordenadas de influência, que corroem os pilares do diálogo democrático. A União Europeia tem procurado responder a esses desafios com uma estratégia normativa em constante evolução. Se, numa fase inicial, se privilegiou uma abordagem voluntarista, assente em mecanismos de autorregulação e códigos de conduta não vinculativos, a experiência acumulada – e os limites evidenciados por esse modelo – conduziram à adoção de um quadro mais articulado e multifacetado. A articulação entre o Regulamento dos Serviços Digitais e o Código de Conduta Reforçado de 2022 revela uma tentativa deliberada de estruturar uma resposta normativa robusta e adaptada à complexidade do ambiente digital contemporâneo.

Mas a regulação da desinformação não se limita à imposição de obrigações formais às plataformas digitais. Exige uma compreensão dos mecanismos que moldam a visibilidade da informação, do papel dos algoritmos na curadoria de conteúdos e das assimetrias de poder que se estabelecem entre os grandes intermediários digitais e o espaço público democrático. A moderação opaca, a remoção automatizada de conteúdos e a redução da visibilidade de determinadas vozes, ainda que com propósitos legítimos, levantam interrogações sérias quanto ao equilíbrio entre a luta contra a desinformação e a salvaguarda da liberdade de expressão.

O desafio não é apenas jurídico, é também cultural e político. Não basta legislar, é necessário fomentar uma literacia mediática transversal, consolidar redes de verificação de factos independentes e promover a transparência dos sistemas digitais. A confiança num ecossistema informacional plural e íntegro constrói-se com instituições fortes, mas também com cidadãos informados e críticos. Num cenário global em que as ameaças informacionais são cada vez mais sofisticadas, persistentes e geopolíticas, a regulação europeia oferece um modelo de resposta pautado por valores democráticos, proporcionalidade e responsabilidade partilhada. O caminho está longe de estar concluído. Mas a consolidação de um quadro jurídico eficaz, articulado e centrado nos direitos fundamentais constitui um passo essencial para garantir que o espaço digital europeu permanece um território de liberdade, verdade e democracia.

Bibliografia

- Asimakopoulos, G., Antonopoulou, H., Giotopoulos, K., & Halkiopoulos, C. (2025). Impact of Information and Communication Technologies on Democratic Processes and Citizen Participation. *Societies*, 15(2) 40, 1-41.
- Atzori, M. (2024). The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective. *Atzori, Marcella, The Digital Services Act and the Freedom of Expression in the European Union: A Political Perspective (June 21, 2024). Available at SSRN: <https://ssrn.com/abstract=4887181> or <http://dx.doi.org/10.2139/ssrn.4887181>.*
- Balázs, B.-G. (2021). Regulation of Social Media platforms in the European Union. *Pro Public Bono - Public Administration - Vol. 9 No. 1*.
- Balkin, J. M. (2017). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *Yale Law School, Public Law Research Paper No. 615*.
- Barata, J. (2021). The Digital Services Act and its impact on the right of freedom of expression: special focus on risk mitigation obligations obligations. *Plataforma por la libertad de información*, 12.
- Bartóki-Gönczy, B. (2021). Regulation of Social Media platforms in the European Union. *PRO PUBLICO BONO – Public Administration*.
- Bazarkina, D. Y. (2022). Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States. . *Herald of the Russian Academy of Sciences*, 92.
- Belga, T. B. (2025). Russia and China use 'massive digital arsenal' to manipulate democracies. *The Brussels Times*.
- Board, C. O. (2025). *The recognition of the Code of Practice on Disinformation as a code of conduct pursuant to Article 45 of Regulation 2022/2065 (Digital Services Act or “DSA”)*.
- Borz, G., Francesco, F. D., Montgomerie, T. L., & Bellis, M. P. (2024). The EU soft regulation of digital campaigning: regulatory effectiveness through platform compliance to the code of practice on disinformation. *Policy Studies*, Vol. 45.
- Buttaboni, C., Colangelo, G., & Floridi, L. (2025). The Ethical and Legal Implications of the Digital Services Act and Digital Markets Act in the European Union Legal Framework. *Buttaboni, Carlotta and Colangelo, Giuseppe and Floridi,*

- Luciano, *Governing Platform Power in the EU: A Legal and Ethical Assessment*. (April 18, 2025). Available at SSRN: <https://ssrn.com/abstract=5110753> or <http://dx.doi.org/10.2139/ssrn.5110753>.
- Carvalho, B. H., Louzada, J. P., Rios, L. R., Meine, P. D., Barcelos, S. D., & Schimansh, S. (2021). A União Europeia e sua política de combate à desinformação. *XXX CIC - Congresso de Iniciação Científica*.
- Casero-Ripollés, A., Tuñón, J., & Bouza-García, L. (2023). The European approach to online disinformation: geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications volume 10, Article number: 657*.
- Chung, J. (2019). The Operationalisation of the Rule of Law in the EU Legal Order. *Nordic Journal of European Law Special Issue Vol. 2 No. 2 - The Rule of Law in Europe*, 20-38.
- Comissão Europeia, D.-G. d. (2018). *A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation*. Publications Office.
- Comission, E. (2019). *COMMISSION STAFF WORKING DOCUMENT Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the 2019 elections to the European Parliament*.
- Comission, E. (2025). *COMMISSION OPINION of 13.2.2025 on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065*.
- Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité ds Regiões Combater a desinformação em linha: uma estratégia europeia COM (2018) 236 final*. (26 de 4 de 2018). Obtido de <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0236>
- 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 COM (2020) 790 final*. (3 de 12 de 2020). Obtido de <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020DC0790>
- Contucci, P., Omicini, A., Pianini, D., & Sîrbu, A. (2019). *The Future of Digital Democracy: An Interdisciplinary Approach*. Springer Cham.

- Código de Conduta da UE sobre Desinformação . (2018).
- Código de Conduta sobre Desinformação reforçado de 2022. (2022).
- D’Andrea, A., Fusacchia, G., & D’Ulizia, A. (2025). Policy Review: Countering Disinformation in the Digital Age - Policies and Initiatives to Safeguard Democracy in Europe. . *Information Polity*. .
- Directorate-General for Communications Networks, C. a. (2018). A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation. *EU publications*.
- Dooley, J. (2024). Making European Union digital platform regulation a reality. *Administration Volume 72 (2024): Issue 4*.
- ECtHR. (2013). Ahmet Yildirim v. Turkey.
- Espaliú-Berdud, C. (2023). Use of disinformation as a weapon in contemporary international relations: accountability for Russian actions against states and international organizations. *El Profesional de La Informacion*.
- Europeia, C. (2016). Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia JOIN (2016) 18 final.
- Europeia, C. (2018). Combater a desinformação em linha: uma estratégia europeia COM (2018) 236 final.
- Europeia, C. (2018). COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU, AO CONSELHO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Plano de Ação contra a Desinformação JOIN(2018) 36 final.
- Europeia, C. (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 COM(2018) 236 final.
- Europeia, C. (2018). Comunicação sobre o combate à desinformação em linha, COM(2018) 236 final.
- Europeia, C. (2018). Plano de Ação contra a Desinformação JOIN (2018) 36 final.
- Europeia, C. (2018). Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia JOIN (2016) 18 final.
- Europeia, C. (2020). Combater a desinformação sobre a COVID-19: repor a verdade dos factos JOIN(2020) 8 final.

- Europeia, C. (2021). Proteção dos Direitos Fundamentais na Era Digital - Relatório Anual de 2021 sobre a Aplicação da Carta dos Direitos Fundamentais na UE.
- Europeia, C. (s.d.). Orientações da Comissão Europeia para o Reforço do Código de Conduta em Matéria de Desinformação COM (2021) 262 final.
- Europeu, C. (2015). Reunião do Conselho Europeu (19 e 20 de março de 2015) – Conclusões.
- Europeu, T. d. (2021). Desinformação na UE: fenómeno combatido, mas não controlado.
- Fathaigh, R. Ó., Helberger, N., & Appelman, N. (2021). The perils of legally defining disinformation. *The perils of legally defining disinformation. Internet Policy Review, 10*(4).
- Fraga-Kamas, P., & Fernández-Caramés, T. (2020). Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. *IT Professional (Volume: 22, Issue: 2, 01 March-April , 53-59.*
- Gosztonyi, G. (2024). How the European Union had Tried to Tackle Fake News and Disinformation with Soft Law and what Changed with the Digital Services Act? *Frontiers in Law, 3*, 102-113.
- Gregorio, G. D., & Pollicino, O. (2024). The European Approach to Disinformation: Policy Perspectives. *IEP@BU Policy Brief.*
- Guedes, I. S., Vigo, B., Santos, M., Moreira, S., Cardoso, C. S., & Castro, J. (2025). Disinformation Dynamics and Regulation in Portugal: Insights from a Qualitative Study. *European Journal on Criminal Policy and Research.*
- Hinšt, D. (2021). Disinformation as Geopolitical Risk for Transatlantic Institutions. *Međunarodne Studije, 21*(2), 89.
- Jayakumar, S., Ang, B., & Anwar, N. D. (2020). *Disinformation and Fake News.* Palgrave Macmillan Singapore.
- Jodanovic, A. (2024). The Digital Services Act Package: Protection of the Fundamental Rights of Digital Services Users in the European Union. *Regional Law Review, 43-64.*
- Kachelmann, M., & Reiners, W. (2023). The European Union's Governance Approach to Tackling Disinformation – protection of democracy, foreign influence, and the quest for digital sovereignty. *L'Europe En Formation, n.º 396*, 11-36.

- Karanicolas, M. (2019). Squaring the Circle Between Freedom of Expression and Platform Law. *Pittsburgh Journal of Technology Law & Policy*, 20(1).
- Kuczerawy, A. (2019). Fighting online disinformation: did EU Code of Practice forget about freedom of expression? *Disinformation and Digital Media as a Challenge for Democracy; European Integration and Democracy Series, Vol. 6*.
- Kulesza, J., & Burdiak, P. (2024). Countering disinformation on social media platforms: developments in the EU and Poland. *Mediaforum: Analytics, Forecasts, Information Management*, 143-160.
- Legucka, A. (2020). Russia's Long-Term Campaign of Disinformation in Europe. *Strategic Europe*.
- Leiser, M. (2023). Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News, Disinformation, & Online Manipulation.
- McKay, S., & Tenove, C. (2021). Disinformation as a Threat to Deliberative Democracy. *Political Research Quarterly* 74(3), 703-717.
- Nagasako, T. (2020). Global disinformation campaigns and legal challenges. *Int. Cybersecur. Law Rev*, 126-136.
- Narayanan, A. (2023). Understanding Social Media Recommendation Algorithms. *Knight First Amend. Inst.*
- Nenadić, I., Brogi, E., Bleyer-Simon, K., & Reviglio, U. (2024). *Structural Indicators of the Code of Practice on Disinformation: The 2nd EDMO report*. European Digital Media Observatory.
- Neudert, L.-M. (2020). Hurdles and Pathways to Regulatory Innovation in Digital Political Campaigning. *he Political Quarterly*, 91, 713-721.
- O'Shaughnessy, N. (2020). From Disinformation to Fake News: Forwards into the Past. *The Sage Handbook of Propaganda*, 55-70.
- Oliva, T. D. (2020). Content moderation technologies: Applying human rights standards to protect freedom of expression. *Human Rights Law Review*, 20(4), 607-640.
- Pamment, J. (2020). The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission. *Carnegie Endowment for International Peace*.
- Pamment, J. (2020). The EU's Role in Fighting Disinformation: Taking Back the Initiative. *Carnegie Endowment for International Peace*.

- Pamment, J. (2020). The EU's Role in the Fight Against Disinformation: Developing Policy Interventions for the 2020s. *Carnegie Endowment for International Peace*.
- Pamment, J. (2020b). The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework. *Carnegie Endowment for International Peace*.
- Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., & Markatos, E. (2023). *Before & After: The Effect of EU's 2022 Code of Practice on Disinformation*.
- Pira, F. (2023). Disinformation a problem for democracy: profiling and risks of consensus manipulation. *Sec. Media Governance and the Public Sphere*, V.8, 1-10.
- Ribeiro, N. (2021). *Desinformação Online: O impacto da propaganda participativa*. Universidade Católica Editora.
- Rodotà, S. (2012). *Il diritto di avere diritti*. Laterza.
- Rodrigues, M. I. (2024). Assessing Russia's information warfare in Ukraine (2013-2015) : the role of RT/Russia Today and Sputnik in disinformation campaigns targeting international audiences. *Universidade Católica Portuguesa*.
- Romanishyn, A. (2024). Enhancing Election Integrity by Strengthening EU Defences Against Disinformation. *European View*, 23(2), 266. .
- Santos, S. J., & Lapa, T. (2022). A desinformação pelos olhos e mãos da UE: Descontruindo e interligando narrativas e práticas digitais de (in)segurança. *União Europeia como ator internacional: paz e segurança nas narrativas e práticas*, 249-287.
- Sartor, G., & Loreggia, A. (2020). The Impact of Algorithms for Online Content Filtering and Moderation. *Policy Department for Citizens' Rights and Constitutional Affairs, DG Internal Policies*.
- Saurwein, F., & Spencer-Smith, C. (2020). Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe. *Digital Journalism*, 8(6), 820.
- Schlag, G. (2023). European Union's Regulating of Social Media: A Discourse Analysis of the Digital Services Act. *Politics and Governance*.
- Services, E. B. (2025). *The recognition of the Code of Practice on Disinformation as a code of conduct pursuant to Article 45 of Regulation 2022/2065 (Digital Services Act or "DSA")*.

- Shehaj, E. (2015). Challenges of Albania towards the European Integration . *Mediterranean Journal of Social Sciences - MCSER Publishing, Rome-Italy - Vol. 6 No 4 S2* , 571-577.
- Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T. H., Ding, K., Karami, M., & Liu, H. (2022). Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews Data Mining and Knowledge Discovery*, 10(6).
- Silva, M. M. (2025). At the Digital Crossroads: The Attention Economy, Freedom of Expression, and Platform Regulation — Challenges and Prospects for Solutions in the European Union. *Comunicação e Sociedade*.
- Sleibi, A. (2023). Tackling Disinformation and Inaccuracy: Euro-Med Digital Opportunities in the Context of the Russian Online Invasion. *Euromesco - Policy Brief n.º 124*.
- Social, E. R. (2019). A Desinformação - Contexto Europeu e Nacional.
- Sousa, J. R. (2025). Integração do Código de Conduta sobre Desinformação voluntário no Regulamento dos Serviços Digitais. *Europe Direct - Minho*.
- Spitale, G., Biller-Andorno, N., & Germani, F. (2023). AI model GPT-3 (dis)information us better than humans. *Science Advances* 9, no. 26.
- Szakács, J., & Bognár, É. (2021). The impact of disinformation campaigns about migrants and minority groups in the EU. *EU publications*.
- Tan, C. (2022). Regulating disinformation on Twitter and Facebook. *Griffith Law Review Volume 31 - Issue 4*, 513-536.
- Tenove, C., Buffie, J., McKay, S., & Moscrop, D. (2018). Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy. *Centre for the Study of Democratic Institutions, University of British Columbia*.
- Treverton, Thvedt, Chen, Lee, & McCue. (2018). Addressing hybrid threat. *Arkitektkopia AB, Bromma*.
- What is the Doppelganger operation? List of resources*. (15 de 05 de 2025). Obtido de EU DISINFO LAB: <https://www.disinfo.eu/doppelganger-operation/>
- Woolley, S. C. (2022). Digital Propaganda: The Power of Influencers. *Journal of Democracy* 33(3), 115-129.
- Zenzerović, M. G., & Nenadić, I. (2022). Strengthening resilience to disinformation: the state of affairs and guidelines for action.