Universidade do Minho
Escola de Direito

Eduardo Nuno Fernandes Paiva

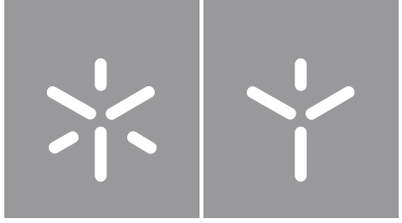
O desafio da disseminação de desinformação na Europa: perspetiva jurídica e técnico-informática

outubro de 2023

O desafio da disseminação de desinformação na Europa: perspetiva jurídica e técnico-informática

Eduardo Nuno Fernandes Paiva

UMinho | 2023



Universidade do Minho
Escola de Direito

Eduardo Nuno Fernandes Paiva

O desafio da disseminação de desinformação na Europa: perspetiva jurídica e técnico-informática

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação da
Professora Doutora Alessandra Aparecida Souza da Silveira
e sob a orientação do
Professor Doutor Paulo Jorge Freitas de Oliveira Novais

outubro de 2023

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição
CC BY

https://creativecommons.org/licenses/by/4.0/

AGRADECIMENTOS

Aos meus pais, por serem a minha base e por todo o seu apoio e confiança durante esta jornada.

À minha psicóloga, pelos excelentes conselhos durante este último ano, essenciais para a redação desta dissertação.

A todos os meus amigos e restantes familiares, pelo ânimo e motivação constantes neste âmbito.

Aos meus orientadores, por toda a disponibilidade, diligência e orientação oferecidas.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

RESUMO

A desinformação, enquanto ameaça ubíqua da contemporaneidade, manifesta-se como um fenómeno de natureza complexa e transfronteiriça, apresentando-se como nociva para as sociedades europeias na medida em que corrompe o tecido democrático que as agrega e sustenta. Esta dissertação assume como seu desígnio central o detalhamento das principais implicações da problemática em determinados pontos nevrálgicos do corpo social, expondo adicionalmente os mais preponderantes instrumentos normativos que compõem a política europeia de combate à manipulação no ecossistema de informação, sem preterir, naturalmente, uma contemplação da atividade desenvolvida – a nível europeu e mundial – por algumas estruturas que complementam a resposta europeia neste domínio. Levando em consideração os objetivos descritos, o trabalho investigativo iniciar-se-á com uma análise conceitual da realidade da desinformação nos dias de hoje, essencial para a construção indagativa que será erigida ao longo da dissertação. Suplementarmente, será conduzida uma análise jurisprudencial de um Acórdão proferido pelo Tribunal de Justiça da União Europeia, aprofundando e concretizando a dimensionalidade aguda que a temática assume para a segurança na União. Por fim, será destacado, de forma mais particular, o impacto da evolução tecnológica – e em particular dos *deepfakes* – no âmbito da disseminação de desinformação. Imergiremos, assim, na complexidade da questão assumindo uma postura plurifacetada que irá reunir uma componente jurídica e uma componente técnico-informática, essenciais para uma cabal perceção do hermetismo que a problemática evidencia. Como veremos, a política europeia atualmente esquematizada constitui um ponto de partida bem alicerçado para promover um ecossistema de informação mais fiável, fundamentado e seguro para todos os europeus. Todavia, os constantes avanços técnico-informáticos rapidamente comprometerão quaisquer avanços positivos alcançados, exigindo-se uma atitude de permanente vigilância e cooperação estratégica internacional para digladiar a ameaça e os seus perpetradores.

Palavras-chave: Deepfakes; Desinformação; Liberdade de Expressão e de Informação; Redes Sociais.

ABSTRACT

Disinformation, as a ubiquitous contemporary threat, manifests itself as a phenomenon of a complex and cross-border nature, presenting itself as harmful to European societies insofar as it corrupts the democratic fabric that sustains and binds them together. The main purpose of this dissertation is to detail the main implications of the problem in certain neuralgic points of the social body, as well as exposing the most important normative instruments that make up the European policy to combat manipulation in the information ecosystem, without, of course, neglecting to contemplate the activity carried out – at European and world level – by some structures that complement the European response in this field. Taking into account the objectives described, the research will begin with a conceptual analysis of the reality of disinformation today, which is essential for the inquisitive construct that will be raised up throughout the dissertation. In addition, a jurisprudential analysis of a judgment handed down by the Court of Justice of the European Union will be carried out, deepening and concretizing the acute dimension that the issue assumes for security matters in the Union. Finally, the impact of technological developments – and in particular of deepfakes – on the dissemination of disinformation will be highlighted more specifically. We will therefore immerse ourselves in the complexity of the issue, taking a multifaceted stance that will bring together both a legal and a technical component, essential for a full understanding of the hermetic nature of the problem. As we shall see, the European policy currently outlined is a sustainable starting point for promoting a more reliable, well-founded and secure information ecosystem for all Europeans. However, the constant technological breakthroughs will quickly jeopardize any positive progress made, requiring an attitude of permanent vigilance and international strategic cooperation to fight the threat and its perpetrators.

Keywords: Deepfakes; Disinformation; Freedom of Expression and Information; Social Networks.

ÍNDICE

Agradecimentos ..... **iii**

Resumo ..... **v**

Abstract ..... **vi**

Lista de Abreviaturas, Siglas e Acrónimos ..... **x**

Introdução **1**

1. Desinformação: Uma Análise Conceitual **4**

1.1 O (atual) conceito de «desinformação» 4

1.1.1 «Desinformação» (em sentido estrito) 5

1.1.2 «Informação incorreta», «tentativas de exercer influência sobre a informação» e a «interferência estrangeira no espaço de informação» (e a «malinformação») 6

1.1.3 Desinformação: conteúdo legal ou ilegal? 8

2. O Fenómeno da Desinformação em Perspetiva **10**

2.1 As repercussões sentidas ao nível dos momentos eleitorais e de crise e no âmbito dos processos de tomada de decisão 10

2.2 O papel das grandes plataformas digitais 14

2.3 A importância da promoção de um jornalismo independente e de qualidade 16

2.4 Os problemas da adoção de uma via exclusivamente legislativa para o combate à problemática 19

2.5 As implicações para o direito à liberdade de expressão e de informação 21

2.5.1 Considerações introdutórias sobre o direito à liberdade de expressão e de informação 22

2.5.5 A polémica com a Carta Portuguesa de Direitos Humanos na Era Digital 27

3. O Papel das Estruturas Europeias na Coordenação de Respostas ao Fenómeno **33**

3.1 O sistema de alerta rápido 35

3.2 Observatório Europeu dos Meios de Comunicação (EDMO) e o Grupo de Reguladores Europeus para os Serviços de Comunicação Social Audiovisual (ERGA) 37

3.2.1 EDMO 37

3.2.2 ERGA 38

3.3 Ameaças híbridas: a Célula de Fusão e o Centro Europeu de Excelência 39

3.4 Os Grupos de Trabalho para a Comunicação Estratégica 42

4. A Política Europeia de Combate à Disseminação de Desinformação 47

4.1 Regulamento dos Serviços Digitais 48

4.1.1 Os objetivos 48

4.1.2 Os serviços intermediários 49

4.1.3 Publicidade em linha e sistemas de recomendação 51

4.1.4 Riscos sistémicos 55

4.1.5 Os momentos de crise 57

4.1.6 O acesso aos dados das plataformas e motores de pesquisa em linha de muito grande dimensão 58

4.1.7 Os relatórios de transparência 60

4.1.8 Os mecanismos de supervisão no RSD 61

4.2 A Proposta de Regulamento sobre a transparência e o direcionamento da propaganda política. 62

4.2.1 Considerações introdutórias 63

4.2.2 O direcionamento de propaganda política 64

4.2.3 A transparência da propaganda política 67

4.2.4 Monitorização e supervisão da aplicação do Regulamento 72

4.3 O Código de Conduta Reforçado em matéria de Desinformação de 2022 73

4.3.1 Escrutínio na colocação de anúncios 76

4.3.2 Propaganda política 77

4.3.3 Integridade dos serviços 78

4.3.4 Capacitação dos utilizadores 80

4.3.5 Capacitação da comunidade de investigação 87

4.3.6 Capacitação da comunidade de verificação de factos 88

4.3.7 O Centro de Transparência e o Grupo de Trabalho Permanente 90

4.3.8 Monitorização do Código 91

5. Caso RT France v Conselho 92

5.1 Contextualização 92

5.2 A questão da competência do Conselho para emanar os atos alvo de impugnação 93

5.2.1 O escopo de competência do Conselho em matéria de política externa e segurança comum e a resposta do Tribunal 94
5.3 A questão da violação dos direitos de defesa da RT France 95
5.3.1 A argumentativa da RT France 95
5.3.2 A resposta do Tribunal 96
5.3.3 A questão da insuficiência de fundamentação dos atos impugnados pela RT France ... 97
5.4 A questão da violação da liberdade de expressão e de informação 98
5.4.1 A argumentativa da RT France 98
5.4.2 A resposta do Tribunal 99
5.5 A questão da violação da liberdade de empresa 109
5.6 A questão relativa à violação do princípio da não discriminação em razão da nacionalidade..... 111
5.7 O pedido de recurso (processo C-620/22 P) e considerações finais 111
6. Tecnologia e Desinformação: As Técnicas de Amplificação e o Caso Particular dos Deepfakes 114
6.1 Os *deepfakes* 119
6.1.1 Os métodos de criação de *deepfakes* 119
6.1.2 As técnicas de deteção de *deepfakes* 121
6.1.3 Outros meios a considerar para a mitigação dos efeitos negativos dos *deepfakes* maliciosos 126
6.1.4 Breve *overview* sobre as implicações da Proposta de Regulamento sobre a Inteligência Artificial para os *deepfakes*..... 127
Conclusão 130
Bibliografia Geral 133
Documentos de Instituições e Estruturas Europeias 138
Bibliografia Normativa 140
Bibliografia Jurisprudencial 142

Lista de Abreviaturas, Siglas e Acrónimos

CDFUE – Carta de Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos Humanos

CNN – Rede neuronal convolucional

CRP – Constituição da República Portuguesa

EDAP – Plano de Ação para a Democracia Europeia

EDMO – Observatório Europeu dos Meios de Comunicação Digitais

ERC – Entidade Reguladora para a Comunicação Social

ERGA – Grupo de Reguladores Europeus dos Serviços de Media Audiovisuais

GAN – Rede Adversária Generativa

IA – Inteligência Artificial

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado Atlântico Norte

RGPD – Regulamento Geral sobre a Proteção de Dados

RNN – Rede neuronal recorrente

RSD – Regulamento Serviços Digitais

SEAE – Serviço Europeu para a Ação Externa

TCE – Tribunal Constitucional Espanhol

TEDH – Tribunal Europeu dos Direitos Humanos

TFUE – Tratado sobre o Funcionamento da União Europeia

TUE – Tratado da União Europeia

UE – União Europeia

INTRODUÇÃO

O desafio colocado pela desinformação às nossas sociedades não é novo. A obtenção de vantagens – sejam elas de ordem social, política, ou económica –, por meio da difusão deliberada de ideias falsas, manipuladas e/ou descontextualizadas, não constitui uma prática nova, mas os recentes e constantes desenvolvimentos tecnológicos, particularmente no campo da inteligência artificial e da automação, colocam uma ênfase especial aos proveitos retirados dessas práticas.

Os avanços técnicos verificados permitem, efetivamente, uma modelação de tudo aquilo que consumimos por meio dos canais digitais de informação, influenciando, consequentemente, a nossa visão sobre o mundo em redor.[1] A digitalização permitiu que determinadas técnicas para a disseminação de desinformação estejam ao alcance de qualquer pessoa com um dispositivo com acesso à internet e a consequente "democratização" desta ameaça torna-a absolutamente incontornável e merece, por isso, toda a nossa atenção logo desde os seus estádios mais iniciais.[2] Assim, da mesma forma que a ameaça é mais perigosa que nunca, também a resposta pode ser a mais eficiente de sempre.

A interferência russa nas eleições presidenciais norte-americanas de 2016[3] representa apenas um exemplo da escala e rapidez com que é possível, nas redes sociais, disseminar narrativas enganosas e manipuladoras intencionalmente. O substrato associado à prática de tais atos reside, principalmente, numa tentativa de desacreditar as instituições democráticas junto das populações dos respetivos países, permitindo a criação de uma espécie de realidade onde impera a pós-verdade, realidade essa que, por vezes, se enquadra nos interesses geopolíticos de outros países, que se intrometem em assuntos internos de países democráticos, procurando, assim, aumentar o seu perímetro de influência.[4]

No caso em específico dos atores políticos, na figura de partidos ou mesmo de Governos eleitos, a repetição de mentiras, ainda que refutadas com bases factuais, acaba por cativar uma parte do eleitorado que confia cegamente em quem discursa, rejeitando todo e qualquer tipo de reinterpretação

---

[1] ALAPHILIPPE, Alexander, *et al.*, *Automated Tackling of Disinformation: Major Challenges Ahead*, Serviço de Estudos do Parlamento Europeu (EPRS), 2019, p. 1.

[2] POLYAKOVA, Alina; FRIED, Daniel, *Democratic Defense Against Disinformation*, Atlantic Council – Eurasia Center, 2018, p. 12.

[3] Sobre este assunto, Cfr. Comité de Inteligência do Senado dos Estados Unidos, *Russian active measures campaigns and interference in the 2016 U.S. election*, Volume 1-5, 2020; PROKOPOVIĆ, Anka Mihajlov; VUJOVIĆ, Marija, "The european approach to regulating disinformation", *in Facta Universitatis Series Law and Politics*, Volume 18, n.º 3, 2020, p. 181.

[4] POLYAKOVA, Alina; FRIED, Daniel, p. 2; PROKOPOVIĆ, Anka Mihajlov; VUJOVIĆ, Marija, p. 181.

– ainda que condicente com a verdade – dos tópicos em discussão.[5] Esta aversão ao processo de impugnação da falsa argumentativa utilizada é reforçada por quem a transmite junto do seu público, intensificando o dano e isolando o valor da verdade. Mesmo em países democráticos, onde o escrutínio é naturalmente mais forte, estes fenómenos sucedem-se, permitindo que a desinformação seja utilizada, vitoriosamente, com o intuito de manipular, confundir e comprometer as bases da democracia.

Particularmente em momentos de maior tensão e polarização social, como é o caso de eleições e referendos (ou mesmo de guerras e pandemias), a disseminação ampla de desinformação afigura-se como uma ameaça basilar a um debate público transparente e informado e, nesse ponto, eleva-se uma problemática de incontornável relevância para o saudável decorrer dos referidos processos democráticos, que defraude o dinamismo e os valores democráticos.

Noutro sentido, especialmente em face da situação de guerra que se gerou num país vizinho à União, não será igualmente de desconsiderar o papel de grande relevância que a disseminação de desinformação pode assumir no domínio da política externa e de segurança, tanto da União, como a nível global. Dada a relevância e suas implicações, a União, particularmente no seguimento da anexação da região da Crimeia por parte da Rússia[6], reconheceu os potenciais efeitos prejudiciais de um forte arsenal de desinformação e iniciou esforços na busca de soluções para a combater o fenómeno de manipulação de informação que se começou a verificar desde a incorporação daquele território. Mais recentemente, com o início da Guerra na Ucrânia, as preocupações neste âmbito ascenderam a novos planos.

Assim, ao longo das próximas páginas pretende-se pintar um retrato da resposta europeia ao fenómeno e, para o efeito, avançar-se-á, logo de início, com uma definição para o objeto de estudo em apreço, para, posteriormente, ser possível salientar as principais implicações que se levantam neste novo mundo de fluxos de desinformação. Com toda esta informação em mente, mergulharemos de seguida nos fundamentos que atuam como alicerces da política europeia neste universo, que pretende, com os seus instrumentos normativos – e as estruturas que complementam e auxiliam uma ação coordenada transfronteiriça – por cobro à ameaça.

Do mesmo modo, será destacado um exemplo prático que possibilitará uma apreciação mais balizada e concreta dos efeitos reais de uma campanha de disseminação de desinformação em

---

[5] ALAPHILIPPE, Alexander, *et al.*, p. 1.

[6] VAN RAEMDONCK, Nathalie; MEYER, Trisha, "Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat", *in Addressing Hybrid Threats: European Law and Policies*, 2022, p. 2.

tempos de guerra e, por fim, efetuar-se-á uma análise mais aprofundada ao modo como certas tecnologias, como *deepfakes* e ferramentas de amplificação com recurso a contas inautênticas, elevam a ameaça a novos níveis nos meios em linha e fora deles.

1. DESINFORMAÇÃO: UMA ANÁLISE CONCEITUAL

A contemporaneidade e a sensibilidade para com a esfera de direitos fundamentais constituem dois vetores que obstam à formação de um consenso universal em torno de uma definição única para o fenómeno da desinformação.

As consequências associadas à recência desta problemática assumem-se, não apenas num domínio de ambiguidade social, mas principalmente no âmbito político-legislativo, afigurando-se, por esse motivo, profundamente dificultoso concluir por uma noção atual e definitiva que compreenda toda a dimensão da realidade em questão.

A correta e adequada definição desta problemática é absolutamente crucial para o delineamento de estratégias para o seu combate, no entanto, e tendo em conta a existência de muitíssimas propostas para a sua definição (circunstância evidenciadora das características de incerteza e novidade associadas ao tema), será dada uma enfâse especial à proposta seguida pelas Instituições Europeias.

Posto isto, e antes do início de uma aprofundada e concreta análise sobre o fenómeno da disseminação de desinformação – e suas possíveis ramificações –, cumpre procurar circunscrever o tema da nossa investigação.

1.1 O (atual) conceito de «desinformação»

Até 2020, a noção do termo «desinformação» apenas se reportava, redundantemente, à simples disseminação intencional de informação falsa e enganosa, mas, atualmente, é-nos apresentado pelo Plano de Ação para a Democracia Europeia (EDAP) um conceito quadripartido que destaca algumas realidades que lhe são complementares e que procede, assim, a uma aceção mais ampla do mesmo.

Assim, e de forma a evitar confusões, é estabelecida uma diferenciação entre «desinformação» (em sentido estrito) e seus conceitos vizinhos: a «informação incorreta», as «tentativas de exercer influência sobre a informação» e a «interferência estrangeira no espaço de informação», sendo que todos estes termos se encontram abrangidos por uma noção mais ampla de «desinformação».[7] Neste sentido, o Código de Conduta Reforçado em matéria de Desinformação de 2022 indica que os seus

[7] Sobre este assunto, Cfr. também PAMMENT, James, "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework" e "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework", *in Future Threats, Future Solutions*, Carnegie Endowment for International Peace – Publications Department, 2020, pp. 16 e 17 e pp. 2-5, respetivamente.

signatários "reconhecem o seu papel na contribuição para a luta contra a desinformação, que, para efeitos do presente Código, é considerada como incluindo a informação incorreta, a desinformação, as operações de influência de informação e a interferência estrangeira no espaço de informação"[8].

1.1.1 «Desinformação» (em sentido estrito)

À boleia do relatório do Grupo de Peritos em notícias falsas e na desinformação em linha, a Comissão Europeia procurou, desde cedo e ao longo de várias comunicações e planos de ação, definir o termo. Mais recentemente, o EDAP descreve a desinformação (em sentido estrito)[9] como sendo "conteúdo falso ou enganador, disseminado com a intenção de enganar ou de obter um benefício económico ou político e que poderá causar danos públicos"[10]. Posto isto, poderemos reunir quatro pontos de análise a partir desta definição:

(1) "conteúdo falso ou enganador"

Neste ponto, ainda que óbvio, a Comissão refere perentoriamente que a desinformação se reporta a conteúdo que não corresponda à verdade ou que induza ao erro.

(2) "disseminado"

Com a utilização deste termo, a Comissão optou por utilizar um vocábulo que permita englobar várias realidades. Formulações anteriores desta definição (previstas, a título de exemplo, na Comunicação «Combater a desinformação em linha: uma estratégia europeia» ou no Plano de Ação contra a Desinformação) previam, em vez de "disseminado", a expressão "criada, apresentada e divulgada" e, nesse sentido, é provável que a Comissão tenha procurado simplificar a definição neste aspeto em concreto, abarcando as suas múltiplas possibilidades de «disseminação» num vocábulo único.

(3) "intenção de enganar ou de obter um benefício económico ou político"

Neste âmbito, a Comissão procurou circunscrever o fenómeno da desinformação a apenas atos voluntários. Assim, a partilha de informação falsa e enganosa – por quem não a reconheça como tal – não constitui um ato disseminação de desinformação nos termos desta definição, não obstante o

---

[8] *O Código de Conduta Reforçado em matéria de Desinformação de 2022*, capítulo 1, parágrafo a).
[9] Sobre este tema, Cfr. também FATHAIGH, R. Ó.; HELBERGER, Natali; APPELMAN, Naomi, *The perils of legally defining disinformation*, Internet Policy Review, 10:4, 2021, pp. 3-7.
[10] Comissão Europeia, *Plano de Ação para a Democracia Europeia*, COM(2020) 790 final, 2020, p. 21.

facto de este fenómeno existir e ser relevante para a lide, denominando-se de disseminação de «informação incorreta», que será alvo de análise posteriormente[11].

É, assim, mencionado que quem atue com a intenção de defraudar o destinatário, ou com o intuito de obter algum benefício económico ou político, estará a incorrer numa disseminação de «desinformação». Neste ponto é, assim, feita uma menção expressa aos principais móveis dos disseminadores de desinformação: as motivações económicas (como veremos, a disseminação de desinformação, dado o atual modelo de funcionamento das redes sociais e do próprio mundo publicitário em linha, pode constituir um negócio muito lucrativo) e políticas (a disseminação de desinformação por motivos políticos é muito frequente enquanto tentativa de criar ou prejudicar determinadas agendas políticas e, neste aspeto em particular, a problemática acarreta riscos mais profundos).

De notar também que, neste âmbito, é sempre utilizada a conjunção alternativa "ou", revelando, a título de exemplo, que quem dissemina desinformação com o mero intuito de enganar não precisa, nesse seu ato, de lograr um benefício económico ou político para que o seu comportamento se enquadre no âmbito deste conceito.

(4) "que poderá causar danos públicos"

Neste âmbito, a presença do termo "poderá" remete para a conclusão de que o requisito do "dano público" não configura uma exigência obrigatória para a caracterização do ato como «disseminador de desinformação»[12]. Neste domínio, a noção de "dano público" consiste na verificação de ameaças aos "processos políticos democráticos e aos processos de elaboração de políticas" e a demais bens públicos, como "a proteção da saúde dos cidadãos da UE, o ambiente ou a segurança".[13]

1.1.2 «Informação incorreta», «tentativas de exercer influência sobre a informação» e a «interferência estrangeira no espaço de informação» (e a «malinformação»)

Como se observou anteriormente, a atual definição de «desinformação» é divisível em 4 subconceitos, sendo os restantes a «informação incorreta», as «tentativas de exercer influência sobre a informação» e a «interferência estrangeira no espaço de informação».

---

[11] Grupo de Peritos em notícias falsas e na desinformação em linha (2018). *A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation*, Publications Office of the European Union, p. 10.
[12] Comissão Europeia, *Plano de Ação contra a Desinformação*, JOIN(2018) 36 final, 2018, p. 1.
[13] Comissão Europeia, *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, COM(2018) 236 final, 2018, p. 4; Grupo de Peritos em notícias falsas e na desinformação em linha, p. 10.

O fenómeno da disseminação de «informação incorreta» relaciona-se com a disseminação imprudente de informação inexata, sem qualquer intenção em causar danos[14]. O EDAP define este termo como constituindo "conteúdo falso ou enganador, partilhado sem intenção de prejudicar, mas cujos efeitos podem causar danos"[15]. Neste último caso, falamos de uma prática muito prevalente nas redes sociais, onde os seus utilizadores partilham, ingenuamente, informação falsa que julgam ser verdadeira. Dada a dificuldade sentida na determinação da vontade do agente, é difícil, na prática, estabelecer uma distinção sólida entre casos de «desinformação» (em sentido estrito) e «informação incorreta»[16].

Por sua vez, as chamadas «tentativas de exercer influência sobre a informação» são definidas, no EDAP, como "esforços coordenados, desenvolvidos por intervenientes internos ou externos, com o objetivo de influenciar uma audiência-alvo através de vários meios enganadores"[17]. A "supressão de fontes de informação independentes"[18] representa um dos exemplos mais proeminentes deste tipo de comportamentos.

Neste seguimento, a «interferência estrangeira no espaço de informação», particularmente incluída e delineada no âmbito de um plano de intromissão de natureza híbrida, é entendida, no documento, como correspondendo a um conjunto de esforços "desenvolvidos por um interveniente estatal estrangeiro ou pelos seus agentes para corromper a livre formação e expressão da vontade política dos indivíduos, utilizando meios coercivos e enganadores"[19].

Por fim, alguns autores ponderam, ainda, a introdução de um outro termo a esta família de vocábulos, a «malinformação». Esta noção reporta-se aos casos onde é disseminada informação, em parte, ou no seu todo, verdadeira[20], mas, dada a forma ardilosa e descontextualizada como essa informação é apresentada, tal divulgação é apenas feita com o intuito de causar danos e alimentar tensões.

Perante toda esta explanação de conceitos, é importante relembrar que todas as realidades aqui descritas não devem ser entendidas como sendo estanques, mas sim como se sobrepondo mutuamente. A introdução de novos conceitos associados à problemática da desinformação é, à vista disso, útil para que se proceda a uma identificação e realçamento – de um modo tendencialmente

---

[14] ALAPHILIPPE, Alexander, *et al.*, p. 5.
[15] Comissão, Plano de Ação para a Democracia Europeia, 2020, p. 21.
[16] ALAPHILIPPE, Alexander, *et al.*, p. 5; Sobre este tema, Cfr. também FALLIS, Don, *A Conceptual Analysis of Disinformation*, 2009.
[17] Plano de Ação para a Democracia Europeia, p. 21.
[18] *Idem.*
[19] *Idem.*
[20] FATHAIGH, R. Ó.; HELBERGER, Natali; APPELMAN, Naomi, p. 4; ALAPHILIPPE, Alexander, *et al.*, p. 5.

abrangente – dos principais e possíveis portais que se formam e que são fontes de ameaças nesta matéria. É, por isso, importante deixar claro que as «interferências estrangeiras no espaço de informação» podem, por sua vez, também constituir «tentativas de exercer influência sobre a informação», tentativas essas que procuram, por seu turno, causar o maior grau de desestabilização nas sociedades, recorrendo, para o efeito, à disseminação de «desinformação», que é posteriormente partilhada incautamente pelos cidadãos na forma de «informação incorreta», para o contentamento dos intervenientes mal-intencionados.

1.1.3 Desinformação: conteúdo legal ou ilegal?

À luz do direito da União, a desinformação não representa, necessariamente e por si só, conteúdo ilegal. Assim, a desinformação não deve desencadear a mesma resposta legal que se encontra já prevista para o conteúdo ilegal, visível na prática de crimes de difamação, de discurso de ódio ou de incitamento à violência, a título de exemplo.

Neste ponto, a Comissão deixa bem claro que a luta contra a desinformação visa proteger, acima de tudo, os direitos fundamentais previstos na Carta – como a liberdade de expressão e de informação –, e, neste sentido, qualquer aproximação político-regulatória a esta temática não deve ir no sentido de "criminalizar ou de proibir a desinformação como tal", mas sim no sentido de "tornar o ambiente em linha e os respetivos intervenientes mais transparentes e responsabilizáveis, dotando as práticas de moderação de conteúdos de maior transparência, capacitando os cidadãos e promovendo um debate democrático aberto"[21].

O Plano de Ação contra a Desinformação é igualmente muito claro a este respeito, referindo que a política de combate prevista nesse documento (e em todo o quadro de respostas unicamente adstrito ao combate à desinformação) se deve aplicar apenas aos conteúdos de desinformação tidos como legais, uma vez que, ultrapassada a linha da ilegalidade, já se encontram previstos os remédios legais a nível europeu e nacional[22].

Neste âmbito, as motivações por detrás de campanhas de desinformação podem centrar-se em questões ideológicas de caráter mais hostil, caracterizadas por traços de xenofobia, misoginia,

---

[21] Comissão Europeia, *Orientações da Comissão Europeia relativas ao reforço do Código de Conduta sobre Desinformação*, COM(2021) 262 final, 2021, p. 1; AMARAL, Maria Lúcia, *Fiscalização da constitucionalidade das normas constantes dos números 5 e 6 do artigo 6.º, da Lei n.º 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital*, Provedoria de Justiça, 2022, parágrafo 13; Sobre este assunto, Cfr. também Comissão Europeia, *Proteção dos Direitos Fundamentais na Era Digital - Relatório Anual de 2021 sobre a Aplicação da Carta dos Direitos Fundamentais na UE*, COM(2021) 819 final, 2021, em especial o capítulo "Tackling the challenges of online content moderation".

[22] *Plano de Ação contra a Desinformação*, JOIN(2018) 36 final, 2018, p. 1.

intolerância religiosa, homofobia, entre outros, que procuram, por meio das narrativas imprecisas e dissimuladas, influenciar os processos de viragem política em curso por via da semeação de tensões sociais[23], como veremos. É precisamente nestes casos que é mais frequente a ultrapassagem desta linha de ilegalidade.

A este propósito, a Provedora de Justiça, Maria Lúcia Amaral, relembra o Regulamento Serviços Digitais, mencionando que existe um "consenso geral" de que o conteúdo considerado lesivo, mas não ilegal – como a desinformação –, "não dev[e] ser objeto de obrigações de remoção, uma vez que este é um domínio delicado com graves implicações para a proteção da liberdade de expressão"[24].

Também a ERC (Entidade Reguladora para a Comunicação Social) entende que as autoridades públicas se devem privar de "interferir e censurar" e, em contrapartida, devem apostar na promoção de uma atmosfera propiciadora de um debate público democrático acessível e diversificado, relembrando que o conteúdo considerado legal – embora nocivo – se encontra, em grande parte, salvaguardado pela garantia constitucional atribuída à liberdade de expressão e de informação e merece, por isso, um tratamento distinto ao reservado para o conteúdo ilegal, que se encontra sujeito a sanções mais drásticas, expressamente previstas na lei aplicável.[25]

Posto isto, o grande e novo desafio que se coloca prende-se, precisamente, com o grau e a envergadura da resposta reservada para o combate à desinformação, que deve obrigatoriamente ser desenhada no sentido da salvaguarda e promoção da verdade dos factos, das instituições democráticas e do jornalismo de qualidade, sob a égide da proteção máxima do direito à liberdade de expressão e de outros direitos conexos.

Assim, a primeira grande ideia que deve ficar clara e assente – e que irá orientar toda a abordagem feita ao longo das próximas páginas – é que a desinformação, por si só, não deve constituir «conteúdo ilegal», ainda que a mesma possa representar uma ameaça para a democracia na União e para as sociedades no seu todo[26], merecendo, pelos motivos expostos, uma resposta adequadamente robusta à sua proliferação.

---

[23] ALAPHILIPPE, Alexander, *et al.*, p. 1.
[24] AMARAL, Maria Lúcia, parágrafo 15.
[25] Entidade Reguladora para a Comunicação Social (ERC), *A Desinformação – Contexto Europeu e Nacional*, 2019, p. 3; AMARAL, Maria Lúcia, parágrafo 35; PALOP, Andrés Boix, "La construcción de los limites a la libertad de expresión en las redes sociales", *in Revista de Estudios Políticos*, número 173, 2016, pp. 106 e 107;
[26] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 5 e 10.

2. O Fenómeno da Desinformação em Perspetiva

Ao longo das próximas páginas procurar-se-á desenhar uma visão geral do fenómeno com um enfoque particular nas principais questões e preocupações que se levantam num momento em que se verifica uma «corrida» ao seu combate.

Nesse sentido, olharemos no presente capítulo para as implicações que a problemática da desinformação causa em múltiplas circunstâncias, desde os processos eleitorais democráticos, ao papel das grandes plataformas digitais enquanto vetores de propagação, sem esquecer a renovada relevância na promoção de um jornalismo isento e de excelência, nem as perturbações e reconfigurações do direito à liberdade de expressão e de informação neste domínio. Por fim, também atentaremos aos principais cuidados a levar em consideração no domínio da aplicação de políticas puramente legislativas de abordagem ao fenómeno.

Neste domínio, será ainda de alertar para o facto de certas realidades, igualmente centrais para a questão e relacionadas com as atividades de investigação, ou de verificação de factos – a título de exemplo –, não se encontrarem expressamente explanadas no presente capítulo, dado que serão mais eficientemente estruturadas no âmbito da política europeia de combate à disseminação de desinformação, que será alvo de análise num momento posterior.

No presente capítulo procurar-se-á, assim, atingir um entendimento relativo às principais dimensões que a ameaça pode representar para as sociedades democráticas, que será, por sua vez, absolutamente relevante para uma compreensão mais totalizante da política europeia que se procurará desenvolver mais adiante, uma vez que todas as implicâncias presentes informam e circunscrevem a atuação das Instituições Europeias neste âmbito.

2.1 As repercussões sentidas ao nível dos momentos eleitorais e de crise e no âmbito dos processos de tomada de decisão

Os períodos eleitorais ou de referendos, que devem naturalmente ser pautados pela máxima independência e transparência dadas as consequências profundamente impactantes associadas aos

processos de sufrágio, representam o maior espelho do dinamismo característico das verdadeiras democracias.[27]

O fenómeno da disseminação de desinformação, para além de se alicerçar na propagação de narrativas que não correspondem total ou parcialmente à verdade, com intuito de deturpar ou influenciar a visão de uma determinada realidade, é também potencialmente criador, a longo prazo, de um clima de desconfiança e dúvida que confunde e afasta os cidadãos da vida pública democrática e das figuras políticas que por si são escolhidas[28].

O sistema político democrático vigente em todos os Estados-Membros da União tem a obrigação de proporcionar aos seus cidadãos uma ampla e ativa participação social e política no debate público, concedendo-lhes a possibilidade de expressarem a sua vontade nas temáticas mais centrais que irão influenciar o rumo que os seus Estados-Membros e a União irão adotar.

Todos os períodos eleitorais são, por isso, absolutamente marcantes pois representam momentos de transformação para o rumo dos projetos político-democráticos em variadíssimas áreas, desde a saúde à educação, passando pela ciência, pela defesa, pelo ambiente e pelo setor económico-financeiro[29] e, nesse sentido, todas as discussões em torno destes setores devem desenrolar-se num clima de verdade, estabilidade e legitimidade.

Neste sentido, o pleno cumprimento dos desígnios democráticos nas sociedades livres reclama que as mesmas disponham de meios de acesso a informação fiável e fundamentada, essenciais para uma autónoma e consciente composição do juízo pessoal no processo de eleição dos seus representantes políticos.

Todavia, o saudável desenrolar dos processos eleitorais democráticos – e da vida em democracia no seu geral – tem sido ameaçado pela disseminação de desinformação por parte de agentes que não defendem os mesmos ideais[30]. Nestas circunstâncias, potencia-se um clima de manipulação e mentira, extrema e particularmente maligno para os cruciais momentos de decisão política[31], uma vez que se verificam tentativas de retirar a relevância e a validade que lhes são inerentes[32], constituindo-se uma das mais perigosas forças deterioradoras das bases democráticas.[33]

---

[27] POLYAKOVA, Alina; FRIED, Daniel, pp. 1 e 2.
[28] Comissão Europeia, *Comunicação: Garantir eleições europeias livres e justas*, COM(2018) 637 final, 2018, p. 1.
[29] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 5.
[30] *Comunicação: Garantir eleições europeias livres e justas*, p. 1.
[31] *Plano de Ação contra a Desinformação*, p. 12.
[32] *Comunicação: Garantir eleições europeias livres e justas*, p. 1
[33] Sobre este tema, Cfr. também Comissão Europeia, *Relatório sobre as eleições de 2019 para o Parlamento Europeu*, COM(2020) 252 final, 2020, em particular o capítulo "Addressing disinformation and protecting the integrity and resilience of the electoral process".

Os momentos de sufrágio são, assim, especialmente vulneráveis a investidas no campo da desinformação e, assim sendo, cuidado extra deve ser tido com a transmissão clara e acessível das informações mais elementares nestes períodos – tais como informações sobre datas e os locais de voto, a elegibilidade de votantes, os meios e a segurança dos sistemas de voto, os candidatos e as suas ideologias, entre outros – de modo a evitar o aparecimento de lacunas que propiciem investidas desestabilizadoras nestes domínios e que prejudicam o bom funcionamento de todo o processo de votação.

Do mesmo modo, dadas as suas especificidades, os momentos eleitorais constituem um dos momentos mais sensíveis no quesito dos ataques cibernéticos e de uma propagação mais estruturada de desinformação. O planeamento de campanhas de desinformação em grande escala, realizadas com o apoio de ataques cibernéticos a infraestruturas e sistemas eleitorais (ex.: sistemas informáticos utilizados para registar os eleitores e os candidatos, ou os destinados a reunir e contar os votos e divulgar os resultados, etc.), representam dos principais riscos neste domínio. A adoção de boas práticas comuns pelas autoridades de cibersegurança dos variados Estados-Membros e o investimento na defesa cibernética da tecnologia eleitoral afigura-se, por isso, de extrema relevância para a manutenção da estabilidade das democracias europeias.[34]

Ainda neste domínio, outros fatores, como momentos de crise (sejam eles de natureza migratória, económica, social, etc.), que são geradores de um sentimento universal de alguma inquietação nas populações, torna-as particularmente suscetíveis aos efeitos mais negativos da disseminação de desinformação e, em momentos de maior tensão social, é ainda mais importante apostar numa comunicação clara e baseada nos factos, procurando-se, desse modo, diluir os efeitos especialmente negativos da propagação de informações incorretas em circunstâncias de maior incerteza.

A este propósito, cumpre fazer uma referência à carta enviada, em outubro de 2023, pelo Comissário Europeu para o Mercado Interno, Thierry Breton, ao proprietário da rede social X (ex-Twitter), Elon Musk. Na aludida carta, o Comissário expressa a sua preocupação com a disseminação, naquela rede social, de desinformação relacionada com os desenvolvimentos recentes no domínio do conflito entre Israel e o Hamas, referindo, para o efeito, que se verificaram denúncias relativas à partilha de informações enganosas, manipuladas e descontextualizadas sobre a situação, como a

[34] Sobre este assunto, Cfr. também Conselho da União Europeia, *Conclusões do Conselho e dos Estados-Membros sobre a garantia de eleições europeias livres e justas - Resultado do processo*, 2019, em particular o capítulo IV.

utilização de imagens antigas relativas a outros conflitos armados e imagens provenientes de videojogos.[35] No seguimento destas observações, a Comissão abriu uma investigação ao caso, dirigindo um pedido de informações, no âmbito do RSD, à rede social X.[36]

Nesta rede social também se observou, em particular, a circulação de conteúdo a sugerir uma eventual intervenção dos Estados Unidos no conflito, como de *tweets* onde se alegava que a Ucrânia tinha vendido, ao Hamas, armas recebidas pela OTAN e, ainda, de áudios falsos a insinuarem que a cobertura noticiosa – levada a cabo pela cadeia de notícias CNN, no caso – era encenado, controlado e se reportava a acontecimentos falsos. Para além disso, verificaram-se, ainda, relatos de bombardeamentos a uma igreja que nunca se sucederam, a circulação de documentos falsos da Casa Branca e de um *tweet* que anunciava a evacuação da embaixada norte-americana no Líbano, seguido de um alerta para que todos os cidadãos norte-americanos saíssem o mais rapidamente possível desse país, inflamando, mais ainda, as posições de força.[37]

A disseminação de desinformação em tempos de guerra é, de um modo geral, potencialmente causadora de um grande sentimento de confusão nas sociedades que, face a um acontecimento tão inquietante para o funcionamento da geopolítica mundial, se encontram a consumir conteúdo falso e enganoso sobre temas sensíveis, particularmente capazes de incendiar tensões sociais e levantar níveis de contestação e dúvida mesmo em países geograficamente distantes e não diretamente envolvidos no conflito armado, como é o caso dos Estados-Membros.

É, por isso, necessário assegurar, particularmente nestes momentos de maior apreensão coletiva, canais de circulação de informação que primem por uma comunicação clara e desambiguada dos factos, reservando-se, para o efeito, especial atenção à análise e verificação do conteúdo «alegadamente» proveniente das áreas geográficas em conflito.

Os processos de tomada de decisão

Tudo que até agora foi exposto acaba também por produzir as suas repercussões ao nível dos processos de tomada de decisão ao mais alto nível. Assim, sabendo que a propagação de desinformação procura, em substância, causar um ambiente social de divisão e disrupção, todo o

[35] BRETON, Thierry, Carta do Comissário Thierry Breton a Elon Musk por conta da disseminação de desinformação e conteúdo ilegal na rede social X no seguimento do conflito entre Israel e o Hamas em 2023, 2023.
[36] Carta do Comissário Thierry Breton.
[37] The New York Times, *False Claims Around Israel Attacks Include Recycled Videos and a Game Clip*, 2023. Disponível em: <https://www.nytimes.com/article/israel-attacks-video-disinformation.html?smid=url-share> [13/10/2023].

processo de deliberação – realizado pelo conjunto de órgãos de soberania – acaba por sair, inevitavelmente, enfraquecido e toldado em circunstâncias de uma tensão pública generalizada e artificialmente fomentada por campanhas de desinformação.

É essencial, por isso, que o comportamento na vida democrática dos cidadãos seja orientado por um amplo e diversificado acesso a informação de confiança sobre os mais variados assuntos de ordem pública que evite a verificação de fenómenos de *confirmation bias*[38] e que corresponda, efetivamente, à realidade dos factos e que não seja manchado por imprecisões cuidadosa e maliciosamente plantadas para torcer a perspetiva das populações sobre tópicos centrais.

A opinião pública deve, por isso, ser única e exclusivamente orientada pela verdade e pelos factos, pois só assim se concretiza plenamente a democracia e se combatem as necessidades mais prementes das sociedades.[39]

2.2 O papel das grandes plataformas digitais

A digitalização das nossas sociedades, e em especial dos canais de comunicação noticiosos, permitiu o surgimento de um novo panorama onde reina a abundância e a diversidade de conteúdos informativos que podem ser consultados à distância de um mero toque ou clique.[40]

As grandes plataformas digitais (desde redes sociais, a aplicações de mensagens[41] e sem esquecer os motores de busca) estão, por seu turno, na vanguarda destes acontecimentos e representam o apogeu do imediatismo na consulta de material noticioso, imediatismo esse que configura uma enormíssima arma ao dispor daqueles que procuram manipular o ecossistema informacional digital a uma escala sem precedentes.[42]

A este propósito, o escândalo do Facebook-Cambridge Analytica demonstrou perfeitamente, por um lado, a quantidade assustadora de dados pessoais ao dispor das redes sociais sobre os seus utilizadores e, por outro, os perigos que daí podem advir caso os mesmos sejam utilizados de forma ilícita e mal-intencionada. O caso ficou precisamente célebre pelo emprego de táticas de manipulação

---

[38] Existe uma tendência natural, por parte do ser humano, no sentido de procurar fontes noticiosas que se ombreiem em opiniões políticas pré-existentes, isto é, a busca por informação noticiosa desagua, involuntariamente, na procura por informações que confirmem as perspetivas que já detemos. No meio em linha, o ato de reconhecimento associado aos processos de definição de perfis, apenas reforça este traço psicológico. Para além disso, e também nos meios digitais, a classificação e organização de conteúdo encontra-se fortemente associada às opiniões e perspetivas dos perfis que seguimos e com quem mais interagimos, que normalmente não diferem muito das nossas, reiterando uma sensação de afunilamento no consumo de notícias. A longo prazo e considerando diferentes setores populacionais, começam a verificar-se fenómenos de polarização social, que facilitam a disseminação de desinformação e dificultam a sua contestação e a recetividade de visões divergentes mais construtivas. Cfr. ALAPHILIPPE, Alexander, *et al.*, p. 21.

[39] ALAPHILIPPE, Alexander, *et al.*, p. 49; *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 2.

[40] Comissão Europeia, *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, JOIN(2018) 16 final, 2018, p. 4.

[41] *Plano de Ação contra a Desinformação*, p. 3.

[42] *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 4.

do comportamento eleitoral dos eleitores, com o recurso a técnicas de identificação e previsão das inclinações políticas de alguns setores do eleitorado, complementadas com a disseminação microdirecionada de informação incorreta, descontextualizada e/ou tendenciosa sobre temas sensíveis e polarizadores[43]. Algumas das lições retiradas deste emblemático caso demonstram particularmente a forma como o uso ilegítimo de dados pessoais consegue atingir o coração da democracia de formas tenebrosas.

A enormíssima capacidade destas plataformas tecnológicas na amplificação e microdirecionamento de conteúdo torna-as extremamente atraentes para a propagação precisa de informação em larga escala, sendo as plataformas, por esse exato motivo, sistematicamente alvo de atividades híbridas no campo da desinformação. No meio desta teia de informação pouco transparente é mais importante que nunca saber que perfis e publicações se preocupam efetivamente em transmitir a realidade dos factos de uma forma isenta e fundamentada.

Deste modo, e dada a enorme relevância pública dos espaços sociais que estas plataformas propiciam, a gestão dos mesmos – que é feita, não esqueçamos, por atores privados – não se deve alhear das necessidades e dificuldades que a desinformação coloca às democracias e à própria liberdade de expressão e de informação.[44]

Deste modo, o papel das grandes plataformas digitais, enquanto detentoras de um vasto poder de controlo e influência sobre os canais de comunicação e informação à escala global, assume-se como crónico e irrenunciável nesta questão e, levando tal em consideração, devem ver-se obrigadas a realizar um exercício de autocrítica no sentido de alguma abertura à implementação de alterações aos seus modelos de negócio.[45]

Sabendo que com grandes poderes surgem grandes responsabilidades, as plataformas digitais devem assumir, por conseguinte, uma posição forte e incontestável contra o abuso e a manipulação dos seus serviços, devendo, para o efeito, investir no desenvolvimento de um ambiente em linha seguro, fidedigno e objetivo, especialmente nos momentos em que tais valores merecem uma especial preponderância, como é o caso de eleições ou referendos, ou em momentos de crise, como também já foi referido. Desta missão comunitária decorre uma responsabilidade da qual as grandes plataformas não se podem evadir e que corresponde ao seu papel na construção de um serviço que liga e informa

---

[43] *Comunicação: Garantir eleições europeias livres e justas*, p. 3; *Plano de Ação contra a Desinformação*, pp. 3 e 4; *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 3.

[44] Como veremos adiante, existem já instrumentos normativos que pretendem, precisamente, chamar as grandes plataformas digitais à razão e responsabilizá-las pelos perigos que estas colocam às democracias.

[45] POLYAKOVA, Alina; FRIED, Daniel, p. 14.

– devida, justa e imparcialmente – o mundo sobre as principais questões que se levantam a cada instante.[46]

Na hipótese de uma campanha de desinformação em grande escala, é absolutamente categórico o auxílio à formulação de uma contraofensiva estratégica de veiculação de informação confiável, fundamentada e congruente de forma rápida para o público. Esta comunicação célere é fundamental dados os já observáveis fenómenos de enraizamento de determinados pontos de tensão que serão muito mais dificilmente combatidos se não forem contestados antecipadamente.[47] É precisamente nesta questão que as grandes plataformas sociais assumem uma importância redobrada, uma vez que constituem um meio de proximidade entre as instâncias governamentais, as organizações de verificação de factos, a comunidade científica e académica, as organizações da sociedade civil, e, claro, os seus cidadãos.

2.3 A importância da promoção de um jornalismo independente e de qualidade

A prossecução de um clima de verdade, independência e pluralismo nos órgãos de comunicação social é igualmente fundamental para a dinamização das nossas democracias e, nesse sentido, também estes devem assumir a sua responsabilidade nesta era da desinformação.

Nas sociedades democráticas livres, a atividade dos media, enquanto guardiões da democracia, encontra-se tradicionalmente ligada a um propósito próximo ao de uma "prestação de contas" sobre a transparência na atividade dos poderes públicos.[48]

Os órgãos de comunicação social mais tradicionais, submetidos a rigorosos critérios deontológicos no âmbito da sua atividade profissional de divulgação ao público de material noticioso, devem empenhar-se na preservação desses elevados padrões de profissionalismo e de autonomia editorial, de forma a garantir a estabilização da confiança da opinião pública nos meios que mais lhes são familiares. Esse esforço é essencial e irá atuar como uma espécie de catalisador no âmbito de todo o processo de combate aos efeitos negativos da desinformação.[49]

---

[46] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 12.
[47] *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 8.
[48] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 1.
[49] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 11; Sobre este tema, Cfr. também PEREIRA, Miguel, "A política de combate à desinformação na União europeia: problemas conceptuais e principais instrumentos", *in E-book do VI seminário internacional hispano-luso-brasileiro sobre direitos Fundamentais e políticas públicas*, Dialética Editora, pp. 347 e 348.

Neste sentido, a promoção de um ecossistema mediático mais transparente e elucidativo é essencial para restaurar e reverter quaisquer perdas de confiança que se tenham verificado ao longo dos últimos tempos[50] e que se traduziram numa movimentação do público para fontes noticiosas alternativas não verificadas ou registadas. Daí ser tão importante uma aposta reforçada no selo de qualidade característico do jornalismo sério, caracterizado pela diversidade e inclusão noticiosa, perfeitamente capaz de "revelar, contrabalançar, e diluir a desinformação"[51].

A busca por uma maior claridade em torno do processo de produção e difusão de material noticioso é, deste modo, essencial para que o público consiga, de uma maneira geral, assimilar a lógica que se encontra subjacente ao conteúdo que se lhes é apresentado, de forma que este também compreenda os motivos pelos quais pode, realmente, confiar nos meios de comunicação devidamente acreditados e registados. Este conhecimento irá, ultimamente, ajudar o público a tomar decisões mais responsáveis no âmbito do consumo de notícias, que procurará fontes onde sejam respeitadas todas as exigências da excelência jornalística.[52]

Assim, uma maior abertura das redações – tanto das televisões, como das rádios e da imprensa em papel – a toda a comunidade, será particularmente relevante para que esta possa compreender todo o processo latente à produção e difusão de informação, algo que irá certamente ajudar a criar um vínculo de confiança entre ambas as partes, reforçando o papel e a importância da adesão a determinados valores éticos e deontológicos relacionados com a verificação, preparação e difusão de notícias.[53]

As fontes noticiosas alternativas e não registadas não se encontram, por sua vez, legalmente obrigadas a atingir os ditos princípios éticos que se expressam em toda a atividade jornalística, não conseguindo, pelo menos com a mesma facilidade, demonstrar de modo transparente o profissionalismo e o método subjacentes à produção do seu material noticioso. É exatamente este fator diferenciador – revelador do que é o bom jornalismo e de quem faz esse bom jornalismo – que deve ser explorado para um eficaz combate à propagação de desinformação.

A promoção da importância deste fator diferenciador encontra-se, por sua vez, dependente de uma maior visibilidade do conteúdo de qualidade provindo de órgãos noticiosos que exercem a sua atividade com independência e excelência. Nesse sentido, e uma vez que o consumo de notícias se

---

[50] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 11; MARWICK, Alice; LEWIS, Rebecca, *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017, pp. 40 e 45.

[51] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 15.

[52] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 22.

[53] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 22.

encontra cada vez mais orientado para os meios tecnológicos, é importante estabelecer uma relação mais estreita de cooperação entre os órgãos de comunicação social e outros intervenientes relevantes para esta questão, como as organizações de verificação de factos e as plataformas digitais[54], em nome de um ecossistema informacional mais transparente, responsabilizável e fidedigno.

Do mesmo modo, o jornalismo e a investigação jornalística caracterizados por traços de independência e isenção merecem também ser apoiados pelas autoridades públicas e, nesse sentido, é preciso acautelar o tema dos apoios institucionais.

Assim, os Estados-Membros e as Instituições Europeias podem (e devem) contribuir com apoios em áreas que não comprometam a autonomia e a liberdade que distingue e caracteriza o ambiente informacional. Todo e qualquer apoio deve, assim, afastar-se de qualquer tentativa de interferência no encadeamento noticioso das entidades às quais são concedidos apoios e deve, em alternativa, materializar-se unicamente em atos que promovam a independência, a cooperação transfronteiriça e a qualidade jornalística dos órgãos auxiliados por estas medidas.[55]

No campo dos media, esta figura de apoio financeiro poderia, a título de exemplo, dirigir-se à formação de jornalistas e à promoção da inovação nas redações noticiosas, no âmbito da criação de instrumentos avançados de monitorização de conteúdo nas redações, baseados nas mais avançadas tecnologias de inteligência artificial e do *big data*.[56]

Todo e qualquer processo de atribuição de apoios estatais a órgãos de comunicação social deve, em particular no âmbito dos seus critérios de candidatura e métodos de execução[57], ser enunciado de um modo claro, objetivo e prognosticável e promover uma execução harmonizada a nível europeu[58] – não prejudicando nem desvirtuando as regras de concorrência[59].

A propósito, a própria Comissão sugere, em nome da promoção da transparência na atribuição destes apoios, o registo – na forma de um repositório em linha – de todas as decisões que se

---

[54] ALAPHILIPPE, Alexander, *et al.,* p. 13.

[55] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 37.

[56] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 6 e 37.

[57] Comissão Europeia, *Relatório da Comissão sobre a aplicação da Comunicação «Combater a desinformação em linha: uma estratégia europeia»*, COM(2018) 794 final, 2018, p. 12.

[58] Já existem, atualmente, alguns documentos europeus que instituem as normas e/ou orientações a ser observadas na concessão de tais apoios e são eles a Comunicação da Comissão relativa à aplicação das regras em matéria de auxílios estatais ao serviço público de radiodifusão, a Comunicação da Comissão sobre o enquadramento dos auxílios estatais à investigação, desenvolvimento e inovação e, ainda, o Regulamento Geral de Isenção por Categoria. Cfr. *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 16.

[59] Várias decisões da Comissão vieram declarar que os apoios estatais desta natureza são compatíveis com o Direito Europeu (ex.: http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_30481; http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_36366; http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=3_SA_47973.) Cfr. *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 16.

traduzam na concessão destes apoios estatais, possibilitando a consulta e o acesso amplo a todos os factos que desembocaram na concessão (ou não) de tais apoios[60].

2.4 Os problemas da adoção de uma via exclusivamente legislativa para o combate à problemática

A política europeia de combate ao fenómeno da desinformação deve assumir as mesmas características da própria ameaça, isto é, uma natureza complexa e multidimensional.

Dadas as preocupações relacionadas com os impactos da problemática ao nível do ceticismo social e na produção de efeitos erodentes no domínio da opinião pública[61], a grande aposta deve residir essencialmente na promoção de medidas de caráter não regulatório que produzam resultados sólidos e prolongados[62].

A atuação das autoridades públicas na defesa das populações e da democracia contra a desinformação deve, assim, assumir uma postura "sistémica", por via do desenvolvimento de meios de atuação que procurem combater a ameaça numa perspetiva mais holística. Essa postura pressupõe, a título de exemplo, a promoção de iniciativas de literacia mediática e de verificação de factos, ou de estudos de investigação sobre o fenómeno, temas esses que serão igualmente desenvolvidos ao longo desta dissertação.[63]

Neste domínio, a resposta europeia deve igualmente assumir uma postura condizente com os valores fundamentais preconizados e, nesse sentido, a construção de respostas não deve assumir um caráter puramente público e legislativo, uma vez que se poderia cair num fenómeno estatal de "contra-propaganda"[64]. Todo e qualquer avanço regulatório nesta sede poderia ser perspetivado como uma ultrapassagem de todas as linhas vermelhas, na forma de uma consumação de autênticos atos de repressão e censura promovidos por órgãos governamentais, situação essa que apenas dificultaria e desviaria a atenção dos objetivos que se pretendem realmente ver alcançados.[65]

A firme resposta europeia que tanto se pretende deve, deste modo, prever um conjunto de mecanismos que amparem a vitalidade do direito à liberdade de expressão e de informação,

---

[60] *Relatório da Comissão sobre a aplicação da Comunicação «Combater a desinformação em linha: uma estratégia europeia»*, p. 12.
[61] POLYAKOVA, Alina; FRIED, Daniel, p. 2.
[62] POLYAKOVA, Alina; FRIED, Daniel, p. 1.
[63] AMARAL, Maria Lúcia, parágrafo 33.
[64] ALAPHILIPPE, Alexander, *et al.,* pp. 45 e 46.
[65] POLYAKOVA, Alina; FRIED, Daniel, p. 3;

particularmente no meio digital, e, levando tal em consideração, qualquer tentativa de censura aos "discursos críticos, dissidentes, satíricos ou chocantes"[66] será sempre inadmissível.

Os próprios agentes disseminadores de desinformação poderiam, mesmo, beneficiar de uma ação regulatória mais musculada neste âmbito, encaminhando os seus esforços para o desenvolvimento de narrativas nas quais interpretam o papel de vítimas de repressão, redirecionando o apoio da sociedade a seu favor, deslegitimando ultimamente qualquer tipo de medida que seja tomada ao nível do erário público[67] e contribuindo para o aquecer de tensões sociais.

Deste modo, e sabendo, ainda assim, que o aspeto regulatório nunca será de descartar, é possível estabelecer algumas noções base que devem informar o processo de formulação de respostas legislativas à problemática: (1) a informação raramente poderá ser classificada como sendo absolutamente verdadeira ou falsa; (2) nenhuma autoridade deve deter exclusividade sobre o conhecimento do concreto; (3) as sociedades livres e abertas prosperam – e realizam-se na sua forma mais pura – num ambiente recetivo à confrontação de ideias e opiniões distintas e incómodas.[68] A par, toda e qualquer medida preparada deve ser continuamente avaliada para que se proceda à apreciação dos seus efeitos, que se esperam ser os pretendidos.[69]

Por fim, a recolha de diversos dados estatísticos relacionados com questões centrais do quotidiano das sociedades – tais como os seus níveis de educação, de adesão aos valores democráticos, de confiabilidade nas organizações governamentais ou, ainda, dados sociais sobre a disparidade e desigualdades a nível social e económico – é particularmente relevante dado que estas informações representam grandes indicadores para os possíveis graus de eficácia das campanhas de desinformação, que visam, precisamente, explorar as debilidades existentes nos vários segmentos demográficos, sendo justamente também a este nível que o modelamento de uma resposta multifacetada e robusta ao fenómeno deverá assentar.[70]

A importância da autorregulação e de outras vias intrinsecamente não regulatórias

A atuação estadual que se pretende ver neste domínio em articulação com todas as partes relevantes, como profissionais de literacia mediática, verificadores de factos, académicos e plataformas

---

[66] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 8.
[67] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 14.
[68] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 20; Acórdão Handyside v. Reino Unido do Tribunal Europeu dos Direitos Humanos, de 07/12/1976, proferido no proc. n.º 5493/72, parágrafo 49.
[69] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 5.
[70] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 4

digitais, é indispensável[71] e deve centrar-se na prossecução de dois grandes objetivos: por um lado, a promoção de um ambiente informativo onde impera a liberdade de expressão e o pluralismo informativo, evitando-se práticas censoras, e, por outro, a promoção dos valores de transparência e inteligibilidade de todos os canais de informação que compõem o ecossistema informativo.[72] [73]

É, assim, da maior importância a efetivação (num primeiro momento, pelo menos) de uma verdadeira cooperação – apoiada pelos profissionais relevantes já mencionados – com as grandes plataformas digitais. O transparente estabelecimento de relações próximas neste âmbito é crucial para a prevenção de situações nas quais sequer se vislumbre qualquer fenómeno de uma "privatização, politicamente ditada, do policiamento e censura do que é, e não é, uma forma aceitável de expressão"[74], casos onde a responsabilidade de controlar conteúdo que constitua desinformação incide, por obra de uma imposição legal opaca e não dialogante, sobre as plataformas digitais[75].

É precisamente neste sentido que surgem os códigos de conduta, enquanto ferramentas importantes para a arquitetação de uma resposta para a ameaça, reunindo, de modo extenso, os intervenientes mais relevantes, que se encontram voluntariamente submetidos a um conjunto de compromissos que pretendem assegurar avanços neste domínio.

2.5 As implicações para o direito à liberdade de expressão e de informação

A temática do combate à disseminação de desinformação prende-se, naturalmente, com a eventual admissão de restrições a direitos fundamentais que formam o cerne das democracias. Procurar-se-á, assim, atingir ao longo das próximas páginas uma visão holística e abrangente da dimensão que os principais direitos e interesses fundamentais representam para este fenómeno.

O desenvolvimento de uma política estratégica de combate à desinformação contende, inevitavelmente, com o exercício do direito à liberdade de expressão e de informação e do direito à liberdade de imprensa e meios de comunicação social (consagrado isoladamente na CRP, e consagrado no âmbito do direito à liberdade de expressão e de informação na CDFUE e na CEDH).

---

[71] POLYAKOVA, Alina; FRIED, Daniel, p. 2.
[72] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 36.
[73] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 1.
[74] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 20.
[75] ALAPHILIPPE, Alexander, *et al.*, p. 58.

Tal como é evidenciado pela escolha do legislador constitucional português e do legislador europeu, a liberdade de informação deve ser entendida como complementar e absolutamente indissociável da liberdade de expressão – que normalmente usufrui de um maior grau de protagonismo – e, nesse sentido, as múltiplas dimensões que a primeira pode assumir devem também ser merecedoras da nossa atenção.

2.5.1 Considerações introdutórias sobre o direito à liberdade de expressão e de informação

O direito à liberdade de expressão e de informação, expresso no artigo 11.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), no artigo 10.º da Convenção Europeia dos Direitos Humanos (CEDH) e, por fim, no artigo 37.º da Constituição da República Portuguesa (CRP), representa um dos alicerces das sociedades verdadeiramente livres e democráticas e estende-se a todas as formas de comunicação, inclusive no meio em linha.

Do compromisso constitucional decorrente do reconhecimento, no artigo 37.º da CRP, do direito à liberdade de expressão e de informação resulta, por um lado, uma tutela do direito a transmitir e receber informações e ideias sem que haja o receio de sofrer interferências ou represálias por parte do poder público («liberdade de expressão»)[76] e, por outro, a tutela aos direitos «de informar», «de se informar» e «de ser informado» («liberdade de informação»).

No âmbito desta visão tripartida do direito à liberdade de informação, na ótica de Gomes Canotilho e Vital Moreira[77], o «direito de informar» assume uma dupla vertente, podendo reportar-se à "liberdade de transmitir ou comunicar informações a outrem, (...) sem impedimentos", como ao "direito de informar" ou o "direito a meios para informar"[78].

O «direito de se informar», por seu turno, titula a "liberdade de recolha de informação, de procura de fontes de informação", ou seja, o "direito de não ser impedido de se informar", ainda que tal não signifique que possam surgir algumas limitações à fruição deste direito, como é o caso da recolha de determinadas informações presentes, a título exemplificativo, nos arquivos secretos dos serviços de informação.[79]

Por fim, o «direito a ser informado» consiste, de modo sucinto, no "direito a ser mantido adequadamente e verdadeiramente informado (...) pelos meios de comunicação (cfr. arts. 38º e 39º) e

---

[76] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 18 e 19; AMARAL, Maria Lúcia, parágrafo 21.
[77] CANOTILHO, J. J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 3.ª edição revista, Coimbra Editora, Coimbra, 1993, p. 225; AMARAL, Maria Lúcia, parágrafo 22.
[78] *Idem.*
[79] *Idem.*

pelos poderes públicos (...), sem esquecer outros direitos específicos à informação reconhecidos na Constituição"[80].

2.5.2 Breves observações sobre o direito à liberdade de imprensa e meios de comunicação social

No âmbito do direito à liberdade de imprensa e meios de comunicação social, o TEDH, sediado em Estrasburgo, veio já salientar o papel da imprensa nas sociedades democráticas, enquanto «cão de guarda dos assuntos públicos».

Deste modo, nunca será de descartar a relevância constitucional que se materializa na necessidade e importância de reconhecer um determinado grau de proteção ao labor jornalístico[81], indispensável para a plena afirmação da liberdade de expressão e de informação.

As garantias concedidas por este direito aos jornalistas – que desenvolvam a sua atividade no domínio da comunicação de assuntos de interesse público – estão sujeitas à verificação de certos requisitos, tais como a boa-fé da sua atuação, a existência de uma base factual para a mesma e a produção de conteúdo que seja sólido e rigoroso, em estrita consonância com o que obriga a deontologia e ética jornalística[82], relembrando, para o efeito, que a imprensa não se pode escudar neste direito em toda e qualquer circunstância.

O direito à liberdade de expressão e de informação enfatiza, por sua vez, a existência de uma obrigação positiva, a ser exercida por parte dos Estados, no sentido de propiciar um ambiente favorável à participação de todos num debate público caracterizado pelo verdadeiro respeito pela fruição destas liberdades. [83] Neste sentido, o Conselho da Europa destaca a adoção de projetos que estimulem e apoiem o pluralismo dos media, a diversidade dos conteúdos transmitidos, a transparência em questões sobre a propriedade, organização e financiamento dos meios de comunicação social e a viabilização de iniciativas de literacia mediática e digital, que, por seu turno, representam alguns exemplos de políticas que contribuem, justamente, para a concretização deste direito tão fundamental, evidenciando-se uma relação simbiótica entre os dois.[84]

---

[80] CANOTILHO, J. J. Gomes; MOREIRA, Vital, pp. 225 e 226; AMARAL, Maria Lúcia, parágrafo 22.

[81] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 19; Acórdão Dink v. Turquia do TEDH, de 14/09/2010, proferido no proc. n.º 2668/07, parágrafo 137; Acórdão Fuentes Bobo v. Espanha do TEDH, de 29/02/2000, proferido no proc. n.º 39293/98, parágrafo 38; Acórdão Özgür Gündem v. Turquia do TEDH, de 16/03/2000, proferido no proc. n.º 23144/93., parágrafos 42-43.

[82] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 18 e Acórdão Stoll v. Suíça do Tribunal Europeu de Direitos Humanos, de 10/12/2007, proferido no proc. n.º 69698/01, parágrafo 20.

[83] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 19; Dink v. Turquia, parágrafo 137; Fuentes Bob v. Espanha, parágrafo 38; Ozgür Güdem v. Turquia, parágrafos 42-43.

[84] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 19; Comité de Ministros do Conselho da Europa, *Recomendação do Comité de Ministros aos Estados-Membros sobre o pluralismo dos meios de comunicação social e a transparência da propriedade dos meios de comunicação social*, CM/Rec(2018)1, 2018, pontos 1., 10. e 11. do Preâmbulo.

2.5.3 O alcance democrático e normativo do direito à liberdade de expressão e de informação (e da liberdade de imprensa e dos meios de comunicação social) à luz das ameaças da atualidade

Em estreita consonância com o referido anteriormente, no domínio do alcance e significado democrático normativo da liberdade de expressão e de informação, a jurisprudência do Tribunal Constitucional Espanhol (TCE, em diante) afigurar-se-á, como veremos, muito oportuna e elucidativa para a questão de fundo.

Segundo o entendimento do TCE, com a promoção da liberdade de expressão e de informação pretende-se proteger o bem jurídico da "formação e preservação de uma opinião pública livre e robusta", enquanto "elemento essencial e fonte de legitimidade do processo político democrático"[85].

Assim, para além do reconhecimento da sua relevância enquanto liberdade individual, é também reconhecida à liberdade de expressão e de informação a sua natureza de "instituição política fundamental", ou seja, a ideia de que a opinião pública – que se pretende que seja o mais desobstruída possível – surge fortemente acoplada ao incomensurável valor da diversidade política, princípio base de qualquer Estado de Direito Democrático[86]. Daqui também se conclui que a integral defesa desta liberdade constitui, na prática, um pré-requisito – uma "condição prévia e necessária"[87] – para o exercício coletivo e desimpedido dos demais direitos e liberdades que caracterizam e dão vida e forma às democracias livres e abertas.

Neste sentido, o TCE procede, ainda, a uma constatação de extrema relevância, não apenas para este capítulo, mas para todo o corpo da dissertação: "Para que o cidadão possa formar livremente as suas opiniões e participar de modo responsável nos assuntos públicos, tem que ser também amplamente informado de modo que possa ponderar opiniões diversas e inclusivamente opostas"[88], sendo que "o direito de um profissional do jornalismo a informar, assim como o dos seus leitores a receber uma informação integral e verdadeira, constitui (...) uma garantia institucional de caráter objetivo".[89]

No seguimento do disposto, o TCE aborda, então, a questão da liberdade de informação e, de forma conexa, a questão da liberdade e regulação da imprensa e meios de comunicação social, alertando, para o efeito, que a Constituição (a Constituição Espanhola, no caso), ao estabelecer como exigência a «veracidade» da informação veiculada pelos órgãos jornalísticos, não procura retirar

---

[85] AMARAL, Maria Lúcia, parágrafos 23 e 25.
[86] Acórdão do Tribunal Constitucional Espanhol, de 31/03/1982, proferido na sentença n.º 12/1982, parágrafo 3; AMARAL, Maria Lúcia, parágrafo 27.
[87] Acórdão do TCE, de 16/12/1986, proferido na sentença n.º 159/1986, parágrafo 6; AMARAL, Maria Lúcia, parágrafo 28.
[88] Sentença n.º 159/1986, parágrafo 6; AMARAL, Maria Lúcia, parágrafo 28.
[89] Sentença n.º 159/1986, parágrafo 8; AMARAL, Maria Lúcia, parágrafo 28.

qualquer tipo de amparo constitucional às informações que eventualmente se venham a demonstrar como incorretas ou imprecisas, mas procura, sim, "estabelecer um (...) dever de diligência sobre o informador, a quem se pode e deve exigir que aquilo que transmite como factos haja sido objeto de prévia confrontação com dados objetivos", sendo apenas privado de tal amparo constitucional aqueles que, no incumprimento do direito à informação, atuam "com menosprezo da verdade ou falsidade do objeto de comunicação"[90]. Posto isto, será também relevante mencionar a posição da Provedora de Justiça que indica que, do direito consagrado na Constituição Portuguesa à liberdade de expressão e de informação, resulta uma verdadeira responsabilidade do poder público em escudar os cidadãos contra a desinformação.[91]

Assim, na opinião do TCE, um ordenamento jurídico democrático não deve conferir uma garantia constitucional à conduta improvidente, nem à conduta "de quem comuni[ca] como factos aquilo que são simples rumores ou (...) meras invenções ou insinuações insidiosas", devendo, sim, proteger "a informação corretamente obtida e difundida ainda que a sua total exatidão seja controversa".[92]

O TCE termina, como vimos, esta última parte em jeito de advertência para a natural e inevitável presença de debilidades no domínio da informação jornalística, na medida em que a absoluta verdade dos acontecimentos é, não raras vezes, de um alcance impossível e, por isso, a veiculação de informações equívocas e menos precisas são inexoráveis em países democráticos onde vigora a liberdade e a abertura dos debates públicos. Assim, o que se deve promover e tutelar é, justamente, a defesa da ética deontológica jornalística[93], na medida em que, caso a «verdade» fosse a única "condição para o reconhecimento do direito", a única garantia de segurança jurídica – diz o TCE – "seria o silêncio".[94]

(É verdade que, até ao momento, todas as observações foram efetuadas sob a perspetiva jurídica de um país vizinho, mas, ainda assim, a leitura, tanto a nível europeu como nacional, não deve desvirtuar muito do que foi mencionado, dada a lógica, a adequação e o sentido extremamente apurado daquele Tribunal Espanhol na defesa dos direitos fundamentais comuns a todos os povos europeus.)

---

[90] Acórdão do TCE, de 21/01/1988, proferido na sentença n.° 6/1988, parágrafo 5; AMARAL, Maria Lúcia, parágrafo 29.
[91] AMARAL, Maria Lúcia, parágrafo 19.
[92] Sentença n.° 6/1988, parágrafo 5; AMARAL, Maria Lúcia, parágrafo 29.
[93] Será relevante aludir, neste momento, aos Estatutos da Entidade Reguladora para a Comunicação Social (ERC), responsável pelas atividades de regulação e supervisão do setor da comunicação social em Portugal, que demonstram, também, – na alínea d) do artigo 7.°, relativo aos «Objetivos da regulação» – a tónica da promoção de um jornalismo de isenção e qualidade, enquanto meta de supervisão: "assegurar que a informação fornecida pelos prestadores de serviços de natureza editorial se pauta por critérios de exigência e rigor jornalísticos (...)".
[94] Sentença n.° 6/1988, parágrafo 5; AMARAL, Maria Lúcia, parágrafo 29.

2.5.4 A imposição de restrições aos direitos fundamentais mencionados

O ecossistema de consumo de conteúdos noticiosos mudou profundamente desde a década de 80 (data dos aludidos acórdãos) e, neste momento, o *status quo* do consumo de notícias nas sociedades contemporâneas encontra-se aberto a atores que possuem uma influência pública, até então, reservada aos órgãos de comunicação social mais tradicionais, motivo pelo qual as regras de ética e deontológica jornalísticas já não conseguem assegurar, por si só, a excelência no ecossistema noticioso.[95]

A mais preeminente força motriz associada à disseminação de desinformação surge, precisamente, coligada a um fenómeno de «trivialização» da profissão de jornalista – a figura de autoridade tradicionalmente responsável pela comunicação dos principais assuntos de relevância pública – e tal circunstância acaba por representar uma ampla ameaça ao direito, de todo e qualquer cidadão, a ser informado com base num conteúdo rigoroso e isento[96] e, simultaneamente, ao processo de formação de uma opinião pública aberta e vigorosa. Verifica-se, consequentemente, uma potencial deterioração dos processos democráticos[97], que se alicerçam na pressuposição de que todo eleitor exerce o seu direito de voto, quando o é chamado a fazer, de um modo informado[98].

Posto isto, é precisamente com base no enquadramento descrito ao longo das últimas páginas que se deve idealizar a imposição – justificada e proporcional – de restrições a direitos fundamentais neste domínio, isto é, com base numa mitigação das graves perturbações verificadas ao nível do normal funcionamento das sociedades democráticas, que se evidenciam caso não se adotem as ditas medidas restritivas de direitos.[99]

Assim, será de relembrar que o direito à liberdade de expressão e de informação – e seus direitos conexos – não é absoluto e pode, por isso, ser alvo de restrições, respeitando-se as exigências previstas para o efeito.

Assim, segundo o disposto no artigo 18.º da CRP, qualquer restrição a direitos, liberdades e garantias (1) apenas se pode verificar nos casos explicitamente previstos na Constituição, (2) deve ser necessária para preservar outros direitos ou interesses previstos nesta, (3) deve revestir um caráter

---

[95] AMARAL, Maria Lúcia, parágrafo 32.
[96] CHULVI, Cristina Pauner, "Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red", *in Teoría y Realidad Constitucional*, número 41, 2018, p. 310; AMARAL, Maria Lúcia, parágrafo 32.
[97] AMARAL, Maria Lúcia, parágrafo 32.
[98] CHULVI, Cristina Pauner, p. 299; AMARAL, Maria Lúcia, parágrafo 32; Entidade Reguladora para a Comunicação Social (ERC), p. 3; Sobre este tema, Cfr. também ABA-CATOIRA, Ana, "Los desórdenes informativos en un sistema de comunicación democrático", *in Revista De Derecho Político*, 2020 (109).
[99] CHULVI, Cristina Pauner, p. 310; AMARAL, Maria Lúcia, parágrafo 32.

geral e abstrato e (4) não pode assumir um efeito retroativo nem diminuir a extensão e o alcance do conteúdo essencial dos mesmos.

Por sua vez, de acordo com o artigo 52.º, n.º1 da CDFUE, quaisquer restrições aos direitos fundamentais previstos na Carta deverão preencher um conjunto de três requisitos para que as limitações impostas sejam legítimas: (1) a previsão legal das restrições; (2) o respeito pelo conteúdo essencial dos direitos e liberdades; (3) e, no respeito pelo princípio da proporcionalidade, a restrição em causa deve ser necessária e corresponder a "objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros"[100]

Destes preceitos se retira que será sempre necessário e importante realizar um diligente exercício em vista ao alcance de um delicado equilíbrio entre o respeito pelo direito à liberdade de expressão e de informação – e suas possíveis múltiplas manifestações – e todos os pontos positivos, a diversos níveis, que se encontram associados à existência de uma população verdadeiramente esclarecida e consciente[101].

Mais adiante – aquando da abordagem ao caso RT France v Conselho – será minuciosamente apreciada uma questão prática sobre a eventual violação do direito à liberdade de expressão e de informação em face de um caso de disseminação de desinformação. Nesse capítulo, os requisitos mencionados anteriormente serão alvo de um estudo mais rigoroso, específico, prático e concreto.

2.5.5 A polémica com a Carta Portuguesa de Direitos Humanos na Era Digital

A questão da restrição dos direitos fundamentais resultantes do desenvolvimento de políticas legislativas de combate à desinformação, que até então foi aprofundada, não constitui assunto meramente teórico e a prova disso é, também, a discussão em torno de algumas disposições da Carta Portuguesa de Direitos Humanos na Era Digital.

Desenrolar-se-á, assim e ao longo dos próximos parágrafos, um estudo que propõe demonstrar as dificuldades do poder político no desenvolvimento de medidas legislativas de combate à propagação de desinformação, explorando – para o efeito – as principais preocupações que se levantaram especificamente nesta questão.

---

[100] Acórdão RT France v Conselho do Tribunal Geral, de 27/07/2022, proferido no proc. n.º T–125/22, parágrafo 77; Carta dos Direitos Fundamentais da União Europeia, artigo 52.º, n.º 1.

[101] *Relatório da Comissão sobre a aplicação da Comunicação «Combater a desinformação em linha: uma estratégia europeia»*, p. 6.

O caso em concreto

Em Portugal, um dos diplomas legislativos mais recentes no qual é destacada a importância do combate à disseminação de desinformação corresponde à Carta Portuguesa de Direitos Humanos na Era Digital. Nos termos do artigo 6.º da Lei n.º 27/2021, de 17 de maio, que aprovou este diploma, é protegido o «Direito à proteção contra a desinformação».

No seu n.º 1, é referido que o Estado "assegura o cumprimento em Portugal do Plano Europeu de Ação contra a Desinformação", de modo a proteger a sociedade portuguesa contra aqueles que "produzam, reproduzam ou difundam narrativa considerada desinformação".

No seu n.º 2, o diploma legislativo adota a mesma definição que se encontra prevista no Plano Europeu de Ação Contra a Desinformação, referindo que a desinformação corresponde a "toda a narrativa comprovadamente falsa ou enganadora criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que seja suscetível de causar um prejuízo público, nomeadamente uma ameaça aos processos políticos democráticos, aos processos de elaboração de políticas públicas e a bens públicos".

Por seu turno, o n.º 3 do artigo 6.º da Carta procede a uma exemplificação, pouco exaustiva, de algumas realidades que podem materializar-se como narrativas de desinformação, tais como a "utilização de textos ou vídeos manipulados ou fabricados", as "práticas para inundar as caixas de correio eletrónico", ou, ainda, o "uso de redes de seguidores fictícios".

No seguimento do que já vem descrito no Plano de Ação Europeu, o n.º 4 do presente artigo enumera as realidades que, desta vez, não podem ser abarcadas pela noção de «desinformação», referindo-se o artigo aos "meros erros na comunicação de informações" e às "sátiras e paródias".

Por fim, os números 5 e 6 preveem, respetivamente, o direito de qualquer cidadão a ver apreciadas pela ERC as queixas apresentadas com base no disposto nos primeiros 4 pontos do artigo 6.º e, para além disso, o compromisso assumido pelo Estado no sentido de um apoio ao desenvolvimento de "estruturas de verificação de factos por órgãos de comunicação social devidamente registados" e de um sistema de "atribuição de selos de qualidade por entidades fidedignas dotadas do estatuto de utilidade pública".

O «direito à proteção contra a desinformação» é, por este meio, criado com o intuito assegurar o envolvimento de qualquer cidadão num ambiente digital de liberdade e, para o efeito, as medidas

desenvolvidas neste sentido devem ser sensatas e adequadas, respeitando-se os limites constitucionais da liberdade de expressão e de informação.[102]

Neste ponto, a Provedora de Justiça assinala que as medidas previstas devem fomentar o desenvolvimento de um diálogo público multiforme e promover a cultura democrática, alertando, pelo contrário, que não deve ser admitido qualquer comportamento político que seja reprodutor de uma sensação de repressão e de constrangimento, cerceadora do exercício da liberdade de expressão e de informação no meio digital[103].

A Provedora de Justiça conclui referindo, assim, que a legalidade e a validade das políticas de combate à desinformação residem na defesa e promoção da própria liberdade de expressão e de informação.[104]

Todavia, dois números levantaram algumas preocupações na Provedoria de Justiça, que levaram a Provedora Maria Lúcia Amaral a requerer, nos termos do artigo 281.º da CRP, ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade dos números 5 e 6 do artigo 6.º da Carta por representarem, na sua opinião, uma limitação "injustificada e desproporcionada" das liberdades constitucionais de expressão e informação e de imprensa, nos termos do artigo 18.º, n.º 2 da CRP.[105]

Por sua vez, a título subsidiário, a Provedora de Justiça vem requerer a fiscalização abstrata da ilegalidade do n.º 5 do artigo 6.º da Carta Portuguesa de Direitos Humanos na Era Digital, por conta de uma violação dos artigos 5.º e 6.º dos Estatutos da ERC[106]. [107]

O caráter inadequado e desnecessário do n.º 5 do artigo 6.º da Carta

Segundo o entendimento da Provedora, o modelo de queixa à ERC que se encontra previsto no ponto n.º 5 do artigo 6.º da Carta constitui uma interferência "inadequada" e "desnecessária"[108] à liberdade de expressão e de informação.

A sua inadequação surge por conta da sua natureza lenta, inócua, "obsoleta" e "da era analógica", incapaz de responder a uma realidade iminentemente digital, caracterizada pela instantaneidade da sua velocidade de replicação e que, por vezes, necessita – inclusive – de uma base

[102] AMARAL, Maria Lúcia, parágrafo 16.
[103] *Idem.*
[104] *Idem.*
[105] AMARAL, Maria Lúcia, p. 1; Sobre este tema, Cfr. também PEREIRA, Miguel, "A política de combate à desinformação na União europeia: problemas conceptuais e principais instrumentos", pp. 344 e 345.
[106] Lei n.º 53/2005, de 8 de novembro, publicada em Diário da República n.º 214/2005, Série I-A de 2005-11-08, pp. 6396 – 6409.
[107] AMARAL, Maria Lúcia, p. 1.
[108] AMARAL, Maria Lúcia, parágrafo 37.

tecnológica bastante complexa que a acompanhe, dotada de mecanismos que permitam a emissão de alertas em tempo real e uma cooperação estreita com as grandes plataformas em linha para que a sua eficácia seja assegurada.[109]

Por sua vez, o seu caráter desnecessário resulta do facto de ser uma entidade pública, ainda que estatutariamente autónoma, a controlar de modo "concentrado e vertical" a fidedignidade e genuinidade do conteúdo[110], quando tanto se apregoa constitucionalmente a não interferência de entidades de natureza pública no exercício da liberdade de expressão e de informação, por conta das possibilidades de um enviesamento do debate público democrático saudável[111]. A verificação de conteúdos deve, *a contrario*, ser levada a cabo "de forma desconcentrada, difusa e horizontal" e sustentar-se em parâmetros claros e imparciais desenvolvidos por entidades ligadas ao meio noticioso, como órgãos de comunicação social[112] ou verificadores de factos, sem nunca esquecer, claro está, o papel que o utilizador comum pode assumir na deteção de conteúdo que não cumpra os requisitos mínimos de qualidade, por via da utilização de mecanismos de denúncia diligentemente supervisionados[113].

Para além disso, Maria Lúcia Amaral, considera inconstitucional o facto de que um cidadão possa ser alvo de procedimentos contraordenacionais resultantes da partilha de conteúdo que, embora seja nocivo, não perde o seu caráter legal.[114]

Nesta linha de pensamento, a Provedora lança ainda algumas dúvidas quanto à incerteza legal existente em torno das consequências jurídicas decorrentes do regime sancionatório previsto nos Estatutos da ERC, relativos à prática de uma infração relacionada com a disseminação de desinformação. Levando em consideração as bases principiológicas constitucionais da precedência e da reserva de lei, as normas em questão encontram-se feridas de inconstitucionalidade, uma vez que "não especific[am] minimamente nem o âmbito da sua intervenção nem os poderes especificamente atribuídos à ERC para efeitos de combate à desinformação"[115]. A este respeito, fica-se sem saber se a atividade da ERC neste domínio se aplica apenas aos órgãos de comunicação social, ou também às redes sociais, a título de exemplificativo, e, como se não bastasse, mantém-se ainda uma incógnita relativa à amplitude dos seus poderes de regulação, permanecendo uma questão de caráter central:

---

[109] AMARAL, Maria Lúcia, parágrafo 36.
[110] PALOP, Andrés Boix, pp. 102-105; AMARAL, Maria Lúcia, parágrafo 37.
[111] AMARAL, Maria Lúcia, parágrafo 37.
[112] *Idem*.
[113] *Idem.*
[114] AMARAL, Maria Lúcia, parágrafos 38 e 39.
[115] AMARAL, Maria Lúcia, parágrafos 39 e 52.

será que existe uma efetiva atribuição de um poder de remoção de conteúdo, ou apenas de uma prerrogativa que obriga as plataformas a desencadearem a sua própria resposta (como a aplicação de rótulos a determinado conteúdo)?[116]

Vale também salientar que, para além da falta de uma pormenorização dos limites da atuação da ERC neste domínio, encontra-se omissa uma exigência básica para o correto exercício dos seus novos poderes: a existência de um mecanismo de controlo devidamente estruturado para analisar a atuação da entidade reguladora neste domínio, em especial no âmbito da interposição de recursos contra as decisões por si tomadas. Neste sentido, a Provedora de Justiça refere-se a uma "política regulatória de sentido único" prevista na Carta, manifestamente atentatória da liberdade de expressão e de informação daqueles que sofrem prejuízos por conta destas decisões.[117]

Esta falta de clareza e rigor das normas da Carta acaba por inquinar, à luz do artigo 18.º, n.º 2 da CRP, toda a boa vontade que subsista neste diploma legislativo e, posto isto, a Provedora conclui referindo que nos encontramos perante uma proteção excludente da liberdade de expressão e de informação e fala, mesmo, na existência de um "corpo estranho" incabível num Estado de Direito democrático[118].

A indefinição normativa do n.º 6 do artigo 6.º da Carta

Relativamente ao n.º 6 do artigo 6.º da Carta Portuguesa de Direitos Humanos na Era Digital, a Provedora de Justiça levanta questões, uma vez mais, a respeito da falta de precisão do texto da norma legal no tocante ao modo como esse incentivo público se desdobrará na prática, situação essa que desemboca irremediavelmente numa violação do artigo 18.º, n.º 2 da CRP por conta da falta de consideração pelas "exigências de densidade normativa de uma lei restritiva de direitos, liberdades e garantias"[119].

A Provedora de Justiça alerta que esta indefinição normativa resulta numa grande incógnita relativamente a diversas questões centrais tais como a de saber, para os efeitos da lei, o que constitui uma «estrutura de verificação de factos», quais os critérios de admissibilidade para a atribuição dos ditos apoios públicos e de que modo esse apoio se iria materializar (por via da concessão de benefícios fiscais, o financiamento direto de projetos, etc.?), qual a entidade responsável pela acreditação dos

[116] AMARAL, Maria Lúcia, parágrafo 54.
[117] AMARAL, Maria Lúcia, parágrafos 57 e 58.
[118] AMARAL, Maria Lúcia, parágrafos 39 e 56-58.
[119] AMARAL, Maria Lúcia, parágrafos 62 e 63.

interessados e pela elaboração do procedimento de admissibilidade, quais seriam as políticas legais aplicadas para garantir a imparcialidade, transparência, seriedade e isenção das organizações de verificação de factos, entre muitíssimas outras questões que acabam por impossibilitar a aplicação prática e eficiente da presente lei.[120] Para além disso, a mesma incerteza legal estaria presente no âmbito do mecanismo de atribuição de selos de «qualidade» pelas ditas «entidades fidedignas dotadas do estatuto de utilidade pública», conceitos também eles parcamente desenvolvidos no texto legal.

O pedido subsidiário

A título subsidiário, a Provedora de Justiça enviou, igualmente, um pedido de requerimento da ilegalidade do n.º 5 do artigo 6.º da Carta Portuguesa de Direitos Humanos na Era Digital ao Tribunal Constitucional, baseando-se para o efeito na violação dos artigos 5.º e 6.º dos Estatutos da ERC.

Como vimos, a norma da Carta em questão prevê um novo vetor de atuação para ERC. Para além de chamar à atenção para a escassez que se verifica atualmente ao nível dos recursos humanos nesta entidade, a Provedora alerta para o facto da norma da Carta não possuir qualquer tipo acolhimento nas alíneas do artigo 6.º dos Estatutos da ERC, relativo ao seu âmbito de intervenção.

No caso ainda se procedeu a uma tentativa de se alocar a alínea e) do artigo 6.º dos Estatutos para o efeito, que estipula que "as pessoas singulares ou coletivas que disponibilizem regularmente ao público, através de redes de comunicações eletrónicas, conteúdos submetidos a tratamento editorial e organizados como um todo coerente" também se encontram sob o poder de supervisão da ERC. No entanto, tendo em conta que a grande ameaça da desinformação origina principalmente das grandes plataformas digitais, é consensual que estas não disponibilizam ao público "conteúdos submetidos a tratamento editorial e organizados como um todo coerente"[121].

Assim, a execução e aplicação, sem mais, deste novo vetor de atuação iria significar para a ERC uma atuação fora das suas atribuições, em clara violação dos seus Estatutos, em particular do artigo 5.º.

Em resultado de todas estas observações destacadas pela Provedoria de Justiça, o Governo Português procedeu à alteração da Lei n.º 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital, revogando os n.ºs 2 a 6 do artigo 6.º.[122]

---

[120] AMARAL, Maria Lúcia, parágrafos 64 e 66.
[121] AMARAL, Maria Lúcia, parágrafo 76; Lei n.º 53/2005 de 8 de novembro, artigo 6.º.
[122] Diário da República, 11 de agosto de 2022, n.º 155.

3. O Papel das Estruturas Europeias na Coordenação de Respostas ao Fenómeno

A disseminação de desinformação constitui uma realidade que se insere numa extensa gama de «ameaças híbridas»[123].[124] As campanhas de desinformação, por vezes dificilmente detetáveis e atribuíveis, são orquestradas com o intuito de influenciar, polarizar e minar o debate público característico dos regimes democráticos, e constituem uma das mais recentes ameaças às instituições democráticas e aos valores nos quais se alicerça o projeto europeu.[125]

Estes atos tumultuadores procuram dificultar todo o processo de tomada de decisões, semeando a confusão nas sociedades, agudizando questões onde é já evidente um certo grau de divisão social e minando a confiança nas autoridades públicas.[126]

O conceito de "ameaça híbrida", dada a ambígua natureza do seu objeto, encontra-se em constante mutação e, segundo o Quadro comum em matéria de luta contra as ameaças híbridas [JOIN (2016) 18 final], consiste na "combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada".[127] O referido quadro comum aprofunda um pouco mais esta definição indicando dois aspetos[128] que caracterizam e diferenciam as ameaças híbridas: por um lado, a "exploração das vulnerabilidades do alvo" e, por outro, a "criação de ambiguidade para entravar o processo de tomada de decisões".

---

[123] Os métodos utilizados nas atividades híbridas são múltiplos e diversificados e verificam-se, particularmente, ao nível de ciberataques a sistemas de informação de infraestruturas críticas, tais como redes de energia, redes de transporte e cadeias de abastecimento, estruturas europeias de segurança sanitária, proteção do ambiente e da segurança dos alimentos, sistemas financeiros, ou, até mesmo, das infraestruturas espaciais.

[124] Comissão Europeia, *Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, JOIN(2016) 18 final, 2016, p. 2

[125] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia* e *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 1; VAN RAEMDONCK, Nathalie; MEYER, Trisha, p. 12.; Sobre este assunto, Cfr. também Comissão Europeia, *Mapeamento das medidas relacionadas com o reforço da resiliência e a luta contra as ameaças híbridas*, SWD(2020) 152 final, 2020.

[126] Comissão Europeia, *Relatório conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, JOIN(2017) 30 final, 2017, p. 19.

[127] *Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, p. 2; Conselho da União Europeia, *Conclusões do Conselho sobre o reforço da resiliência e a luta contra as ameaças híbridas, incluindo a desinformação no contexto da pandemia de COVID-19*, 2020, p. 2.

[128] *Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, p. 2.

As campanhas de desinformação, dados os seus princípios motivadores e potenciais danos, enquadram-se, assim, na noção de "vetores de ameaças híbridas"[129], particularmente quando as mesmas são orquestradas por países terceiros[130].

O combate a ameaças desta natureza é, primeiramente, uma questão de segurança e defesa nacionais de cada Estado-Membro. No entanto, e tendo em conta que as vulnerabilidades dos Estados-Membros a estas ameaças são comuns, não conhecem fronteiras e contendem com um conjunto de competências de atuação que, por vezes, se encontram divididas entre os Estados-Membros e a União[131], uma resposta europeia coletiva, estruturada, e complementada por todos os instrumentos, políticas[132] e programas que são proporcionados a nível europeu[133], deve representar a opção a ser priorizada. Posto isto, as ações a serem implementadas requerem uma resposta globalizante comum, assente na capacidade de vigilância, reconhecimento e prevenção da ameaça, que retire partido máximo das vantagens que uma cooperação estreita entre todos os intervenientes possibilita.[134]

Esta resposta encontra-se, por efeito, dependente do estabelecimento de vetores de auxílio entre os governos dos Estados-Membros, as Instituições Europeias e todos os parceiros internacionais relevantes, de modo a atingir-se um grau de coparticipação caracterizado por um expediente agregado e transnacional que atua em múltiplas frentes.[135]

A atuação de autoridades nacionais e internacionais a diversos níveis (proteção de dados, comunicação estratégica, cibersegurança e ameaças híbridas, serviços de inteligência, entidades reguladoras, órgãos de polícia criminal e órgãos eleitorais – sem esquecer o *input* vital produzido pelo setor privado e pela própria sociedade civil –)[136] é crucial para a construção de uma resposta ativa e dinâmica que verdadeiramente contribui para reforçar a resiliência das sociedades e suas infraestruturas nevrálgicas.[137]

Daqui procede um princípio fundamental orientador de toda a política de combate às ameaças híbridas na União, que reside na ideia de que uma resposta aos desafios futuros deve, obrigatoriamente, ser articulada a nível europeu, pois nenhum Estado-Membro conseguirá enfrentar,

---

[129] *Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, p. 2; VAN RAEMDONCK, Nathalie; MEYER, Trisha, p. 3.

[130] *Plano de Ação contra a Desinformação*, p. 3; BRADSHAW, Samantha; HOWARD, Philip N., *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford Internet Institute, 2019, pp. 1-3.

[131] *Comunicação: Garantir eleições europeias livres e justas*, p. 7

[132] *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 3

[133] *Relatório conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 20.

[134] Sobre este tema, Cfr. também Comissão Europeia, *Relatório sobre a execução do Plano de Ação contra a Desinformação*, JOIN(2019) 12 final, 2019, em especial o capítulo "Rumo a uma abordagem coordenada para combater a desinformação".

[135] *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 7.

[136] *Plano de Ação contra a Desinformação*, pp. 5 e 6.

[137] *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, pp. 3 e 8.

isoladamente, fenómenos que, pela sua natureza, extravasam as suas próprias fronteiras. Esta ideia é também enfatizada no «Relatório relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia», onde é referido que "a cooperação em matéria de defesa e segurança não é uma opção; é uma necessidade, para permitir à Europa proteger os seus cidadãos".[138]

O primeiro grande passo a ser dado nesta esfera prende-se, então, com a necessidade de se identificarem os domínios mais expostos a ataques híbridos informacionais e os respetivos sinais indiciadores de tais atividades, de forma a tornar mais eficaz o funcionamento dos dispositivos de deteção e avaliação precoce de riscos, absolutamente indispensáveis para a modelação de respostas coordenadas e eficazes.[139]

Nesta esteira, e dado o caráter tendencialmente obscuro associado a algumas práticas híbridas no campo da desinformação, o eficiente emprego de todos os instrumentos e conjuntos de dados disponíveis – por profissionais dotados do conhecimento especializado necessário – é importantíssimo para, a título de exemplo, estabelecer elementos de conexão entre eventos alegadamente desconectados, conexões essas que são normalmente desencadeadoras de uma atuação mais adequada.[140]

Para que o grau de cooperação que até então tem sido destacado se consubstancie, torna-se importante a criação de centros especializados no intercâmbio de conhecimento desta índole[141] e, neste âmbito, serão apresentados de seguida algumas das principais estruturas existentes que se dedicam total ou parcialmente ao combate à disseminação de desinformação.

3.1 O sistema de alerta rápido

Em 2018, o Plano de Ação contra a Desinformação introduziu um meio de cooperação europeu para o combate à desinformação: o sistema de alerta rápido (SAR).

A participação nesta plataforma é dedicada, por um lado, às Instituições Europeias e, por outro, aos Estados-Membros – e seus órgãos internos que, para o efeito, devem nomear uma figura de

---

[138] *Relatório conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, p. 3.

[139] *Comunicação conjunta: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 5; *Relatório conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, p. 20; *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia,* p. 3.

[140] *Comunicação conjunta: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 5

[141] *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, pp. 2 e 7.

contacto, encarregue de comunicar e trocar informações com os restantes participantes, sempre que tal se justifique.[142]

A criação deste mecanismo é essencial para, em primeiro lugar, promover, entre as mais altas instâncias, uma ponte de diálogo e de avaliação de tendências «(des)informativas» no espaço europeu e, em segundo, para a estruturação de respostas coletivas ao fenómeno – prontamente auxiliadas pelos *inputs* fornecidos por investigadores, verificadores de factos independentes e plataformas digitais –, permitindo o rápido alerta das entidades mais relevantes (sejam elas órgãos eleitorais, serviços de informação, autoridades de proteção de dados, gabinetes de crise, entre outros organismos nacionais e europeus)[143] em caso de campanhas de desinformação particularmente gravosas.

As primeiras horas após o início de uma campanha de desinformação são fundamentais para a identificação e neutralização da ameaça e, nesse sentido, esta plataforma aposta numa característica única do seu funcionamento e crítica neste quesito: a operação em tempo-real e sem interrupções, que permitirá uma atuação rápida e robusta sobre qualquer situação de eventual perigo, por meio de uma eficiente e atempada avaliação dos seus possíveis impactos e das respostas que se afigurem adequadas.[144]

Na prática, o funcionamento do mecanismo de alerta rápido assenta num trabalho de avaliação exercido pelo Serviço Europeu para a Ação Externa (SEAE) e pela Comissão que, com base nas contribuições recolhidas, poderão desencadear a execução de um conjunto de atuações, desde chamadas de atenção a plataformas digitais para situações de desinformação de maior gravidade, à direta divulgação de algum anúncio público, entre outros. Neste domínio, a capacidade das plataformas digitais conseguirem transmitir informações a um grande número de pessoas rapidamente representa um aspeto muito relevante no domínio do SAR, dado que este alcance e imediatismo são importantíssimos na transmissão de explicações ou esclarecimentos sobre qualquer ocorrência.[145]

A final, será igualmente de se insistir na ideia da coordenação e cooperação entre as Instituições Europeias e Estados-Membros com as organizações e parceiros internacionais (G7 e OTAN, essencialmente), uma vez que o eficiente e oportuno intercâmbio de informações com estruturas que atuam à escala global apenas complementa e otimiza a formulação da resposta mais efetiva.[146]

---

[142] *Plano de Ação contra a Desinformação*, p. 7.
[143] *Idem.*
[144] *Idem.*
[145] *Plano de Ação contra a Desinformação*, p. 9.
[146] *Plano de Ação contra a Desinformação*, p. 8.

3.2 Observatório Europeu dos Meios de Comunicação (EDMO) e o Grupo de Reguladores Europeus para os Serviços de Comunicação Social Audiovisual (ERGA)

3.2.1 EDMO

Em 2018, o Grupo de Peritos em notícias falsas e na desinformação em linha alertava para a necessidade de criação de uma rede independente de centros europeus que promovesse uma estratégia europeia baseada nas múltiplas ramificações que o problema apresentava, insistindo, para o efeito, na introdução de um espaço onde todos os intervenientes relevantes possam reunir, interagir e debater sobre a temática.[147]

Dois anos depois, em junho de 2020, surge o EDMO, uma estrutura central para a resposta europeia no combate à desinformação[148]. Esta plataforma independente funciona como um centro dedicado ao estudo e análise do fenómeno da desinformação, reunindo, para o efeito, profissionais da área da literacia mediática, investigadores académicos, verificadores de factos, as plataformas digitais e órgãos de comunicação social. O EDMO funciona com base em 14 centros nacionais e multinacionais espalhados por toda a Europa, sendo que o centro que Portugal integra se chama IBERIFIER e funciona em articulação com Espanha.

Este observatório europeu atua em cinco grandes áreas: verificação de factos, investigação do fenómeno, sensibilização pública para a problemática, promoção de um enquadramento de acesso aos dados das plataformas e, por fim, o apoio às autoridades.

No âmbito da primeira grande área, o EDMO procura, sucintamente, organizar e conectar as principais organizações de verificação de factos a nível europeu, promovendo a organização conjunta de atividades, o intercâmbio de melhores práticas e a criação de programas de aprendizagem e instrução.[149]

Como sabemos, a análise contínua de todos os aspetos relacionados com a desinformação (as dimensões que pode assumir, os seus atores, os mecanismos que contribuem para a sua amplificação no meio digital, as fontes, as técnicas e os instrumentos utilizados, os seus impactos, etc.) é

[147] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 22.
[148] Tribunal de Contas Europeu, *Special Report: Disinformation affecting the EU: tackled but not tamed*, Serviço das Publicações da União Europeia, 2021, p. 41.
[149] Comissão Europeia, *Observatório Europeu dos Meios de Comunicação Digitais (EDMO)*, 2023. Disponível em: <https://digital-strategy.ec.europa.eu/pt/policies/european-digital-media-observatory> [02/10/2023].

fundamental para a criação de uma estratégia eficaz de combate. Nesse sentido, o Observatório procura, na sua segunda grande área, auxiliar e estruturar os programas de investigação sobre o fenómeno que se encontram a ser desenvolvidos a nível europeu, agilizando e otimizando todo esse processo com o apoio de um repositório de artigos científicos sobre a problemática.[150]

No domínio da terceira grande área identificada, o EDMO assume-se como um núcleo que pretende sensibilizar o grande público para os perigos da desinformação, levando a cabo tal propósito por meio da partilha de conhecimentos adquiridos no domínio sua atividade e apoiando projetos e iniciativas no campo da literacia mediática digital.[151]

No âmbito da quarta área de atuação, esta estrutura pretende atuar como um catalisador para a criação de um enquadramento legal mais justo e previsível de acesso aos dados das grandes plataformas digitais.[152] Como veremos adiante, a questão do acesso aos dados é um tema preocupante neste domínio e, sabendo disso, o EDMO pretende harmonizar os dois lados desta situação, de forma a permitir uma atividade de investigação mais transparente que respeita e promove os interesses de todas as partes envolvidas.

Por fim, o EDMO também pretende apoiar a atividade das Instituições Europeias e dos Estados-Membros no âmbito da monitorização das normas constantes de determinados instrumentos normativos relevantes para a questão, como o Regulamento Serviços Digitais.[153]

3.2.2 ERGA

O ERGA, por seu turno, representa uma estrutura europeia constituída pelas autoridades nacionais reguladoras no campo da comunicação social audiovisual[154], entre as quais figura naturalmente a ERC.

À semelhança do EDMO, o ERGA promove o contacto e a troca de boas práticas entre todas as entidades reguladoras adstritas a este domínio[155] e aconselha a Comissão Europeia nas questões relacionadas com a concretização da Diretiva Serviços de Comunicação Social Audiovisual e noutras

[150] Comissão Europeia, *Observatório Europeu dos Meios de Comunicação Digitais (EDMO)*, 2023.
[151] *Idem.*
[152] *Idem.*
[153] *Idem.*
[154] ERGA, *Press release: ERGA and EDMO meet to further strengthen cooperation in meeting disinformation challenges*, 2022, p. 2.
[155] *Press release: ERGA and EDMO meet to further strengthen cooperation in meeting disinformation challenges*, p. 2.

questões, também sob a alçada da Comissão, que estejam relacionadas com o mundo dos órgãos de comunicação social europeus.[156]

Os principais pontos de atuação do ERGA no domínio da manipulação de informação encontram-se relacionados com atividades desenvolvidas no campo do combate à desinformação, no «fortalecimento da democracia no meio digital» e na pluralidade dos media.[157]

3.3 Ameaças híbridas: a Célula de Fusão e o Centro Europeu de Excelência

3.3.1 Célula de Fusão da UE contra as ameaças híbridas

A Célula de Fusão da UE contra as ameaças híbridas – instituída em 2016 na esfera do Centro de Análise de Informações da UE (INTCEN) do SEAE – funciona como um centro de receção[158], partilha e análise de informações relacionadas com a problemática das ameaças híbridas[159] e atua como um auxiliar para a idealização, a nível europeu, de possíveis respostas a incidentes desta natureza[160].

De modo a viabilizar um nível de participação mais sólido entre os Estados-Membros, foi criada, em 2017, uma rede de pontos de contacto nacionais, que se reúne bianualmente e funciona como um ponto de intercâmbio de melhores práticas e discussão de assuntos de relevância para a questão. Nesta circunstância, os pontos de contacto nacionais atuam como vetores agregadores dos vários órgãos nacionais relevantes para a lide, de modo a facilitar e possibilitar a construção de uma resposta mais harmonizadora por toda a Europa.[161]

O cabal prosseguimento das atribuições da Célula encontra-se dependente de um vasto conjunto de causas, sendo que uma das principais é, precisamente, a aposta num reforço generalizado das capacidades de resiliência das principais Instituições Europeias, normalmente alvos de atividades de informação hostis.[162]

---

[156] ERGA, *About ERGA*, (não datado). Disponível em: <https://erga-online.eu/?page_id=7> [29/09/2023].
[157] ERGA, *Work Programme and current activities*, (não datado). Disponível em: <https://erga-online.eu/?page_id=12> [29/09/2023].
[158] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 4.
[159] Comissão Europeia, *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018,* JOIN(2018) 14 final, 2018, p. 2.
[160] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 4.
[161] Comissão Europeia, *Relatório sobre a aplicação do Quadro Comum de 2016 sobre a luta contra as ameaças híbridas e da Comunicação Conjunta de 2018 sobre o aumento da resiliência e o reforço das capacidades para enfrentar as ameaças híbridas*, SWD(2019) 200 final, 2019, p. 2; *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, pp. 2, 3 e 19.
[162] *Comunicação conjunta: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 11.

Posto isto, a formação e sensibilização do *staff* dessas mesmas instituições representa uma componente essencial da sua atuação e incide, justamente, para possibilitar a correta interpretação de manifestações precoces de eventuais ameaças híbridas. O alargamento dos conhecimentos nesta área é, por isso, importantíssimo para a conceção de respostas mais atempadas a ocorrências desta natureza, decisivas no contexto do controlo e mitigação de danos.[163]

3.3.2 O Centro Europeu de Excelência para o Combate às Ameaças Híbridas

A resposta europeia ao fenómeno da desinformação também reúne esforços juntos do Centro Europeu de Excelência para o Combate às Ameaças Híbridas. Este Centro de Excelência – uma organização internacional autónoma liderada pela Finlândia, criada em abril de 2017 e atualmente composta por 33 Estados participantes[164], entre os quais Estados-Membros e aliados da OTAN – é responsável pelo desenvolvimento de atividades de investigação sobre a temática e promove, enquanto núcleo internacional, a partilha de conhecimento estratégico e de boas práticas entre os seus vários participantes[165], como também a realização de exercícios conjuntos[166], em vista à preparação de todo o processo de *decision-making* na eventualidade da verificação de uma ameaça híbrida de bastante impacto. Todo este processo de tomada de decisão alicerça-se, assim, num estado de prontidão constante, ininterruptamente disponível para dar respostas, previamente testadas, aos momentos de crise.[167]

A investigação desenvolvida no Centro de Excelência procura, deste modo, auxiliar a formulação e uniformização das políticas adotadas pelos seus participantes nesta questão, informando as Instituições Europeias e a OTAN de todas as especificidades a considerar nos seus processos de deliberação político-legislativa[168]. Neste seguimento, o Centro de Excelência procura, igualmente, incentivar o desenvolvimento de novos mecanismos tecnológicos – também eles elaborados no seio do setor privado – com o propósito de aumentar a resiliência dos Estados participantes nas áreas que apresentem maiores níveis de vulnerabilidade[169], nomeadamente na área do reforço e inovação dos instrumentos de deteção de campanhas de desinformação.

---

[163] *Comunicação conjunta: Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*; *Comunicação conjunta: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 5.
[164] O Centro Europeu de Excelência é aberto à participação de Estados-Membros da União e aliados da OTAN.
[165] *Plano de Ação contra a Desinformação*, p. 2.
[166] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 6.
[167] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 18; *Comunicação: Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, p. 8.
[168] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 18.
[169] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 20.

O Centro, desde a sua incepção, já publicou inúmeros documentos de análise sobre fenómenos híbridos, tornou-se sede de diversas reuniões destinadas à conceção de um entendimento coletivo sobre os mesmos e atua, como já vimos, com o primordial intuito de fomentar a partilha de mais e melhores práticas e métodos para a arquitetação de respostas adequadas e coordenadas ao fenómeno.[170]

A promoção de laços de parceria e colaboração no seio da Célula

A cooperação internacional é chave no combate às ameaças híbridas e, nessa medida, todo o trabalho desenvolvido nesta sede terá, obrigatoriamente, de ser sempre realizado em estreita conexão com outras estruturas.

Para o efeito, as atividades do Centro de Excelência são promovidas, a título exemplificativo, em forte conexão e complementaridade com a atuação da Célula de Fusão, também ela já responsável pela formulação de respostas funcionais e eficazes para os problemas levantados pelas atividades híbridas, como foi observado.[171] O grau de ligação entre estas duas entidades é profundamente simbiótico e concretiza-se em várias camadas, como na realização sincrónica de operações e *workshops*, mas também de mesas-redondas de discussão sobre os métodos mais apropriados para enfrentar estas ameaças.[172]

Para além disso, a reação europeia a esta problemática pode – e deve – ultrapassar a própria dimensão da União e procurar – ou aprofundar – o estabelecimento de laços de colaboração com outros países e organizações destacadas nesta esteira, no âmbito da OTAN[173], da OSCE ou da ONU, a título de exemplo. A este propósito, será naturalmente de mencionar as vantagens trazidas pelo desdobramento de pontos de cooperação com determinadas estruturas da OTAN[174], nomeadamente a sua Célula de Análise de Ameaças Híbridas, ou mesmo com os demais centros de excelência presentes na União.[175]

---

[170] *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, pp. 2 e 13.
[171] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 6; *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 4.
[172] *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, p. 2.
[173] A título exemplificativo, na Declaração Conjunta UE-OTAN de 2016, identifica-se o combate às ameaças híbridas como um dos sete domínios onde a colaboração entre a União e a Aliança Militar deve ser fortalecida.
[174] A resposta da UE e dos aliados da OTAN às ameaças híbridas é testada pelo meio da realização de exercícios conjuntos, que possibilitam uma análise da eficácia das respostas implementadas. Cfr. *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, p. 13.
[175] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, pp. 6 e 19.

É de salientar, por fim, que a cooperação, proporcionada pelo Centro de Excelência, entre Estados-Membros e os restantes países da OTAN, pode configurar uma espécie de ponto de partida para uma "Coligação Internacional"[176] contra o fenómeno da desinformação, onde se esboçam estratégias de ataque e defesa contra uma problemática que se renova drasticamente de dia para dia.

Países terceiros, que prossigam os mesmos interesses, e agentes privados cuja influência se apresente incontornável para a busca de soluções[177] devem igualmente ser englobados neste esforço coletivo, uma vez que tal fusão possibilita a chegada a conclusões – a respeito de temáticas fraturantes (como os limites à liberdade de expressão no mundo digital e as estratégias para a promoção de um ambiente mundial em linha mais seguro, previsível e de confiança) – mais abrangentes, apropriadas e respeitadoras, a múltiplas latitudes, dos direitos humanos.[178]

3.4 Os Grupos de Trabalho para a Comunicação Estratégica

O combate à desinformação na UE é também apoiado pela criação dos grupos de trabalho *StratCom* – formados no seio do SEAE – cujos mandatos preveem, como principais objetivos, a prevenção e o combate mais eficiente a casos de desinformação e a transmissão mais clara de informações, tanto sobre a UE e suas Instituições, como sobre as suas políticas e ideais, nas regiões geográficas que se encontrem abrangidas pelas respetivas missões.[179]

As missões desenvolvidas por estas *task-forces* no âmbito da comunicação estratégica (STRATegic COMmunication) devem ser perspetivadas como sendo um complemento ao trabalho já realizado pelos Estados-Membros e outras Instituições Europeias neste domínio e incidem, como se constatou, no contexto da previsão, acompanhamento e neutralização de situações de propagação de desinformação, mas, também, no âmbito da promoção de ações de sensibilização acerca do impacto das mesmas[180], particularmente com o recurso a políticas de literacia digital[181].

Por seu turno, as sistemáticas campanhas de desinformação de origem russa – com particular incidência nos países da Vizinhança Oriental e capazes de causar profundas consequências no já frágil

[176] POLYAKOVA, Alina; FRIED, Daniel, pp. 13 e 14.
[177] POLYAKOVA, Alina; FRIED, Daniel, pp. 13 e 14.
[178] POLYAKOVA, Alina; FRIED, Daniel, p. 3; Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 2, 5 e 14.
[179] Sobre este assunto, Cfr. também PAMMENT, James, "The EU's Role in Fighting Disinformation: Taking Back the Initiative", *in Future Threats, Future Solutions*, Carnegie Endowment for International Peace – Publications Department, 2020.
[180] Comissão Europeia, *Plano de Ação para a Comunicação Estratégica*, 2015, p. 3.
[181] *Plano de Ação para a Comunicação Estratégica*, p. 4.

ambiente político, económico e de segurança dessas regiões – forçaram a União a adotar medidas no campo da comunicação estratégica.

Para além das tensões que se pretendem criar nessas regiões, a semeação de instabilidade e sentimentos eurocéticos em regiões tão próximas ao espaço europeu acaba por inevitavelmente colocar problemas relacionados com a segurança da própria União e, diante disso, as Instituições Europeias não poderiam simplesmente ficar de braços cruzados. Nesta senda, foi criada a primeira equipa de comunicação estratégica, a *East StratCom*.[182]

Os resultados positivos que se verificaram ao longo dos anos na sua atividade de supervisão permitiram[183] que a mesma também se estendesse à área territorial dos Balcãs Ocidentais e dos países vizinhos do Sul.[184] Assim, existem atualmente três grupos de trabalho formados, cada um com a sua respetiva incidência geográfica: o grupo de trabalho *East StratCom*, criado em março de 2015 na sequência de uma reunião do Conselho Europeu; o grupo de trabalho para os Balcãs Ocidentais, fruto das Conclusões do Conselho sobre o alargamento e o Processo de Estabilização e de Associação, também em 2015; e, por fim, o grupo de trabalho Sul, resultante das Conclusões do Conselho sobre a luta contra o terrorismo, em 2017, e que atua junto do Mundo Árabe.[185]

A comunicação estratégica e atos de diplomacia pública

Os esforços da capacidade operacional da *task-force East StratCom* – a mais relevante para a questão da desinformação – é direcionada, principalmente, para um domínio de apoio às delegações europeias inseridas nos países que compõem o grupo da Parceria Oriental[186] (Arménia, Azerbaijão, Bielorrússia, Geórgia, República da Moldova e Ucrânia[187]), mas, também, na Rússia. Ainda assim, algum do seu trabalho é também prosseguido em algumas regiões da Ásia Central.[188]

Muito do trabalho desenvolvido nesta sede é feito na forma de atos de diplomacia pública, com o apoio das embaixadas europeias, e que é orientado para o desmascaramento de operações de informação manipuladoras e/ou descontextualizadas. Pretende-se, assim, que a divulgação clara e objetiva de determinadas mensagens junto das massas populacionais contribua, por um lado, para a

---

[182] *Plano de Ação para a Comunicação Estratégica*, p. 1.
[183] *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, p. 2.
[184] EUvsDisinfo, *About: Our Team*. Disponível em: <https://euvsdisinfo.eu/about/> [16/06/2023].
[185] *Plano de Ação contra a Desinformação*, p. 5.
[186] Esta parceria foi reconhecida oficialmente no âmbito da Declaração adotada na Cimeira da Parceria Oriental, em Riga, no ano de 2015.
[187] Serviço Europeu de Ação Externa, *Countering Disinformation: Questions and Answers about the East StratCom Task Force*, 2021. Disponível em: <https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232> [09/05/2023].
[188] *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, p. 2.

compreensão mais exata da atividade e dos interesses da União nessas regiões e, por outro, para a efetiva responsabilização dos agentes que se encontram por detrás das atividades de manipulação.[189]

O combate a grandes campanhas de desinformação demanda, assim, uma capacidade de resposta firme e consistente, baseada numa robusta política de comunicação estratégica alicerçada numa clara exposição da verdade[190]. A ampla difusão de refutações sobre conteúdo manipulador e uma aposta na sensibilização da população europeia e dos países vizinhos para este fenómeno constitui, deste modo, uma das principais vias para a construção de sociedades resilientes e cientes da problemática e seus perigos.[191] Assim, ainda que atuação das *task-forces* se foque numa realidade extraeuropeia, certos elementos destas mensagens merecem igualmente respaldo junto das populações europeias, que devem, de igual modo, apoiar a denúncia de falsidades e a difusão dos factos.[192]

Para que a exposição da verdade dos factos seja profícua, é crucial a aposta num método de comunicação claro, eficaz e atento às particularidades das populações destinatárias, de forma que a mensagem veiculada seja mais relacionável e facilmente digerida por aquelas.

A este propósito, aquando da implementação destas missões, foi deixado bem claro que a comunicação dos planos e objetivos europeus para as regiões não se devia focar numa exaustiva publicitação dos programas políticos previstos para as mesmas, mas antes no reforço, num formato claro, do princípio-base de que as reformas político-económicas encetadas pela União nas regiões da parceria Oriental iriam, a médio-longo prazo, suscetibilizar alterações favoráveis para o quotidiano das populações. Do mesmo modo, o teor destas mensagens deve espelhar claramente o compromisso da União com os seus valores mais fundamentais e distintivos, como a democracia, o respeito pelo Estado de Direito, a proteção das minorias e dos direitos à liberdade de expressão e de imprensa, bem como a luta contra a corrupção.[193]

O pleno desenvolvimento desta e de quaisquer políticas de comunicação estratégica apenas é alcançado em contacto com os vários *stakeholders*, desde instâncias governativas nos países-alvo, a jornalistas e outros representantes dos meios de comunicação regionais[194], uma vez que a promoção de

---

[189] POLYAKOVA, Alina; FRIED, Daniel, pp. 9 e 10.
[190] *Plano de Ação contra a Desinformação*, p. 8.
[191] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 5.
[192] *Plano de Ação contra a Desinformação*, p. 8; A este propósito será de mencionar o sítio na internet EUvsDisinfo (que será desenvolvido um pouco mais adiante), que constitui um portal para uma compreensão mais incrementada deste fenómeno nos países vizinhos à União.
[193] *Plano de Ação para a Comunicação Estratégica*, p. 2.
[194] *Plano de Ação para a Comunicação Estratégica*, p. 3.

uma narrativa mais apelativa e, simultaneamente, condicente com a realidade, apenas penetra nas camadas populacionais com o apoio logístico das entidades locais.

Para além disso, todas as ações enquadradas no âmbito da política de comunicação estratégica devem naturalmente incidir sobre as principais fontes a que os cidadãos dos ditos países-alvo recorrem para se informarem, entre as quais, os meios de comunicação tradicionais, mas cada vez mais as redes sociais, responsáveis por uma grande fatia do ecossistema noticioso atual.[195]

É por esta razão que se afirma taxativamente que a prossecução dos objetivos constantes dos mandatos das *task-forces* é especialmente conseguida por meio de um fortalecimento do ecossistema mediático[196] nas áreas geográficas referenciadas.

Para o efeito, deve ser conduzida uma aposta no reforço dos apoios aos meios de comunicação locais independentes e na promoção de intercâmbios de melhores práticas, garantindo-se a devida assistência – sempre nas suas línguas locais (como o russo) – a jornalistas e fontes noticiosas que primam pelo rigor e pela imparcialidade, de forma a atender às necessidades destes e dos mais variados setores demográficos alvo da sua atividade.[197]

A *East Stratcom* desenvolve, igualmente, programas de treino para o staff presente nos países da Parceria Oriental, de modo que estes possam retirar máximo partido dos recursos proporcionados.[198]

O trabalho da *task-force,* no âmbito do combate e sensibilização das sociedades para a ameaça, também se materializa no seu sítio Web EUvsDisinfo[199], dotado de uma base dados em permanente atualização que, desde 2015, "identifica, compila e expõe casos de desinformação com origem em meios de comunicação pró-Kremlin, que estão espalhados pela UE e em países da Parceria Oriental"[200]. Como foi referido anteriormente, ainda que as atividades desta *task-force* se fixem num conjunto países vizinhos, iniciativas como o sítio EUvsDisinfo são extremamente pertinentes e interessantes para qualquer cidadão europeu, que pode, desta forma, desvendar a verdade por detrás das campanhas de desinformação e manipulação.

Um outro aspeto significativo do trabalho desenvolvido pelas *task-forces* reside no facto de este ser reiteradamente realizado em estreito contacto com os Estados-Membros, a Célula de Fusão, o Centro de Excelência e as próprias estruturas da OTAN. Este grau de coordenação e cooperação

---

[195] *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 5.
[196] *Plano de Ação para a Comunicação Estratégica*, p. 2.
[197] *Plano de Ação para a Comunicação Estratégica*, pp. 2 e 4.
[198] *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, p. 2.
[199] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 5.
[200] EUvsDisinfo, *About: Our Team*. Disponível em: <https://euvsdisinfo.eu/about/> [16/06/2023].

permite avanços relevantes no campo da partilha de informações ou, a título mais exemplificativo e concreto, no âmbito da realização de seminários para a formação de jornalistas.[201]

[201] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 3.

4. A Política Europeia de Combate à Disseminação de Desinformação

O estudo e a investigação que será discorrido adiante pretende focar nas atuais e futuras propostas que buscam a promoção de um debate público democrático livre e transparente a todos os níveis, onde a factualidade constitui princípio, meio e fim.

Toda e qualquer política desenvolvida em vista à promoção de uma «sociedade informada» terá sempre o máximo respeito pelos mais importantes direitos fundamentais em questão.[202] Nesse sentido, a via de atuação que se bate por um equilíbrio perfeito entre o respeito pelos valores europeus e a luta por um ecossistema informativo mais seguro e confiável será sempre a que produzirá os melhores resultados.

Assim, o desenvolvimento da política de combate à desinformação será sempre enquadrado no âmbito da Carta dos Direitos Fundamentais da União Europeia, da Convenção Europeia dos Direitos Humanos e, ainda, no contexto de todas as diretivas e regulamentos que tratem da temática das ameaças híbridas.

A resposta europeia neste domínio é algo extensa e reflete-se, principalmente, num conjunto de instrumentos normativos nos quais a temática é especialmente acionada. O Regulamento Serviços Digitais (RSD) e a futura proposta de Regulamento sobre a transparência e o direcionamento da propaganda política são os principais instrumentos de caráter regulatório, ao passo que o Código de Conduta Reforçado em matéria de Desinformação de 2022 representa, tal como o seu nome já deixa adivinhar, o instrumento de autorregulação de maior relevância nesta esfera.

Nos próximos capítulos será, então, desvendado o caminho que a União Europeia se encontra atualmente a desbravar nestas temáticas.

[202] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 2 e 3.

4.1 Regulamento dos Serviços Digitais

4.1.1 Os objetivos

O RSD constitui um dos mais recentes esforços a nível europeu que se propõe a suplantar uma miríade de problemas que se colocam no mundo em linha. A redação deste diploma constitui um enorme passo no combate à desinformação por constituir o primeiro instrumento legislativo da União, com aplicação vinculativa imediata a todos os Estados-Membros e sem necessidade de atos de transposição para as ordens jurídicas nacionais (não obstante a necessidade de desenvolvimento de certos atos de concretização das políticas nele consagradas, como, por exemplo, na matéria da imposição de medidas sancionatórias[203]), dado que assume a forma de Regulamento.[204]

As políticas legislativas detalhadas no RSD encontram-se ligadas à prossecução de diversos objetivos centrais, entre os quais a verificação de melhorias no funcionamento do mercado interno[205], a formação de um ambiente em linha mais sólido, previsível e fidedigno, no qual os direitos fundamentais consagrados na CDFUE, como a liberdade de expressão e de informação e a liberdade e o pluralismo dos órgãos de comunicação social, se encontram plenamente acautelados[206].

A este respeito, será relevante desde já mencionar algumas das preocupações que contribuíram para a redação deste instrumento legislativo e que se prendiam com a verificação de um fenómeno de multiplicação de leis nacionais de combate aos fenómenos contemplados pelo RSD, comprometedoras do amplo e harmonioso funcionamento do mercado interno e que levantam questões relacionadas com a segurança jurídica em todo o espaço europeu[207].

A Comissão, neste aspeto, salienta que as metas e os objetivos que o RSD se propõe a prosseguir não são satisfatoriamente alcançáveis pelos Estados-Membros a título individual e circunscrito[208], uma vez que estes, de forma isolada, não possuem – como se constatou – os meios adequados para assegurarem os graus de uniformização e colaboração essenciais para a prossecução dos objetivos almejados[209], mais exequíveis num panorama de consenso a nível europeu[210].

---

[203] Comissão Europeia, 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 dos Serviços Digitais), considerando 117.
[204] Sobre este tema, Cfr. PEREIRA, Miguel, "Taming Europe's digital landscape? Brief notes on the proposal for a Digital Services Act", *in UNIO – EU Law Journal*, Volume 7, n.º 2, 2021.
[205] RSD, considerandos 40 e 155.
[206] RSD, considerandos 3 e 153 e artigo 1.º, n.º 1.
[207] RSD, considerandos 2 e 4.
[208] RSD, considerando 155.
[209] *Idem.*
[210] *Idem.*

Paralelamente, e tendo em conta que o escopo de atuação do RSD atinge de forma particular as grandes companhias tecnológicas, o Regulamento reconhece simultaneamente a importância de promover e proteger a inovação tecnológica e salvaguardar a liberdade de negócio e empresa.[211]

Por fim, este Regulamento fornece igualmente definições importantes para o fenómeno que se analisa nesta dissertação e para uma compreensão mais delimitada do alcance das medidas nele previstas.

A noção de «disseminação» ou «difusão ao público», central para a temática da desinformação e para as obrigações dispostas no Regulamento, é definida como sendo a "disponibilização de informação a um número potencialmente ilimitado de pessoas", informação essa que é, por sua vez, "facilmente acessível aos destinatários do serviço em geral, sem que seja necessária qualquer outra ação por parte do destinatário do serviço que presta a informação, independentemente de essas pessoas acederem efetivamente à informação em questão".[212]

Neste âmbito são feitas, ainda, algumas salvaguardas, aos casos de envio de e-mails ou mensagens pessoais privadas que, pela sua natureza, não se destinam a um "número potencialmente ilimitado de pessoas"[213]. No entanto, no texto legal subsistem, de igual modo, algumas exceções a estas salvaguardas, relacionadas com a realidade dos grupos públicos e canais abertos, que possibilitam a "disponibilização de informações a um número potencialmente ilimitado de destinatários, não determinado pelo remetente da comunicação"[214].

4.1.2 Os serviços intermediários

De forma sucinta, o RSD aplica-se a prestadores de serviços intermediários de «simples transporte», de «armazenagem temporária» e de «alojamento virtual»[215], sendo que é nesta última categoria de serviços que encontramos as principais plataformas digitais, como as redes sociais ou as plataformas que possibilitam a celebração de contratos à distância com comerciantes, a título de exemplo[216].

As principais obrigações estabelecidas pelo Regulamento estão ligadas a exigências que perpassam diversos domínios e nos próximos parágrafos será feita uma menção aos principais pontos

---

[211] RSD, considerandos 3 e 9.
[212] RSD, considerando 14.
[213] *Idem.*
[214] *Idem.*
[215] RSD, considerando 5.
[216] RSD, considerandos 13 e 30.

a que o RSD pretende dar cobro, com objetivo de elucidar um pouco mais o papel deste no prosseguimento dos objetivos gerais já identificados. Ao longo deste instrumento encontraremos, assim, diversas disposições legais que procuram impor obrigações aos prestadores de serviços intermediários nas suas mais diversas áreas de atuação.

O RSD estabelece, deste modo, obrigações em vários domínios, como regras relativas à produção de relatórios de transparência, à realização de auditorias independentes, a ordens de atuação contra conteúdo ilegal e para a disponibilização de informações, a exigências relacionadas com níveis mais elevados de transparência e de simplificação em questões relativas a decisões tomadas em relação aos seus utilizadores, aos seus mecanismos de moderação de conteúdo (algoritmos utilizados e supervisão humana) e de exibição de anúncios, ao seu sistema interno de reclamações, entre muitíssimos outros.[217] São também visíveis, a título exemplificativo, obrigações relativas aos modos de atuação em situações de crise e ao conjunto de procedimentos que se devem observar aquando da realização de alterações significativas aos seus termos e serviços (por exemplo, alterações que incidam sobre o tipo de conteúdo permitido no seu serviço ou quaisquer outras mudanças que possam diretamente impactar a utilização do serviço), entre outras. [218]

O RSD constitui, assim, um ato legislativo há já muito esperado dada a relevância e o impacto cada vez mais incontornável das grandes plataformas digitais nas sociedades e na economia do espaço europeu, comportando estas – simultaneamente – um grande risco e uma grande oportunidade para o sonho e para a estabilidade europeia[219]. Assim, considerando a importância das plataformas e motores de pesquisa em linha de muito grande dimensão[220] – em especial – enquanto meios propiciadores para a realização de amplos debates públicos, da partilha de conteúdos a um incontável número de pessoas[221], e enquanto agentes modeladores do modo como a informação chega a milhões de europeus, o Regulamento prevê algumas obrigações de caráter adicional[222] especificamente aplicáveis a estes[223].

---

[217] RSD, artigos 9.º, 10.º, 15.º, 17.º e 37.º.
[218] RSD, artigos 14.º e 36.º e considerando 45.
[219] RSD, considerando 1.
[220] RSD, considerando 76.
[221] RSD, considerando 14.
[222] A este propósito é de ressalvar que o considerando 30 do RSD estabelece, de modo perentório, o princípio geral base de que nenhuma das normas previstas no diploma deve ser interpretada como impondo uma obrigação de vigilância de caráter geral ou de uma "obrigação geral de apuramento ativo dos factos".
[223] RSD, considerandos 41, 48 e 75. De notar, ainda, que as plataformas em linha de muito grande dimensão e os motores de pesquisa em linha de muito grande dimensão correspondem aos serviços que possuem um número de utilizadores europeus igual ou superior a 10% da população europeia (Cfr. considerando 76).

Face a este abrangente conjunto de obrigações, o RSD procura, acima de tudo, assegurar o respeito pelos principais direitos e liberdades dos cidadãos europeus nas circunstâncias em que se justifique, por força das suas previsões, a imposição de algum tipo de restrições em nome da prossecução dos objetivos de grande interesse já identificados, como o combate à disseminação de desinformação no seio das plataformas digitais de grande dimensão.[224]

Neste âmbito e a título exemplo, a decisão de uma plataforma em linha de muito grande dimensão no sentido da imposição de uma restrição ao nível da visibilidade de determinado conteúdo (a "despromoção nos sistemas de classificação ou de recomendação", a título exemplificativo), ou da desmonetização do mesmo – algumas das possibilidades de atuação na limitação da propagação de desinformação –, devem obrigatoriamente ser seguidas de uma comunicação em linguagem objetiva e desambiguada ao seu respetivo destinatário, que contenham os motivos subjacentes àquela decisão e os meios disponíveis para a contestação, desde a utilização do mecanismo interno de reclamações à resolução extrajudicial de litígios[225], sem esquecer o direito ao recurso judicial[226], em nome do respeito pelo seu direito à liberdade de expressão e de informação[227].

A este respeito será, por isso, de relembrar que o conteúdo identificado como desinformação não é englobável no elenco de conteúdo ilegal à luz do direito da União. Levando tal em consideração, as opções disponíveis para o combate ao fenómeno da propagação de desinformação nas grandes plataformas digitais – que constituem o principal ambiente pelo qual esta prolifera – não devem desaguar (conjeturando o fenómeno isoladamente) numa remoção desse conteúdo ou numa suspensão definitiva do utilizador, por conta da violação do núcleo mais íntimo do seu direito à liberdade de expressão e de informação. Neste sentido, e apelando à importância de combater a ameaça, restam apenas algumas atitudes menos radicais e definitivas, tal como a já mencionada restrição de visibilidade ou desmonetização do conteúdo sinalizado.

4.1.3 Publicidade em linha e sistemas de recomendação

O RSD chama à atenção, neste âmbito, para uma grande problemática associada à atividade da exibição de publicidade no meio em linha, que efetivamente contribui para o fenómeno da

[224] RSD, considerando 47.
[225] RSD, considerando 59 e artigos 20.º, n.º 5 e 21.º.
[226] RSD, considerando 55.
[227] RSD, considerando 54.

monetização da partilha de conteúdos nocivos, como a desinformação[228]. É de notar, igualmente, que este tema (como outros) será alvo de análise nos restantes instrumentos normativos analisados, dada a centralidade da temática para a lide.

O fenómeno da publicidade em linha evidencia-se especialmente com o recurso a táticas de direcionamento, utilizadas para apresentar anúncios publicitários de um modo mais personalizado e canalizado a determinado utilizador, oportunizando a particularidade da ameaça. As redes sociais, enquanto meios especialmente propícios à verificação de circunstâncias desta natureza, representam um risco acrescido para toda a sociedade, uma vez que acabam por apoiar, ainda que involuntariamente, a propagação direcionada de campanhas de desinformação manipuladoras[229].

Com estas preocupações em mente, o RSD propõe um conjunto apertado de regras para que se atinjam maiores graus de transparência ao nível do conteúdo patrocinado. Existem, assim, um conjunto de informações que devem ser fornecidas ao utilizador e que perpassam diversos domínios. Tais informações devem, no seu essencial, proceder à identificação da natureza do conteúdo em questão (caráter publicitário/patrocinado, no caso)[230], à colocação de informações relativamente à pessoa (singular ou coletiva) em nome da qual o anúncio é exibido (ou a pessoa que paga o anúncio, quando não se trate da mesma)[231] e de informações acerca dos critérios mais relevantes que foram utilizados para a sua exibição, acopladas de uma breve explicação da lógica subjacente ao mecanismo de recomendação utilizado – algo particularmente relevante quando se verifica a utilização de técnicas de definição de perfis[232] – e, por fim, à disponibilização de instrumentos que permitam ao utilizador modificar o funcionamento do dito mecanismo de recomendação[233]. Todas estas informações devem ser veiculadas diretamente na interface em linha de um modo proeminente, simples e "claramente identificável", por meio de "marcas sonoras ou visuais estandardizadas".[234]

Ainda no tema da publicidade em linha, mais exigências são previstas no RSD relativamente às plataformas e motores de pesquisa em linha de muito grande dimensão, que devem, por seu turno, proceder à criação de repositórios de anúncios publicitários acessíveis publicamente. Estes repositórios devem ser idealizados com o intuito de apoiar as atividades de supervisão deste tipo de conteúdo, facilitando, para o efeito, o acesso da comunidade de investigação a estes dados, que acaba por

---

[228] RSD, considerando 68.
[229] RSD, considerando 69.
[230] RSD, considerando 68 e artigo 26.º, n.º 1, alínea a) e n.º 2.
[231] RSD, considerando 68 e artigo 26.º, n.º 1, alínea c).
[232] A exibição de conteúdo publicitário com recurso a categorias especiais de dados pessoais – descritas no artigo 4.º, ponto 4, do Regulamento (UE) 2016/679 – não é permitida (considerando 69 e artigo 26.º, n.º 3).
[233] RSD, considerando 68 e artigo 26.º, n.º 1, alínea d).
[234] RSD, considerando 68.

proporcionar um estudo mais pormenorizado dos principais perigos (ao nível da saúde e segurança públicas e da igualdade e do envolvimento cívico nos assuntos públicos democráticos, entre outros[235]) que resultam da exibição de conteúdo publicitário manipulador e nocivo no ambiente digital.[236]

Estes repositórios devem, por isso, conter várias informações sobre os anúncios que são apresentados nos seus serviços, tais como o conteúdo em si, o seu objeto, as já referidas informações sobre a identidade da pessoa em nome da qual o anúncio é apresentado ou a identidade da pessoa que pagou pelo mesmo, o período durante o qual o anúncio se encontra visível, dados relativos à quantidade de pessoas alcançadas e, ainda, os parâmetros de direcionamento utilizados, caso se verifique um direcionamento (ou uma exclusão de direcionamento) a um grupo de utilizadores mais restrito[237].

A principal diferença entre as informações presentes diretamente no anúncio e as que estão presentes nos repositórios de anúncios prende-se, então, com o grau de informação disponibilizado. Na interface em linha onde o anúncio é visualizado habitualmente, esse conjunto de dados é fornecido com o intuito de transmitir uma informação rápida ao utilizador sobre a natureza do conteúdo que lhe é apresentando, permitindo que este aja em conformidade e com conhecimento, sendo que quem procura uma visão mais detalhada e abrangente, não apenas dos anúncios que lhe são recomendados, mas também de outros que não o foram, deve utilizar a ferramenta que o repositório de anúncios cria para este efeito.

A elaboração de códigos de conduta constitui, do mesmo modo, um caminho importante para o estabelecimento de normas que garantam um maior grau de transparência em torno da publicidade em linha. O artigo 46.º do RSD menciona, a propósito, a importância do desenvolvimento de códigos de conduta especificamente orientados para a realidade da exibição de anúncios publicitários em linha. Aqui, a Comissão encoraja a criação de uma ferramenta de autorregulação que vá para além do que já se encontra estabelecido no RSD, que procure, para o efeito, o estabelecimento de maiores níveis de transparência[238] que estimulem, simultaneamente, os direitos e interesses dos agentes implicados e um ecossistema mais concorrencial e sério[239]. O RSD recomenda, por isso, que futuros códigos de conduta prevejam normas promotoras de uma maior lisura entre todos os participantes da cadeia de valor

[235] RSD, considerando 95.
[236] RSD, considerando 95.
[237] RSD, artigo 39.º, n.º 1 e 2.
[238] RSD, artigo 46.º, n.º 1.
[239] RSD, artigo 46.º, n.º 2.

característica da indústria da publicidade em linha, nomeadamente ao nível de informações relativas à monetização dos dados[240].

No caso, o Código de Conduta Reforçado em matéria de Desinformação de 2022 e, numa perspetiva mais regulatória, a proposta de Regulamento que incidirá sobre a vertente política desta questão, representam os instrumentos normativos mais recentes e próximos destas recomendações.

Adiante, mas ainda na mesma linha de raciocínio, o tema da desinformação também se coloca, naturalmente, por conta do funcionamento dos sistemas de recomendação do conteúdo não patrocinado, que nos oferece *feeds* personalizados de acordo com os nossos padrões de comportamento. Sabendo, assim, que o modelo de negócio das grandes plataformas digitais gira muito em torno da forma como a informação é apresentada aos seus utilizadores, a ordem pela qual a mesma é exibida resulta de um vasto conjunto de operações algorítmicas que pretendem influenciar e individualizar a experiência de cada utilizador.

Essas técnicas toldam, consequente e consideravelmente, o simples, mas poderoso, ato diário de consumo de notícias nos meios digitais, influenciando, ultimamente, qual o conteúdo que «viraliza», ou não, sendo que esta questão da «viralização» não deve, na verdade, ser encarada de ânimo leve, uma vez que não corresponde a apenas um jogo de números ou dados estatísticos, podendo causar reais repercussões e disrupções[241].

Posto isto, o RSD estabelece um conjunto de obrigações de transparência semelhantes ao exposto aquando da personalização dos anúncios publicitários em linha, forçando as plataformas a informarem os seus utilizadores, numa linguagem clara e acessível, sobre quais são os principais critérios subjacentes ao funcionamento desses sistemas de recomendação, que acabam por influenciar a forma como a informação lhes é apresentada e priorizada, como se observou.[242] Para além disso, o RSD impõe ainda como obrigação a introdução de mecanismos que facilitem a alteração do funcionamento destes sistemas.[243] Assim, quem preferir uma navegação menos direcionada, pode sempre optar por deixar de partilhar dados pessoais e informações sobre os seus padrões de comportamento para efeitos de recomendação de conteúdo, desabilitando a opção que permite uma navegação mais personalizada e apoiada em interesses pessoais.

---

[240] RSD, considerando 107.
[241] RSD, considerando 70; MARWICK, Alice; LEWIS, Rebecca, pp. 42 e 43.
[242] RSD, artigo 27.º, n.º 1.
[243] RSD, artigo 27.º, n.º 1.

4.1.4 Riscos sistémicos

O RSD procede, de igual modo, a uma categorização de riscos sistémicos, isto é, perigos que resultam da utilização de ferramentas essenciais para a formação ou operação do serviço que é disponibilizado pelas plataformas digitais[244]. Esta noção de riscos sistémicos encontra-se englobada na secção 5 do Regulamento e, assim sendo, aplica-se particularmente às plataformas e motores de pesquisa em linha de muito grande dimensão, que, dado o seu grau de influência, detêm serviços especialmente influentes para a esfera pública.

A noção de propagação de desinformação[245] engloba-se, logicamente, nesta noção de «risco sistémico», sendo que o considerando 104 do Regulamento é perentório ao fazer esta associação.

Neste ponto, o RSD procede a uma categorização quadripartida dos riscos sistémicos[246], sendo que o fenómeno da disseminação de desinformação será aplicável à terceira e à quarta categoria de riscos[247], onde é mencionada a produção de efeitos negativos para alguns dos alicerces das sociedades livres, tais como os direitos fundamentais (como o direito à liberdade de expressão e de informação, ou da liberdade e pluralismo dos media), o discurso cívico independente, os processos eleitorais e a segurança e saúde[248] públicas.[249]

A este propósito, e como veremos posteriormente no capítulo relativo ao caso RT France v Conselho, a disseminação de desinformação, particularmente se for levada a cabo de forma organizada e financiada, pode colocar em perigo, de um modo quase direto, a segurança pública em situações extremas, como a de uma guerra. Para além disso, a disseminação de desinformação observada ao longo da pandemia de COVID-19[250] – principalmente em torno da seriedade da situação, ou da segurança e eficácia das vacinas – acarretou, efetivamente, algumas preocupações na ordem da saúde pública, demonstrando, uma vez mais, que esta ameaça pode atingir um efeito profundamente corrosivo e desestabilizador junto das sociedades.[251]

Para além disso, um dos grandes tópicos que cumpre também aqui relembrar corresponde à questão da utilização frequente de *bots* e contas falsas para a disseminação de desinformação. A

---

[244] RSD, artigo 34.°, n.° 1.
[245] O Regulamento refere que as plataformas e motores de pesquisa em linha de muito grande dimensão devem "prestar especial atenção à forma como os seus serviços são utilizados para difundir ou amplificar conteúdos enganosos ou suscetíveis de induzir em erro, como a desinformação" (considerando 84).
[246] RSD, considerando 80.
[247] RSD, considerando 82.
[248] RSD, considerando 83.
[249] RSD, artigo 34.°, n.° 1., alínea b) e c).
[250] Sobre este assunto, Cfr. também BAYER, Judit *et al., Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States (2021 update)*, Parlamento Europeu, 2021, em particular, o capítulo "COVID-19".
[251] Comissão Europeia, *Comunicação: Combater a desinformação sobre a COVID-19: repor a verdade dos factos*, JOIN(2020) 8 final, 2020, p. 5; VAN RAEMDONCK, Nathalie; MEYER, Trisha, p. 2.

utilização inautêntica do serviço torna, logicamente, ainda mais inquietante e impactante a questão dos riscos sistémicos e, nesse sentido, deve verificar-se, ao nível das grandes plataformas digitais da área, uma atenção extra no desenvolvimento de ferramentas que tornem mais difícil e detetável a prática deste tipo de comportamento alarmante.[252]

Com tudo isto em mente, a Comissão procurou, deste modo, estabelecer primeiramente uma obrigação de as plataformas e motores de pesquisa em linha de muito grande dimensão identificarem e investigarem os riscos sistémicos que emergem da utilização dos seus serviços[253] e, consequentemente, a obrigação de implementarem as devidas providências para dar uma resposta decisiva e eficiente que contrarie os riscos sistémicos que eventualmente hajam identificado.[254]

A priori, torna-se, assim, categórico implementar um conjunto de métodos de identificação e avaliação de riscos sistémicos (especialmente nas zonas passíveis de um maior abuso) que sejam baseados nos maiores padrões de exigência, tanto técnico-científicos, como legais, dado que o respeito pelos direitos fundamentais dos utilizadores corre, não raras vezes, riscos no desenho destes procedimentos.[255]

Por seu turno, a realidade dos riscos sistémicos encontra-se naturalmente associada aos vários instrumentos que o próprio serviço propicia, que são, por isso, os responsáveis por criar ou amplificar a sua ameaça. São eles os sistemas de recomendação, os mecanismos de exibição de anúncios e de moderação de conteúdos, as práticas de recolha de dados e o texto dos seus termos de serviço, e a sua respetiva aplicação.[256]

No âmbito dos anúncios publicitários, para além do já exposto, são mencionados ainda alguns pontos de atuação para a minimização de riscos sistémicos, tais como a cessação das receitas publicitárias de um determinado tipo de conteúdo, cuja relevância esteja a ser explorada maliciosamente[257]. Por seu turno, no caso dos sistemas de recomendação, é sugerido um aumento da visibilidade das fontes noticiosas autoritativas e de confiança[258], bem como a realização de testes de segurança aos algoritmos que informam esses sistemas[259]. No âmbito do tema da utilização inautêntica

---

[252] RSD, considerando 84 e artigo 34.°, n.° 2, parte final; MORGAN, Susan, "Fake news, disinformation, manipulation and online tactics to undermine democracy", in Journal of Cyber Policy, 3:1, 2018, pp. 42 e 43.
[253] RSD, artigo 34.°.
[254] RSD, artigo 35.°, n.° 1.
[255] RSD, considerando 86.
[256] RSD, considerando 84.
[257] RSD, considerando 88.
[258] RSD, considerando 88.
[259] RSD, artigo 35.°, n.° 1, alínea e).

e abusiva do serviço, as melhores recomendações seguem a lógica de um maior investimento em tecnologia de deteção deste tipo de comportamentos, como referido anteriormente.

A mitigação de riscos sistémicos nas plataformas e motores de pesquisa em linha de muito grande dimensão deve, assim, também passar por uma introdução de meios que procurem sensibilizar os utilizadores para uma navegação mais informada do seu serviço, alertando para os maiores perigos que possam surgir e para os mecanismos de denúncia existentes.[260] A título exemplificativo, a utilização de *deepfakes* (áudios, imagens ou vídeos manipulados digitalmente) representa, igualmente, um dos grandes desafios para uma utilização segura dos serviços digitais e, nesse domínio, é importante alertar o utilizador, por meio de avisos, da inautenticidade de todo o conteúdo que preencha estas características[261], visto que os avanços galopantes da IA tornaram a verdade e a mentira praticamente indistinguíveis, tornando tão atual e importante a batalha pela preservação do verdadeiro e do factual.

Neste domínio, a questão do desenvolvimento de códigos de conduta é um aspeto novamente enfatizado[262], dado que a adesão aos mesmos constitui uma medida apropriada à atenuação de riscos sistémicos[263]. Precisamente no seu artigo 45.º, o RSD reitera expressamente o seu incentivo à preparação e implementação de códigos de conduta ao nível da União, códigos esses que são, como veremos, um meio complementar precioso à aplicação e prossecução dos objetivos já delineados neste Regulamento.

4.1.5 Os momentos de crise

O exemplo recente da pandemia de COVID-19 configurou um momento de crise sem precedentes na Europa e no mundo, no qual os fenómenos de propagação de desinformação ganharam uma preponderância nunca vista, tornando-se profundamente perigosos para o bem-estar das populações.[264]

É com base nestes (e noutros) períodos de maior desafio que o RSD dá uma particular atenção às chamadas situações de «crise», definidas como uma "ocorrência de circunstâncias extraordinárias

[260] RSD, artigo 35.º, n.º 1, alínea i) e considerando 88.
[261] RSD, artigo 35.º, n.º 1, alínea k).
[262] RSD, considerando 103 e 106.
[263] RSD, considerando 104 e artigo 35.º, n.º 1, alínea h).
[264] VAN RAEMDONCK, Nathalie; MEYER, Trisha, p. 2; *Conclusões do Conselho sobre o reforço da resiliência e a luta contra as ameaças híbridas, incluindo a desinformação no contexto da pandemia de COVID-19*, p. 3.

passíveis de resultar numa ameaça grave para a segurança pública ou a saúde pública na União ou em grande parte do seu território"[265].

É nestas situações que o RSD confere um poder especial à Comissão, que passa a poder exigir que as plataformas e motores de pesquisa em linha de muito grande dimensão adotem, de uma forma urgente, uma série de medidas para mitigar os efeitos da situação de crise que se formou[266] que, a título exemplificativo, se podem materializar numa adaptação dos seus mecanismos de moderação de conteúdo e de exibição de publicidade, ou do funcionamento dos seus algoritmos. Perante este tipo de circunstâncias, também se encontra prevista a promoção de ações de sensibilização e de uma maior proeminência na visibilidade de informação de confiança[267].

No âmbito deste mecanismo de resposta a momentos de crise, Comissão terá igualmente ao seu dispor a possibilidade de desenvolver «protocolos de crise voluntários», necessários para desencadear uma resposta transfronteiriça célere e unida, perante perigos que, de uma forma particularmente expressiva, estejam a causar alguma turbulência nos canais digitais e, consequentemente, no quotidiano de todos os europeus.[268] Estes protocolos configuram mecanismos de resposta essenciais e especialmente úteis para preparar uma reação eficaz em casos de especial gravidade no campo da informação, caracterizados por uma acelerada proliferação de desinformação que exige a disseminação, também ela rápida, de informação fidedigna e rigorosa[269].

4.1.6 O acesso aos dados das plataformas e motores de pesquisa em linha de muito grande dimensão

A questão do acesso aos dados das plataformas e motores de pesquisa em linha de muito grande dimensão é também abordada no RSD, tanto nos casos onde o acesso é praticado por parte das autoridades competentes – para que estas possam realizar uma avaliação diligente do cumprimento da legislação –[270] como por outras figuras, como investigadores.

Neste último caso, a situação assume peculiar relevância, uma vez que estes – detentores de um papel crucial no aprofundamento do conhecimento sobre o fenómeno da disseminação de desinformação – enfrentam muitos obstáculos no acesso aos dados das grandes plataformas digitais,

[265] RSD, considerando 91.
[266] RSD, artigo 36.°, n.° 1.
[267] RSD, considerando 91.
[268] RSD, considerando 108.
[269] RSD, considerando 108.
[270] RSD, considerando 141 e artigo 40.°, n.° 1.

acesso esse que se apresenta como vital para a relevância e aplicabilidade das suas pesquisas e indagações. Com isso em mente, o RSD pretende fortalecer a posição dos investigadores que exercem o seu labor investigativo de boa-fé, sem esquecer as legítimas preocupações levantadas pelas plataformas e motores de pesquisa em linha de muito grande dimensão.

O texto do RSD reconhece, de modo expresso e categórico, o valor dos esforços de investigação, mencionando que o trabalho investigativo desenvolvido é "particularmente importante para colmatar as assimetrias de informação e estabelecer um sistema resiliente de atenuação dos riscos"[271], do qual todos os atores envolvidos, desde a sociedade civil às plataformas e motores de busca, iriam naturalmente beneficiar. O texto legislativo é também claro ao referir que a atividade de investigação que a Comissão pretende incentivar deve radicar-se no propósito da realização de uma "investigação que contribua para a deteção, identificação e compreensão dos riscos sistémicos na União" e para uma "avaliação da adequação, eficiência e impacto das medidas de atenuação dos riscos". [272] Neste sentido, o RSD pugna pela criação de um justo e seguro regime de acesso a dados que torne possível a prossecução de um abrangente conjunto de valores de interesse público[273].

O Regulamento indica, para o efeito, que o procedimento de acesso aos dados, por parte de investigadores habilitados, deve ser iniciado por meio de um pedido fundamentado ao coordenador dos serviços digitais de estabelecimento[274], que irá posteriormente entrar em contacto com a plataforma ou motor de pesquisa em linha de muito grande dimensão em causa. [275]

É, assim, necessário assegurar um cuidadoso processo de seleção de investigadores que ateste a independência da sua atividade e que acautele os direitos e os interesses de todas as partes envolvidas, entre os quais a preservação da segurança dos serviços[276] e a proteção de dados pessoais e de informações comerciais confidenciais[277], que constituem, precisamente, algumas das preocupações que as plataformas e motores de pesquisa em linha de muito grande dimensão principalmente levantam.[278]

---

[271] RSD, considerando 96.
[272] RSD, artigo 40.°, n.° 4.
[273] RSD, considerando 91.
[274] A figura do coordenador dos serviços digitais de estabelecimento corresponde à entidade responsável pela supervisão do Regulamento no Estado-Membro de estabelecimento do prestador de serviços intermediários em causa.
[275] RSD, artigo 40.°, n.° 8.
[276] RSD, artigo 40.°, n.° 13.
[277] RSD, considerando 98.
[278] O RSD estabelece um conjunto de exigências que graduam um «investigador qualificado», tais como a sua filiação num organismo de investigação, a sua independência de interesses comerciais, a capacidade para assegurar a confidencialidade e segurança dos dados analisados e a descrição das técnicas utilizadas na investigação, entre outras (artigo 40.°, n.° 8).

O RSD procede, no entanto, a uma ressalva, indicando que o acesso aos dados, por motivos relacionados com a monitorização dos riscos sociais identificados, poderá (e deverá) ir mais longe sempre que exista um entendimento para tal, por meio do estabelecimento de códigos de conduta ou de acordos entre investigadores e as próprias plataformas e motores de pesquisa em linha de muito grande dimensão, a título de exemplo.[279]

4.1.7 Os relatórios de transparência

Intimamente relacionado com a questão do acesso aos dados, surge um ponto associado à obrigação de apresentação de relatórios de transparência, essenciais para uma apreciação do efeito útil das medidas implementadas e, em especial, para uma supervisão mais detalhada do trabalho realizado em sede de moderação de conteúdos[280].

Os relatórios, que devem ser comunicados pelo menos uma vez por ano, devem incluir um conjunto abrangente de métricas essenciais para o estudo da problemática da disseminação de desinformação e da defesa dos direitos fundamentais nesta sede. As informações extraídas destes relatórios são centrais para se obter um olhar mais atento sobre o funcionamento dos meios automatizados para a moderação de conteúdos, que são particularmente relevantes para a produção de um retrato rigoroso desta realidade no meio em linha.

O artigo 15.º do RSD detalha que os prestadores de serviços intermediários devem incluir uma série de informações nos seus relatórios a este respeito.

Na alínea e), do seu n.º 1., é feita uma referência à necessidade de disponibilização de informações sobre qualquer recurso a meios automatizados com intuito de proceder a atividades de moderação do conteúdo em linha. Destas informações deve constar uma "descrição qualitativa" do propósito da moderação, o detalhamento dos seus objetivos, os indicadores de precisão utilizados, as taxas de erro associadas a estes sistemas de moderação e as respetivas garantias aplicadas.

Por sua vez, a alínea c) indica a necessidade de publicar, por um lado, as ações que foram empreendidas de encontro à instrução e apoio dos responsáveis pela moderação de conteúdos e, por outro, os dados quantitativos e qualitativos sobre as medidas tomadas "que afetam a disponibilidade, a visibilidade e a acessibilidade das informações fornecidas pelos destinatários do serviço", bem como a sua "capacidade (...) em fornecerem informações através do serviço".

---

[279] O já mencionado Código de Conduta Reforçado em matéria de Desinformação de 2022 prevê, justamente, algumas regras relativamente ao acesso de dados das plataformas e motores de pesquisa, por parte da comunidade de investigação.
[280] RSD, artigo 15.º, n.º 1.

A alínea d) estabelece, por fim, um conjunto de obrigações relativamente à disponibilização de dados sobre o funcionamento dos sistemas de reclamação internos, como o número de reclamações recebidas ou o tempo mediano para uma decisão.

A imposição de obrigações legais nesta sede é essencial para traçar mais precisamente a evolução do fenómeno e explorar eventuais e necessárias mudanças na política legislativa para um combate mais eficaz ao problema. Com isso em mente, é importante que a publicação destes dados, nos relatórios de transparência, seja feita de uma forma percetível e francamente ilustradora da realidade.[281]

4.1.8 Os mecanismos de supervisão no RSD

A Comissão, em articulação com os coordenadores de serviços digitais, enquanto principais figuras responsáveis pela cabal monitorização do cumprimento deste Regulamento, devem cooperar proximamente na sua supervisão e aplicação[282] e, para tal, possuem alguns poderes de investigação para os auxiliar nesta tarefa.

O conjunto de poderes atribuídos aos coordenadores de serviços digitais encontra-se naturalmente limitado aos prestadores de serviços intermediários abrangidos pela competência do seu respetivo Estado-Membro e resume-se à possibilidade de, mas não só, exigir informações face a possíveis violações do Regulamento[283], o poder de realizar inspeções[284], o poder de ordenar a cessação de infrações – impondo medidas de reparação, para o efeito –[285], e de impor coimas ou sanções pecuniárias compulsórias[286], e, em situações limite, ordenar a restrição temporária do serviço, mediante pedido ao órgão judicial competente[287].

Por sua vez, os poderes atribuídos à Comissão recaem, em particular, sobre uma monitorização das obrigações estabelecidas relativamente às plataformas e motores de pesquisa em linha de muito grande dimensão[288], sendo que, no que se refere às obrigações adicionais e extensíveis especialmente a estes, previstas na secção 5 do capítulo III, detém um poder exclusivo de supervisão[289]. O alcance dos poderes de monitorização e investigação da Comissão centra-se, assim,

---

[281] RSD, artigo 15.°, n.° 1.
[282] RSD, artigos 56.°, n.° 5 e 57.°, n.° 1.
[283] RSD, artigo 51.°, n.° 1, alínea a) e c).
[284] RSD, artigo 51.°, n.° 1, alínea b).
[285] RSD, artigo 51.°, n.° 2, alínea b).
[286] RSD, artigo 51.°, n.° 2, alínea c) e d).
[287] RSD, artigo 51.°, n.° 3, alínea b).
[288] RSD, artigo 56.°, n.° 3.
[289] RSD, artigo 56.°, n.° 2.

especialmente sobre as entidades que poderão levantar riscos sistémicos para o coletivo europeu e, nesses casos de maior gravidade e proporção, a Comissão é a figura mais adequada a tomar as rédeas[290].

Por seu turno, os poderes da Comissão sobre estas entidades de muito grande dimensão são semelhantes aos que já foram expostos nos parágrafos anteriores e, de forma não taxativa, correspondem à possibilidade de emitir pedidos de informação e de realização de entrevistas[291], o poder para a realização de inspeções[292], a aplicação de medidas de acompanhamento – como ordens de acesso às bases de dados e algoritmos –[293], a emissão de decisões de incumprimento – seguidas de uma ordem para que se tomem as medidas necessárias à cessação do dito incumprimento –[294] e o poder para aplicar coimas e sanções pecuniárias compulsórias[295].

4.2 A Proposta de Regulamento sobre a transparência e o direcionamento da propaganda política

A temática da publicidade política – especialmente quando esta é veiculada nos canais digitais – representa um ponto essencial a abordar na conceção de respostas eficazes ao problema da disseminação de desinformação.[296] Nesse sentido, em nome dos mais centrais princípios democráticos – como o princípio do Estado de Direito ou o princípio da não discriminação (no âmbito do fornecimento transfronteiriço de serviços de propaganda política[297]) – e em nome da defesa dos direitos, liberdades e interesses fundamentais (em particular "[d]a confiança do público na supervisão da propaganda política"[298]), encontra-se atualmente a ser delineado o futuro Regulamento sobre a transparência e o direcionamento da propaganda política.

Para efeitos da análise deste capítulo e antes de um avanço mais aprofundado na matéria, levando em consideração que o documento legislativo em evidência não assumiu, ainda, uma forma definitiva e final, toda e qualquer observação e menção à proposta de Regulamento será efetuada

---

[290] RSD, considerando 138.
[291] RSD, artigos 67.º e 68.º.
[292] RSD, artigo 69.º.
[293] RSD, artigo 72.º.
[294] RSD, artigo 73.º, n.º 1 e 3.
[295] RSD, artigos 74.º e 76.º.
[296] VAN RAEMDONCK, Nathalie; MEYER, Trisha, p. 16.
[297] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho sobre a transparência e o direcionamento da propaganda política – Alterações aprovadas pelo Parlamento Europeu, em 2 de fevereiro de 2023, (COM(2021)0731 – C9-0433/2021 – 2021/0381(COD)) (1), alteração ao considerando 14-B.
[298] Alteração ao considerando 58 da proposta de Regulamento.

levando em atenção as alterações aprovadas pelo Parlamento Europeu, datadas de 2 de fevereiro de 2023.

4.2.1 Considerações introdutórias

A realidade da propaganda política é, de uma forma geral, regulamentada de um modo multiforme nos vários Estados-Membros e encontra-se desfasada, em grande medida, face aos riscos de natureza transfronteiriça e tecnológica que atualmente emergem[299].

Tal como no RSD, as consequências mais diretas desta inomogeneidade surgem ao nível da verificação de uma fragmentação do mercado interno provocada por toda a incerteza e diferença jurídica, que pode apenas ser combatida através da implementação de um instrumento de harmonização legislativa[300], aplicável aos agentes que atuam no âmbito da propaganda política e suas áreas afins[301].

A proposta de Regulamento procura avançar, igualmente, com uma possível definição de «propaganda política», na tentativa de delimitar, mais rigorosa e formalmente, o principal objeto deste instrumento legislativo. É, assim, referido que a noção de «propaganda política» se reporta à "preparação, colocação, promoção, publicação, distribuição ou difusão, por qualquer meio, de uma mensagem: por, para ou em nome de um interveniente político[302] (...) *ou* suscetível de influenciar um comportamento eleitoral ou o resultado de uma eleição, de um referendo ou de um processo legislativo ou regulamentar"[303].

A redação legislativa desta definição é, assim, particularmente relevante pois não exige que a propaganda política seja apenas aquela veiculada por figuras políticas, bastando a capacidade de influenciar o resultado dos processos eleitorais democráticos, tornando ainda mais inclusivo o leque de situações abrangidas pelas disposições que iremos analisar posteriormente.

Por fim, ficará claro que o escopo de atuação desta proposta de Regulamento sobrepõe-se, até certa medida, às matérias previstas noutros instrumentos legislativos já nossos conhecidos – como o Regulamento Geral sobre a Proteção de Dados (RGPD) ou o RSD. Nesse sentido, as disposições elencadas nesta proposta de Regulamento não prejudicam o disposto no RSD, mas devem, sim, apoiar

---

[299] Alteração ao considerando 6 da proposta de Regulamento.
[300] Alterações aos considerandos 8 e 10 da proposta de Regulamento.
[301] Alteração ao considerando 14 da proposta de Regulamento.
[302] Cumpre ressalvar que, quando se mencionam as mensagens "por, para ou em nome de um interveniente político", se encontram excluídas as mensagens que assumam uma natureza puramente particular ou comercial.
[303] Alteração ao artigo 2.°, n.° 2 da proposta de Regulamento.

as plataformas e motores de pesquisa em linha de muito grande dimensão na formulação de respostas de graduação e atenuação de riscos provenientes dos seus mecanismos de exibição de propaganda política[304], uma vez que o funcionamento dos sistemas de direcionamento e distribuição de anúncios publicitários pode comportar, como já se pôde observar, alguns riscos sistémicos[305].

Assim, a proposta de Regulamento aponta para a imprescindibilidade de uma aplicação mais efetiva das normas já em vigor – necessárias para garantir o cumprimento eficiente de todos os textos legislativos – e para a condução de uma atenção particular à necessidade de implementação de disposições legislativas, «à prova de futuro», que combatam as problemáticas mais emergentes.[306]

4.2.2 O direcionamento de propaganda política

O novo mundo de possibilidades que se abriu ao nível do direcionamento de conteúdo de caráter político (e não só) coloca riscos à dinâmica livre, aberta e esclarecida das sociedades democráticas europeias e aos direitos fundamentais dos seus cidadãos.

É justamente nesse sentido que alerta a proposta de Regulamento ao indicar que o possível abuso destes mecanismos de tratamento de dados pessoais – normalmente pouco transparentes – é potencialmente disruptivo para o exercício de diversos interesses, direitos e liberdades fundamentais, tais como a liberdade de expressão, a não discriminação, a transparência dos atos democráticos, a igualdade de oportunidades, o direito "a ser informado de forma objetiva, transparente e pluralista" e, ainda, a esfera de direitos interconectados com a privacidade e proteção de dados.[307]

É atualmente possível, no meio em linha, por via do conforto das nossas casas e com o apoio do sofisticado processamento algorítmico de dados pessoais[308], chegar (ou evitar) a determinados grupos de pessoas, de diversos países, com conteúdo especificamente adaptado às características recolhidas[309].

As técnicas de direcionamento dependem, para o efeito, de vastas práticas de recolha de dados pessoais. A recolha de um grande conjunto de dados – e o seu posterior tratamento com recurso a sofisticadas técnicas de análise de comportamentos em linha e de definição de perfis – é essencial para iniciar o processo de classificação do utilizador de acordo com os seus interesses e

[304] Alteração ao considerando 32 da proposta de Regulamento.
[305] Alteração ao considerando 32 da proposta de Regulamento.
[306] Alteração aos considerandos 47 e 47-D da proposta de Regulamento.
[307] Alteração ao considerando 5 da proposta de Regulamento.
[308] Alteração ao considerando 5 da proposta de Regulamento.
[309] Alteração ao considerando 1 da proposta de Regulamento.

preferências.[310] A informação que é possível extrair da mecanização de toda esta realidade permite o direcionamento, extensivamente preciso, de anúncios políticos ao utilizador.

Ora, o fenómeno do direcionamento de conteúdo político, caracterizado pela sua extrema precisão, – se realizado em condições inapropriadas[311] – poderá ter um efeito alienante e manipulador junto do eleitorado, uma vez que esta prática pode ser utilizada para selecionar e explorar as fragilidades de determinados segmentos populacionais.[312] Relativamente a este ponto, a proposta de Regulamento alerta precisamente para uma divulgação maliciosa de anúncios políticos, ou seja, quando o mesmo é exibido em cenários e circunstâncias cuidadosamente escolhidos para explorar as vulnerabilidades do público-alvo que, por uma miríade de motivos, se encontra – naquele momento em particular – mais sensível a esse tipo de mensagem ou informação.[313]

Contextos como o descrito anteriormente penalizam fortemente os direitos mais elementares do cidadão europeu eleitor, que sofre uma invasão ao seu mais íntimo livre-arbítrio por meio de uma tentativa de manipulação da sua inteligência emocional e intelectual, defraudando uma composição mais apropriada do seu juízo crítico e lógico sobre questões centrais de enorme relevância pública. Verifica-se, ainda, uma violação do seu direito à recolha e tratamento legítimo de dados pessoais e dos seus direitos a "ser tratado de forma justa e equitativa", de "não ser manipulado", e de "receber informações objetivas, formar a sua opinião, tomar decisões políticas e exercer os seus direitos de voto"[314].

É, para além disso, importante atentar que os efeitos negativos associados a estas práticas assumem dimensões extraordinárias quando se observa o número de utilizadores de redes sociais no espaço europeu, desenrolando-se – nesses casos – um massivo ataque aos direitos políticos e democráticos de todo o coletivo europeu.[315] Numa grande escala, a utilização ilegítima de instrumentos que permitam a categorização dos utilizadores para efeitos de exibição de propaganda política direcionada propicia fenómenos preocupantes, tais como a verificação de grandes divisões sociais em assuntos basilares, sobre os quais é crucial existir o mais alargado e informado consenso possível.

A utilização maliciosa dos instrumentos de direcionamento de anúncios de cariz político – facilmente acessíveis a atores mal-intencionados que assumem, não raras vezes, uma origem estatal –

---

[310] Alteração ao considerando 47 da proposta de Regulamento.
[311] Alteração ao considerando 47-E da proposta de Regulamento.
[312] Alteração ao considerando 47 da proposta de Regulamento.
[313] *Idem.*
[314] *Idem.*
[315] MORGAN, Susan, p. 42.

permite uma autêntica "anális[e] predatóri[a] do eleitorado"[316] com efeitos observáveis na semeação de instabilidade e desconfiança por meio da disseminação de desinformação. Todas estas inquietações, que com os avanços computacionais alcançam novos patamares[317], merecem naturalmente uma resposta musculada e assertiva por parte dos decisores políticos a nível europeu.

Assim, e em vista a uma sanação das fragilidades já identificadas, todo e qualquer ato de direcionamento e distribuição de anúncios publicitários de cariz político deve ter apenas, como base, dados pessoais expressamente fornecidos – pelo utilizador ao editor de propaganda política[318] – para tal propósito.[319] Para além disso, pugna-se por uma proibição de tratamento de dados pessoais obtidos indiretamente, isto é, dados pessoais que derivam da observância do comportamento em linha do utilizador.[320] Ainda neste domínio, caso se verifique uma recusa em fornecer dados pessoais para o tratamento com base nestas finalidades – que é uma possibilidade que não deve nunca ser descartada –, não se pode observar uma alienação do utilizador que avançou com a mencionada recusa, ao qual devem ser dadas "outras opções justas e razoáveis para aceder aos serviços da sociedade da informação".[321]

Ainda com estas inquietações em mente, a proposta de Regulamento indica que, no período especialmente crítico relativo ao espaço temporal de 60 dias que precede uma qualquer eleição ou referendo, constitui-se urgente o estabelecimento de normas adicionais relativas ao direcionamento e distribuição de anúncios de cariz político com recurso a dados pessoais.[322] Nestas circunstâncias, o direcionamento e distribuição deve somente recorrer a três categorias de dados do seu titular: a localização, as línguas por si faladas e o facto de este ser um eleitor pela primeira vez[323].[324]

As restrições relativamente ao direcionamento não se ficam, no entanto, por aqui. A proposta legislativa entende, ainda, implementar algumas restrições às categorias de parâmetros utilizadas para essas técnicas de direcionamento.[325] Assim, depois de apurado o público-alvo potencial para a receção do conteúdo político publicitário, os agentes relevantes não poderão, com sustento num tratamento de dados pessoais subsequente, proceder a qualquer ato adicional de triagem relacionado com a

---

[316] Alteração ao considerando 47 da proposta de Regulamento.
[317] Alteração ao considerando 47 da proposta de Regulamento.
[318] «Editor de propaganda política»: "o prestador de um serviço de propaganda política que coloca, promove, publica, distribui ou divulga propaganda política através de qualquer meio" (alteração ao ponto 11., do parágrafo 1., do artigo 2.° da proposta de Regulamento)
[319] Alteração ao considerando 47-F da proposta de Regulamento.
[320] *Idem.*
[321] *Idem.*
[322] Alteração ao considerando 47-I da proposta de Regulamento.
[323] Esta circunstância é especialmente tida em conta dada a importância em abrir os canais de comunicação – acerca da eleição ou referendo em causa – a este segmento da população, de modo a aumentar a afluência às urnas e a criar hábitos democráticos.
[324] Alteração ao considerando 47-I da proposta de Regulamento.
[325] Alteração ao considerando 47-K da proposta de Regulamento.

distribuição do material publicitário político a esse público-alvo.[326] A implementação destas limitações pretende, acima de tudo, garantir um certo grau de aleatoriedade e segurança no processo de direcionamento dos anúncios publicitários de cariz político.[327] Estas restrições são, também, implementadas com o intuito de evitar a criação de fenómenos de *echo chambers*[328], *filter bubbles*[329] ou, ainda, de casos de discriminação (nos quais se verificam "distorç[ões] demográfica[s]" em razão da raça ou do género, a título de exemplo).

Por fim, o texto da proposta de Regulamento que até então tem sido salientado, de modo a afastar eventuais acusações relativas a uma desproporcionalidade das obrigações que se pretendem ver implementadas, refere expressamente que as restrições impostas são equilibradas, uma vez que não impedem os patrocinadores de optarem por outras vias de prosseguirem o seu interesse de divulgar anúncios publicitários políticos, tais como o direcionamento baseado em informação contextual.[330]

A proposta de Regulamento defende, ainda, a legalidade das restrições impostas ao direito a "transmitir informações e ideias de interesse geral [ao público]", referindo, para o efeito, que as ditas limitações são introduzidas "de forma razoável, cuidadosa e de boa-fé" e são "proporcionada[s] e justificada[s] por razões relevantes e suficientes, em particular, para a proteção dos direitos de terceiros".[331]

4.2.3 A transparência da propaganda política

A busca por maiores níveis de transparência constitui, igualmente, um dos principais motes para o desenvolvimento deste instrumento legislativo. O conjunto de exigências estabelecidas na proposta ao nível da transparência da propaganda política assume um caráter necessário para promover um debate e processos políticos democráticos independentes e íntegros, combatendo-se,

---

[326] *Idem.*

[327] *Idem.*

[328] Fenómeno característico das redes sociais onde se verifica uma "limitação da exposição [do utilizador] a perspetivas diversas" e, consequentemente, um aumento dos níveis de "aparecimento de grupos de utilizadores, com os mesmos ideais e opiniões, que delimitam e fortalecem uma narrativa partilhada". Cfr. CINELLI, Matteo, *et al.,* "The echo chamber effect on social media", *in Proceedings of the National Academy of Sciences of the United States of America*, 2021, 118:9, p. 1.

[329] As redes sociais, de modo a aumentar os seus níveis de *engagement*, exibem aos seus utilizadores conteúdos com os quais é mais provável que eles se identifiquem pessoalmente, levando à formação dos já mencionados *echo chambers*, compostos por grupos de utilizadores que partilham opiniões e pontos de vista muito próximos. Cfr. CHITRA, Uthsav; MUSCO, Christopher, "Analyzing the Impact of Filter Bubbles on Social Network Polarization", *in Proceedings of the 13th International Conference on Web Search and Data Mining (WSDM '20)*, 2020, pp. 1 e 2.

[330] Alteração ao considerando 47-J da proposta de Regulamento.

[331] Alteração ao considerando 47-J da proposta de Regulamento.

para o efeito, as ameaças que a desinformação e as intromissões estrangeiras no campo da informação colocam[332].

A interferência por parte de países terceiros nos processos democráticos eleitorais ganha, assim, especial relevância nesta proposta de Regulamento[333]. Estas ingerências, normalmente associada a práticas de manipulação de informação e de propagação de desinformação, constituem abusos ao direito à liberdade de expressão e de informação e representam ataques diretos ao coração da democracia europeia e, à vista disso, devem ser perentoriamente contrariados todos os esforços de intromissão que utilizem a propaganda de natureza política para defraudar e degradar o ambiente informacional livre que é vivido na União[334].

Uma das medidas apontadas neste domínio reporta-se, justamente, à implementação de uma disposição que obrigue toda a propaganda política exibida na União a ser disponibilizada apenas por patrocinadores[335] que sejam cidadãos da União e a prestadores de serviços[336] que atuem em nome desses patrocinadores.[337]

Neste ponto, surge igualmente a questão da rotulação ou da colocação de avisos, também ela importantíssima para assegurar uma maior segurança no meio em linha e um maior grau de transparência no ecossistema da publicidade política. Assim, a proposta de Regulamento defende a importância de os cidadãos saberem reconhecer quando estão perante um anúncio político, em nome de quem a propaganda é veiculada e o motivo pelo qual determinado anúncio lhes está a ser direcionado[338], requisitos considerados essenciais para que estes exerçam as suas liberdades e garantias democráticas de modo consciente e informado[339].

A proposta de Regulamento estabelece, ainda, um vasto conjunto de regras de transparência em torno da preparação e divulgação da propaganda política. A título de exemplo, é referido que, quando um patrocinador indica que o anúncio publicitário que pretende disponibilizar assume uma natureza política, tal informação deve ser veiculada, atempadamente aos demais prestadores de serviços de propaganda política envolvidos[340]. Trata-se de um ato essencial para assegurar que os

---

[332] Alteração ao considerando 4 da proposta de Regulamento.
[333] Alteração ao considerando 14-C da proposta de Regulamento.
[334] Alteração ao considerando 14-C da proposta de Regulamento.
[335] «Patrocinador»: "pessoa singular ou coletiva em cujo nome um anúncio político é preparado, colocado, promovido, publicado, distribuído ou divulgado" (Alteração ao artigo 2.º, n.º 1, ponto 8., da proposta de Regulamento).
[336] «Prestador de serviços de propaganda política»: "pessoa singular ou coletiva envolvida na prestação de serviços de propaganda política, com exceção de serviços puramente auxiliares" (Alteração ao artigo 2.º, n.º 1, ponto 5-A., da proposta de Regulamento).
[337] Alteração ao considerando 14-C da proposta de Regulamento.
[338] Alteração ao considerando 4 da proposta de Regulamento.
[339] Alteração ao considerando 4 da proposta de Regulamento.
[340] Alteração ao considerando 28 da proposta de Regulamento.

prestadores de serviços podem colocar em prática todos os seus procedimentos de segurança legalmente exigidos para avaliar da conformidade do anúncio em causa, em tempo adequado.

Impende igualmente sobre os editores de propaganda política uma obrigação de garantir que, em todo e qualquer anúncio publicitário de cariz político, consta um «aviso de transparência» no qual se incluem, de forma clara e objetiva, uma série de informações relevantes, entre as quais o cariz político do anúncio, a identidade do seu patrocinador (e a entidade que controla o patrocinador, quando não correspondam à mesma pessoa), a campanha política em que está inserido, o local de estabelecimento do patrocinador, a sua natureza jurídica (pessoa singular ou coletiva), o período de divulgação do anúncio, o processo eleitoral associado ao anúncio (com informações relativas a esses processos, procedentes de *links* de fontes oficiais), os montantes dos fundos utilizados e a sua proveniência (pública ou privada / dentro ou fora da União) e, por fim, o valor de demais vantagens recebidas em troca.[341]

Para além disso, e quando se trate de um anúncio político disponibilizado com recurso a técnicas de direcionamento ou distribuição, devem constar igualmente deste aviso de transparência informações que esclareçam o utilizador relativamente aos parâmetros utilizados, à lógica por detrás deste mecanismo e outras informações relevantes, como os meios existentes para retirar o seu consentimento.[342]

O referido aviso de transparência é disponibilizado assim que o anúncio esteja pronto para divulgação e todas as informações que dele constam devem ser constantemente atualizadas.[343] Ademais, é importante garantir que, nos casos em que o anúncio seja publicado noutra plataforma ou reencaminhado por meio de mensagens privadas, tais informações de transparência acompanhem sempre o anúncio.[344]

De resto, está ainda prevista a implementação de um mecanismo – por parte dos editores de propaganda política – que permita a qualquer utilizador assinalar a natureza política de um anúncio[345], reforçando assim o controlo desta realidade.[346] A par, surge igualmente a obrigação de os editores de propaganda política criarem instrumentos de denúncia para o reporte de anúncios políticos que não cumpram com demais obrigações dispostas no Regulamento.[347]

---

[341] Alteração aos considerandos 38 e 39 da proposta de Regulamento.
[342] Alteração aos considerandos 49, 50 e 51 da proposta de Regulamento.
[343] Alteração ao considerando 39 da proposta de Regulamento.
[344] Alteração ao considerando 41 da proposta de Regulamento.
[345] Alteração ao considerando 36, da proposta de Regulamento.
[346] As informações acerca dos modos de acionar este mecanismo devem igualmente constar do aviso de transparência (alteração ao considerando 39).
[347] Alteração ao Considerando 45 da proposta de Regulamento.

Do mesmo modo, quando os prestadores de serviços de propaganda política se apercebam da existência de erros "manifestos" ou de alguma informação incompleta ou inexata, tanto na declaração de cariz político do anúncio, como na informação por si veiculada, deve ser feito um contacto ao patrocinador para que este proceda à resolução das deficiências identificadas[348].

A figura dos instrumentos de denúncia assume, de igual forma, uma especial relevância em período de eleições ou referendos e, posto isso, a proposta de Regulamento estabelece que os editores de propaganda política – no mês anterior à realização da eleição ou do referendo – deverão tratar as notificações, relativas ao processo democrático em questão, num prazo máximo de 48 horas.[349]

A proposta de Regulamento alerta que, também neste espaço temporal, qualquer violação do disposto no Regulamento deve ser interpretada como "afetando negativa e gravemente os direitos dos indivíduos" e, levando isso em consideração, o escopo do poder de supervisão das autoridades – que pode surgir na forma de um pedido de informações aos prestadores de serviços de propaganda política – sai reforçado durante este período[350]. Estas disposições demonstram, justamente, a importância das épocas mais próximas a uma dada eleição ou referendo para a formação da vontade política do eleitor e, tendo isso em conta, o texto da proposta legislativa sugere que um pedido de informações submetido no prazo referido merece uma resposta no período máximo de 48 horas, caso não se trate de micro ou pequenas empresas.[351]

É também de notar que, para além dos avanços ao nível da transparência – que se repercutem num reforço da esfera dos direitos do cidadão enquanto eleitor –, as medidas previstas favorecem, semelhantemente, uma efetiva responsabilização dos próprios representantes políticos[352], contribuindo positivamente para o debate político que se gera particularmente em altura de eleições e referendos[353].

Do mesmo modo, as obrigações até então descritas acabam por auxiliar o trabalho de supervisão realizado por terceiros, tais como investigadores, jornalistas, observadores eleitorais independentes, organizações da sociedade civil e outros profissionais dedicados ao tema.[354] A atividade desenvolvida por estas figuras, que reproduz efeitos consistentes em prol da democracia, não é esquecido na proposta legislativa e, nesse sentido, é merecedora de um apoio reforçado. Posto isto, é

---

[348] Alteração ao Considerando 28-B da proposta de Regulamento.
[349] Às micro e pequenas empresas não se aplica este prazo de 48 horas que devem, no entanto, tratar estes casos sem demoras (alteração ao considerando 45-C).
[350] Alteração ao considerando 61 da proposta de Regulamento.
[351] Alteração ao considerando 61 da proposta de Regulamento.
[352] Alteração ao considerando 39 da proposta de Regulamento.
[353] Alteração ao considerando 44 da proposta de Regulamento.
[354] Alteração aos considerandos 42-B e 46 da proposta de Regulamento.

incentivada a formulação de um conjunto de regras que promovam a partilha de informações entre os prestadores de serviços e todas as entidades anteriormente mencionadas.[355]

A proposta de regulamento prevê, ainda, um mecanismo que já se encontra, até certo ponto, previsto no RSD. Fala-se na introdução de um repositório europeu de anúncios políticos em linha, cuja peculiaridade se centra no facto deste repositório se focar em anúncios de cariz político.[356] Este mecanismo destina-se, principalmente, a apoiar os editores de propaganda política – que não configurem plataformas ou motores de pesquisa em linha de muito grande dimensão – a atuar em conformidade com as obrigações dispostas no Regulamento[357], obrigando-os, para o efeito, a garantir, no prazo de 24 horas, que a informação presente no aviso de transparência esteja igualmente acessível – num formato legível por máquina – no repositório europeu de anúncios.[358]

As plataformas ou motores de pesquisa em linha de muito grande dimensão já possuem, por sua vez, os seus próprios repositórios de anúncios e as informações neles constantes devem, por meio de uma *application programming interface* (API) comum, ser publicamente acessíveis e estar interconectadas às informações deste repositório europeu.[359]

Adiante, e dada a centralidade dos prestadores de serviços de propaganda política nesta questão, a proposta também prevê uma obrigação – que incidirá sobre estes – no sentido de se envidarem esforços para a criação e implementação de um conjunto de diretrizes de combate à colocação de propaganda política em espaços que veiculem desinformação, como parte de uma estratégia de apoio ativo à desmonetização desta[360]. No caso da propaganda política, a situação é particularmente mais perigosa e urgente, não apenas por conta do caráter influenciador da opinião pública que é associado aos anúncios de cariz político, mas também pelo facto de, no caso, a colocação de publicidade de cariz político poder transmitir alguma sensação de legitimidade ao sítio disseminador de desinformação ou, em casos mais extremos, de algum tipo de «aval» ou «aprovação» oficial, por parte de figuras ou partidos políticos, do conteúdo veiculado nesses espaços em linha.

[355] Alteração ao considerando 46 da proposta de Regulamento.
[356] Alteração ao considerando 42-C da proposta de Regulamento.
[357] Alteração ao considerando 42-C da proposta de Regulamento.
[358] *Idem.*
[359] *Idem.*
[360] Alteração ao considerando 4-A da proposta de Regulamento.

O papel complementar dos órgãos de comunicação social e das iniciativas de literacia digital

A proposta de Regulamento não deixa igualmente de relevar o papel dos órgãos de comunicação social enquanto intervenientes decisivos para a prossecução da liberdade fundamental de expressão e de informação e do direito à qualidade de órgãos propiciadores de um espaço público e livre para o debate democrático, que contribui vivamente para o esclarecimento e para a instrução do cidadão eleitor.[361] De igual modo, não é também esquecido todo o interesse associado à promoção de iniciativas na área da literacia digital, que propiciam o saudável exercício dos direitos e liberdades fundamentais, mencionados ao longo das últimas páginas, de uma forma mais responsável e informada[362].

4.2.4 Monitorização e supervisão da aplicação do Regulamento

Relativamente ao papel de supervisão da aplicação das normas estabelecidas nesta proposta de Regulamento, o mesmo é assumido pelas autoridades judiciais ou administrativas nacionais nomeadas para o efeito (nomeação essa que, dada a similitude das matérias tratadas, deve ser feita em consonância com as autoridades já adstritas à supervisão do RGPD e do RSD), cuja independência e suficiência (ao nível de recursos humanos e financeiros) deve, desde logo e como em qualquer cargo de supervisão, ser assegurada.[363]

Para além do exposto, torna-se essencial o desenvolvimento de um quadro sancionatório em vista ao controlo do alojamento da publicidade política, sendo importante o estabelecimento de sanções numa perspetiva ampla e incisiva. A União Europeia, idealmente em articulação com os seus parceiros internacionais, deve impor sanções financeiras àqueles que empregam atos contra a democracia, na existência de provas da prática de tais comportamentos. O processo de implementação das ditas sanções deve, por esse motivo, ser meticulosamente acompanhado de forma a evitar o subterfúgio do efeito útil das mesmas[364]. A União já admitiu expressamente, na sua Comunicação "Garantir eleições europeias livres e justas", a possibilidade de impor sanções a todos aqueles que

[361] Alteração ao considerando 19 da proposta de Regulamento.
[362] Alteração ao considerando 19-A da proposta de Regulamento.
[363] Alteração aos considerandos 56, 57 e 58 da proposta de Regulamento.
[364] A criação de empresas de fachada, a título de exemplo, corresponde a um tipo de meios que pode, facilmente, comprometer os objetivos prosseguidos pelas sanções. Cfr. POLYAKOVA, Alina; FRIED, Daniel, p. 8.

empreguem atos premeditados conducentes à criação de um clima de deturpação em torno de eleições.[365]

À vista disso, a violação das disposições previstas no Regulamento pode, por seu turno, resultar na aplicação de coimas ou sanções financeiras, como sanções pecuniárias compulsórias.[366]

4.3 O Código de Conduta Reforçado em matéria de Desinformação de 2022

O desenvolvimento de instrumentos de auto e corregulação vocacionados para a problemática da disseminação de desinformação prende-se, em larga medida, por uma tentativa de não interferência direta do poder público na criação de soluções para o fenómeno, dada a particular sensibilidade da questão para com direitos fundamentais[367]. Nesse sentido, e tendo em conta que as grandes plataformas digitais e outros atores privados assumem um grande papel na disseminação de desinformação, a criação de códigos de conduta é vista como um incentivo de caráter voluntário ao desenvolvimento de normas de combate a este fenómeno[368].

A redação do primeiro Código de Conduta neste domínio, datado de 2018, revelou a intenção das Instituições Europeias em combater a problemática da desinformação, servindo esta versão como uma espécie de «campo de ensaio» para o propósito. O RSD e a proposta de Regulamento sobre a transparência e direcionamento da propaganda política seguiram-lhe e correspondem aos dois primeiros grandes instrumentos regulatórios a abordar mais expressamente o fenómeno, sendo que o Código de Conduta Reforçado em matéria de Desinformação de 2022 se apresenta, neste meio, como um instrumento complementar essencial para levar mais longe as bases daquelas pretensões legislativas.

Assim, o Código de 2022 – como será em diante denominado – apresenta-se como o sucessor do Código de 2018 e surge por força da necessidade de criar um corpo normativo mais eficiente e eficaz na luta contra a disseminação de desinformação[369].

---

[365] *Comunicação: Garantir eleições europeias livres e justas*, p. 2

[366] Alteração aos considerandos 63 e 63-A da proposta de Regulamento.

[367] ALAPHILIPPE, Alexander, *et al.*, p. 58.

[368] ALAPHILIPPE, Alexander, *et al.*, p. 58.

[369] Código de Conduta Reforçado em matéria de Desinformação de 2022, capítulo I, parágrafo e); A este propósito, Cfr. também PLASILOVA, Iva, et al., *Study for the "Assessment of the implementation of the Code of Practice on Disinformation"*, Serviço das Publicações da União Europeia, 2020, pp. 96-100, ERGA, *Report on disinformation: Assessment of the implementation of the Code of Practice*, 2020, pp. 46-53 e Comissão Europeia, *Avaliação do Código de Conduta sobre Desinformação - Resultados e domínios a melhorar*, SWD(2020) 180 final, 2020, que deriva de uma análise dos dois estudos anteriormente mencionados.

O Código de 2022, tal como as restantes tentativas elaboradas para combater o fenómeno da desinformação, procura estabelecer um equilíbrio entre a proteção dos direitos fundamentais tipicamente mais afetados por iniciativas desta natureza e o interesse público de formar cidadãos mais bem informados sobre os temas de maior relevância social, tornando-os mais aptos a tomar as suas decisões políticas esclarecidamente.[370] Da mesma forma, a proteção da legitimidade e da liberdade inerente aos processos eleitorais democráticos constituem valores que também se encontram em perigo face a esta ameaça e devem, por isso, ser preservados.[371]

Levando em consideração todo o enquadramento legislativo em que o Código de 2022 foi desenvolvido, o mesmo irá funcionar paralela e complementarmente ao RSD, em particular, ao abrigo do seu artigo 45.º[372].

Neste seguimento, o RSD prevê no seu texto legal um modelo "que envolve e corresponsabiliza vários intervenientes"[373], modelo esse que é também baseado em códigos de conduta que apoiam a resposta aos principais riscos levantados pela atividade das grandes plataformas e motores de pesquisa em linha no domínio da disseminação de desinformação.[374] A adesão destes ao Código de 2022 – e a consequente implementação dos compromissos nele assumidos – representa, de acordo com os artigos 34.º e 35.º do RSD, uma das várias medidas de atenuação de riscos sistémicos e, consequentemente, um quadro normativo que responsabiliza mais eficiente e abrangentemente os grandes serviços digitais[375], constituindo, por isso, uma das ferramentas essenciais no combate ao fenómeno da manipulação de informação.

Como se observou, o modelo previsto no RSD assenta num acompanhamento sobre o modo como as plataformas e motores de pesquisa em linha de muito grande dimensão irão assumir os seus novos papéis de destaque ao abrigo desse diploma[376] e, nas palavras da Provedora de Justiça, "as plataformas mantêm o controlo, mas passam a estar sujeitas a obrigações harmonizadas de devida diligência"[377]. Este modelo de corregulação é, precisamente, complementado pelo Código de 2022[378], constituindo-se a opção mais acertada e eficaz para os momentos que correm, dado, por um lado, a natureza rapidamente mutável da base que se procura «regular» e acautelar[379] e, por outro, a

[370] Código de 2022, capítulo I, parágrafo b).
[371] Código de 2022, capítulo I, parágrafo b);
[372] Código de 2022, capítulo I, parágrafo h) e i);
[373] AMARAL, Maria Lúcia, parágrafo 14.
[374] AMARAL, Maria Lúcia, parágrafo 10.
[375] AMARAL, Maria Lúcia, parágrafo 5.
[376] AMARAL, Maria Lúcia, parágrafo 11.
[377] AMARAL, Maria Lúcia, parágrafo 11.
[378] AMARAL, Maria Lúcia, parágrafo 12.
[379] AMARAL, Maria Lúcia, parágrafo 14.

preocupação constitucional em "dispersar os mecanismos de controlo pelos vários atores envolvidos"[380].

O Código de 2022 prevê, assim, um conjunto de compromissos aos quais se juntam as medidas consideradas necessárias para viabilizar o cumprimento dos mesmos e, representado a monitorização da efetividade das medidas previstas no Código de 2022 um aspeto central para o sucesso desta abordagem, serão introduzidos, no seio de cada medida, uma série de elementos de reporte qualitativo (QRE's) e de indicadores de nível de serviço (SLI's).[381] Estes QRE's[382] e SLI's[383] permitirão, desta forma, um acompanhamento mais próximo de todos os progressos alcançados pelos signatários.[384]

Por fim, o Código de 2022 conta já com vários signatários de relevo, como o TikTok, a Meta, a Microsoft, a Google, a Twitch, a Adobe, a Federação Mundial de Anunciantes (WFA) ou a Rede Europeia de Normas de Verificação de Factos (EFCSN), todos eles parte de um importantíssimo esforço para garantir o mais amplo cumprimento das suas disposições.

As áreas de atuação

Os compromissos estabelecidos no Código de 2022 encontram-se inseridos num conjunto de capítulos que o dividem estruturalmente e refletem os objetivos a prosseguir pelos signatários. As medidas previstas no Código de 2022 retratam um total de 9 capítulos que enumeram as principais áreas de atuação: «Escrutínio na colocação de anúncios»; «Propaganda política»; «Integridade dos serviços»; «Capacitação dos utilizadores»; «Capacitação da comunidade de investigação»; «Capacitação da comunidade de verificação de factos»; «Centro de transparência»; e «Monitorização do código».[385]

Ao longo dos próximos subcapítulos realizar-se-á um desenvolvimento dos principais compromissos – e das suas respetivas medidas – incluídos em cada um dos capítulos norteadores do plano de combate à desinformação estabelecido no Código de 2022.

---

[380] AMARAL, Maria Lúcia, parágrafo 14.

[381] A questão do acompanhamento e monitorização dos efeitos da aplicação do Código de 2018 representa uma das insuficiências apontadas, que agora se procura colmatar.

[382] Os QRE's correspondem à descrição dos mecanismos introduzidos para levar o cumprimento de um determinado compromisso a bom-porto, bem como o seu modo de implementação nos vários Estados-Membros.

[383] Os SLI's correspondem, por seu turno, ao conjunto de dados que exprimem, quantitativamente, informações sobre uma determinada realidade relevante para a prossecução do compromisso em causa.

[384] Código de 2022, capítulo I, parágrafo o);

[385] Sobre este assunto, Cfr. também PEREIRA, Miguel, "A trial run for the EU's coregulatory approach: the Strengthened Code of Practice on Disinformation", *in Official Blog of UNIO – EU Law Journal*, 2022. Disponível em: <https://officialblogofunio.com/2022/07/15/a-trial-run-for-the-eus-co-regulatory-approach-the strengthened-code-of-practice-on-disinformation/> [08/09/2022]

4.3.1 Escrutínio na colocação de anúncios

O primeiro capítulo provido de compromissos e medidas específicas ocupa-se da temática do escrutínio da colocação de anúncios, absolutamente central para a redução e extinção das avenidas de monetização ao dispor dos disseminadores de desinformação[386].

A propagação de conteúdo de caráter (des)informador, para além de constituir uma ferramenta com uma capacidade extrema para manipular a opinião pública[387], pode igualmente representar uma atividade bastante lucrativa economicamente, por conta da monetização publicitária auferida pelos agentes mal-intencionados[388]. Por conseguinte, o conjunto de linhas orientadoras que se propõe de seguida assenta num composto de princípios aplicados de forma equitativa, coerente, transparente e, principalmente, politicamente imparcial,[389] que procura, deste modo, desmontar os elementos que tornam o negócio da proliferação de mentiras tão atrativo do ponto de vista económico.

Posto isto, o trabalho desenvolvido neste parâmetro deve, primeiramente e sob pena de se frustrar o efeito útil pretendido, juntar todas as figuras relevantes na cadeia de valor da colocação de anúncios, desde agências de publicidade às plataformas e motores de pesquisa em linha, sem esquecer os organismos de controlo e as empresas que desenvolvem tecnologia para este meio. [390]

A reunião de esforços no sentido de impedir, por um lado, a colocação de anúncios propagadores de desinformação e, por outro, a colocação de anúncios publicitários em páginas onde é disseminada desinformação, assume-se, assim, como ponto essencial neste domínio para eliminar o ganho económico associado a esta realidade, dissuadindo quem considere enveredar por esta via enriquecimento.[391]

Mecanismos de escrutínio e verificação prévia de identidade

A implementação de critérios mais rigorosos para a monetização de conteúdo publicitário é, assim, uma necessidade e, posto isto, a realização de extensivos *background checks* às partes envolvidas deve constituir, desde logo, prática recorrente.[392]

---

[386] Código de 2022, capítulo II, parágrafo a).
[387] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 5.
[388] *Comunicação: Garantir eleições europeias livres e justas*, p. 6; Grupo de Peritos em notícias falsas e na desinformação em linha, p. 15.
[389] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 20.
[390] O Código de 2022, capítulo II, parágrafo b).
[391] O Código de 2022, capítulo II, parágrafo b).
[392] O Código de 2022, capítulo II, medida 1.2.

As preocupações relacionadas com a identidade dos patrocinadores e prestadores de serviços de propaganda política e publicidade temática[393] devem assumir uma relevância central no combate à disseminação de desinformação neste meio e, posto isso, o Código de 2022 pugna pela implementação de um mecanismo transparente de escrutínio e verificação prévia da identidade daqueles que pretendem distribuir propaganda política ou temática no meio em linha.[394]

Neste âmbito, o estabelecimento de pontos de contacto próximo e de centros de discussão, entre os vários signatários relevantes, afigura-se essencial para o acompanhamento das principais tendências no campo da desinformação e, nesse domínio, o debate sobre as principais TTP's (Táticas, Técnicas e Procedimentos)[395] utilizadas pelos intervenientes mal-intencionados é crucial para um seguimento vigilante da evolução das práticas associadas à disseminação de desinformação na esfera dos anúncios publicitários e para a consequente supressão dos seus efeitos negativos.[396] A troca de informações e de melhores práticas representa, assim, uma grande contribuição para o combate a esta problemática, uma vez que diferentes signatários cobrem diferentes segmentos da indústria e apenas uma cooperação globalizante e holística poderá resultar numa resposta mais eficaz e frutífera a todas as fontes de ameaça.[397]

4.3.2 Propaganda política

O segundo capítulo ocupa-se, por seu turno, de uma área intimamente ligada aos conteúdos do capítulo anterior, que se desdobrou sobre a questão da colocação de anúncios, entre os quais – naturalmente – os de caráter político. No presente capítulo proceder-se-á, portanto, a um aprofundamento das questões relacionadas com os graus de transparência que os anúncios publicitários desta natureza, especialmente sensíveis para o normal decorrer da vida democrática, merecem.[398]

A questão do direcionamento e da distribuição de propaganda política é, uma vez mais, tema central nesta matéria, tendo em conta todos os receios que o uso indevido dessas técnicas pode levantar para o exercício dos direitos fundamentais do cidadão eleitor.

---

[393] Não foi alcançado, ainda, um consenso abrangente sobre uma definição de «publicidade temática», no entanto, na página 10 das *Orientações da Comissão Europeia relativas ao reforço do Código de Conduta sobre Desinformação* (COM(2021) 262 final), é referido que a publicidade temática se poderá reportar a "conteúdos patrocinados relativos a questões societais ou ligadas a um debate de interesse geral que pode influenciar o discurso público", constituindo exemplos "as alterações climáticas, questões ambientais, a imigração ou a COVID-19".

[394] O Código de 2022, capítulo III, compromisso 7.

[395] A este propósito, Cfr. também GRAY, John F.; TERP, Sara-Jayne, *Misinformation: We're Four Steps Behind Its Creators*, 2019.

[396] O Código de 2022, capítulo II, medida 3.2.

[397] O Código de 2022, capítulo II, compromisso 3 e medida 3.1.

[398] O Código de 2022, capítulo III, parágrafo a).

As medidas expostas no Código de 2022 alinham-se, por isso, intensamente com o que já se encontra definido, tanto no RSD, como na proposta de Regulamento relativa à transparência e direcionamento da propaganda política. A este propósito, será de fazer uma remissão expressa para os instrumentos legislativos já analisados, levando em consideração que a reiteração de alguns dos meios de atuação é apenas reveladora do caráter central e medular que algumas medidas representam, neste domínio, para a política europeia de combate à desinformação[399].

Adiante, e para além da assunção de compromissos relacionados com uma maior preocupação ao nível da investigação e da supervisão das principais ameaças ligadas à indústria da propaganda política e publicidade temática[400], é equacionada, também pelo Código de 2022, uma análise das vantagens da introdução de períodos limitados de *blackout*, em momentos especificamente críticos de um dado período eleitoral, exclusivamente aplicáveis aos anúncios publicitários de natureza política ou temática.[401]

A propósito, seria importante efetuar, neste momento, uma pequena menção à figura do «dia de reflexão», em jeito de analogia. Embora a figura tenha, no meio em linha, pouca ou nenhuma expressão, dado o papel e a centralidade de determinados serviços digitais para a democracia e para o quotidiano de todos os europeus, seria de equacionar uma medida semelhante à exposta no parágrafo anterior. O intuito seria, naturalmente, muito próximo ao do «dia de reflexão», por todos nós já conhecido, isto é, um espaço temporal que favoreça uma tomada de decisão mais informada e abstraída de toda a tensão e divisão que mais vem ao de cima durante o período eleitoral.

4.3.3 Integridade dos serviços

No domínio deste capítulo, uma das principais inquietações encontra-se relacionada com a garantia da integridade dos serviços em linha face aos chamados «comportamentos e práticas de manipulação não permitidos»[402], que causam perturbações ao funcionamento daqueles. [403]

De forma a limitar a ocorrência deste tipo de comportamentos e práticas, é proposta a criação de uma lista abrangente dos mesmos, regularmente atualizada com base nas TTP's que se encontram, em determinado momento, a causar um maior grau de disrupção nos fluxos de informação.[404]

---

[399] O Código de 2022, capítulo III, compromisso 10.
[400] O Código de 2022, capítulo III, compromissos 12 e 13.
[401] O Código de 2022, capítulo III, medida 13.2.
[402] O Código de 2022, capítulo IV, parágrafo (b).
[403] O Código de 2022, capítulo IV, parágrafo (a).
[404] O Código de 2022, capítulo IV, parágrafo (d).

Neste âmbito, o Código de 2022 avança, desde logo, com uma lista provisória que inclui várias realidades: a «criação e utilização de contas falsas», «tomadas de controlo de conta» («*account takeovers*»), «amplificação por meio do uso de *bots*», «operações de *hack-and-leak*» (acesso indevido a informação confidencial e sua posterior disponibilização ao público[405]), a «falsificação de identidade», «*deep fakes* maliciosos», a «compra de falsos *engagements*», a «falta de transparência em mensagens patrocinadas ou em promoção feita por *influencers*», a «criação e uso de contas para comportamentos coordenados inautênticos» e a «amplificação artificial do alcance ou da perceção do apoio público pela desinformação».[406]

Neste âmbito, surge uma preocupação especial relacionada com os signatários que criem ou trabalhem com sistemas de IA e que exibam conteúdo gerado e manipulado por IA nos seus serviços – ex.: *deepfakes*. A perigosidade que resulta da manipulação deste conteúdo força o Código de 2022 a prever algumas obrigações relativamente aos signatários que atuem nesta vertente, instando-os a desenvolver um conjunto de políticas que pugnem pela transparência e combatam a utilização abusiva e condenável desses sistemas de IA, sendo que o incentivo ao desenvolvimento de avançados algoritmos para a deteção deste tipo de comportamentos, no respeito pelos direitos do utilizador, representa uma das principais vias de enfraquecimento da ameaça.[407]

Paralelamente à identificação dos principais comportamentos e práticas de manipulação não autorizados, é necessária, então, uma atuação que vá no sentido da criação e implementação de políticas eficazes de combate à sua manifestação nos serviços e, consequentemente, será indispensável proceder a uma apreciação aprofundada dos impactos destas junto da base de utilizadores.[408]

Para terminar, o estabelecimento de pontos de contacto entre os signatários mais relevantes – na forma de um subgrupo no âmbito do Grupo de Trabalho Permanente (que será analisado adiante), a título de exemplo – representa, de igual modo, um passo essencial para fomentar uma conveniente troca de informações[409] sobre vários assuntos, como operações de influência ou interferências estrangeiras no espaço da informação, e sobre melhores práticas, tais como os mais corretos modelos

---

[405] SHIRES, James, *The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and US Politics (Fall 2020)*, Texas National Security Review, 2020, p. 12.
[406] O Código de 2022, capítulo IV, compromisso 14.
[407] O Código de 2022, capítulo IV, medidas 15.1 e 15.2.
[408] O Código de 2022, capítulo IV, medida 14.3.
[409] A propósito, a análise de «migrações táticas» entre plataformas é importantíssima a este respeito e constitui um exemplo prático da relevância do estabelecimento de laços de cooperação nesta área (Código de 2022, capítulo IV, medida 16.2.).

de atuação perante uma ameaça concreta.[410] Um elevado grau de coordenação e comunicação a este nível é essencial para vigiar, controlar e limitar a propagação de vetores de risco a outras plataformas, face aos frequentes fenómenos de "migração tática" empregues por agentes mal-intencionados que constituem canais de disseminação de desinformação profundamente impactantes.[411]

4.3.4 Capacitação dos utilizadores

O quinto capítulo do Código de 2022 coloca em destaque a importância da capacitação dos utilizadores enquanto dispositivo de luta contra a disseminação de desinformação. É neste campo que surge, justamente, uma miríade de medidas destinadas a tornar a navegação do utilizador comum mais segura, informada, integrada e responsável.

Mecanismos de denúncia

Dada a centralidade do utilizador no mundo digital atual, é elementar a arquitetação de serviços em linha assentes na disponibilização de ferramentas, acessíveis e eficazes, que permitam a deteção e a denúncia de conteúdo de desinformação.

Neste domínio, é também importante acautelar os possíveis perigos associados a estes mecanismos e, tendo isso em conta, é importante não esquecer, por um lado, a criação de provisões que procurem evitar situações de abuso dos mesmos – tais como as que se verificam em casos de «denúncias em massa» para silenciar pessoas – e, por outro, a conceção de meios de recurso inclusivos e eficientes que assegurem atempadamente a tutela dos direitos daqueles que são afetados por sanções, tais como o *downranking* ou a rotulação de conteúdo.[412]

Ferramentas de proveniência, fact-checking e rotulação

Neste seguimento, é também enfatizado o desenvolvimento de mecanismos que permitam ao utilizador comum aferir da proveniência, autenticidade e exatidão do conteúdo que lhe é exibido, de modo que este consiga controlar, interrogar e refletir sobre as perspetivas que lhe são apresentadas.[413]

---

[410] O Código de 2022, capítulo IV, compromisso 16.
[411] O Código de 2022, capítulo IV, compromisso 16.
[412] O Código de 2022, capítulo V, compromisso 24.
[413] O Código de 2022, capítulo V, parágrafo (b) e (f).

Aqui, será relevante mencionar a alocação de espaços visuais ao trabalho desenvolvido por verificadores de factos e outras figuras de fiabilidade reconhecida, que auxiliarão – especialmente em situações de crise ou de proteção de algum interesse público em específico[414] – o utilizador a tomar decisões de um modo mais informado nos momentos em que tal se afigura mais relevante.

A este propósito e a título de exemplo, seria positiva a introdução de rótulos com *ratings* – fornecidos por organizações de verificação de factos – sobre a qualidade, fidedignidade e isenção do conteúdo e da fonte em questão. Por seu turno, num momento pospositivo, a emissão de uma notificação-alerta de que o utilizador interagiu com conteúdo que foi posteriormente rotulado como constituindo desinformação[415], representa uma medida de atuação equitativamente importante e que, por isso, não deve ser esquecida.

A utilização de rótulos – aplicados a publicações, perfis e comunidades[416] e informados por indicadores de confiança e transparência amplamente reconhecidos e discutidos[417] – surge, precisamente, como um meio facilitador da leitura do conteúdo noticioso apresentado, funcionando como uma espécie de "guia norteador" sobre o tipo de informação que reúne os mais elevados graus de confiança.[418]

Com isso em mente, seria igualmente importante que, por uma questão de transparência, todos os órgãos de comunicação social com perfis que se dediquem à difusão de notícias nos canais digitais, fossem obrigados a revelar, de forma explícita, a informação de registo necessária para que os utilizadores possam saber quem se encontra por detrás da página que distribui elementos noticiosos. No caso português, a indicação do seu número de registo, junto da ERC, seria uma relevante contribuição para o utilizador poder selecionar com mais segurança as suas fontes de informação.

Neste âmbito, será ainda de mencionar uma abordagem muito interessante à problemática, refletora de uma verdadeira capacitação dos utilizadores neste contexto.[419] A iniciativa *Community Notes*, desenvolvida pelo X (ex-Twitter) – que infelizmente abandonou recentemente o Código Reforçado[420]–, permite que os próprios utilizadores se registem para serem, eles mesmos, uma espécie de verificadores de factos na plataforma. Se diferentes utilizadores, registados como contribuidores,

---

[414] O Código de 2022, capítulo V, medida 22.7.
[415] O Código de 2022, capítulo V, parágrafo (f).
[416] ALAPHILIPPE, Alexander, *et al.*, p. 14.
[417] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 7.
[418] POLYAKOVA, Alina; FRIED, Daniel, p. 11.
[419] X - Central de Ajuda, *Sobre as Notas da Comunidade no X*, (não datado). Disponível em: <https://help.twitter.com/pt/using-x/community-notes> [06/08/2023]
[420] BBC News, *Twitter pulls out of voluntary EU disinformation code*, 2023. Disponível em: https://www.bbc.com/news/world-europe-65733969 [12/08/2023].

considerarem que uma determinada *«note»* – previamente adicionada por um contribuidor – é útil para uma compreensão mais adequada e contextualizada de um *tweet*, a nota de explicação irá acompanhar o *tweet* sempre que este surja no *feed* de todos os utilizadores[421]. Para além disso, a companhia indica que as *Community Notes* "não representam o ponto de vista do Twitter" e que as suas informações "não podem ser editadas ou modificadas" pelo seu pessoal[422]. Por fim, é ainda referido que os *tweets*, com *Community Notes* acoplados, nunca serão "rotulados, removidos ou tratados pelo Twitter", a menos, claro está, que o mesmo viole as regras de utilização da plataforma[423].

Claro está também que qualquer ação no sentido de implementar mecanismos de rótulos de classificação do conteúdo em linha se deve alicerçar num método lógico, bem estruturado, garantístico, continuamente apreciado e fruto de deliberações abrangentes entre entidades das mais variadas naturezas, como jornalistas, órgãos de comunicação social, especialistas em literacia digital, profissionais de organizações da sociedade civil (ligadas à área do direito à liberdade de expressão, por exemplo), investigadores e académicos, organizações de verificação de factos e figuras da indústria da publicidade e do mundo das plataformas e motores de pesquisa em linha.[424]

Literacia Mediática Digital

(Ainda que o Código de 2022 tenha, e bem, mencionado esta questão no âmbito do domínio das estratégias de capacitação do utilizador, tal menção, face à sua importância no plano geral de combate à desinformação, é insuficiente e, nesse sentido, este subcapítulo será também utilizado para desenvolver o tema com alguma profundidade.)

A área da literacia mediática digital constitui, possivelmente, aquela que poderá, de modo mais eficaz, causar uma redução dos efeitos negativos da propagação de desinformação e, nesse sentido, a educação e sensibilização do público para a temática deve ser, também ela, abrangente e multifacetada para fazer face à complexa teia de ameaças que o fenómeno atualmente representa.

A aposta efetiva na formação sobre estes temas é crucial para auxiliar os utilizadores a examinar de forma mais ponderada, crítica e autónoma o ambiente noticioso que os rodeia[425],

---

[421] X - Central de Ajuda, *Sobre as Notas da Comunidade no X*.
[422] *Idem.*
[423] *Idem.*
[424] O Código de 2022, capítulo V, medidas 22.1, 22.4. e 22.5.
[425] MORGAN, Susan, p. 43.

particularmente em situações de maior relevância, como eleições ou momentos de crise.[426] Muitos autores consideram, mesmo, que a literacia digital deve constituir a "força motriz" de toda a resposta a esta problemática[427], dado o caráter preventivo – e não reativo – das medidas adotadas neste campo, que permitem a criação de soluções com resultados observáveis a longo prazo[428].

De igual forma, é salientado, tanto no Plano de Ação para os Media, como no Plano de Ação para a Educação Digital 2021-2027, a importância da promoção de competências no sentido de "absorver, filtrar e avaliar as informações numa perspetiva crítica, nomeadamente para identificar a desinformação", de modo a garantir uma "participação efetiva na sociedade e nos processos democráticos, especialmente no caso dos jovens".[429]

Para o efeito, a definição de «literacia mediática» encontra-se plasmada na Diretiva Serviços de Comunicação Social Audiovisual e reporta-se "às competências, aos conhecimentos e à compreensão que permitem aos cidadãos utilizar os meios de comunicação social de forma eficaz e segura"[430]. Para além de fornecer uma definição, a Diretiva também estabelece uma obrigação geral sobre os Estados-Membros, instando-os a adotar medidas que promovam este conjunto de conhecimentos junto das populações, reconhecendo, desde logo, as suas vantagens neste domínio.[431]

A este propósito, vale igualmente relembrar que a deteção e combate ao conteúdo de desinformação constitui, por vezes, um processo complicado e pouco profícuo, tornando ainda mais substancial a promoção de iniciativas neste âmbito.[432] As próprias plataformas digitais, cientes do seu papel influenciador em toda esta questão e das potencialidades que os avanços técnico-informáticos propiciam ao fenómeno da desinformação, devem, por esse motivo, contribuir no sentido de apoiar uma navegação mais responsável e segura dos utilizadores nos seus serviços[433]. Nesta esteira, também no âmbito da Diretiva Serviços de Comunicação Audiovisual, encontra-se prevista uma obrigação onde é indicado que os serviços de plataformas de partilha de vídeos (Youtube, Facebook, Instagram, TikTok,

---

[426] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 22; *Comunicação: Combater a desinformação em linha: uma estratégia europeia*. pp. 14 e 20; *Special Report: Disinformation affecting the EU: tackled but not tamed*, p. 13.

[427] POLYAKOVA, Alina; FRIED, Daniel, p. 13.

[428] *Special Report: Disinformation affecting the EU: tackled but not tamed*, p. 13.

[429] Comissão Europeia, *Plano de Ação para a Educação Digital 2021-2027: Reconfigurar a educação e a formação para a era digital*, COM(2020) 624 final, 2020, p. 15. Neste sentido, Cfr. também COOK, John; ECKER, Ullrich; LEWANDOWSKY, Stephan, "Misinformation and How to Correct It", *in Emerging trends in the social and behavioral sciences: An interdisciplinary, searchable, and linkable resource*, 2015, pp. 6 e 7.

[430] Comissão Europeia, Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que altera a Diretiva 2010/13/UE relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual), para a adaptar à evolução das realidades do mercado, 2018, considerando 59.

[431] Diretiva (UE) 2018/1808, artigo 33.º-A; *Special Report: Disinformation affecting the EU: tackled but not tamed*, p. 35.

[432] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 26.

[433] *Relatório da Comissão sobre a aplicação da Comunicação «Combater a desinformação em linha: uma estratégia europeia»*, pp. 10 e 11.

X, etc.) devem "prever medidas e instrumentos eficazes em matéria de literacia mediática e sensibilizar os utilizadores para essas medidas e instrumentos"[434].

A concertação de esforços – dirigidos a todas as camadas demográficas – irá, ulteriormente, resultar num fortalecimento dos níveis de resiliência da sociedade contra a desinformação e os desafios futuros que esta levantará, uma vez que o conteúdo falso e enganador apenas causa danos se os próprios cidadãos lhe derem voz e tomarem decisões na vida pública democrática com base nos mesmos[435]. A força e o caráter único das políticas orientadas para a promoção de conhecimentos nesta área residem, justamente, no facto de os próprios cidadãos representarem os principais amplificadores de desinformação e, à vista disso, o processo de transformação, de uma sociedade que amplifica este tipo de conteúdo, numa que está atenta e combate ativamente o fenómeno, configura o principal trunfo ao nosso dispor e é, por esse motivo, fulcral aprofundar as opções existentes neste domínio[436].

De modo que este processo de transformação societal conceba os seus frutos é igualmente necessário que o lançamento de projetos nesta área assente numa transmissão de conhecimentos firmada numa vertente mais utilitária, vibrante e dinâmica, tornando mais apelativa a apreensão de todas as informações[437]. Para além disso, uma aposta musculada nesta esfera acaba por produzir mudanças em domínios colaterais, uma vez que, a título de exemplo, populações mais formadas e mais conscientes no ambiente digital demandam a disponibilização de serviços com mais qualidade por parte dos media, obrigando estes últimos a investir mais na excelência dos respetivos conteúdos.[438]

É, então, indispensável apostar num alargado e profundo plano formativo que contribua para uma consciente participação no debate público em linha, debate esse que se desenrola, ainda, num terreno fértil para o florescimento de narrativas falsas e enganadoras[439] que levam ao agravamento dos níveis de polarização e de tensões sociais pré-existentes.[440]

Neste âmbito, surge um conjunto de medidas que deve ser levado a cabo para sensibilizar as populações sobre esta temática, como a partilha de conhecimentos sobre as principais TTP's utilizadas[441], as estratégias de persuasão empregues e seus principais sinais de alerta, e sobre os

---

[434] Comissão Europeia, Diretiva 2010/13/UE do Parlamento Europeu e do Conselho de 10 de Março de 2010 relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva «Serviços de Comunicação Social Audiovisual»), artigo 28.º-B, n.º 3, alínea j).
[435] Grupo de Peritos em notícias falsas e na desinformação em linha (2018), pp. 11, 25 e 26.
[436] ALAPHILIPPE, Alexander, *et al.*, p. 50.
[437] *Plano de Ação contra a Desinformação*, p. 12.
[438] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 25.
[439] Grupo de Peritos em notícias falsas e na desinformação em linha, p. 11.
[440] PROKOPOVIĆ, Anka Mihajlov; VUJOVIĆ, Marija, p. 181.
[441] O Código de 2022, capítulo V, parágrafo (c) e medidas 17.1. e 17.2.

móveis e as ações de financiamento que suportam estas atividades, sem esquecer a divulgação de guias de auxílio ao correto julgamento do conteúdo consumido em linha[442].

O melhor antídoto para a problemática da desinformação reside, assim, numa sociedade resiliente e sensibilizada para os principais perigos associados a este fenómeno, pois apenas um coletivo que reúne estes dois critérios será eficaz no bloqueio de investidas que apenas pretendem fomentar, de forma artificial, um clima generalizado de desconfiança e ambiguidade.[443]

A visibilidade de conteúdo confiável produzido pelo jornalismo de excelência

Todo o tipo de ações empreendidas com o intuito de promover, por um lado, uma diminuição da preponderância ao nível da exibição de desinformação e, por outro, um aumento na facilidade de acesso a conteúdo de fontes confiáveis – que adotam os mais elevados padrões da excelência jornalística – representam medidas determinantes para o apoio a uma navegação mais segura e informada do utilizador.[444]

Posto isto, a prossecução dos ditos objetivos deve passar pela própria conceção dos sistemas de recomendação, de modo que estes sugiram, de um modo mais frequente e transparente, conteúdo que respeite os requisitos editoriais descritos anteriormente.[445] Torna-se, assim, crítico alertar para a importância de atribuir uma maior preponderância ao conteúdo de qualidade resultante de uma boa prática jornalística, que expõe o utilizador aos múltiplos pontos de vista existentes, pois só assim se cumprirá da forma mais plena a verdadeira função de informar o público.

Os algoritmos que influenciam o *ranking* e o modo como acedemos à informação noticiosa em linha detêm, como vimos, a capacidade de moldar e influenciar a nossa compreensão do mundo e, nesse sentido, grandes alterações neste quesito devem ser sempre anunciadas de forma antecipada e transparente para que todos possam avaliar o impacto de eventuais alterações no domínio da distribuição e classificação de conteúdo.[446]

É também essencial que o utilizador consiga compreender facilmente os motivos pelos quais o seu *feed* de notícias, ou os resultados da sua pesquisa, se encontram ordenados e classificados de

[442] O Código de 2022, capítulo V, parágrafo (c) e medidas 17.1. e 17.2.
[443] *Relatório conjunto relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*, p. 6.
[444] O Código de 2022, capítulo V, parágrafo (a).
[445] O Código de 2022, capítulo V, medida 18.1.
[446] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 16 e 17.

determinado modo, de forma a evitar que se gere um sentimento de suspeita em redor destas práticas.[447]

Por seu turno, o adequado, coerente e desambiguado delineamento prático e conceitual dos indicadores de transparência – que irão informar e definir os critérios para a classificação do conteúdo (e das fontes) como sendo «de confiança», «isento», «rigoroso», «transparente», ou «de acordo com as práticas jornalísticas reconhecidas» – é essencial para uma boa implementação dos mecanismos de priorização de conteúdo[448] e, como também já foi observado, a respetiva concretização de todos estes pontos encontra-se, naturalmente, dependente de uma ampla cooperação e do estabelecimento de um alargado consenso entre os mais variados *stakeholders*.[449]

É, ainda, absolutamente crítico assegurar que a classificação algorítmica do conteúdo que organiza a experiência do utilizador não se encontre apenas entregue a algoritmos, uma vez que estes, por vezes, cometem erros e, em situações de especial relevância e gravidade, é importantíssimo prever algum tipo de observação e vigilância humana que favoreça uma disposição de conteúdos propiciadora da diversidade, da exatidão e da sustentação sólida[450].

Ainda neste domínio, o Código de 2022 procede a uma menção às situações onde o *downranking*, ou a simples não recomendação, constituem atitudes sancionatórias consideradas insuficientes face à gravidade de determinada situação. Assim, nos casos mais extremos – e como já foi mencionado – pode recorrer-se a uma proibição da partilha de "informações falsas nocivas ou enganosas", quando se verifique um determinado grau de "severidade" nas repercussões causadas, reservando-se, para o efeito, especial atenção às consequências para a esfera do direito à liberdade de expressão dos visados.[451]

Relativamente a este ponto, afigura-se imperativo ir ao encontro do princípio-base da não proibição da desinformação. Este deve ser o caminho a seguir, não apenas por uma questão de proteção dos princípios democráticos e dos direitos fundamentais, mas também como meio de consciencializar o público de que a ameaça existe e de que somos confrontados com ela mais frequentemente do que o que poderíamos imaginar. Ainda assim, cada situação deve merecer uma análise isolada e, caso esteja associada a esta partilha de desinformação a disseminação de conteúdo ilegal ou de opiniões não verificadas e falsas que coloquem em causa – de um modo particularmente

---

[447] POLYAKOVA, Alina; FRIED, Daniel, p. 11.
[448] A título de exemplo, a (pouca) longevidade de um determinado *site* na internet pode representar um indicador neste domínio, dado o fenómeno dos *pop-up sites* de desinformação. Cfr. POLYAKOVA, Alina; FRIED, Daniel, p. 11.
[449] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 11, 23 e 36.
[450] ALAPHILIPPE, Alexander, *et al.*, p. 13.
[451] O Código de 2022, capítulo V, medida 18.2.;

grave – a saúde e a segurança públicas na União, a proibição deste tipo de conteúdo deve ser sempre uma possibilidade «em cima da mesa». Posto isto, cada caso é um caso e é a gravidade das possíveis e previsíveis implicações que deve informar a tomada de decisões mais restritivas e radicais.[452]

As aplicações de mensagens

A questão das aplicações de mensagens é também relevante neste aspeto e é merecedora de uma atenção especial no Código de 2022, que procura acautelar algumas preocupações neste meio que, pela sua natureza, é menos transparente. Assim, é também necessário criar, neste ambiente, mecanismos de bloqueio à propagação de desinformação que não resultem, nem num decréscimo dos níveis de encriptação, nem num decréscimo dos níveis de proteção da privacidade do utilizador.[453] Nesse sentido, o Código de 2022 aponta, para além da já mencionada importância na continuidade dos avisos e rótulos de transparência, para a aplicação de um limite ao número de reencaminhamentos permitidos, em especial para conversas de grupo.[454]

4.3.5 Capacitação da comunidade de investigação

O capítulo VI aborda as questões mais prementes relacionadas com o tópico da capacitação da comunidade de investigação. Como veremos, grande parte dos compromissos e medidas aqui expostos acabam por complementar, direta ou indiretamente, o trabalho legislativo já alcançado pelo RSD ou a alcançar pela proposta de Regulamento da transparência e direcionamento da propaganda política.

Um dos pontos mais centrais nesta questão prende-se com os mecanismos de acesso aos dados por parte dos investigadores e académicos, cujo enquadramento merece uma reformulação para garantir uma maior utilidade e apoio ao seu trabalho indagativo, crucial para o combate à disseminação de desinformação.[455] O apoio às suas atividades é, deste modo, determinante para que se atinja um maior e melhor entendimento sobre as suas causas, os seus vetores, as dimensões que podem assumir, os seus impactos e as respostas disponíveis[456].

[452] PALOP, Andrés Boix, p. 106.
[453] O Código de 2022, capítulo V, medida 25.2.
[454] O Código de 2022, capítulo V, medida 25.2.
[455] O Código de 2022, capítulo VI, parágrafo (a); MORGAN, Susan, p. 42.
[456] *Plano de Ação contra a Desinformação*, p. 6.

Neste âmbito, devem estar, por isso, bem assentes três princípios: (1) o total respeito pelos vários direitos e liberdades fundamentais, entre os quais o do direito à comunicação privada[457]; (2) o acesso concedido aos dados não pode ser extensível a órgãos governamentais nem autoridades policiais[458]; e (3) a existência de diálogo, apoio e respeito, entre investigadores e plataformas, é essencial para criar um ambiente fausto ao saudável desenvolvimento de uma investigação de boa-fé sobre a desinformação nos seus serviços[459].

É com base nestas traves-mestras que se assume o primeiro compromisso neste capítulo, relacionado com a promoção de um acesso público – efetivo, ininterrupto, navegável e em tempo real (ou quase) – a "dados não pessoais e dados públicos anónimos, agregados ou manifestamente tornados públicos", por via de API's que permitam o seguro, sistematizado e cabal exame das múltiplas informações disponibilizadas.[460]

Tendo em conta que o acesso aos dados pode, por vezes, obrigar à consulta de informações de caráter pessoal, prevê-se, à semelhança do acautelado no RSD, a colocação em prática de processos de acreditação de investigadores.[461] Este processo de acreditação e de autorizações de acesso deve estar a cargo de uma entidade criada para o efeito.[462]

A comunidade de investigação deverá, por sua vez, demonstrar que leva a cabo o seu labor investigativo de acordo com uma "metodologia transparente" e em consonância com as normas deontológicas aplicáveis, comprometendo-se a partilhar instrumentos e os resultados da sua investigação aos "públicos relevantes".[463] O seu trabalho será igualmente relevante para avaliar a eficácia e o alcance das medidas estabelecidas no Código de 2022, com o intuito de informar futuras opções legislativas.[464]

4.3.6 Capacitação da comunidade de verificação de factos

Um dos últimos capítulos do Código de 2022 dá destaque à comunidade e ao trabalho desenvolvido pelos verificadores de factos na Europa, porventura englobados em organizações que

[457] O Código de 2022, capítulo VI, parágrafo (d).
[458] O Código de 2022, capítulo VI, parágrafo (e).
[459] O EDMO é, neste aspeto, um ator importante no favorecimento de um bom ambiente entre a comunidade de investigação e as plataformas, mas também para a criação de um código de conduta sobre o acesso aos dados das plataformas por parte dos investigadores (Cfr. parágrafo (f) do capítulo VI e medidas 27.1, 28.1 e 28.4).
[460] O Código de 2022, capítulo VI, compromisso 26. Neste âmbito, será de mencionar, a título exemplificativo, os avanços já alcançados com a criação de API's que permitem uma pesquisa detalhada, por informações concretas, no seio dos repositórios de anúncios (Cfr. capítulo III, compromisso 11).
[461] O Código de 2022, capítulo VI, compromisso 27.
[462] O Código de 2022, capítulo VI, compromisso 27.
[463] O Código de 2022, capítulo VI, compromisso 29 e medida 29.1.
[464] O Código de 2022, capítulo VI, medida 29.2.

procedem à verificação da veracidade dos conteúdos de relevância pública que circulam, tanto no meio em linha como fora dele, expondo publicamente casos de desinformação, com o intuito de alertar o público para a imprecisão das matérias aí relatadas.[465]

As principais inquietações levantadas, também elas partilhadas com a comunidade de investigação, prendem-se com a questão da disponibilização de um estável, sólido e seguro mecanismo de acesso aos dados das plataformas, crítico para o efeito útil das suas atividades nos seus serviços digitais.[466]

O êxito da atividade do *fact-cheking* nos meios digitais encontra-se dependente do fornecimento de informações representativas da eficácia desta atuação junto dos utilizadores das plataformas, de modo que a comunidade de verificadores de factos possa, firme e constantemente, melhorar a qualidade das repercussões resultantes da sua atividade.[467] Tais informações – que apenas são fornecidas pelas grandes plataformas em linha – devem permitir, tanto quanto possível, qualificar e quantificar os efeitos da sua atividade e, para tal, todos os dados relativos às ações levadas a cabo (como dados relativos às ordens de decréscimo sentidas ao nível do número de impressões, cliques e interações depois de determinado conteúdo ser alvo de rotulação, despromoção, etc.) configuram elementos essenciais que ajudam e norteiam a atividade da verificação de factos.[468]

À vista do exposto, o sucesso da atuação desta comunidade encontra-se dependente de uma formação basilar assente na confiança, excelência, imparcialidade, objetividade e transparência, sendo que, para o efeito, serão de mencionar algumas estruturas que se dedicam a promover, por um lado, os valores anteriormente descritos e, por outro, o estreitamento de relações com as grandes plataformas. São elas o IFCN (*International Fact-Checking Network*)[469], a rede de verificadores de factos do EDMO (Observatório Europeu dos Meios de Comunicação Digitais) e o EFCSN (*European Fact-Checking Standards Network*) e o seu Código relativo à integridade e independência da verificação de factos na Europa.

Estas estruturas funcionam, assim, como os baluartes da promoção de um *fact-checking* cimentado nos mais altos padrões de exigência, independência e transparência[470] e, nesse sentido, é

---

[465] POLYAKOVA, Alina; FRIED, Daniel, p. 8.
[466] O Código de 2022, capítulo VII, parágrafo (a) e (b) e medida 30.2.
[467] O Código de 2022, capítulo VII, parágrafo (d).
[468] O Código de 2022, capítulo VII, medida 32.1.
[469] À data de setembro de 2023, existiam em Portugal um total de quatro iniciativas de *fact-checking* certificadas de acordo com os princípios do IFCN: o Público, o Viral Check (verificação de factos na área da saúde), o Observador – Fact Check e o Polígrafo.
[470] Grupo de Peritos em notícias falsas e na desinformação em linha, pp. 16 e 24.

incentivada a adesão das organizações de verificação de factos a estas iniciativas, dada a importância e o valor que reside na demonstração e comprovação da qualidade da atividade desenvolvida.[471]

Do lado das plataformas, por sua vez, para além do envidamento de esforços no sentido de criar um ambiente favorável à partilha de dados relevantes, é, como também se já observou, necessário um compromisso no sentido de alocar espaço, nos seus serviços, à atividade desenvolvida pela comunidade de verificação de factos[472], por meio da utilização de rótulos e painéis de informação, a título exemplificativo.[473] Neste sentido, deve existir uma preocupação para que o desenvolvimento destes laços se estenda também a todos os Estados-Membros e línguas oficiais, pois não nos devemos esquecer que a desinformação sobre questões europeias apenas pode ser definitivamente combatida se a verdade dos factos for reposta em todas as línguas da União.

Por último, é igualmente mencionada a criação de um repositório, como aquele já referido relativamente aos anúncios publicitários políticos, mas, desta vez, versando o mesmo sobre o conteúdo cuja factualidade e veracidade haja sido verificada, de modo a garantir a segurança, a transparência e a responsabilização em todo o processo de verificação de factos.[474]

4.3.7 O Centro de Transparência e o Grupo de Trabalho Permanente

O capítulo VIII e IX do Código de 2022 preveem a criação de duas estruturas substanciais: um Centro de Transparência e um Grupo de Trabalho Permanente.

O Centro de Transparência, erigido sob a égide do interesse público em obter informações atualizadas, claras e precisas sobre o processo de aplicação do Código de 2022[475], funciona como uma espécie de "ponto comum de referência e transparência"[476] dirigido ao público, de modo que este possa consultar os passos que estão a ser dados no sentido da concretização dos preceitos inscritos no Código.[477] Neste sentido, o Centro disponibiliza, também na forma de um repositório, informações detalhadas sobre as ações levadas a cabo pelos signatários em vista à prossecução dos compromissos e medidas assumidos.[478]

---

[471] O Código de 2022, capítulo VII, parágrafo (e).
[472] O Código de 2022, capítulo VII, compromisso 31.
[473] O Código de 2022, capítulo VII, medida 31.2.
[474] O Código de 2022, capítulo VII, medida 31.3.
[475] O Código de 2022, capítulo VIII, parágrafo (a).
[476] O Código de 2022, capítulo VIII, parágrafo (a).
[477] O Código de 2022, capítulo VIII, parágrafo (b) e medida 35.5.
[478] O Código de 2022, capítulo VIII, compromisso 35 e medida 35.3.

Por sua vez, o Grupo de Trabalho Permanente – presidido pela Comissão e do qual participam os signatários do Código e representantes do EDMO, do ERGA e do EEAS – ocupa-se da atividade de avaliar continuamente a eficácia e relevância do Código, procedendo, para o efeito, a uma permanente otimização do mesmo (por via da implementação de alterações aos seus compromissos e medidas, quando tal se afigure oportuno, por exemplo[479]) perante as necessidades e características mais urgentes da atualidade[480].

4.3.8 Monitorização do Código

Por fim, o seu último capítulo estabelece um conjunto de linhas gerais relativamente à monitorização da implementação do Código de 2022. Encontra-se previsto, para o efeito, um enquadramento que defende o desenvolvimento de relatórios periódicos, por parte dos signatários, que permitam aferir do empenho e dos resultados atingidos em relação a cada compromisso e suas respetivas medidas – tanto a nível europeu como, também, dos vários Estados-Membros, com base nos SLI's e QRE's.[481]

O último capítulo prevê, igualmente, algumas situações especiais.

A título de exemplo, no âmbito do compromisso 42., surge a obrigação de certos signatários fornecerem, a pedido da Comissão, informações particulares e pertinentes em períodos de crise ou eleições. Por seu turno, o compromisso 44. reitera a preocupação com o poder das plataformas e motores de pesquisa em linha de muito grande dimensão no âmbito desta problemática, estabelecendo, em consonância com o RSD, que estas devem consentir à realização, a suas expensas, de auditorias às suas empresas, de modo a possibilitar um meio de supervisão mais personalizado e atento ao cumprimento dos compromissos e medidas assumidos por estas entidades.

[479] O Código de 2022, capítulo IX, medida 37.2.
[480] O Código de 2022, capítulo IX, parágrafo (a).
[481] O período entre cada relatório varia consoante a natureza do signatário. As plataformas e motores de pesquisa em linha de muito grande dimensão devem enviar relatórios de 6 em 6 meses e os restantes de ano a ano (Cfr. capítulo X, parágrafos (b) e (c), compromisso 40. e medida 40.2).

5. CASO RT FRANCE V CONSELHO

Chegados a este ponto, é possível concluir de forma distintiva que a disseminação de desinformação ganhou um novo fulgor desde a invenção e o acesso generalizado das populações à internet. Ainda assim, e não deixando tal afirmação de corresponder logicamente à verdade, não é exclusivamente nos meios digitais que a problemática se assume com força nos dias de hoje, e este caso da jurisprudência do Tribunal Geral (uma das jurisdições do Tribunal de Justiça da União Europeia) espelha precisamente isso.

Posto isto, ao longo das próximas páginas, será levada a cabo uma exposição dos principais tópicos característicos do acórdão, sendo que primeiramente será conduzida uma contextualização das circunstâncias mais relevantes e, num momento posterior, proceder-se-á à exposição da argumentativa utilizada pelo Tribunal Geral numa decisão onde a temática da desinformação assumiu um papel de destaque.

5.1 Contextualização

No presente caso, o órgão de comunicação social RT France encontra-se em rota de colisão com o Conselho por conta de algumas medidas adotadas por este último em resposta às ações de desestabilização desencadeadas pela agressão militar russa na Ucrânia, iniciada em fevereiro de 2022.

Para o efeito, a RT France solicitava do Tribunal a anulação de uma Decisão [(PESC) 2022/351 do Conselho, de 1 março de 2022, que altera a Decisão 2015/512/PESC] e de um Regulamento [Regulamento (UE) 2022/350 do Conselho, de 1 de março de 2022, que altera o Regulamento (UE) 833/2014)] que impuseram um conjunto de medidas restritivas à Federação da Rússia, por conta das suas ações beligerantes em território ucraniano.[482]

Na circunstância em concreto, algumas das medidas restritivas prejudicavam as atividades de radiodifusão da RT France no território da União, uma vez que esta se encontrava elencada numa lista de entidades em relação às quais se determinava a obrigação, temporária, de cessação das atividades de radiodifusão nesta área geográfica.[483]

No âmbito da fundamentação para a aplicação destas medidas, o Conselho menciona que a Federação da Rússia tem vindo a desenvolver "uma campanha sistemática e internacional de

[482] Acórdão RT France v Conselho do Tribunal Geral, de 27/07/2022, proferido no proc. n.º T–125/22.
[483] Proc. T–125/22, parágrafo 22;

manipulação dos meios de comunicação social e de distorção dos factos a fim de reforçar a sua estratégia de desestabilização dos países vizinhos, bem como da União e dos seus Estados-Membros", campanha essa que era difundida com o apoio de órgãos de comunicação social controlados, na sua essência, pelo Governo da Federação da Rússia. À vista disso, a RT France possui, por força da associação-mãe à qual pertence, fortes laços económicos que a ligam ao governo da Federação Russa, princípio ativo responsável pelo clima de conflito e perigo que acabou por se gerar e, deste modo, foi abrangida por esta proibição temporária das suas atividades de radiodifusão[484], precisamente por conta do enquadramento destas suas atividades no âmbito das ditas ações de manipulação e desinformação.

O Conselho concluiu, assim, que tais ações representam – de um modo particularmente grave – um conjunto de ameaças à segurança e à ordem públicas no espaço da União.[485]

A RT France, por sua vez e de modo a sustentar o seu pedido, apresentou quatro argumentos centrais para obter do Tribunal uma resposta no sentido ao provimento do recurso que apresentou. São eles: (1) a violação dos seus direitos de defesa; (2) a violação do seu direito à liberdade de expressão e de informação; (3) a violação do seu direito à liberdade de empresa; e (4) a violação do princípio da não discriminação em razão da nacionalidade.[486] A RT France levantou ainda, de forma acidental, a competência do Conselho para emanar os atos que pretende ver impugnados pelo Tribunal. [487]

5.2 A questão da competência do Conselho para emanar os atos alvo de impugnação

A competência do Conselho é, assim, um dos tópicos levantados pela RT France no seu pedido, com base na ideia de que apenas as entidades reguladoras nacionais – no caso a *Autorité de régulation de la communication audiovisuelle et numérique* (Arcom) (a autoridade reguladora francesa para o setor da comunicação audiovisual e digital) – poderiam emanar atos desta natureza.[488]

[484] Proc. T–125/22, parágrafo 52.
[485] Proc. T–125/22, parágrafo 22.
[486] Proc. T–125/22, parágrafo 45.
[487] Proc. T–125/22, parágrafo 45.
[488] Proc. T–125/22, parágrafo 46.

5.2.1 O escopo de competência do Conselho em matéria de política externa e segurança comum e a resposta do Tribunal

No seguimento do exposto, cumpre referir que, no que diz respeito à decisão adotada pelo Conselho e alvo de impugnação, a mesma foi implementada ao abrigo dos artigos 21.º, 23.º, 24.º, 25.º e 29.º, todos do Título V do Tratado da União Europeia (TUE), relativos às "Disposições Gerais Relativas à Ação Externa da União e Disposições Específicas Relativas à Política Externa e de Segurança Comum".

Do artigo 21.º do TUE – em ligação com o artigo 3.º do mesmo diploma – resulta que a atuação da União no panorama internacional se encontra regrada pela promoção dos seus valores a nível global, tais como a democracia e o Estado de direito, a valorização e preservação da paz e da segurança, o respeito pelos direitos e liberdades fundamentais e a consideração máxima pelos princípios inscritos na Carta das Nações Unidas e pelas normas de direito internacional[489].

Por seu turno, o artigo 24.º do TUE refere, complementarmente, que o poder de autoridade da União em matéria relativa à política externa e segurança comum "abrange todos os domínios da política externa, bem como todas as questões relativas à segurança da União" e, levando ainda em conta o disposto nos artigos 25.º e 29.º do TUE, resulta que o Conselho pode adotar decisões que definam a "abordagem global de uma questão específica de natureza geográfica ou temática pela União"[490]. [491]

Dada esta grande margem de atuação fornecida ao Conselho, o Tribunal entendeu não condenar a sua posição ao adotar estas medidas restritivas. Neste sentido, face às ameaças que se verificaram à paz, à segurança e à ordem públicas no espaço da União – resultantes do início de uma agressão armada não provocada e acentuada por ações de manipulação e desinformação dirigidas à sociedade europeia, plasmadoras de um apoio à ofensiva e à violação da integridade territorial e da soberania de um Estado vizinho –, as medidas adotadas procuraram, simplesmente, colocar um ponto final à agressão militar por meios pacíficos.[492]

Por fim, o artigo 215.º, n.º 2 do TFUE é ainda referido para enrobustecer a posição do Tribunal no sentido da defesa da atuação do Conselho.[493] Para o efeito, o Tribunal relembra que quando uma decisão é tomada em consonância com o Capítulo 2 do Título V do TUE – do qual constam grande

[489] Tratado da União Europeia, artigo 21.°; Proc. T–125/22], parágrafo 49.
[490] Tratado da União Europeia, artigos 24.° e 29.°; Proc. T–125/22, parágrafo 49.
[491] Proc. T–125/22, parágrafo 51.
[492] Proc. T–125/22, parágrafos 52 e 55.
[493] Proc. T–125/22, parágrafo 62.

parte dos artigos já mencionados – o Conselho pode adotar "medidas restritivas relativamente a pessoas singulares ou coletivas, a grupos ou a entidades não estatais"[494], que assumem naturalmente a capacidade de "alterar diretamente a situação jurídica dos particulares"[495].

Assim, e voltando à questão inicial da competência exclusiva das entidades reguladoras nacionais para a tomada de decisões desta envergadura, o Tribunal entendeu não acolher o argumento da RT France. Para além da argumentação já deduzida, referiu ainda, por um lado, que a atribuição de incumbências a órgãos nacionais não pode significar o enfraquecimento dos poderes da União numa área tão sensível como a da política externa e de segurança comum e, por outro, que o alcance de uma decisão exalada a nível europeu, e que se aplica, por isso, a qualquer Estado-Membro, produz os efeitos sólidos e alargados tão desejados[496] numa situação de urgência, por comparação a uma decisão que apenas produz efeitos num único Estado-Membro.

5.3 A questão da violação dos direitos de defesa da RT France

5.3.1 A argumentativa da RT France

A RT France invocou, igualmente, que os seus direitos de defesa se encontravam a ser violados. De forma a sustentar esta sua afirmação, elencou os artigos – inscritos na CDFUE – que, na sua opinião, não foram observados no decorrer de todo este processo.

Assim, procedeu a uma referência ao artigo 41.º, relativo ao «Direito a uma boa administração», no qual se encontra inscrito o direito de qualquer pessoa "ser ouvida antes de a seu respeito ser tomada qualquer medida individual que a afete desfavoravelmente" e, ainda, o direito a fazer as suas apreciações com base num acesso prévio aos documentos processuais relevantes[497]. Para além disso, avançou com uma menção ao artigo 47.º, relativo ao «Direito à ação e a um tribunal imparcial», particularmente por considerar que não obteve a oportunidade de conhecer, em nome da tutela plena dos seus direitos e antes da tomada de uma decisão, as razões que levaram o Conselho a

[494] Proc. T–125/22, parágrafos 63 e 64.
[495] Proc. T–125/22, parágrafo 51.
[496] Proc. T–125/22, parágrafo 57.
[497] Carta dos Direitos Fundamentais da União Europeia, artigo 41.º, n.º 2, alíneas a) e b; Proc. T–125/22, parágrafo 65.

incluir o seu nome na lista em questão[498]. Por fim, aludiu igualmente ao artigo 48.º, relativo à «Presunção de inocência e direitos de defesa».[499]

Neste seguimento, a ausência de uma notificação para exercer os direitos acima descritos traduziram-se, na opinião da RT France, na aplicação de atos que causam uma lesão particularmente "grave e irreversível" dos seus interesses "económic[os], financeir[os] e human[os]", uma vez se encontra impedida de continuar a exercer a atividade que até então desempenhava, sendo que a situação de urgência subjacente não pode razoavelmente justificar a violação dos seus direitos de defesa, uma vez que, na sua leitura dos acontecimentos, as medidas restritivas impostas representam uma atitude "meramente simbólica", que "não pode ser considerada uma resposta consistente para restabelecer a paz e a estabilidade no continente europeu".[500]

Por fim, a RT France indica que, caso os seus direitos de defesa tivessem sido respeitados plenamente, poderia ter contestado eficazmente alguns dos argumentos que serviram de base à imposição das proibições, nomeadamente as alegações de que a reportagem dos factos feita pelos seus canais de comunicação não era propiciadora de uma leitura de múltiplas perspetivas da situação.[501]

5.3.2 A resposta do Tribunal

Por seu turno, o Tribunal começa, na sua argumentação, por recorrer a uma analogia para demonstrar o seu posicionamento face a esta questão.

Assim, relembra que, segundo a jurisprudência, a decisão de incluir o nome de uma figura numa lista de entidades com os fundos congelados, a título de exemplo, não dá lugar a qualquer comunicação prévia, sob o perigo de se frustrar o efeito útil da medida e, seguindo semelhante linha de raciocínio, a mesma lógica deverá ser aplicada ao caso em questão, uma vez que subsistem, de igual modo, um conjunto de interesses que devem ser prosseguidos com celeridade e eficácia.[502]

Nesse sentido, atendendo a um vasto conjunto de circunstâncias – como o "contexto extraordinário e de extrema urgência" vivenciado, a rápida escalação de tensões no território europeu, a belicista "atividade [de] contínua e concertada (...) desinformação e de manipulação dos factos" por parte de órgãos de comunicação social propagandistas ligados ao Estado Russo e, por último, o facto

[498] Proc. T–125/22, parágrafo 65.
[499] Carta dos Direitos Fundamentais da União Europeia, artigo 48.º; Proc. T–125/22, parágrafo 65.
[500] Proc. T–125/22, parágrafos 66, 67, 69 e 70.
[501] Proc. T–125/22, parágrafos 71.
[502] Proc. T–125/22, parágrafos 80 e 84.

destas medidas restritivas se reportarem, na verdade, a um pacote de medidas ainda mais abrangente e de uma "envergadura inédita" –, tornou-se absolutamente impossível a audição da recorrente.[503]

O Conselho procurou, assim, adotar agilmente uma posição firme, sólida e pacífica, essencial para a mitigação da situação de conflito e, francamente, tornou-se particularmente difícil – para não dizer impossível – fornecer um prazo justo para que a RT France se pudesse pronunciar sobre a questão, sob pena, de, uma vez mais, se frustrarem os interesses gerais centrais que se prosseguiam, a saber: a preservação da segurança e a ordem públicas na União e a seriedade do debate democrático[504], entre outros.

Para além disso, é de referir que os elementos de prova, que serviram de base à imposição de medidas restritivas por parte do Conselho, derivam de um conjunto claro de dados sobre as suas emissões de televisão e artigos que havia publicado no seu espaço em linha, dados esses que são demonstradores de uma clara anuência e justificação da invasão iniciada pela Federação da Rússia, refletida, também, por meio de uma exposição desequilibrada das várias perspetivas sobre o conflito. No caso, mesmo que as circunstâncias permitissem a realização de uma audição prévia, tal não iria provocar qualquer tipo de alteração ao material probatório subjacente à tomada desta decisão e, nesse sentido, não seria de todo concebível descortinar uma interpretação diferente dos acontecimentos.[505]

Posto isto, e em jeito de conclusão, é do entendimento do Tribunal que nenhum dos argumentos invocados pela RT France seria capaz de demonstrar que a sua audição prévia iria desencadear resultados diferentes aos verificados[506].

5.3.3 A questão da insuficiência de fundamentação dos atos impugnados pela RT France

O Tribunal começa por reconhecer, neste âmbito, com base no artigo 41.º, n.º 2, alínea c) da Carta e com base no artigo 296.º do TFUE, um princípio base relativo ao dever de fundamentação de um ato lesivo, em nome da proteção dos direitos de defesa da pessoa visada por este.[507]

Neste âmbito, o Conselho aplicou as medidas restritivas com base em 2 critérios: (1) órgãos de comunicação social sob o controlo, seja ele direto ou indireto, do Estado da Federação Russa; (2) que, por meio das suas atividades de radiodifusão dirigidas às populações da União, se encontram a

[503] Proc. T–125/22, parágrafos 86, 87 e 88.
[504] Proc. T–125/22, parágrafos 86, 87 e 88.
[505] Proc. T–125/22, parágrafo 96
[506] Proc. T–125/22, parágrafo 99.
[507] Proc. T–125/22, parágrafos 102 e 103.

produzir e emitir conteúdo de apoio à agressão militar na Ucrânia[508], isto é, "ações de propaganda contínuas e concertadas" que representam um perigo para a ordem e a segurança na União.[509]

Neste sentido, o Tribunal concluiu que, atendendo às circunstâncias sem precedentes que se formaram com a invasão da Ucrânia[510], o fundamento apontado pelo Conselho para aplicar estas medidas restritivas é "compreensível e suficientemente preciso". De resto, os parâmetros utilizados para a tomada desta decisão reportam-se precisamente à atuação levada a cabo pela RT France, como veremos, expondo de forma abastadamente rigorosa e precisa os motivos pelos quais as limitações se lhe aplicam, não havendo, por isso, qualquer vício de fundamentação.[511]

5.4 A questão da violação da liberdade de expressão e de informação

5.4.1 A argumentativa da RT France

Dada a centralidade deste argumento para o processo, a fundamentação da RT France para sustentar a violação deste direito fundamental – previsto no artigo 11.º da Carta – assenta em múltiplos pontos, sendo que os principais irão ser expostos ao longo dos próximos parágrafos.

A RT France refere, primeiramente, que a imposição das medidas restritivas não representa um instrumento apropriado a prosseguir os objetivos de interesse geral delineados pelo Conselho.[512]

Por outro lado, indica que uma proibição total das suas atividades e a ausência de um prazo específico para o seu término constituem um grande desrespeito pelo seu direito à liberdade de expressão e de informação.[513]

Por conseguinte, refere que as acusações de que foi alvo relativamente às práticas de propaganda não se encontram "minimamente sustentadas" e que a sua dependência financeira da Federação Russa não deve ser confundida com uma dependência ao nível do seu plano editorial, não podendo, deste modo, tais factos constituírem fundamento para aplicação destas sanções –

[508] Proc. T–125/22, parágrafo 108.
[509] Proc. T–125/22, parágrafos 108 e 112.
[510] O Tribunal – no parágrafo 103 – refere que, de acordo com a sua jurisprudência, a natureza do ato e o contexto em que o mesmo é adotado são dados que devem ser levados em consideração na apreciação da sua fundamentação.
[511] Proc. T–125/22, parágrafos 109, 113 e 115.
[512] Proc. T–125/22, parágrafo 118.
[513] Proc. T–125/22, parágrafos 119 e 120.

relembrando, para o efeito, a existência de muitos canais que dependem de apoios do Estado, como o canal estatal France 24.[514]

Para além disso, a RT France contesta as alegações de que o tratamento noticioso do conflito, que levou a cabo nos primeiros dias da invasão, não contemplava de forma equilibrada as múltiplas interpretações relativamente ao mesmo. Refere, ainda, que a justificação utilizada pelo Conselho para sustentar a proporcionalidade das restrições aplicadas – isto é, o facto da RT France e dos seus jornalistas não se encontrarem totalmente impedidos de realizarem outras atividades, como "pesquisas e entrevistas", mesmo após a aplicação de sanções – não colhe, uma vez que, a título exemplificativo, a Comissão da Carteira Profissional de Jornalista francesa já rejeitou a acreditação dos seus profissionais e, ainda neste domínio, toda esta situação já levou também à cessação de imensas relações contratuais importantíssimas para a continuação do seu funcionamento.[515] Tudo isto, na opinião da RT France, torna impossível a prossecução das suas atividades no seu todo.[516]

5.4.2 A resposta do Tribunal

O sentido e a dimensão do direito à liberdade de expressão e de informação

Na sua resposta, o Tribunal começa por realizar uma contextualização do significado e alcance do direito à liberdade de expressão e de informação. Este direito, inscrito como vimos no artigo 11.º da Carta, indica que "qualquer pessoa tem direito à liberdade de expressão" e que o mesmo compreende a "liberdade de opinião" e a "liberdade de receber e de transmitir informações ou ideias", alertando, tanto para a inadmissibilidade da "ingerência de quaisquer poderes públicos", como para a total "[des]consideração de fronteiras"[517]. No seu número 2, é feita uma especial menção ao facto de serem reconhecidas, da mesma forma, a "liberdade e o pluralismo dos meios de comunicação social".[518]

O Tribunal indica que este direito e liberdade constitui um dos alicerces das nações democráticas e que esta liberdade se aplica, tanto às informações mais inofensivas e consensuais,

[514] Proc. T–125/22, parágrafos 121 a 123.
[515] Proc. T–125/22, parágrafos 126 e 127.
[516] Proc. T–125/22, parágrafos 126 e 127.
[517] Carta dos Direitos Fundamentais da União Europeia, artigo 11.º, n.º 1; Proc. T–125/22, parágrafo 132.
[518] Carta dos Direitos Fundamentais da União Europeia, artigo 11.º, n.º 2; Proc. T–125/22, parágrafo 132.

como àquelas que "ofendem, chocam ou inquietam", desde que em consonância com os ideais de "pluralismo, da tolerância e [d]o espírito de abertura".[519]

De igual modo, refere também que, por vezes, pode ser necessário estabelecer limitações à fruição desta liberdade, de acordo com os propósitos legítimos que se pretendam alcançar. Cumpridos todos os requisitos, previstos no artigo 52.º da Carta, poderão impor-se limitações à disseminação de mensagens que "propaguem, incitem a, promovam ou justifiquem o ódio com base na intolerância, [ou] na utilização e na apologia da violência".[520]

De seguida, o Tribunal procede a uma aplicação destes corolários à atividade jornalística, indicando que atividade destes, em nome do interesse público, deve ser conduzida de "boa-fé, com base em factos exatos, e (...) [a partir de] informações «fiáveis e precisas» no respeito da ética jornalística"[521].

Estudo da violação do direito à liberdade de expressão e de informação no caso em concreto

É sob o auspício do disposto nos últimos parágrafos que o Tribunal procede, de seguida, a um estudo mais minucioso da eventual existência de uma certa apologia à agressão e ao conflito armado por parte da RT France. Assim, a sua observação incidirá particularmente sobre os "termos utilizados" por esta nas suas comunicações, a "maneira como as afirmações foram formuladas" e o "contexto em que a sua divulgação se insere".[522]

No entanto, antes de proceder à sua apreciação, o Tribunal enumera ainda o conjunto de requisitos que, preenchidos cumulativamente, significam a admissibilidade de restrições à liberdade fundamental em questão. São eles a (1) a previsão legal da dita restrição; (2) o respeito pelo conteúdo essencial dos direitos e liberdades; (3) e, no respeito pelo princípio da proporcionalidade, a exigência de que a limitação em causa deve ser necessária e corresponder a "objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros".[523]

[519] Proc. T–125/22, parágrafo 133.
[520] Proc. T–125/22, parágrafo 134.
[521] Proc. T–125/22, parágrafo 136.
[522] Proc. T–125/22, parágrafo 140.
[523] Carta dos Direitos Fundamentais da União Europeia, Artigo 52.º, n.º 1; Proc. T–125/22, parágrafo 145.

A previsão legal das restrições

Relativamente ao primeiro requisito, já foi referido que os atos impugnados foram adotados de acordo com artigo 29.º TUE (Decisão) e o artigo 215.º TFUE (Regulamento) e, tendo isso em mente, o Tribunal entendeu tratar-se de normas legais "suficientemente previsíveis para os interessados".[524]

Relativamente a este requisito da previsão legal, é igualmente necessário aferir, hipoteticamente, o grau de capacidade da pessoa visada em conseguir prever as possíveis consequências jurídicas de determinada norma legal na sua esfera jurídica, de modo a permitir o desencadeamento de um "ajust[e] [à] sua conduta".[525] Ora, neste quesito, é da opinião do Tribunal que era, sim, previsível que um amplo apoio mediático a uma invasão militar pudesse resultar na aplicação de medidas restritivas das atividades de radiodifusão que veiculam material dessa natureza.[526] Posto isto, o Tribunal concluiu pela verificação deste primeiro pressuposto.[527]

O respeito pelo conteúdo essencial dos direitos e liberdades

Em relação ao segundo requisito, o Tribunal começa por relembrar, por um lado, que as medidas restritivas aplicadas possuem um caráter "temporário e reversível"[528] e que o levantamento das sanções está apenas dependente do preenchimento de dois requisitos alternativos: (1) o término da guerra na Ucrânia ou (2) a cessação das atividades e ações de propaganda dirigidas à União.[529] Assim, não colhe o argumento de que as medidas foram aplicadas sem um limite de tempo previamente estabelecido, até porque o seu levantamento só depende de atos no sentido de uma pacificação.[530]

Ainda neste âmbito, e relativamente à questão levantada pela RT France relativa à impossibilidade de prosseguir com as suas atividades, o Tribunal reitera que aos profissionais da recorrente não foi retirado o direito a encetarem ações vinculadas à liberdade de informação e de

---

[524] Proc. T–125/22, parágrafo 149.
[525] Proc. T–125/22, parágrafo 150.
[526] Proc. T–125/22, parágrafo 151.
[527] Proc. T–125/22, parágrafo 152.
[528] A aplicação das medidas vigorava até dia 31 de julho de 2022, sem prejuízo da possibilidade de adoção de uma nova decisão no sentido da continuação da proibição (proc. T–125/22, parágrafo 154). A propósito, o Conselho, no dia 20 de julho de 2023, decidiu prorrogar por mais 6 meses – até dia 31 de janeiro de 2024 – as sanções à Federação da Rússia, entre as quais, a interrupção das atividades de radiodifusão de alguns órgãos de comunicação social apoiados pelo Estado Russo (Cfr. Conselho da União Europeia, *Rússia: UE renova sanções em resposta à agressão militar da Rússia contra a Ucrânia*, 2023. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2023/07/20/russia-eu-renews-sanctions-over-russia-s-military-aggression-against-ukraine/> [19/10/2023].
[529] Proc. T–125/22, parágrafos 154 e 155.
[530] Proc. T–125/22, parágrafo 155.

expressão, virtualmente capazes de produzir rendimentos.[531] Recorda, igualmente, que este órgão de comunicação social apenas se encontra desautorizado a emitir no espaço da União, podendo prosseguir as suas emissões noutros países francófonos, e, nesse sentido, estas sanções "não violam a substância do seu direito de exercer a sua liberdade de expressão"[532], dado que "a natureza e o alcance da proibição temporária em causa respeitam o conteúdo essencial da liberdade de expressão e não põem em causa esta liberdade enquanto tal".[533]

O respeito pelo princípio da proporcionalidade

A respeito do terceiro requisito, são mencionadas, novamente, algumas preocupações ligadas à manutenção da ordem e da segurança públicas na União, particularmente relacionadas com a ameaça das campanhas de desinformação.

Neste subcapítulo será, assim, essencial analisar a proporcionalidade desta atuação, sendo que a análise do referido princípio se desdobrará na avaliação da adequação, necessidade e proporcionalidade em sentido estrito das medidas restritivas implementadas para alcançar os objetivos de interesse geral.[534]

A título preliminar, tal avaliação irá resumir-se a uma análise dos elementos de prova que levaram o Conselho a adotar tais decisões, no sentido de averiguar a existência de uma ligação sólida entre estas e a sua base de fundamentação.

Assim, será primeiramente de explorar, por um lado, a questão do controlo da RT France pelo Estado Russo e, por outro, o caráter propagandista e de apoio à guerra das suas atividades de radiodifusão na União, uma vez que estas duas conclusões foram das mais importantíssimas para fundamentar as ações restritivas iniciadas pelo Conselho.[535] Após esse estudo, irá finalmente proceder-se à verificação da adequação, necessidade e proporcionalidade em sentido estrito das ditas medidas, face aos objetivos de interesse geral identificados.[536]

---

[531] Proc. T–125/22, parágrafo 156.
[532] Proc. T–125/22, parágrafo 157.
[533] Proc. T–125/22, parágrafo 159.
[534] Proc. T–125/22, parágrafo 169; A este propósito, Cfr. também o Acórdão do Tribunal Constitucional, de 04/11/1993, proferido no proc. n.º 634/1993, 94/92, ponto n.º 7.
[535] Proc. T–125/22, parágrafo 169.
[536] Proc. T–125/22, parágrafo 169.

O alegado controlo da RT France por parte da Federação da Rússia

Relativamente às alegações de controlo da RT France por parte da Federação da Rússia, é referido que o capital social desta é detido pela TV Novosti, que é, por sua vez, "inteiramente financiada pelo orçamento do Estado Russo".[537]

Para além disso, o Tribunal refere também algumas declarações proferidas por importantes figuras russas acerca do funcionamento do grupo RT. A chefe de redação, a título de exemplo, já referiu que o grupo RT funciona como um "canal internacional que representa o país" e como uma "arma de informação" de oposição ao ocidente.[538] Por sua vez, o Presidente da Federação da Rússia já afirmou que a RT "não podia deixar de refletir as posições do poder oficial sobre o que se passa[va] no [seu] país e no estrangeiro".[539]

Para mais, no entendimento do Tribunal, a RT France foi incapaz de demonstrar no processo – a nível institucional, regulamentar ou legal – a sua "independência editorial e (...) autonomia institucional" relativamente à influência de qualquer poder político.[540]

Dadas estas conclusões, o Tribunal concluiu pela existência de um efetivo controlo por parte do governo russo.

O caráter propagandista e de apoio à guerra das atividades de radiodifusão da RT France

De seguida, o Tribunal apresenta, muito detalhadamente, os principais argumentos que desaguam na conclusão de que a RT France levava efetivamente a cabo um *modus operandi* que veiculava uma visão manipuladora e pretensiosa de apoio a um conflito armado.

Neste domínio, a análise pormenorizada que será levada a cabo levará em conta os "termos utilizados", o modo como as declarações foram estruturadas e o "contexto em que as (...) emissões foram difundidas".[541] Assim, nos próximos parágrafos pretende emanar-se uma exemplificação das variadas situações que contribuíram para o adensamento da grande narrativa de apoio e justificação à agressão militar na Ucrânia, exposta por meio das atividades jornalísticas da RT France.

---

[537] Proc. T–125/22, parágrafo 172.
[538] Proc. T–125/22, parágrafo 172.
[539] Proc. T–125/22, parágrafo 172.
[540] Proc. T–125/22, parágrafo 173.
[541] Proc. T–125/22, parágrafo 179.

A título preliminar, é de destacar a leitura que foi feita aquando das primeiras movimentações das tropas russas no período do pré-guerra, denominadas como «ações de prevenção» cujo intuito se reportava à defesa da soberania das Repúblicas de Donetsk e Lugansk. Num outro contexto, 12 dias antes do início da invasão, é exibida a intervenção de um professor convidado de uma Universidade russa que alegava a existência de jihadistas na linha da frente ucraniana, receando-se a possibilidade de confrontações.

No dia 21 de fevereiro, poucos dias antes da invasão, foi publicado um artigo onde era referida uma declaração do Ministro dos Negócios Estrangeiros da Rússia no qual se acusava o Ocidente pelo agravamento das tensões e pela criação de "um confronto inultrapassável entre a Rússia e a OTAN".[542] Num outro artigo, datado do mesmo dia, é feita uma alusão às "atrocidades iminentes" que seriam praticadas pelo exército ucraniano relativamente à população russófona do Donbass.

Durante o primeiro dia da invasão, o acompanhamento jornalístico da situação seguia uma lógica de «ação defensiva» de «prevenção», motivada pela, na opinião de um politólogo convidado, "manipulação dos «ocidentais»" e das "suas marionetes ucranianas". [543] Durante a emissão televisiva, outro interveniente reitera de que não se tratava "evidentemente de uma invasão", mas sim de uma "libertação dos cidadãos do Donbass".[544] No período da tarde, a opinião dos intervenientes continuava a ser uníssona e pouco destoante, no qual, a título de exemplo, foi declarado que "a Ucrânia [era] uma criação da Rússia", que se estava a assistir à reconstituição de "uma forma de configuração territorial que tem em conta a presença de uma minoria russófona importante" e, ainda, de que se tratava de uma "espécie de ação preventiva, de proteção de um perigo", algo que acabava por "justifica[r] um pouco tudo a que assistimos". Por fim, são ainda reforçados os ditos "problemas territoriais na Ucrânia", com o intuito de acrescer a forte e uniforme narrativa que pretende influenciar a opinião do público no sentido de um apoio à agressão militar russa.[545]

Durante o dia seguinte, dia 22, um convidado fala mesmo num "genocídio", "preparado pelo Governo de Kiev" com o auxílio dos Estados Unidos e da União Europeia, sendo também referido que, na dita «operação especial», se procura desmilitarizar (uma vez que a Ucrânia, no entendimento da convidada, foi armada pelos países da OTAN) e «desnazificar» a Ucrânia, insinuando, ainda, que esta se encontra a ser "dirigid[a] do estrangeiro", sendo "perigoso" deixar o país nesse "estado". No mesmo sentido, é ainda referido que, numa aceção teórica, "o Estado ucraniano não existe" e que, por

[542] Proc. T–125/22, parágrafo 177.
[543] Proc. T–125/22, parágrafo 180.
[544] Proc. T–125/22, parágrafo 180.
[546] Proc. T–125/22, parágrafo 181.

isso, não se poderá falar de «integridade territorial» da Ucrânia se não existe Estado Ucraniano.[546] Durante a tarde desse mesmo dia, um outro convidado, geopolitólogo e diretor de curso numa Universidade suíça, afirma que não se trata de uma "invasão enquanto tal", indicando, por oposição, que "os Russos foram, de certa maneira, fazer a limpeza". Para além disso, o referido geopolitólogo afirma que é necessário refletir sobre uma "redefinição das fronteiras" desde o período da URSS. Ainda durante a emissão da tarde, um outro convidado indica que os Estados Unidos procuram "cercar a Rússia" e fazê-la "desaparecer", caracterizando posteriormente a OTAN como uma "organização hostil" e, por esse motivo, os desenvolvimentos recentes são, no seu entendimento, algo "normal".

Durante o dia 27, um convidado, anunciado como consultor em inteligência estratégica, defende que a invasão russa pode "ser revestida de uma certa forma de legitimidade". Nesse mesmo dia, foi emitida uma reportagem – gravada no Donbass ainda antes do início da invasão – que demonstrava exclusivamente o «sentimento pró-russo» que se sentia nessa região, sendo que na peça a Ucrânia era apresentada como o "Estado agressor" e "único responsável pelos bombardeamentos do Donbass", ainda que persistam dúvidas a nível internacional acerca da autoria de tais bombardeamentos.

Com base nos documentos de prova recolhidos, é notório que a retórica praticada pelas autoridades russas foi reproduzida de forma constante e pouco desviante ao longo das emissões nos dias analisados, demonstrada pelo uso de "vocabulário semelhante, ou mesmo idêntico" ao que vinha sendo utilizado por aquelas, tais como «operação militar especial», «operação de polícia», «ação defensiva e preventiva», «República de Lugansk e Donetsk», etc...[547]

As intervenções e comentários das figuras convidadas para a emissão – e não só – claramente pendiam no sentido de uma amplificação da narrativa de justificação da agressão militar e de responsabilização e vilanização da Ucrânia e do Ocidente pelo sucedido, intervenções essas que eram, apenas muito raramente, questionadas e/ou desafiadas pelos pivôs.[548]

Com base em todo este material probatório, o Tribunal revela que ficou demonstrado, por meio da atividade de propaganda que foi levada a cabo pela RT France, um claro incentivo, mesmo antes do início da invasão, à formação e manutenção da situação de violência e instabilidade iniciada pela

[546] Proc. T–125/22, parágrafo 182.
[547] Proc. T–125/22, parágrafos 178, 182 e 190.
[548] Proc. T–125/22, parágrafo 187.

Federação da Rússia, perigando, de modo "importante e diret[o]", a ordem e a segurança públicas na União.[549]

Por fim, e depois do estudo dos elementos probatórios principais, é momento de averiguar concretamente o preenchimento das condições das quais depende a verificação do último requisito, relativo ao princípio da proporcionalidade.

A prossecução de um interesse geral

Relativamente ao requisito da prossecução de um interesse geral, é de concluir que as ameaças em questão, substancializadas pelos órgãos de comunicação social sob a esfera de influência da Federação Russa, constituem "parte[s] integrante[s] do arsenal de guerra moderno" capazes, por conta da verificação de um amplo apoio a uma agressão militar sem precedentes a um país vizinho da União[550], de colocar em causa os alicerces dos coletivos democráticos, posicionando ulteriormente toda a União sob níveis de perigo e ameaça inadmissíveis[551]. O Tribunal refere, assim, que a aplicação destas medidas pretende colocar – com recurso aos meios pacíficos à disposição – um ponto final ao *status quo* de guerra que se gerou na Ucrânia, dados os seus efeitos profundamente desestabilizadores para toda a União.[552]

Posto isto, e em conformidade com o disposto nos artigos 3.º, nº 5 e 21.º, n.º 1, alínea a), b) e c), ambos do TUE, o Conselho procurou, por via da imposição destas medidas, defender os valores da União, os seus interesses fundamentais, a sua segurança e a dos seus cidadãos, a sua independência, a sua integridade e, por fim, o respeito pelos princípios do direito internacional, alvo de uma total desconsideração com a intervenção militar na Ucrânia, que se traduziu numa infração ao vital artigo 2.º, n.º 4 da Carta das Nações Unidas.[553]

Em jeito de conclusão, e como se encontra especialmente demarcado no artigo 21.º, n.º 2, alínea c) do TUE, a atuação da União foi pautada, logo desde início, por um envidamento de esforços não-bélicos que fossem ao encontro da manutenção da paz e da prevenção de conflitos na cena

[549] Proc. T–125/22, parágrafo 188.
[550] Proc. T–125/22, parágrafos 160 e 162.
[551] Proc. T–125/22, parágrafos 160 e 162.
[552] Proc. T–125/22, parágrafo 163.
[553] Proc. T–125/22, parágrafos 161 e 163.

internacional e, face a todos os desenvolvimentos observados, é clara a urgência na prossecução dos objetivos de interesse geral já mencionados, concluindo-se pela verificação deste requisito.[554]

A adequação das medidas restritivas à prossecução dos objetivos de interesse geral

O Tribunal reconheceu, igualmente, a adequação e a pertinência das medidas restritivas para alcançar os objetivos de interesse geral identificados.

A aplicação destas medidas – que se encontra incluída no domínio de um pacote de medidas mais amplo – constitui, deste modo, um meio adequado para exercer pressão sobre a Rússia para que esta suspenda a sua política internacional agressiva, promovendo, neste aspeto, vários objetivos, como o de proteção e manutenção da paz, da ordem e da segurança públicas e da seriedade e integridade do debate público democrático no espaço da União e a nível internacional.[555]

A necessidade das medidas restritivas para a prossecução dos objetivos de interesse geral

Agora, em relação à questão da necessidade das medidas implementadas, é importante avaliar se estas limitações não vão para além do necessário para prosseguir os objetivos de interesse geral já delineados.[556] O princípio da proporcionalidade exige que, na circunstância de várias serem as soluções adequadas à prossecução dos fins identificados, deve sempre optar-se pela que menos enfraqueça a tutela jurídica de direitos fundamentais, observando-se, para o efeito, um equilíbrio entre o dano que as restrições irão causar e os benefícios provenientes da prossecução dos objetivos de interesse geral, de modo a evitar-se uma consumação de excessos.[557]

O estudo da eventual necessidade destas medidas obriga, assim, à realização de um exercício de ponderação relativamente à existência de outras medidas, menos gravosas, para os interesses das pessoas e entidades visadas (a título de exemplo: a aplicação da proibição em apenas alguns países da União, a proibição de apenas algumas "modalidades de radiodifusão de programas", ou a obrigação de colocar um aviso durante as emissões).[558]

---

[554] Proc. T–125/22, parágrafos 161 e 163 a 167.
[555] Proc. T–125/22, parágrafos 193 e 194.
[556] Proc. T–125/22, parágrafo 168.
[557] Proc. T–125/22, parágrafos 168 e 201.
[558] Proc. T–125/22, parágrafo 201.

Neste domínio, é do entendimento do Tribunal que outras medidas alternativas menos restritivas não conseguiriam alcançar, com o mesmo grau de segurança e celeridade, os objetivos que sustentam a aplicação das ditas proibições, dado o "contexto extraordinário e de extrema urgência" que determinou, em primeiro lugar, a aplicação das mesmas.[559]

Aquando da adoção das medidas restritivas, refere o Tribunal, era importante atuar com desenvoltura para combater as "operações de manipulação e de influência hostil" empregues pelos meios de propaganda, dada a particularidade dos primeiros dias corresponderem sempre aos mais sensíveis, impactantes e aos que mais poderiam facilmente moldar a opinião pública sobre a situação de guerra.[560] Posto isso, o Tribunal concluiu pela necessidade das medidas para a prossecução dos fins anteriormente identificados.[561]

A proporcionalidade, em sentido estrito, das medidas restritivas para a prossecução dos objetivos de interesse geral

O Tribunal, neste domínio, propôs-se a analisar a proporcionalidade das medidas em causa, à luz de vários argumentos que serão expostos de seguida.

Em primeiro lugar, dada a importância e centralidade dos objetivos de interesse geral que se pretendem acautelar com o recurso à imposição destas medidas restritivas, é inevitável que determinadas pessoas e entidades possam sair prejudicadas com a aplicação das mesmas.[562] Assim, ainda que o direito à liberdade de expressão e de informação assuma um caráter especial quando é apreciado à luz da atividade de um órgão de comunicação social, no particular âmbito da sua deontológica jornalística[563], o Tribunal entendeu que, face ao tratamento noticioso relatado, a RT France não pode, de modo algum, beneficiar do grau de "proteção reforçada" que o artigo 11.º da Carta concede à liberdade de imprensa.[564]

Nesta circunstância, é de salientar também o artigo 20.º do Pacto Internacional sobre os Direitos Civis e Políticos – adotado em 1966 – do qual são parte os Estados-Membros e a Federação da Rússia.

---

[559] Proc. T–125/22, parágrafos 196 a 198.
[560] Proc. T–125/22, parágrafo 199.
[561] Proc. T–125/22, parágrafos 198 e 200.
[562] Proc. T–125/22, parágrafo 202.
[563] Proc. T–125/22, parágrafo 206.
[564] Proc. T–125/22, parágrafo 206.

O seu n.º 1 refere, por sua vez, que "será proibida por lei qualquer propaganda em favor da guerra" e, por outro lado, o n.º 2 do artigo prevê a proibição por lei de "qualquer apologia do ódio nacional, racial ou religioso que constitua incitamento à discriminação, à hostilidade ou à violência".[565]

Em razão dos elementos de prova carreados para o processo, é facilmente percetível que a RT France e, em última instância, a Federação da Rússia, se encontram a violar flagrantemente as disposições deste pacto, por conta "[d]as afirmações (...) contínua[s], repetida[s] e concertada[s] a favor de uma guerra em curso, contrária ao direito internacional", situação que se torna ainda mais grave pelo facto "[d]essas afirmações emana[rem] de um meio de comunicação social controlado, direta ou indiretamente, pelo Estado agressor".[566]

A RT France encetou, por isso, uma "ação sistemática de disseminação de informações «selecionadas», incluindo informações manifestamente falsas ou enganosas, reveladoras de um desequilíbrio manifesto na apresentação dos diferentes pontos de vista opostos, com o objetivo preciso de justificar e apoiar a referida agressão", sendo, na opinião do Tribunal, imperativo agir – num momento sem precedentes e de absoluta emergência e anormalidade – para bloquear este vetor de propaganda e desinformação construído para amparar os esforços de guerra ilegais na Ucrânia.[567]

Posto isto, o Tribunal concluiu pela proporcionalidade, em sentido estrito, das medidas restritivas – temporárias – que foram aplicadas, deduzindo, por final, pelo preenchimento de todas as exigências legais para a restrição de direitos e interesses fundamentais previstos na Carta, ainda que com todas as desvantagens que isso envolva para a esfera jurídica dos que são prejudicados com a sua adoção.[568]

5.5 A questão da violação da liberdade de empresa

Antes de averiguar o sentido de uma potencial violação do princípio da não discriminação em razão da nacionalidade, o Tribunal analisa a alegada violação do direito à liberdade de empresa da RT France, consagrado no artigo 16.º da Carta.

Tal como resulta do juízo relativo às questões previamente apreciadas, o Tribunal relembra que esta liberdade não é absoluta, podendo comportar algumas restrições à luz dos requisitos do artigo

[565] Proc. T–125/22, parágrafo 209.
[566] Proc. T–125/22, parágrafo 210.
[567] Proc. T–125/22, parágrafos 211 e 212.
[568] Proc. T–125/22, parágrafo 213.

52.º da Carta.[569] De modo a proceder à análise da eventual violação desta liberdade, recorrer-se-á, novamente, aos três critérios enunciados anteriormente.

Relativamente à exigência da previsão por lei da restrição em causa, será de fazer uma referência direta e expressa ao já mencionado aquando da análise da violação da liberdade de expressão e de informação neste domínio, que levou o Tribunal a concluir que tais medidas possuem um "alcance geral", um fundamento legal nitidamente tangível no direito da União, como, também, uma "previsibilidade suficiente".[570]

No que diz respeito ao requisito relativo ao respeito pelo conteúdo essencial da liberdade, o Tribunal relembra, uma vez mais à luz do que já foi exposto nos parágrafos anteriores, que as medidas assumem um caráter reversível e temporário e, nesse sentido, pode concluir-se pelo preenchimento deste requisito.[571]

No que concerne ao terceiro requisito, o Tribunal recorda os interesses fundamentais que estão em jogo e que obrigaram à adoção de um conjunto de medidas, num curto espaço de tempo, para salvaguardar a produção do seu efeito útil.[572]

Neste sentido, é agora possível iniciar um estudo à adequação, necessidade e proporcionalidade em sentido estrito das medidas adotadas. Para o efeito, estabelece-se uma remissão para o disposto, no que concerne a este domínio, aquando da apreciação da alegada violação da liberdade de expressão e de informação. Recordando, o Tribunal referiu que as restrições impostas "parec[iam] plenamente justificada[s]" à luz dos interesses gerais que se procuravam salvaguardar, uma vez que a questão da sua liquidação financeira – por conta da impossibilidade em prosseguir com as suas atividades de radiodifusão – não a impede de realizar outras atividades e, para além disso, a RT France pertence a uma associação que é, na prática, totalmente financiada pelo orçamento do Estado Russo.[573]

Por conta do disposto, o Tribunal julgou improcedente esta questão. [574]

---

[569] Proc. T–125/22, parágrafo 220.
[570] Proc. T–125/22, parágrafo 224.
[571] Proc. T–125/22, parágrafo 225.
[572] Proc. T–125/22, parágrafo 226.
[573] Proc. T–125/22, parágrafos 227 e 228.
[574] Proc. T–125/22, parágrafo 229.

5.6 A questão relativa à violação do princípio da não discriminação em razão da nacionalidade

O último fundamento da RT France reside na violação do princípio da não discriminação em razão da nacionalidade, previsto no artigo 21.º da Carta, com base no argumento de que as medidas apenas se aplicam por conta das suas ligações, financeiras e não só, ao Estado da Federação Russa, e não por conta do seu próprio comportamento e conduta.[575]

O Tribunal rebate estes argumentos referindo que a RT France foi incluída na lista de pessoas e entidades objeto de medidas restritivas "na sequência de uma apreciação d[e] elementos de prova concretos" que demonstram as suas ações de promoção e apoio à agressão militar, enquanto "arma de informação estratégica e de propaganda sob controlo permanente, direto ou indireto, dos dirigentes da Federação da Rússia".[576]

Tendo em conta todas estas circunstâncias, as ligações financeiras da associação a que a RT France pertence, ao Estado da Federação Russa, não podem de qualquer modo ser ignoradas e, numa visão holística da situação, todas estas factualidades desaguam no facto de que a RT France é uma arma de informação ao serviço dos interesses bélicos da Federação da Rússia, uma vez que se verifica uma dependência, a múltiplos níveis, desta.[577]

O Tribunal entendeu, por fim, pela não verificação de uma violação a este princípio e, por conseguinte, nenhum dos pontos de argumentação apresentados pela RT France obteve entendimento favorável junto do Tribunal, sendo que foi negado provimento ao recurso na sua totalidade.[578]

5.7 O pedido de recurso (processo C-620/22 P) e considerações finais

No dia 27 de setembro de 2022, passados dois meses da decisão, a RT France interpôs recurso da decisão emanada pelo Tribunal Geral, pedindo ao Tribunal de Justiça que anule o acórdão proferido no processo T-125/22.

Na sua base de fundamentação, a RT France entende que o Tribunal Geral violou o artigo 41.º, n.º 2 da CDFUE (a respeito, em particular, do direito a ser ouvida e o direito a ter acesso aos processos) ao considerar que não existiu – com base na argumentativa relacionada com a verificação

[575] Proc. T–125/22, parágrafo 232.
[576] Proc. T–125/22, parágrafo 239.
[577] Proc. T–125/22, parágrafo 239.
[578] Proc. T–125/22, parágrafo 242.

de um cenário de extrema urgência e nos objetivos de interesse geral que o Conselho prosseguia – uma violação do seu direito a ser ouvida.[579] Ainda neste sentido, a RT France invoca que os elementos probatórios carreados para o processo foram "desvirtuados" quando o Tribunal Geral conclui que nada que a recorrente pudesse invocar alteraria o curso dos acontecimentos dos procedimentos em apreço.[580]

Para além disso, a RT France alega uma violação do artigo 11.º da CDFUE (relativo à «Liberdade de expressão e de informação»), referindo, uma vez mais, que o material probatório foi desvirtuado pelo Tribunal Geral, tendo em conta que este admitiu que as medidas implementadas eram "necessária[s], adequada[s] e proporcionada[s]" aos objetivos que se pretendiam ver prosseguidos.[581]

Ademais, é igualmente mencionado pela RT France que o Tribunal Geral violou o artigo 16.º da CDFUE (relativo à «Liberdade de empresa») quando inferiu – com a base no caráter provisório das medidas aplicadas e, nas palavras da recorrente, numa "inexistência de prova" que sustentasse o argumento relativo à sua viabilidade financeira – que as restrições em apreço eram proporcionais.[582]

Por fim, a RT France alega a violação do artigo 21.º da CDFUE (relativo à «Não discriminação»), reiterando que os elementos de prova foram, uma vez mais, desvirtuados pelo Tribunal Geral quando este conclui pela não verificação de um ato de discriminação.[583]

Não obstante, a RT France acabou por apresentar, alguns meses depois, a sua intenção de desistir do recurso, o que levou, por seu turno, ao cancelamento do processo no registo do Tribunal, colocando-se um ponto final na lide.[584]

Considerações finais

Constitui facto notório que o início da guerra na Ucrânia foi configurador de um *status quo* absolutamente sem precedentes que acabou por determinar que certos meios de comunicação fossem impedidos de prosseguir com as suas atividades de transmissão no espaço europeu.

---

[579] Recurso interposto em 27 de setembro de 2022 pela RT France do Acórdão proferido pelo Tribunal Geral (Grande Secção) em 27 de julho de 2022 no processo T-125/22, RT France/Conselho (Processo C-620/22 P), 1.º parágrafo dos fundamentos e argumentos.
[580] Segundo parágrafo dos fundamentos e argumentos.
[581] Terceiro parágrafo dos fundamentos e argumentos.
[582] Quarto parágrafo dos fundamentos e argumentos.
[583] Quinto parágrafo dos fundamentos e argumentos.
[584] Despachos do Presidente do Tribunal de Justiça de 28 de julho de 2023. Disponíveis em: <https://curia.europa.eu/juris/document/document.jsf?docid=276144&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=2543151> [19/10/2023].

Ainda que a política europeia neste âmbito continue a ser norteada pelo princípio de uma não intervenção direta, cada caso deve ser analisado à luz das suas circunstâncias e, por vezes, uma decisão mais radical terá de ser forçosamente acionada. O completo encerramento das atividades de radiodifusão de um órgão de comunicação social, por conta da verificação reiterada de casos de disseminação de desinformação e manipulação (que representam perigos intoleráveis para o substrato social e de segurança europeus), corresponde a uma medida que deve apenas ser tomada em *ultima ratio* e contemplar situações completamente inéditas. É precisamente por conta destes motivos e em face do sucedido que a União se viu no papel de implementar medidas de tal envergadura.

6. Tecnologia e Desinformação: As Técnicas de Amplificação e o Caso Particular dos Deepfakes

As táticas empregues para a disseminação de desinformação absorvem extensivamente, como foi possível depreender de toda exposição até então levada a cabo, os grandes resultados observados por conta do progresso tecnológico constante, que possibilita, por seu turno, estratégias de manipulação cada vez mais evoluídas e rebuscadas[585].

As metodologias mais tradicionais aplicadas na disseminação de desinformação, que recorrem, a título de exemplo, ao apoio de páginas falsas de notícias ou publicações orgânicas enganadoras e/ou descontextualizadas em redes sociais, encontram-se rapidamente a ser amparadas, ou mesmo substituídas, por métodos mais automatizados e avançados no âmbito da inteligência artificial, de modo a tornar mais credível e visível o conteúdo falso e enganador que se pretende difundir pelos canais de informação digital.[586]

Ainda que sejam raras as ocasiões onde os métodos mais tradicionais (de disseminação de desinformação) conseguem, efetivamente, produzir os seus efeitos mais nefastos, tal acaba por não ser profundamente relevante, pois o seu propósito é muito maior.[587] Nas sociedades atuais, são já patentes, neste sentido, alguns fenómenos que merecem a nossa atenção, como o crescimento dos níveis de descrença sobre os ecossistemas noticiosos (mesmo naqueles pautados por níveis médios de excelência jornalística mais elevados) e um aumento da paridade de importância entre uma mera opinião e a própria verdade dos factos. No seguimento, é precisamente sob este ceticismo que se encontra a ser construído o alicerce para que os meios tecnicamente mais avançados de manipulação possam, com mais certezas, dar os seus frutos no futuro.[588]

A centralidade que a comunicação visual assume nos dias de hoje torna os *deepfakes* – e em particular os *deepfakes* com motivações políticas – um dos maiores riscos para as democracias e para a própria segurança nacional, dadas as potencialidades danosas observáveis com a prática de atos de manipulação de conteúdo, entre as quais, a distorção da verdade e semeação de dúvida, incerteza,

[585] HELMUS, Todd C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. Santa Monica, CA: RAND Corporation, 2022, p. 1.
[586] HELMUS, Todd C., p. 1.
[587] HELMUS, Todd C., p. 2.
[588] HELMUS, Todd C., p. 2.

desconfiança e desunião que corroem as instituições democráticas, mas também o debate público político livre e transparente e a idoneidade nos canais de informação digital.[589]

Os correntes níveis de autenticidade propiciados pelas avançadas técnicas de *deepfakes*, capazes de retratar fielmente figuras políticas a exprimirem, de viva-voz, pensamentos e ideais que nunca foram por si pronunciados – ou a adotar comportamentos nunca praticados[590], em locais nos quais nunca estiveram – tornará cada vez mais difícil a demonstração empírica de que um acontecimento é real e ocorreu efetivamente, constituindo-se, desta forma, a maior ameaça à verdade e à democracia num futuro próximo.[591]

Posto isto, é possível fornecer um exemplo muito prático das consequências diretamente caóticas da utilização de *deepfakes* em situações de maior sensibilidade. Imaginemos que, no dia anterior à realização de uma eleição – durante o qual o período de reflexão se deve observar, não esqueçamos –, começa a circular pelos canais digitais um *deepfake*, na forma de vídeo e com um nível de autenticidade nunca antes visto, de um dos principais candidatos políticos, ou a comportar-se de uma forma indecente, ou a proferir algumas palavras profundamente ultrajantes e questionáveis.[592] A meras horas da abertura das mesas de voto, seria difícil demonstrar de forma sólida e célere que o dito vídeo se tratava de uma construção artificial, situação essa que iria mais que certamente afetar o desempenho eleitoral do candidato.

Esta questão poderia, igualmente, aplicar-se a outros casos, também eles potencialmente causadores de grandes níveis de tensão social em múltiplas áreas e de uma elevada desconfiança nas instituições e nos órgãos de soberania.[593] Veja-se, a título de exemplo, o caso de um vídeo falso de um agente de segurança pública envolvido em atos de violência policial, de um juiz a aceitar subornos, de uma figura religiosa influente a destratar elementos sagrados de outras religiões[594], ou, até, de um diretor de informação de um canal de televisão generalista líder de audiências a ser alvo de pressões por parte de uma figura política, entre muitíssimos outros.[595]

---

[589] FRAGA-LAMAS, Paula; FERNÁNDEZ-CARAMÉS, Tiago M., *Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality*, IT Professional, 22:2, 2020, pp. 54 e 55; VACCARI, Cristian; CHADWICK, Andrew, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News", *in Social Media and Society*, 6:1, 2020, pp. 1 e 2; GREGORY, Sam, *Mal-uses of AI-generated Synthetic Media and Deepfakes: Pragmatic Solutions Discovery Convening, June 2018: Summary of Discussions and Next Step Recommendations*, Witness, 2018, p. 18; ALAPHILIPPE, Alexander, *et al.,* p. 25.

[590] HELMUS, Todd C., p. 1.

[591] VACCARI, Cristian; CHADWICK, Andrew, p. 2; GREGORY, Sam, p. 18; ALAPHILIPPE, Alexander, *et al.,* p. 25.

[592] HELMUS, Todd C., p. 6.

[593] HELMUS, Todd C., p. 7.

[594] NGUYEN, Thanh Thi *et al., Deep learning for deepfakes creation and detection: A survey*. Computer Vision and Image Understanding, 223, 2022, p. 1.

[595] HELMUS, Todd C., p. 7.

É, assim, extremamente perigoso viver num mundo onde estas ameaças não são combatidas de forma séria, dado que, para além de ser bastante difícil demonstrar a verdade dos factos num tempo útil, "o efeito cumulativo de múltiplas mensagens contraditórias, sem sentido e desorientadoras, que os agentes maliciosos introduzem no discurso digital, pode gerar um estado sistémico de incerteza"[596].

Este "estado sistémico de incerteza" produz, como seria de esperar, efeitos profundamente negativos para o funcionamento das sociedades democráticas, uma vez que todo este grau de ambiguidade deixa as camadas populacionais confusas e abaladas, desconfiando do papel dirigente das autoridades, que, por seu turno, conduz à observação de fenómenos de polarização e de autoexclusão dos assuntos públicos.[597] Para além disso, um grande contexto de indefinição no meio em linha leva os próprios utilizadores a preocuparem-se, ainda menos, com a «verdade» ou «mentira» do que partilham, já que, como vimos, as linhas que separam uma da outra encontram-se mais esbatidas que nunca, contribuindo para uma perspetiva global progressivamente negativa.[598]

Ainda que os *deepfakes* de qualidade imponham um conjunto de exigências aos seus utilizadores – como tecnologia de ponta, avultadas quantidades de dinheiro e recursos para treinar e executar os sistemas, tempo (uma vez que um vídeo *deepfake* de qualidade demora meses para ser criado, hoje em dia) e expertise –, representam uma tecnologia cujos efeitos podem ser explorados de modo cada vez mais vulgarizado e, nesse sentido, é crucial assumir desde já que nos encontramos perante uma corrida contra o tempo enquanto não se criam *deepfakes* de elevada autenticidade com «apenas um clique».[599]

Para ainda «adicionar insulto à injúria», os agentes mal-intencionados recorrem a certas realidades, como *bots* (capazes de atuar nos meios em linha por meio de comportamentos automatizados)[600], *trolls*[601] *e cyborgs* (quando nos referimos a atos que derivam de uma combinação de esforços automatizados e humanos), para amplificar artificialmente (com o apoio de contas falsas, a título de exemplo) o alcance deste conteúdo perigoso, com o objetivo de o tornar mais facilmente sugerível a utilizadores reais.[602]

---

[596] VACCARI, Cristian; CHADWICK, Andrew, p. 3.
[597] VACCARI, Cristian; CHADWICK, Andrew, p. 9.
[598] VACCARI, Cristian; CHADWICK, Andrew, p. 9.
[599] HELMUS, Todd C., pp. 3 e 9.
[600] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 6.
[601] Os *trolls* correspondem, de forma muito sucinta, a "pessoa[s], muitas vezes por detrás de um ou mais perfis inautênticos, que publica[m] ou se envolve[m] em ações provocatórias, dissimuladas e divagantes na Internet com o objetivo de provocar reações emocionais". Cfr. MARCONDES, Francisco Supino; ALMEIDA, José João; NOVAIS, Paulo, "An Exploratory Design Science Research on Troll Factories", *in Journal Integrated Computer-Aided Engineering*, 2023, pp. 1 e 2.
[602] BRADSHAW, Samantha; HOWARD, Philip N., p. 11.

Para o efeito, os seus perpetradores exploram abusivamente os mecanismos de recomendação e de exibição de anúncios das plataformas sociais – baseados nas taxas de retenção do utilizador e nas taxas de cliques e engajamento – para disseminar amplamente as suas narrativas controversas e emotivas.[603] Com as suas atividades de propagação e amplificação de desinformação, verifica-se consequentemente um aumento ao nível do número de interações com esse conteúdo/tópico, garantindo-lhe uma espécie de «legitimidade» que, simultaneamente, força a relegação de conteúdo de confiança para um segundo plano. O atual estado da tecnologia permite, mesmo, – por meio de uma engenhosa circunvenção às políticas de utilização das plataformas – que uma única pessoa consiga controlar e sistematizar o comportamento de centenas de *bots* para a produção de resultados em grande escala[604].

Neste domínio, será de fazer um rápido apontamento ao funcionamento das *troll factories* (agrupamentos coordenados e estruturados de *trolls*), tanto de origem estatal como privada, que podem causar profundas disrupções no ecossistema de informação face ao tipo de atividades que levam a cabo.[605] Ainda que o seu modo de operação seja um pouco enigmático, acredita-se que o seu funcionamento não seja totalmente automatizado, sendo apoiado por figuras humanas, no caso, *cyborgs*.[606] Neste sentido, os avanços tecnológicos vivenciados ultimamente, particularmente ao nível das LLM's (*Large Language Models*) – como o ChatGPT ou o Bard – constituem, naturalmente a par dos *deepfakes* (e, mesmo, de outros instrumentos de IA mais orientados para o caráter visual), ferramentas perigosíssimas nas mãos de *troll factories* com sofisticados e extensos recursos.[607]

Este fenómeno possui igualmente uma vertente financeira associada, uma vez que existe todo um mercado dedicado à compra e venda de contas falsas e ao *bypass* de mecanismos de segurança. A título exemplificativo, este tipo de negócios acaba também por se tornar muito recorrente em situações onde se procura inflacionar o número de seguidores de uma determinada conta (ou comunidade/grupo), de modo tornar o seu perfil e o conteúdo por si distribuído mais credível e legítimo[608].

---

[603] VAN RAEMDONCK, Nathalie; MEYER, Trisha, pp. 4 e 5.

[604] A título de exemplo, no México, estimava-se que 18% de todo o tráfego do Twitter era criado a partir de *bots*, bloqueando a visualização de conteúdo orgânico de qualidade (Cfr. ALAPHILIPPE, Alexander, *et al.,* pp. 14 e 22).

[605] MARCONDES, Francisco Supino; ALMEIDA, José João; NOVAIS, Paulo, pp. 1 e 2.

[606] MARCONDES, Francisco Supino; ALMEIDA, José João; NOVAIS, Paulo, pp. 1 e 16.

[607] MARCONDES, Francisco Supino; ALMEIDA, José João; NOVAIS, Paulo, pp. 11-14.

[608] Em 2018, estimava-se que mais de metade dos 55 milhões de seguidores da conta de Twitter do ex-Presidente dos Estados Unidos da América, Donald Trump, provinham de contas inautênticas (Cfr. ALAPHILIPPE, Alexander, *et al.,* p. 23); A este propósito, Cfr. MARWICK, Alice; LEWIS, Rebecca, p. 38.

Numa outra vertente, a utilização de contas inautênticas – criadas para fazer dilatar o número de seguidores, "gostos", comentários e partilhas em contas de figuras políticas e entidades governamentais, ou, até mesmo, do número de assinaturas e opiniões em petições e consultas públicas em linha – pode, efetivamente, manipular e perturbar os processos democráticos e a própria perceção do público sobre a imagem destes atores e entidades, exigindo-se, por esse motivo, uma maior e mais profunda atuação de todas as partes envolvidas no combate a comportamentos inautênticos em linha.[609]

A importância na deteção e neutralização precoce das contas inautênticas é crucial uma vez que estas assumem a sua maior relevância nos momentos iniciais de uma campanha de desinformação, atuando massivamente para que determinado conteúdo ou tópico figure nos grandes fluxos de informação e se torne viral o mais cedo possível[610]. A partir daí, são os utilizadores orgânicos que levam, involuntariamente (ou não), a desinformação a ainda mais públicos, por via de sucessivas interações com o mesmo.[611]

Posto isto, traduzem igualmente uma enorme relevância esforços relacionados com a rotulação de contas automatizadas – e, naturalmente, com a suspensão/remoção, quando se verifique a violação das políticas de utilização das plataformas – para que seja mais fácil ao utilizador compreender e ficar mais sensibilizado para o método de funcionamento dos fluxos de informação e, por conseguinte, para o facto de estar rodeado de perfis que nem sempre são controlados diretamente por uma figura humana.[612]

Ainda assim, o veloz aparecimento e desaparecimento deste tipo de contas aliado ao surgimento de *bots* cada vez mais sofisticados – com comportamentos mais e mais indetetáveis – torna essa missão bastante complexa, mesmo para quem atua com base num acesso tendencialmente ilimitado, como é o caso das grandes plataformas[613]. Torna-se, assim, fundamental a canalização de maiores investimentos, especialmente por parte das plataformas digitais – que possuem um acesso mais detalhado e desimpedido ao funcionamento dos seus próprios sistemas –, no domínio da identificação e remoção de contas inautênticas e ilegítimas.

Levando todo o exposto em consideração, a utilização das novas tecnologias pode – e deve – ser explorada para construir ferramentas que protejam e favoreçam um ambiente em linha mais

---

[609] ALAPHILIPPE, Alexander, *et al.,* p. 23; MARWICK, Alice; LEWIS, Rebecca, p. 38.
[610] ALAPHILIPPE, Alexander, *et al.,* p. 34.
[611] Sobre este tema, Cfr. SCHÜNEMANN, Wolf J., "A threat to democracies? An overview of theoretical approaches and empirical measurements for studying the effects of disinformation", in Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, Routledge, 2022, p. 42.
[612] ALAPHILIPPE, Alexander, *et al.,* p. 75.
[613] ALAPHILIPPE, Alexander, *et al.,* p. 34.

seguro e confiável. Neste ponto, é necessário apostar em técnicas de verificação, deteção e rastreio de conteúdos, fontes e fluxos de desinformação, como em metodologias de análise de parâmetros que permitam a atribuição de níveis de confiança ao trabalho jornalístico desenvolvido pelos órgãos de comunicação social, sem esquecer a criação de demais instrumentos que concretizem, de forma extensiva, um ecossistema em linha mais diversificado, conversacional, adaptável e transparente.[614]

6.1 Os *deepfakes*

Antes de avançarmos para uma apreciação mais cuidada a respeito dos métodos de criação e deteção de *deepfakes*, afigura-se obrigatório analisar conceitualmente o significado proporcionado por estes no âmbito da tecnologia de IA, que os tornam atualmente uma das principais ameaças no campo da desinformação.

A etimologia da palavra deriva da junção dos termos *«deep learning»* (um subdomínio do *machine learning,* que, por seu turno, é também um subdomínio da IA) e *«fake»*[615], e corresponde ao "produto de aplicações de IA que fundem, combinam, substituem e sobrepõem imagens e clips de vídeo para criar vídeos falsos que parecem autênticos"[616], podendo fabricar, a título de exemplo, "vídeo[s] humorístico[s], pornográfico[s] ou político[s] de uma pessoa a dizer qualquer coisa, sem o consentimento da pessoa cuja imagem e voz estão envolvidas", com poucos ou nenhuns sinais de adulteração visíveis a olho nu[617].

6.1.1 Os métodos de criação de *deepfakes*

Os *deepfakes* podem ser gerados com recurso a diversas técnicas relacionadas com tecnologias no âmbito do *deep learning*[618], como *deep autoencoders* e redes adversárias generativas (*Generative Adversarial Networks*, GAN's).[619] Para efeitos do presente subcapítulo, proceder-se-á a uma explicação sumária das capacidades apresentadas por estas duas técnicas.

Todo o ser humano detém uma faixa previsível relativa aos movimentos da sua boca, dos seus maxilares, da sua cabeça (entre outros), que coincidem, por seu turno, com os sons que emitem e que

[614] *Comunicação: Combater a desinformação em linha: uma estratégia europeia*, p. 12.
[615] NGUYEN, Thanh Thi, *et al.,* p. 1.
[616] WESTERLUND, Mika, *The Emergence of Deepfake Technology: A Review*, Technology Innovation Management Review, 9:11, 2019, p. 1.
[617] WESTERLUND, Mika, p. 1.
[618] NGUYEN, Thanh Thi, *et al.,* p. 1.
[619] FRAGA-LAMAS, Paula; FERNÁNDEZ-CARAMÉS, Tiago M., p. 55; VACCARI, Cristian; CHADWICK, Andrew, p. 2.

caracterizam a articulação da sua fala.[620] Essas características serão, precisamente, analisadas e reconstruídas pelos *softwares* para a criação de *deepfakes* genuínos, sendo necessária, assim, uma elevada quantidade de conteúdo audiovisual do alvo para que a construção do *deepfake* seja a mais convincente possível.[621]

Dada a exposição mediática de determinadas figuras de enorme relevância pública – como políticos e políticas –, e a facilidade e imediatismo associados à propagação de conteúdo em linha, não será difícil reunir o material necessário para criar e disseminar, com o apoio da mais sofisticada tecnologia, *deepfakes* bastante fidedignos, surgindo aí o nosso principal problema.

GAN's

As GAN's são informadas por imagens de vídeo genuínas que funcionam como *sets* de treino e atuam com o intuito de criar uma mecânica de oposição e contradição entre duas redes neuronais de *software*, de modo que uma vá sempre melhorando com base no desempenho da outra.[622]

Uma delas consiste num gerador que, num momento inicial, cria imagens ou vídeos a partir de ruídos aleatórios, com o intuito final de criar imagens ou vídeos falsos de elevada qualidade. A outra rede, por sua vez, corresponde a um discriminador que avalia se a imagem de entrada é genuína ou falsificada pelo gerador.[623]

Graças à competição constante entre as duas redes, como se de um "falsificador e detetive" se tratasse[624], o gerador será cada vez mais capaz de produzir imagens sintetizadas de elevada autenticidade, uma vez que vai corrigindo os erros levantados pela atividade de deteção levada a cabo pelo discriminador.[625]

---

[620] VACCARI, Cristian; CHADWICK, Andrew, p. 2.
[621] VACCARI, Cristian; CHADWICK, Andrew, p. 3.
[622] VACCARI, Cristian; CHADWICK, Andrew, pp. 2 e 3; BROWNLEE, Jason, *A Gentle Introduction to Generative Adversarial Networks (GANs)*, Machine Learning Mastery, 2019. Disponível em: <https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/> [06/10/2023].
[623] SHEN, Tianxiang, *et al., "Deep Fakes" using Generative Adversarial Networks (GAN)*. Noiselab, 2018, p. 2.
[624] SHEN, Tianxiang, *et al.,* p. 2.
[625] SHEN, Tianxiang, *et al.,* p. 2.

Deep autoencoders

A técnica utilizada no domínio dos *deep autoencoders* reúne, à semelhança dos GAN's, uma dupla atuação, que inclui codificadores e descodificadores.[626]

Neste domínio, é utilizado um codificador que reúne, na forma de um vetor latente, as características mais relevantes da imagem ou vídeo original, com o apoio de tecnologia de redução de dimensionalidade e compressão de imagem.[627]

Com base nessa informação recolhida, inicia-se um processo de adulteração da imagem ou vídeo, por via da manipulação desse vetor latente, com o intuito de formar uma aparência distinta por comparação à imagem ou vídeo original.[628]

Por fim, é utilizado um descodificador para transformar o vetor latente, manipulado, novamente numa imagem, que retratará uma reprodução sintetizada de acordo com as alterações pretendidas.[629]

6.1.2 As técnicas de deteção de *deepfakes*

Dados os constantes avanços no campo do *deep learning*, as imprecisões observadas nos resultados apresentados por *software* de criação de *deepfakes* são cada vez mais difíceis de detetar mesmo à luz de um olhar mais atento. Para além disso, os processos relacionados com o desenvolvimento de programas informáticos de deteção de *deepfakes* encontra-se, infelizmente, atrás dos esforços atualmente empregues para a criação dos mesmos.[630] Torna-se, assim, ainda mais premente a necessidade de investir no desenvolvimento de programas de deteção especialmente direcionados, tanto para o mundo das redes sociais e das aplicações de mensagens, como para o setor dos media e seus jornalistas[631].

Como se observou anteriormente, as GAN's, responsáveis pela criação de *deepfakes*, funcionam com o apoio de um gerador e de um discriminador. No domínio da criação de *software* de deteção é, deste modo, crucial focar a atenção no desenvolvimento de discriminadores mais eficientes na deteção de conteúdo adulterado.[632]

---

[626] VACCARI, Cristian; CHADWICK, Andrew, p. 2.
[627] NGUYEN, Thanh Thi, *et al.,* p. 2.
[628] NGUYEN, Thanh Thi, *et al.,* pp. 2 e 3.
[629] NGUYEN, Thanh Thi, *et al.,* pp. 2 e 3.
[630] HELMUS, Todd C., p. 10.
[631] ALAPHILIPPE, Alexander, *et al.,* p. 25.
[632] HELMUS, Todd C., p. 10.

Uma avaliação mais aprofundada neste sentido incidirá, sobretudo, sobre algumas informações relacionadas com as fontes e metadados do conteúdo em questão, passando, também, por técnicas de diminuição da velocidade e análise de *frames*, de modo a identificar sinais que indiciem alguma adulteração, como "movimentos não naturais e imprecisões, falta de nitidez em comparação com as zonas não-faciais do vídeo, alterações do tom de pele junto dos limites do rosto", entre muitíssimos outros.[633]

De relembrar, por fim, que a eficácia das técnicas a serem descritas nas próximas páginas, face à natureza dinâmica e de constante mutação do avanço tecnológico, é limitada, não só pelo tempo, mas também pelas características dos sistemas utilizados para criar *deepfakes*, que podem, de um modo mais facilitado – no caso de sistemas mais avançados –, evadir-se de determinados sistemas de deteção.

Combinação de redes neuronais convolucionais (CNN) e redes neuronais recorrentes (RNN)

Um dos principais métodos de deteção de adulteração de rostos em vídeos *deepfake* assenta num método que compreende duas fases.[634]

Numa primeira fase, denominada de pré-processamento, procura-se identificar e posteriormente recortar e ordenar os movimentos da cara ao longo de uma sequência de *frames* (quadros), de modo a identificar disparidades.[635]

Por sua vez, numa segunda fase, inicia-se um processo de discriminação de *frames* manipulados face aos originais, por meio da combinação de redes neuronais convolucionais (CNN)[636] e redes neuronais recorrentes (RNN)[637].[638]

---

[633] ALAPHILIPPE, Alexander, *et al.,* p. 25.
[634] NGUYEN, Thanh Thi, *et al.,* p. 6.
[635] NGUYEN, Thanh Thi, *et al.,* p. 6.
[636] As redes neuronais convolucionais correspondem a um conjunto de "camadas convolucionais e de agrupamento que extraem características relevantes de uma imagem de entrada, seguidas de uma ou mais camadas totalmente ligadas que utilizam essas características para fazer uma previsão" (Cfr. KRICHEN, Moez, *Convolutional Neural Networks: A Survey*. Computers, 12(8):151, 2023, p. 4.
[637] As redes neuronais recorrentes representam, por sua vez, "um tipo de rede neuronal que contém *loops*, permitindo que as informações sejam armazenadas dentro da rede", utilizando, para o efeito, "o raciocínio de experiências anteriores para informar eventos futuros" (Cfr. DeepAI, *Recurrent Neural Network*. Disponível em: <https://deepai.org/machine-learning-glossary-and-terms/recurrent-neural-network> [30/09/2023]).
[638] NGUYEN, Thanh Thi, *et al.,* p. 6.

A utilização de um descritor de sequência temporal

Um outro método, também utilizado para detetar manipulações em forma de vídeo, reúne novamente as redes neuronais convolucionais (CNN) com um tipo de redes neuronais recorrentes (RNN), as LSTM (*long short-term memory*, ou memória longa a curto prazo).

Os vídeos *deepfake* revelam, normalmente, algumas incoerências intra e entre *frames* e, sabendo disso, as CNN's são primeiramente utilizadas para deduzir algumas características da imagem justamente ao nível de cada *frame*, características essas que são depois enviadas para o LSTM para criar um "descritor de sequência temporal", que apoiará, por fim, um processo de deteção dos vídeos manipulados, tendo por base uma análise probabilística da natureza que cada *frame* assume: genuína ou sintetizada.[639]

Análise do pestanejar dos olhos

Sabendo que, em alguns vídeos *deepfake,* o sujeito pestaneja os olhos de forma muito pouco frequente, face ao considerado comum para um ser humano – uma vez que as imagens disponíveis de figuras públicas, e que são depois utilizadas para treinar os modelos, raramente contêm o sujeito de olhos fechados –, o próximo método de deteção procura observar, com atenção, precisamente as áreas mais próximas dos olhos para, com o auxílio de uma rede neuronal convolucional recorrente de longo prazo (LRCN), estabelecer uma "previsão dinâmica de estado".

Neste LRCN, veremos em funcionamento, como se pode depreender pelo nome, uma CNN e um LSTM, que, em articulação, procuram antecipar a probabilidade do pestanejar – probabilidade essa que é reveladora, por sua vez, de "fortes dependências temporais" – que apoiará a criação de padrões para ajudar na deteção de inconsistências.[640]

A análise de artefactos visuais

Alguns métodos de deteção de *deepfakes* procuram, igualmente, atentar à presença de artefactos e inconstâncias visuais para mais facilmente detetar um vídeo sintetizado.

---

[639] NGUYEN, Thanh Thi, *et al.,* p. 6.
[640] NGUYEN, Thanh Thi, *et al.,* pp. 6 e 7.

Neste sentido, sugere-se a observação de vários pontos do rosto – como olhos, dentes e contornos faciais – nos quais mais facilmente se notam alguns erros ao nível da incidência luminosa, de pormenores ligados aos reflexos e texturas e outras "estimativas imprecisas da geometria subjacente".[641]

Estas imprecisões são, assim, exploradas por mecanismos de deteção baseados em dois classificadores (regressão logística e uma rede neuronal pequena) que separam os *deepfakes* de vídeos autênticos.[642]

PRNU

Uma das técnicas igualmente utilizada no domínio da deteção de vídeos sintetizados prende-se com a análise da *«photo response non uniformity»*, que corresponde a uma parte do ruído-padrão no sensor de imagem das câmaras e que está presente nas capturas feitas pelas mesmas, funcionando, por isso, como uma espécie de «impressão digital» da câmara.[643]

No caso, tendo em conta que os vídeos modificados com *software* de criação de *deepfakes* alteram as informações associadas aos padrões originais de PRNU na área do rosto, as diferenças registadas constituem automaticamente um sinal de alerta.[644]

Marcas radioativas

Outras das técnicas que pode resultar num avanço dos métodos de deteção consiste na integração de «marcas radioativas» em conteúdo genuíno que é posteriormente utilizado como meio de aprendizagem para a criação de *deepfakes*.[645]

Com esta aproximação, os sistemas de deteção podem identificar, de forma muito tênue, material sintetizado, uma vez que este iria estar «contaminado», dado que foi treinado com base em dados «poluídos», cujas marcas iriam reconduzir os discriminadores à conclusão de que foi usado um *software* de criação de *deepfakes*.[646]

---

[641] NGUYEN, Thanh Thi, *et al.,* p. 7.
[642] NGUYEN, Thanh Thi, *et al.,* p. 7.
[643] NGUYEN, Thanh Thi, *et al.,* p. 8.
[644] NGUYEN, Thanh Thi, *et al.,* p. 8.
[645] HELMUS, Todd C., p. 11.
[646] HELMUS, Todd C., p. 12.

Deste modo, as marcas radioativas, cuidadosamente plantadas em conteúdo original, iriam acompanhar todo o processo de adulteração e contaminar o conteúdo manipulado, tornando-o mais detetável.[647]

Para que esta metodologia produza os seus frutos, será naturalmente necessário um empenho no sentido de «infetar» os *sets* de treino que se encontram disponibilizados publicamente. Mais que isso, será especialmente importante contaminar o conteúdo no qual figuras de relevância pública – mais comummente alvo de investidas nesta esfera – assumam uma certa preponderância, de modo que, caso esse conteúdo seja utilizado para treinar e criar *deepfakes*, as máquinas de deteção consigam ver claramente «para além de toda a neblina».[648]

Ferramentas de proveniência

Na senda do disposto anteriormente, e assumindo que existe um "limite matemático fundamental" que impende sobre a habilidade de um discriminador em detetar *deepfakes* – dado que os contínuos avanços tecnológicos irão incontornavelmente desaguar na criação de imagens tão semelhantes e indiscrimináveis que, mesmo um sistema avançado, não será capaz de detetar as diferenças[649] –, torna-se necessário apostar em alternativas e uma delas corresponde, precisamente, à utilização de ferramentas de proveniência.

Neste sentido, a Iniciativa para a Autenticidade de Conteúdo (CAI) elaborou uma abordagem que possibilita o registo da proveniência de imagens, importante para garantir que as fotos contêm, no seu conjunto de metadados, um aglomerado de referências que permite, por meio de um *hashing* de ativos criptográficos, criar assinaturas que denunciam se o conteúdo em causa foi alvo de adulteração.

Esta iniciativa promove, deste modo, a transparência, uma vez que todo o registo fotográfico realizado ao abrigo desta tecnologia verá – sempre que for partilhado nos meios em linha – acoplado um botão de informações bem visível e rapidamente acessível no canto superior direito da foto, do qual constará a foto original (se a foto partilhada tiver sido alterada), quando e quem tirou foto, o dispositivo utilizado, entre muitas outras informações.

Este mecanismo de transparência, que irá ser gradualmente estendido ao conteúdo em forma de vídeo, deve, desde logo, ser utilizado pelas profissões mais relevantes (na área do jornalismo, a

[647] HELMUS, Todd C., p. 12.
[648] HELMUS, Todd C., p. 12.
[649] FRAGA-LAMAS, Paula; FERNÁNDEZ-CARAMÉS, Tiago M., p. 55; HELMUS, Todd C., p. 11.

título de exemplo), de modo a garantir alguma segurança e tranquilidade aos internautas que navegam em linha, que terão, ao seu dispor, um indicador de confiança.[650]

6.1.3 Outros meios a considerar para a mitigação dos efeitos negativos dos *deepfakes* maliciosos

Disponibilização de deep repositories e organização de concursos para a deteção de deepfakes

As grandes plataformas digitais possuem, neste domínio, um papel muito relevante que as permite apoiar amplamente a gama de esforços de deteção. Para esse efeito, e como já fez a Google em 2019[651], é importante a disponibilização de um acesso vasto a *«deep repositories»* dos quais conste conteúdo sintetizado, essencial para treinar os sistemas de deteção[652], de modo que estes estejam sempre a par das últimas incursões maliciosas neste domínio.

O papel das plataformas em linha não se fica, no entanto, por aqui. A organização de concursos – nos quais são contemplados prémios para os participantes – que estimulem a criação de mecanismos de deteção é uma via, também ela muito relevante, para desbravar caminho neste domínio.[653]

Limitar o acesso a software de deteção de deepfakes

Uma das maiores preocupações neste domínio prende-se com o facto dos agentes mal-intencionados recorrerem aos mecanismos de deteção mais avançados para treinarem os seus próprios sistemas, de modo a criar uma espécie de «sistema definitivo para a criação de *deepfakes*».

É, assim, crucial limitar o acesso a este tipo de tecnologias – particularmente àquelas que são mais avançadas computacionalmente[654] –, que devem apenas ser utilizadas por entidades credenciadas para o efeito. Do mesmo modo, é importante também tornar os *training data sets* menos acessíveis, pelos mesmos motivos.[655] Neste sentido, seria interessante verificar-se uma onda de reuniões entre os

---

[650] HELMUS, Todd C., p. 13.
[651] MIT Technology Review, *Google has released a giant database of deepfakes to help fight deepfakes*, 2019. Disponível em: <https://www.technologyreview.com/2019/09/25/132884/google-has-released-a-giant-database-of-deepfakes-to-help-fight-deepfakes/> [10/10/2023].
[652] FRAGA-LAMAS, Paula; FERNÁNDEZ-CARAMÉS, Tiago M., p. 58.
[653] HELMUS, Todd C., p. 14.
[654] HELMUS, Todd C., p. 17.
[655] HELMUS, Todd C., p. 12.

principais *stakeholders*, para a estipulação de um conjunto de regras relativamente à obtenção de acesso a este tipo de sistemas e dados.[656]

6.1.4 Breve *overview* sobre as implicações da Proposta de Regulamento sobre a Inteligência Artificial para os *deepfakes*

Face aos riscos e às grandes oportunidades que decorrem da exposição da população humana à IA, as Instituições Europeias encontram-se já a delinear um conjunto de obrigações – baseadas numa abordagem centrada no risco que pretende não representar um entrave à inovação na área – para controlar os efeitos mais indesejáveis da proliferação de determinados sistemas de IA no âmbito dos direitos fundamentais.[657]

Por conseguinte, resta tecer sumárias observações acerca das implicações da mais recente proposta de Regulamento sobre a Inteligência Artificial para a temática da criação e manipulação de conteúdos.

Para o efeito, esta proposta de Regulamento agrupa os sistemas de IA de acordo com uma classificação de risco, de quatro níveis, feita com base em sistemas que apresentem riscos mínimos, limitados, elevados e inaceitáveis.[658] No caso dos *deepfakes*, será de analisar primeiramente o elenco de riscos limitados, que determinam a implementação de obrigações de transparência e informação aos seus utilizadores. No caso, e observando o disposto no artigo 52.º, n.º 3 da proposta, encontram-se justamente englobados neste grupo os sistemas de geração ou manipulação de conteúdo.

Levando em mente os perigos que estes sistemas de IA representam para a segurança e a identidade de uma pessoa, os utilizadores[659] que recorram a mecanismos de criação ou manipulação de conteúdo multimodal (imagem, vídeo ou áudio) – "consideravelmente semelhant[e] a pessoas, objetos, locais ou outras entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa" –, terão obrigatoriamente de revelar, de um modo claro, que os ditos

---

[656] HELMUS, Todd C., p. 12.

[657] Comissão Europeia, Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, COM(2021) 206 final – Alterações de 13 de junho de 2023 – subcapítulo 1.1 relativo às «Razões e objetivos da proposta» e subcapítulo 1.2. relativo à «Coerência com as disposições existentes da mesma política setorial».

[658] RAMOS, José Ricardo Marcondes, "Supervisão, classificação e certificação dos sistemas de IA na Proposta de Regulamento sobre Inteligência Artificial", *in Direito em Mudança: A Proposta de Regulamento Europeu sobre Inteligência Artificial - Algumas questões jurídicas*, 2023, p. 35.

[659] De acordo com a definição prevista no artigo 3.º, n.º 4 da Proposta, um «Utilizador» corresponde a "uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional".

conteúdos artificiais foram criados ou manipulados com o recurso a estes sistemas automatizados, permitindo que o destinatário do material sintetizado tome decisões ponderadamente.

As únicas exceções a estas obrigações de transparência verificam-se quando é efetuada uma utilização destes sistemas de IA para fins considerados legítimos, como o seu uso no âmbito da manutenção da ordem pública, ou em casos de liberdade de expressão.[660]

É com base neste ponto que cumpre, agora, fazer uma ligação lógica ao elenco de sistemas de risco elevado, dado que o grupo de sistemas de IA destinados a assegurar a manutenção da ordem pública é assinalado como detendo este risco elevado, grupo esse que, por conseguinte, se pode materializar justamente num mecanismo utilizado por autoridades policiais para a deteção de *deepfakes.*[661]

Sabendo, então, que o futuro da atividade de investigação penal beneficiará do apoio de sistemas de IA[662], existem, naturalmente, algumas inquietações que devem ser acauteladas logo desde início e que estão relacionadas com a atividade das autoridades policiais em nome da defesa da segurança e da ordem públicas.[663]

A propósito, a utilização de ferramentas de IA por parte de autoridades policiais é passível de resultar num estado de vigilância avançada, no qual os cidadãos se encontram, particularmente no âmbito da tutela efetiva dos seus direitos fundamentais e processuais, numa situação de inferioridade e desigualdade.[664] Para além disso, os próprios sistemas de IA podem cometer imprecisões e erros, sendo que nessas circunstâncias se podem consubstanciar resultados profundamente negativos que tornam ainda mais frágil esta posição de desigualdade em que o cidadão comum se encontra.[665]

Precisamente por todos esses motivos, torna-se indispensável garantir fiabilidade e a transparência dos dados utilizados para o treino destes sistemas e, consequentemente, dos resultados por eles apresentados, sob o risco de se gerar um ambiente de opressão e suspeição discriminatória junto das populações.[666]

Assim, a proposta de Regulamento, atendendo ao risco particularmente elevado, defende a implementação inicial de um conjunto de normas que assegurem a testagem exaustiva deste tipo de

---

[660] RAMOS, José Ricardo Marcondes, p. 41.
[661] De acordo com o Anexo III, n.º 6, alínea c) da Proposta de Regulamento.
[662] Proposta de Regulamento Inteligência Artificial, considerando 38.
[663] Proposta de Regulamento Inteligência Artificial, considerando 38.
[664] Proposta de Regulamento Inteligência Artificial, considerando 38; Comissão Europeia, *Plano de Ação da UE para os Direitos Humanos e Democracia 2020-2024*, JOIN(2020) 5 final, 2020, p. 3.
[665] Proposta de Regulamento Inteligência Artificial, considerando 38.
[666] Proposta de Regulamento Inteligência Artificial, considerando 38; RAMOS, José Ricardo Marcondes, pp. 47-49.

sistemas antes da sua aplicação a casos concretos[667] – em prol da minimização do risco e da maximização da segurança na sua utilização – e, numa fase posterior, afigura-se tão ou mais relevante assegurar um acompanhamento vigilante do funcionamento estável e eficiente dos ditos sistemas, uma vez que – tratando-se de IA – existe toda uma curva de aprendizagem e melhoria contínua que deve ser examinada constantemente.[668]

[667] Proposta de Regulamento Inteligência Artificial, considerando 62.
[668] RAMOS, José Ricardo Marcondes, pp. 50, 52, 54 e 55.

Conclusão

A revolução tecnológica que presenciamos no dia-a-dia coloca mais e mais quebra-cabeças no domínio do combate à disseminação de desinformação, com consequências potencialmente devastadoras para áreas vitais da nossa democracia, para as quais a integridade da informação constitui pré-condição.

Nesta esteira, será importante refletir e valorizar o jornalismo de excelência, acautelar a atual situação de progressiva desconfiança com uma comunicação estratégica eficiente, fomentar um papel de destaque na promoção de sociedades mais resilientes e conscientes e equacionar outros impreteríveis ajustes levando em consideração o impacto das grandes plataformas digitais privadas.

O caminho que tem vindo a ser trilhado pela União Europeia – alicerçado numa resposta multifacetada, estruturada e holística – constitui um passo importante em direção a um ecossistema informativo mais seguro, responsável e fidedigno. Não obstante, subsistem algumas vulnerabilidades no escopo de soluções pugnadas pelas Instituições Europeias. Neste sentido, os instrumentos normativos tratados assumem, ainda, uma postura muito comedida, dadas as possíveis implicações negativas para a esfera de direitos fundamentais, contexto esse que merece, naturalmente, uma aproximação mais cuidadosa e delicada.

A este propósito, ainda que o RSD disponha de um enquadramento inicial hábil nesta matéria, o seu texto legal apresenta-se muito centrado na defesa contra o conteúdo ilegal, sendo que a temática de combate à disseminação de desinformação encontra-se, consequentemente, relegada para um segundo plano, remanescendo a ideia de que a resposta a esta ameaça ainda se apresenta numa fase precária e instável.

Neste seguimento, é igualmente importante salientar que o modelo de corregulação previsto no RSD se destaca pela atribuição de um elevado grau de responsabilidade às plataformas neste âmbito, que, por seu lado, resulta numa dificultação das diligências efetuadas pelas entidades responsáveis pela monitorização da aplicação do Regulamento. Nesse sentido, conjetura-se automaticamente uma situação de possível evasão silenciosa ao cumprimento das normas nele previstas, comprometendo-se, ulteriormente, a produção dos resultados pretendidos.

Para além disso, e como se viu, a aposta na autorregulação patente no Código de 2022, apesar de permitir uma resposta mais flexibilizada à ameaça e possibilitar um maior grau de protagonismo dos principais agentes privados – acautelando-se uma grande preocupação e cooperação com os interesses destes intervenientes imprescindíveis –, caracteriza uma abordagem assente numa

voluntariedade que se acha à mercê dos vários interesses, entre os quais financeiros, dos vários diretores executivos das grandes plataformas digitais. O súbito abandono da rede social X do Código de 2022 – uma figura fortíssima a este respeito – representa, justamente, um dos exemplos mais plasmadores da sensação de incerteza e irresolução que assombra os esforços de autorregulação.

Nesta continuidade, a proposta de Regulamento sobre a transparência e o direcionamento da propaganda política representa, no que lhe toca, uma grande expectativa neste âmbito, uma vez que apresenta medidas mais concretas e resolutas. Sem embargo, o seu propósito de atuação encontra-se circunscrito à propaganda política, não revelando soluções de fundo para a problemática que se coloca ao nível do conteúdo falso e enganador organicamente difundido pelas redes e partilhado, de forma consciente ou não, pelos canais de informação incessantemente.

Por fim, a aposta na literacia mediática deve ser encarada com mais seriedade e sensatez. Como foi descrito, a aposta na sensibilização das sociedades para existência e para os perigos desta ameaça torna-as, instintivamente, mais vigilantes e predispostas a defender a verdade nos assuntos que produzam implicações para temas de interesse e mobilização pública. Em Portugal, o trabalho levado a cabo por determinados projetos neste enredo – como o Polígrafo, o Observador – Fact Check e o Público – desempenham, tanto no meio em linha como no horário nobre da televisão portuguesa, um prolífico esforço para dar a conhecer o caráter manipulador e/ou descontextualizado que determinados conteúdos podem evidenciar.

Por este conjunto de motivos, afigura-se necessário apoiar as estruturas (como o EDMO) que desenvolvem a sua atividade neste âmbito e colocar em prática as normas que pugnam pela expansão de projetos neste domínio. É, assim, particularmente importante atuar nos Estados-Membros onde esta realidade – por ser mais raramente divulgada – causa mais danos, por meio de iniciativas que reúnem e incluem, de forma transparente, todos os quadrantes da sociedade, em nome de uma finalidade comum: a defesa da verdade.

Por seu turno, a nível tecnológico, a trajetória de ascensão dos novos perigos no mundo da IA encontra-se longe de atingir um nível de cristalização – bem pelo contrário –, percorrendo atualmente um curso longo que se vai evidenciando dissimuladamente.

No futuro, os ataques perpetrados por agentes mal-intencionados ao coração e às liberdades mais representativas das democracias desvendará traços de criatividade e malignidade nunca antes vistos e, por esse motivo, configura-se obrigatório ir para além da adoção exclusiva de instrumentos legislativos – incapazes de acompanhar apropriadamente o avanço tecnológico – e optar, complementarmente, por estratégias diversificadas e impulsionadoras de pontos de cooperação

dinâmicos, tanto ao nível dos Estados-Membros e da União, como a nível internacional, decisivos para o cabal entendimento das potenciais proporções que o fenómeno pode comportar.

Assim, perante um horizonte temporal caracterizado por profundas e constantes transformações e pela verificação de progressivos ataques ao valor e à relevância do veraz e factual[669], exige-se das mais altas instâncias um acompanhamento multidisciplinar, agregado, proativo, ousado, dúctil e permanentemente vigilante, que encare – de modo diligente – as ameaças a todo e qualquer princípio democrático que a desinformação procure subverter.

Em jeito de término, cumpre apenas citar uma frase de Hannah Arendt, cuja forma de pensar – brindada de uma intemporalidade singular – deve servir como alerta para o conjunto de desafios que se avizinham:

"Um povo que já não pode acreditar em nada não pode decidir-se por si próprio. Está privado não só da sua capacidade de ação, mas também da sua capacidade de pensar e de julgar. E com um povo assim, podeis fazer o que quiserdes."[670]

[669] VACCARI, Cristian; CHADWICK, Andrew, p. 9.
[670] The New York Review, *Hannah Arendt: From an Interview*, 1978. Disponível em: <https://www.nybooks.com/articles/1978/10/26/hannah-arendt-from-an-interview/> [10/10/2023]; VACCARI, Cristian; CHADWICK, Andrew, p. 9.

BIBLIOGRAFIA GERAL

ABA-CATOIRA, Ana, "Los desórdenes informativos en un sistema de comunicación democrático", *in Revista De Derecho Político*, 2020 (109), pp. 119–151. doi: 10.5944/rdp.109.2020.29056;

ALAPHILIPPE, Alexander; GIZIKIS, Alexis; HANOT, Clara; BONTCHEVA, Kalina, *Automated Tackling of Disinformation: Major Challenges Ahead*, Serviço de Estudos do Parlamento Europeu (EPRS), 2019. doi: 10.2861/368879;

AMARAL, Maria Lúcia, *Fiscalização da constitucionalidade das normas constantes dos números 5 e 6 do artigo 6.º, da Lei n.º 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital*, Provedoria de Justiça, 2022.

BAYER, Judit; HOLZNAGEL, Bernd; LUBIANIEC, Katarzyna; PINTEA, Adela; SCHMITT, Josephine B.; SZAKÁCS, Judit; USZKIEWICZ, Erik, *Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States (2021 update)*, Parlamento Europeu, 2021.

BBC News, *Twitter pulls out of voluntary EU disinformation code*, 2023. Disponível em: https://www.bbc.com/news/world-europe-65733969 [12/08/2023].

BRADSHAW, Samantha; HOWARD, Philip N., *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, Oxford Internet Institute, 2019.

BROWNLEE, Jason, *A Gentle Introduction to Generative Adversarial Networks (GANs)*, Machine Learning Mastery, 2019. Disponível em: https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/ [06/10/2023].

CANOTILHO, J. J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, 3.ª edição revista, Coimbra Editora, Coimbra, 1993, pp. 225-238.

CHITRA, Uthsav; MUSCO, Christopher, "Analyzing the Impact of Filter Bubbles on Social Network Polarization", *in Proceedings of the 13th International Conference on Web Search and Data Mining (WSDM '20)*, 2020, pp. 115–123. doi: https://doi.org/10.1145/3336191.3371825

CHULVI, Cristina Pauner, "Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red", *in Teoría y Realidad Constitucional*, núm. 41, 2018, pp. 297-318. doi: 10.5944/trc.41.2018.22123.

CINELLI, Matteo; DE FRANCISCI MORALES, Gianmarco; GALEAZZI, Alessandro; QUATTROCIOCCHI, Walter; STARNINI, Michele, "The echo chamber effect on social media", *in Proceedings of the National Academy of Sciences of the United States of America*, 2021, 118:9. doi: 10.1073/pnas.2023301118

COOK, John; ECKER, Ullrich; LEWANDOWSKY, Stephan, "Misinformation and How to Correct It", *in Emerging trends in the social and behavioral sciences: An interdisciplinary, searchable, and linkable resource*, 2015, pp. 1-17.

DeepAI, *Recurrent Neural Network*, (não datado). Disponível em: https://deepai.org/machine-learning-glossary-and-terms/recurrent-neural-network [30/09/2023].

Entidade Reguladora para a Comunicação Social (ERC), *A Desinformação – Contexto Europeu e Nacional*, 2019.

EUvsDisinfo, *About: Our Team*, (não datado). Disponível em: <https://euvsdisinfo.eu/about/> [16/06/2023].

FALLIS, Don, *A Conceptual Analysis of Disinformation*, 2009.

FATHAIGH, R. Ó.; HELBERGER, Natali; APPELMAN, Naomi, *The perils of legally defining disinformation*, Internet Policy Review, 10:4, 2021. doi: https://doi.org/10.14763/.

FRAGA-LAMAS, Paula; FERNÁNDEZ-CARAMÉS, Tiago M., *Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality*, IT Professional, 22:2, 2020, pp. 53-59. doi: 10.1109/MITP.2020.2977589.

GRAY, John F.; TERP, Sara-Jayne, *Misinformation: We're Four Steps Behind Its Creators*, 2019.

GREGORY, Sam, *Mal-uses of AI-generated Synthetic Media and Deepfakes: Pragmatic Solutions Discovery Convening, June 2018: Summary of Discussions and Next Step Recommendations*, Witness, 2018.

Grupo de Peritos em notícias falsas e na desinformação em linha, *A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation*, Serviço das Publicações da União Europeia, 2018.

HELMUS, Todd C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*, RAND Corporation, 2022. doi: https://doi.org/10.7249/PEA1043-1.

KRICHEN, Moez, *Convolutional Neural Networks: A Survey*. Computers, 12(8):151, 2023. doi: https://doi.org/10.3390/computers12080151

MARCONDES, Francisco Supino; ALMEIDA, José João; NOVAIS, Paulo, "An Exploratory Design Science Research on Troll Factories", *in Journal Integrated Computer-Aided Engineering*, 2023, pp. 1-21. doi: https://doi.org/10.3233/ICA-230720

MARWICK, Alice; LEWIS, Rebecca, *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017.

MIT Technology Review, *Google has released a giant database of deepfakes to help fight deepfakes*, 2019. Disponível em: <https://www.technologyreview.com/2019/09/25/132884/google-has-released-a-giant-database-of-deepfakes-to-help-fight-deepfakes> [10/10/2023].

MORGAN, Susan, "Fake news, disinformation, manipulation and online tactics to undermine democracy", *in Journal of Cyber Policy*, 3:1, 2018, pp. 39-43. doi: 10.1080/23738871.2018.1462395.

NGUYEN, Thanh Thi; NGUYEN, Quoc Viet Hung; NGUYEN, Dung Tien; NGUYEN, Duc Thanh; HUYNH-THE, Thien; NAHAVANDI, Saeid; NGUYEN, Thanh Tam; PHAM, Quoc-Viet; NGUYEN, Cuong M., *Deep learning for deepfakes creation and detection: A survey*. Computer Vision and Image Understanding, 223, 2022. doi: 10.1016/j.cviu.2022.103525.

PALOP, Andrés Boix, "La construcción de los limites a la libertad de expresión en las redes sociales"*, in Revista de Estudios Políticos*, n.° 173, 2016, pp. 55-112. doi: https://doi.org/10.18042/cepc/rep.173.02

PAMMENT, James, "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework", *in Future Threats, Future Solutions*, Carnegie Endowment for International Peace – Publications Department, 2020.

PAMMENT, James, "The EU's Role in Fighting Disinformation: Developing Policy Interventions for the 2020s", *in Future Threats, Future Solutions*, Carnegie Endowment for International Peace – Publications Department, 2020.

PAMMENT, James, "The EU's Role in Fighting Disinformation: Taking Back the Initiative", *in Future Threats, Future Solutions*, Carnegie Endowment for International Peace – Publications Department, 2020.

PEREIRA, Miguel, "A política de combate à desinformação na União europeia: problemas conceptuais e principais instrumentos", *in E-book do VI seminário internacional hispano-luso-brasileiro sobre direitos Fundamentais e políticas públicas*, Dialética Editora, pp. 339-361.

PEREIRA, Miguel, "A trial run for the EU's coregulatory approach: the Strengthened Code of Practice on Disinformation", *in Official Blog of UNIO – EU Law Journal*, 2022. Disponível em: https://officialblogofunio.com/2022/07/15/a-trial-run-for-the-eus-co-regulatory-approach-the strengthened-code-of-practice-on-disinformation/ [08/09/2022].

PEREIRA, Miguel, "Taming Europe's digital landscape? Brief notes on the proposal for a Digital Services Act", *in UNIO – EU Law Journal*, Volume 7, n.º 2, 2021, pp. 78-94.

PLASILOVA, Iva; HILL, Jordan; CARLBERG, Malin; GOUBET, Marion; PROCEE, Richard, *Study for the "Assessment of the implementation of the Code of Practice on Disinformation"*, Serviço das Publicações da União Europeia, 2020. doi: 10.2759/188091

POLYAKOVA, Alina; FRIED, Daniel, *Democratic Defense Against Disinformation*, Atlantic Council – Eurasia Center, 2018.

PROKOPOVIĆ, Anka Mihajlov; VUJOVIĆ, Marija, "The european approach to regulating disinformation", *in Facta Universitatis Series Law and Politics*, Volume 18, n.º 3, 2020, pp. 175-183. doi: 10.22190/fulp2003175m.

RAMOS, José Ricardo Marcondes, "Supervisão, classificação e certificação dos sistemas de IA na Proposta de Regulamento sobre Inteligência Artificial", *in Direito em Mudança: A Proposta de Regulamento Europeu sobre Inteligência Artificial - Algumas questões jurídicas*, 2023, pp. 31-63.

SCHÜNEMANN, Wolf J., "A threat to democracies? An overview of theoretical approaches and empirical measurements for studying the effects of disinformation", *in Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, Routledge, 2022, pp. 33-47. doi: 10.4324/9781003110224-4.

SHEN, Tianxiang; LIU, Ruixian; BAI, Ju; LI, Zheng, *"Deep Fakes" using Generative Adversarial Networks (GAN)*, Noiselab, 2018.

SHIRES, James, *The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and US Politics (Fall 2020)*, Texas National Security Review, 2020.

The New York Review, *Hannah Arendt: From an Interview*, 1978. Disponível em: https://www.nybooks.com/articles/1978/10/26/hannah-arendt-from-an-interview/ [10/10/2023].

The New York Times, *False Claims Around Israel Attacks Include Recycled Videos and a Game Clip*, 2023. Disponível em: <https://www.nytimes.com/article/israel-attacks-video-disinformation.html?smid=url-share> [13/10/2023].

VACCARI, Cristian; CHADWICK, Andrew, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News", *in Social Media and Society*, 6:1, 2020. doi: 10.1177/2056305120903408.

VAN RAEMDONCK, Nathalie; MEYER, Trisha, "Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat", *in Addressing Hybrid Threats: European Law and Policies*, 2022.

WESTERLUND, Mika, *The Emergence of Deepfake Technology: A Review*, Technology Innovation Management Review, 9:11, 2019, pp. 39-52. doi: 10.22215/timreview/1282

X - Central de Ajuda, *Sobre as Notas da Comunidade no X*, (não datado). Disponível em: https://help.twitter.com/pt/using-x/community-notes [06/08/2023].

DOCUMENTOS DE INSTITUIÇÕES E ESTRUTURAS EUROPEIAS

Comissão Europeia, *Plano de Ação para a Comunicação Estratégica*, 2015.

Comissão Europeia, *Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, JOIN(2016) 18 final, 2016.

Comissão Europeia, *Relatório conjunto ao Parlamento Europeu e ao Conselho relativo à aplicação do Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia*, JOIN(2017) 30 final, 2017.

Comissão Europeia, *Relatório conjunto relativo à aplicação do Quadro comum de luta contra as ameaças híbridas, de julho de 2017 a junho de 2018*, JOIN(2018) 14 final, 2018.

Comissão Europeia, *Plano de Ação contra a Desinformação*, JOIN(2018) 36 final, 2018.

Comissão Europeia, *Combater a desinformação em linha: uma estratégia europeia*, COM(2018) 236 final, 2018.

Comissão Europeia, *Relatório da Comissão sobre a aplicação da Comunicação «Combater a desinformação em linha: uma estratégia europeia»*, COM(2018) 794 final, 2018.

Comité de Ministros do Conselho da Europa, *Recomendação do Comité de Ministros aos Estados-Membros sobre o pluralismo dos meios de comunicação social e a transparência da propriedade dos meios de comunicação social*, CM/Rec(2018)1, 2018.

Comissão Europeia, *Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*, JOIN(2018) 16 final, 2018.

Comissão Europeia, *Comunicação: Garantir eleições europeias livres e justas*, COM(2018) 637 final, 2018.

Comissão Europeia, *Relatório sobre a aplicação do Quadro Comum de 2016 sobre a luta contra as ameaças híbridas e da Comunicação Conjunta de 2018 sobre o aumento da resiliência e o reforço das capacidades para enfrentar as ameaças híbridas*, SWD(2019) 200 final, 2019.

Comissão Europeia, *Relatório sobre a execução do Plano de Ação contra a Desinformação*, JOIN(2019) 12 final, 2019.

Conselho da União Europeia, *Conclusões do Conselho e dos Estados-Membros sobre a garantia de eleições europeias livres e justas - Resultado do processo*, 2019.

Comissão Europeia, *Avaliação do Código de Conduta sobre Desinformação - Resultados e domínios a melhorar*, SWD(2020) 180 final, 2020.

ERGA, *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*, 2020.

Conselho da União Europeia, *Conclusões do Conselho sobre o reforço da resiliência e a luta contra as ameaças híbridas, incluindo a desinformação no contexto da pandemia de COVID-19*, 2020.

Comissão Europeia, *Comunicação: Combater a desinformação sobre a COVID-19: repor a verdade dos factos*, JOIN(2020) 8 final, 2020.

Comissão Europeia, *Plano de Ação para a Educação Digital 2021-2027: Reconfigurar a educação e a formação para a era digital,* COM(2020) 624 final, 2020.

Comissão Europeia, *Mapeamento das medidas relacionadas com o reforço da resiliência e a luta contra as ameaças híbridas*, SWD(2020) 152 final, 2020.

Comissão Europeia, *Plano de Ação para a Democracia Europeia*, COM(2020) 790 final, 2020.

Comissão Europeia, *Relatório sobre as eleições de 2019 para o Parlamento Europeu*, COM(2020) 252 final, 2020.

Comissão Europeia, *Plano de Ação da UE para os Direitos Humanos e Democracia 2020-2024*, JOIN(2020) 5 final, 2020.

Comissão Europeia, *Orientações da Comissão Europeia relativas ao reforço do Código de Conduta sobre Desinformação*, COM(2021) 262 final, 2021.

Comissão Europeia, *Proteção dos Direitos Fundamentais na Era Digital - Relatório Anual de 2021 sobre a Aplicação da Carta dos Direitos Fundamentais na UE*, COM(2021) 819 final, 2021.

Serviço Europeu de Ação Externa, *Countering Disinformation: Questions and Answers about the East StratCom Task Force*, 2021. Disponível em: <https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232> [09/05/2023].

Tribunal de Contas Europeu, *Special Report: Disinformation affecting the EU: tackled but not tamed*, Serviço das Publicações da União Europeia, 2021.

ERGA, *Press release: ERGA and EDMO meet to further strengthen cooperation in meeting disinformation challenges*, 2022.

Comissão Europeia, *Observatório Europeu dos Meios de Comunicação Digitais (EDMO)*, última atualização em 2023. Disponível em: https://digital-strategy.ec.europa.eu/pt/policies/european-digital-media-observatory [02/10/2023].

Conselho da União Europeia*, Rússia: UE renova sanções em resposta à agressão militar da Rússia contra a Ucrânia*, 2023*. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2023/07/20/russia-eu-renews-sanctions-over-russia-s-military-aggression-against-ukraine/>* [19/10/2023].

BRETON, Thierry, Carta do Comissário Thierry Breton a Elon Musk por conta da disseminação de desinformação e conteúdo ilegal na rede social X no seguimento do conflito entre Israel e o Hamas em 2023, 2023.

ERGA, *About ERGA*, (não datado). Disponível em: <https://erga-online.eu/?page_id=7> [29/09/2023].

ERGA, *Work Programme and current activities*, (não datado). Disponível em: <https://erga-online.eu/?page_id=12> [29/09/2023].

BIBLIOGRAFIA NORMATIVA

Constituição da República Portuguesa, Decreto de 10 de Abril de 1976, com a última redação conferida pela Lei Constitucional n.º 1/2005, de 12 de agosto.

Lei n.º 115/2022. Diário da República, Série I de 2022-08-11, páginas 2 – 3.

Lei n.º 53/2005, de 8 de novembro, publicada em Diário da República n.º 214/2005, Série I-A de 2005-11-08, pp. 6396 – 6409.

Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02), 2016.

Tratado da União Europeia (versão consolidada) C 202/13, 2016.

Tratado sobre o Funcionamento da União Europeia (versão consolidada), C 202/47, 2016.

O Código de Conduta em matéria de Desinformação de 2018.

O Código de Conduta Reforçado em matéria de Desinformação de 2022.

Decisão (PESC) 2022/351 do Conselho de 1 de março de 2022 que altera a Decisão 2014/512/PESC que impõe medidas restritivas tendo em conta as ações da Rússia que desestabilizam a situação na Ucrânia.

Diretiva 2010/13/UE do Parlamento Europeu e do Conselho de 10 de Março de 2010 relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva «Serviços de Comunicação Social Audiovisual»).

Diretiva (UE) 2018/1808 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 que altera a Diretiva 2010/13/UE relativa à coordenação de certas disposições legislativas, regulamentares e administrativas dos Estados-Membros respeitantes à oferta de serviços de comunicação social audiovisual (Diretiva Serviços de Comunicação Social Audiovisual), para a adaptar à evolução das realidades do mercado.

Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, COM(2021) 206 final, 2021.

Regulamento (UE) 2022/350 do Conselho de 1 de março de 2022 que altera o Regulamento (UE) n.º 833/2014 que impõe medidas restritivas tendo em conta as ações da Rússia que desestabilizam a situação na Ucrânia.

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 dos Serviços Digitais).

Proposta de Regulamento do Parlamento Europeu e do Conselho sobre a transparência e o direcionamento da propaganda política – Alterações aprovadas pelo Parlamento Europeu, em 2 de fevereiro de 2023, (COM(2021)0731 — C9-0433/2021 — 2021/0381(COD)) (1).

BIBLIOGRAFIA JURISPRUDENCIAL

Acórdão do Tribunal Constitucional Espanhol, de 31/03/1982, proferido na sentença n.º 12/1982.

Acórdão do Tribunal Constitucional Espanhol, de 16/12/1986, proferido na sentença n.º 159/1986.

Acórdão do Tribunal Constitucional Espanhol, de 21/01/1988, proferido na sentença n.º 6/1988.

Acórdão do Tribunal Constitucional, de 04/11/1993, proferido no proc. n.º 634/1993, 94/92.

Acórdão Dink v. Turquia do Tribunal Europeu de Direitos Humanos, de 14/09/2010, proferido no proc. n.º 2668/07.

Acórdão Fuentes Bobo v. Espanha do Tribunal Europeu de Direitos Humanos, de 29/02/2000, proferido no proc. n.º 39293/98.

Acórdão Handyside v. Reino Unido do Tribunal Europeu dos Direitos Humanos, de 07/12/1976, proferido no proc. n.º 5493/72.

Acórdão Özgür Gündem v. Turquia do Tribunal Europeu de Direitos Humanos, de 16/03/2000, proferido no proc. n.º 23144/93.

Acórdão Stoll v. Suíça do Tribunal Europeu de Direitos Humanos, de 10/12/2007, proferido no proc. n.º 69698/01.

Acórdão RT France v Conselho do Tribunal Geral, de 27/07/2022, proferido no proc. n.º T–125/22.

Recurso interposto em 27 de setembro de 2022 pela RT France do Acórdão proferido pelo Tribunal Geral (Grande Secção) em 27 de julho de 2022 no processo T-125/22, RT France/Conselho (Processo C-620/22 P).

Despacho do Presidente do Tribunal de Justiça de 28 de julho de 2023 – RT France/Conselho da União Europeia, Reino da Bélgica, República da Estónia, República Francesa, República da Letónia, República da Lituânia, República da Polónia, Comissão Europeia, Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança (Processo C-620/22).