ORIGINAL ARTICLE

DOI: 10.51480/1899-5101.18.3(41).820

Can Disinformation be Regulated? A Comprehensive Overview of the European Union's Pertaining Initiatives

Gergely Ferenc Lendvai
0000-0003-3298-8087
Ludovika University of Public Service

Tamás Attila Szikora
0009-0002-0563-120X
Ludovika University of Public Service

János Tamás Papp
0000-0001-8682-6900
Pázmány Péter Catholic University

Krzysztof Wasilewski
0000-0002-5378-2822
Koszalin University of Technology

Abstract: This paper critically examines the European Union's regulatory approaches to combating disinformation, focusing on the Code of Practice on Disinformation, Digital Services Act, European Media Freedom Act and regulation on transparency and targeting of political advertising. Through legal analysis and literature review, the study assesses the strengths and limitations of these frameworks in addressing disinformation, particularly within the context of advertising transparency and platform accountability. Key findings reveal that while the European Union has made significant strides toward improving transparency and holding platforms accountable, current measures remain largely voluntary and lack sufficient enforcement mechanisms. The paper concludes that regulation alone is insufficient to effectively eradicate disinformation, and proposes a more holistic approach, combining media literacy (critical thinking), cross-border collaboration and adaptive strategies.

Keywords: disinformation, platform regulation, European Union, transparency, fake news

INTRODUCTION

Can disinformation *truly* be regulated? Or are we fighting a losing battle? How *should* governments and international institutions distinguish between curbing harmful disinformation and protecting free speech? Can regulatory frameworks effectively "stem the tide of fake news" without inadvertently becoming tools of censorship (Gosztonyi, 2023)? Or are other policy means (also) needed, such as the promotion of quality journalism and information literacy, as opposed to or in addition to restrictive measures (Török, 2024)? These pressing questions lie at the heart of the present study, which aims to outline the disinformation regulation in the European Union via its ambitious attempts to combat fake news through legislative actions.

The primary objective of the paper is to review whether the European Union's regulatory initiatives, including the Code of Practice on Disinformation, Digital Services Act (DSA), European Media Freedom Act (EMFA) and Regulation on the transparency and targeting of political advertising (RPA) can address the pervasive influence of disinformation in modern society. As a premise, the paper briefly explores the origins and evolution of fake news, the various typologies thereof, and how these forms of information warfare have been weaponized in political and social contexts. The core of the paper lies in the assessment of the impact and effectiveness of the EU's legal frameworks, particularly in scrutinizing the advertising ecosystem that fuels disinformation, ensuring political ads are transparent, and enhancing the integrity of online platforms. By critically examining the legislation, this study aims to reveal the limitations of the current regulatory measures and their key similarities and differences. The paper is built on legal analyses of the instruments examined as well as a comprehensive literature review.

The study aims to contribute to the growing body of literature on disinformation governance. It also sets forth as a goal to enrich the existing scholarship by highlighting gaps in enforcement, the challenges of transnational disinformation and the need for more adaptive, forward-looking strategies. The paper positions itself within broader debates on media regulation, political communication and the safeguarding of democratic processes in the digital age, and invites researchers from the social sciences to take part in the discourse on the critical examination of policymaking concerning fake news within and outside the EU.

THE CONCEPT OF DISINFORMATION AND THE CATEGORIZATION OF "FAKE NEWS"

Though fake news as a concept is not novel, nor is the spreading thereof (cf. the spreading of false information during the World Wars (Barragán-Romero and Bellido-Pérez, 2019)), the term gained notoriety in 2016 before and during the US presidential election campaign (Van Duyn and Collier, 2019; Nordberg et al., 2020).

Research underscores that the proliferation of fake information, especially from then-candidate Donald Trump, caused a significant shift in the spreading of fake news; the quantity of fake information on social media grew rapidly, and the trust in media, as well as the identification of "real" news, deteriorated significantly (Van Duyn and Collier, 2019). The disinformation crisis has significantly influenced policymaking and decision-making processes, too. Bovet and Makse (2019) found that 25 per cent of 171 million tweets during a particular period contained or spread fake or biased news, affecting political preferences and election dynamics. The spread of false information peaked again during the COVID-19 pandemic, considered one of the most severe cases of disinformation (Shrestha and Spezzano, 2022; Palomino-Flores et al., 2024). Al-Zaman (2021) highlights that in India, COVID-19-related fake news not only targeted health issues but also politics and entertainment, exacerbating the pandemic's impact. This widespread misinformation led to lower vaccination rates, disregard for safety measures, and increased infections and deaths. The World Health Organization and experts have referred to this disinformation wave as the "infodemic" (Pagoto et al., 2023), noting its global reach and cross-continental effects.

It is imperative to highlight the typology of fake news, too. Although the term "fake news" is commonly used in both popular and academic discourse, its definition remains unclear (Wasilewski, 2021, p. 5). One of the most popular understandings of "fake news" associates it with "viral posts based on fictitious accounts made to look like news reports" (Tandoc et al., 2018, p. 2). Most media scholars agree that the contemporary understanding of "fake news" should focus on news fabrication and manipulation, along with propaganda (Brennen, 2017). Still others explain "fake news" as "information disorder" together with its related challenges, such as echo chambers (Wardle and Derakhshan, 2017). Moreover, as Wardle (2023) described the above issue, it is also critical to focus on the interrelational aspects of the information disorder as well, given that false information and the disseminator thereof rarely operate in "silos", e.g., someone who posts health misinformation may very well take part in the spreading of untrue information in other "disciplines" as well, such as in politics.

Dealing with "fake news" one must be aware of its various forms. According to the literature, at least 7 main types can be distinguished: satire (parody),

misleading content, fabricated content, false content, imposter content, clickbait, propaganda, conspiracy theories, and partisan content (Bąkowicz, 2019, p. 284–285). Satire aims to fool the recipients but has no intention to harm whereas misleading content purposefully frames an issue or individual. Imposter content, on the other hand, means that reliable sources are impersonated by third parties to cause deception. A similar goal aims to achieve fabricated content, which is false in its entirety. False connections might use true stories but give them headlines that do not support the content. In this way, false context shares genuine content with false contextual information. Finally, fabricated (manipulated) content uses reliable information and modifies it in order to achieve some political (or other) agenda (Wardle, 2017). Other forms of fake news demand much broader definitions, which go beyond the scope of this paper. However, it is important to remember that fake news – or disinformation – can take various forms, which is why the issue is so problematic (Broda & Strömbäck, 2024). Different types vary in their potential to deceive recipients.

INCREASING REGULATORY DEMANDS

IMMEDIATE HISTORY: THE DYNAMICS OF HOW THE YEAR 2016 SHIFTED THE DISCOURSE ON DISINFORMATION

Online platforms have become a prominent space for political communication, including the publication of political advertisements. The harmful influence of political ads on social networking sites gained significant attention following the 2016 US presidential election. While the dissemination of false claims was not new, the scale and impact during this election, along with the 2016 Brexit campaign, raised serious concerns. These events marked the beginning of a new era in political disinformation, further highlighted by the Italian and French presidential elections in 2017.

In itself, the appearance of untrue statements during political campaigns is by no means a recent phenomenon; however, the fact that the term "fake news" has gained considerable attention is due to the platform on which it is disseminated, namely social networking sites. The basic operating principles and structural design of these sites have made it easy to facilitate the spread of previously unknown amounts of information at almost unimaginable speed.

The real novelty was the fact that, in the absence of significant resources, practically anyone can deliver messages to the masses, even in a targeted way, without revealing their identity. In fact, the use of targeted advertising messages is an indisputable feature of social media campaigning. It is also clear that, in addition to the dangers and risks that are often highlighted, they also have

a number of positive benefits for democratic (decision-making) mechanisms. These include the ability to reach voters with messages that are relevant to them, to reach those who are difficult or almost impossible to reach through other channels, and to be effective, efficient and sometimes cost-effective for politicians. At the same time, it can benefit the public by leading to more diverse political campaigns and greater awareness of certain issues among voters (Borgesius et al., 2018; Dobber et al., 2019).

As a result of the issues outlined above, accountability has also faced numerous obstacles. One reason for this is that, unlike media service providers, online platforms (e.g., Facebook) do not bear editorial responsibility for content appearing on their interfaces. Under the DSA, the activities of these services consist primarily of storing and publicly disseminating content (Article 3(i)). Through recommendation systems, ranking by platforms, and content moderation, they cannot be considered completely neutral with regard to content published by users. However, since their activities in the preliminary compilation of content differ significantly from those of "traditional" media service providers, the question of what obligations can be imposed on platforms in order to protect democratic public discourse arises.

PROPOSED SOLUTION: INITIAL EFFORTS TOWARDS TRANSPARENCY

These events have drawn attention to the fact that paid political advertising is an effective tool in large-scale and coordinated disinformation campaigns. The lack of transparency and the publication itself not knowing the identity of the "client" behind each message made it easy to avoid prosecution. The transparency and accountability requirements for political advertising are intended to serve three main purposes: to prevent disinformation and foreign influence, to facilitate the emergence of opposing views in public discourse, and to create at least the same level of transparency in online political discourse as has long been the case for paid political advertising on television and radio (Wood, 2020).

Since the second half of the 2010s, serious efforts have been made to address this problem, seeking to find solutions to ensure credible information in the spirit of transparency. Initially, the European Commission's Communication (COM(2018) 236 final), summarizing the main findings and recommendations of the report and the report's own report on misinformation, published in March 2018 (A multi-dimensional approach to disinformation, 2018), declared the need for transparency in political advertising.

On September 12, 2018, the European Commission adopted a Recommendation on security issues related to the European Parliament elections in spring 2019, in the context of the election campaign and the conduct of the elections, primarily, of course, in the online space (C(2018) 5949). Among the measures to be taken

to ensure that voters are informed and to guarantee freedom of public debate, the Commission's Recommendation mainly set out requirements for transparency in political advertising published before the European Parliament elections and during the election campaign. While the expectations set out in these documents have gone some way toward improving the safe conduct of the 2019 European Parliament elections (free from external interference), the lack of binding regulation has not fully ensured a digital environment that provides the public with transparent and reliable, credible information (Kirk and Teeling, 2022).

SELF-REGULATION OF PLATFORMS

In response to the challenges outlined earlier, platforms like Facebook (now Meta) have taken steps to address these issues through their own regulatory initiatives. In 2018, Meta introduced new rules for political advertising, requiring each ad to display the name of the organization or individual that paid for it. (Dommett, 2014). While this promotes accountability, it carries risks: Leersen and colleagues point out that Facebook's data is often incomplete or inaccurate, potentially misleading journalists (the misleading nature of the advertisement deserves special mention because if the press uses data it considers reliable to inform the public about political issues, and this data later turns out to be inaccurate, the deceptive information can cause serious damage in a democratic public sphere). Moreover, this focus on transparency may divert attention from more obscure issues, like targeted advertising practices, that are less disclosed by the platform (Leerssen et al., 2023).

Other social platforms have not taken the most radical steps against political advertising: Twitter (now known as X) announced at the end of 2019 that it will ban political advertising on its platform in the future. The idea has been widely criticized, with the main criticism being that the decision is a disproportionate restriction on political communication, which is the most precious core of freedom of expression. Another relevant issue raised by the ban concerned the definition of political advertising, namely how to distinguish between purely political advertising and messages dealing with issues that affect a wide range of society and typically give rise to lively public debate.

THE EUROPEAN UNION AND DISINFORMATION

The European Union's Code of Practice on Disinformation was introduced in 2018. It was a manifestation of the EU's so-called "self-regulation" approach to the problem of disinformation (Wasilewski, 2021). This approach can be defined as "a type of voluntary initiative which enables economic operators, social

partners, non-governmental organizations or associations to adopt common guidelines amongst themselves and for themselves" (Ilves et al., 2016). Although some researchers question the effectiveness of the approach (Shattock, 2021), it is by far the most ambitious effort by UE to tackle disinformation. The introduction of the 2018 Code of Practice was part of a broader strategy to counter the rising threat of false information, particularly following the proliferation of digital platforms and the influence of disinformation campaigns on democratic processes, including elections. The Code of Practice has since become a key element of the EU's broader digital policy framework, and its impact warrants detailed academic evaluation. It must be noted, however, that the EU "self-regulation" approach was met with some heavy criticism. Among the critics were representatives of online platforms, advertisers, academics, media, and civil society organizations. Together they issued a statement criticizing the code for being too general in scope, as well as for its lack of a common approach (The Sounding Board's, 2018).

Following critical voices, the EU has sought to strengthen its regulatory framework through the DSA. The Act was proposed in 2020 with the intention of introducing binding obligations for online platforms, including measures to counter disinformation and mandates increased transparency and accountability. The introduction of the DSA manifested a serious change in the EU approach to disinformation, as it moved from voluntary commitments toward more enforceable rules (Nannini et al., 2024; Husovec, 2024). Recognizing the need for a stronger response to the growing threat of disinformation, in 2022, the EU established the Strengthened Code of Practice on Disinformation. Its preamble states that the member states "recognize their collective and individual accountabilities to work together to defund Disinformation in advertising and media across the following types of organizations and their respective" (Code of Conduct, 2022).

A COMPREHENSIVE EXAMINATION OF THE CODE

The Code contains 44 commitments and 128 specific measures and is structured into 10 sections. Table 1 presents the structure of the 2022 Code of Practice on Disinformation.

Table 1. The Structure of the 2022 Code of Practice on Disinformation

Section	Content
Preamble	The role of signatories in combating disinformation, safeguarding democratic processes, and maintaining a balance with fundamental rights like freedom of expression.
Scrutiny of Ad Placements	Focus on reducing the revenues of purveyors of disinformation by improving transparency in advertising and ensuring responsible ad placements.

Section	Content
Political Advertising	Transparency standards for political and issue ads, including labelling, verification, and repositories to ensure users understand the origins and purposes of such ads.
Integrity of Services	Conceptualization and countermeasures regarding manipulative behaviors, such as fake accounts or malicious use of AI systems, with clear transparency obligations.
Empowering Users	The outline of the provisions for users with tools and education to recognize disinformation, including media literacy initiatives and transparency in recommender systems.
Empowering the Research Community	Researchers' access to data for studying disinformation, with structured governance for sensitive data and cooperation between stakeholders.
Empowering the Fact-Checking Community	Collaboration with independent fact-checkers, ensuring they have the necessary resources, tools, and access to data to conduct their work effectively.
Transparency Centre	A central online "hub" where information about the implementation of the Code is made available to the public and regularly updated.
Permanent Task-Force	Establishment of a Task-force which is responsible for monitoring and reviewing the implementation of the Code and ensuring it adapts to technological and societal changes.
Monitoring of the Code	The process for continuous reporting, assessment, and improvements to ensure the Code's effectiveness in reducing disinformation.

The Preamble "sets the stage" by emphasizing the collective responsibility to fight disinformation, a menace that threatens democratic values through misinformation, influence operations, and foreign interference. It stresses the need for a careful balance between combating disinformation and upholding fundamental rights like free speech and privacy, while urging coordinated efforts from platforms, advertisers, researchers, and the European Commission. This creates the framework for a holistic strategy against disinformation.

Sections II and III dive deeper into the mechanisms that fuel disinformation – financial incentives and political manipulation. Section II tackles the economic engine behind disinformation by scrutinizing ad placements, ensuring that harmful actors are denied revenue streams through brand safety policies. Section III focuses on the transparency of political ads, which are frequently weaponized in disinformation campaigns, as demonstrated by Russian interference in elections (Espaliú-Berdud, 2024). As full disclosure of sponsors and public repositories is required for oversight, these sections aim to prevent political discourse from being distorted by hidden agendas. Both sections highlight the importance of collaboration between platforms, advertisers, and fact-checkers to curb disinformation's reach.

Section IV is of critical importance as it addresses the technological side of the issue, focusing on protecting the integrity of services. By cracking down on the use of fake accounts, bots, and deepfakes, this section aims to neutralize the tools that disinformation actors often deploy. The emphasis of this section on evolving safeguards ensures that as new threats arise, the response can adapt and remain effective. Building on these protective measures, the "Empowering

Triangle" in Sections V–VII takes a proactive approach. Section V arms users with the ability to detect and report false information, bolstering media literacy and encouraging informed content consumption. Section VI grants researchers access to crucial platform data, enabling them to analyze disinformation trends and assess the effectiveness of interventions, fostering cooperation between academia and civil society. Section VII supports fact-checkers with automated data access, ensuring that their findings are integrated into platform services. By empowering these groups – users, researchers, and fact-checkers – the Code creates a multi-layered defense system against disinformation. Finally, Section VIII ties it all together with the Transparency Centre, a public platform that ensures accountability and tracks the progress of these measures. By regularly updating with metrics and reports, the Transparency Centre fosters ongoing commitment from signatories and promotes a transparent fight against disinformation. This interconnected approach ensures that every aspect of the disinformation ecosystem is addressed, from economic incentives to technological manipulation, while empowering key stakeholders to act effectively.

THE DIGITAL SERVICES ACT

The Proposal for a Regulation on a Single Market for Digital Services (COM/2020/825 final) was introduced on December 15, 2020, and following a relatively swift negotiation process, the final version was approved by the European Parliament on July 5, 2022. The DSA adopts a tiered regulatory framework, where the obligations increase in accordance with the significance of the role played by the online intermediary. It defines four categories of service providers: online intermediary services, hosting services, online platforms, and very large online platforms (VLOPs). Large social networks, where disinformation circulates with potential systemic impacts, such as the erosion of trust in democracy and institutions, are classified as VLOPs.

With respect to disinformation, the DSA introduces a "co-regulatory" framework that permits service providers to voluntarily adopt codes of conduct aimed at mitigating the harmful effects of illegal content dissemination, as well as manipulative and abusive behaviors. Article 45(1) grants the Commission and the Board the authority to support and facilitate the creation of diverse codes of conduct intended to strengthen the implementation of the DSA. These codes primarily address two areas of concern: illegal content, as defined in Article 3(h), and the broader systemic risks outlined in Article 34. The key function of these codes of conduct is to offer detailed interpretations and enhancements to the existing legal framework. They encourage the adoption of voluntary standards that surpass statutory requirements, or, when necessary, the development of broader guidelines functioning as soft law.

While adherence to these codes is voluntary, the DSA notes that a service provider's refusal to adopt a code, without providing a satisfactory rationale, may be considered when evaluating its compliance with DSA obligations. In instances where specific systemic risks are identified under Article 34, the Commission may invite service providers, relevant authorities, civil society organizations, and other stakeholders to collaborate in the development of these codes. The Commission already expressed that the Code of Practice on Disinformation is set to evolve into a formal Code of Conduct (European Commission, 2024). In this regard, the Commission appears to adopt a rather broad interpretation of co-regulation. While the establishment of the Codes of Conduct was initially voluntary, their subsequent elevation to a status formally recognized under the DSA effectively integrates them into the regulatory framework. As a result, they function as a kind of Trojan horse, gradually transforming a soft law instrument into a form of hard law.

Currently, the protection against disinformation largely relies on the willingness of information society service providers to fulfill their duties of care regarding the content they distribute. This includes their ability to self-assess the "systemic risks" inherent in their activities and implement preventive actions, particularly through content moderation procedures. However, the DSA does not specifically define harmful content, including disinformation, nor does it mandate its removal (Leiser, 2023). Additionally, the effectiveness of these measures also depends on the capacity of relevant public authorities to monitor and enforce compliance with these obligations. Whether this approach will provide enough response to the challenges disinformation poses to democratic societies is still an open question (Vicente, 2023).

Requiring large online platforms to conduct their own risk assessments is logical, as they have exclusive access to user data and understand the risks and remedies of their services. It is equally reasonable for the Commission to expect these platforms to cover compliance costs under the DSA. However, ensuring the independence of private audit firms, which may face conflicts of interest, is crucial. There appears to be a lack of a specific supervisory framework for ensuring compliance, to address this, a broader principle of transparency and a strengthened co-regulatory, multistakeholder model are needed (Strowel, 2023). Also, there needs to be access to researchers who meet certain criteria, for the purpose of conducting research that helps identify and understand systemic risks, and help combat disinformation (Cauffman, 2021).

THE EUROPEAN MEDIA FREEDOM ACT

The European Democracy Action Plan, launched at the end of 2020, is a framework developed by the European Commission to strengthen democracy within the EU. Its objectives include safeguarding the integrity of elections and political advertising, enhancing transparency, supporting independent journalism, and improving the EU's capabilities in detecting and responding to disinformation. As part of this initiative, Ursula von der Leyen announced the proposal for the EMFA in 2021, which builds on the Audiovisual Media Services Directive and establishes various regulations for the media sector (European Commission, 2020). On April 11, 2024, the EU officially adopted the legislation which consolidates various areas of media regulation, including provisions related to public service media, cooperation among national regulatory authorities, transparency of media ownership, and the distribution of state advertising.

These actions target the distribution or access to media services provided by non-EU media outlets that aim at or reach EU audiences, regardless of the distribution method. Such services, particularly when subject to control by third countries, are scrutinized for posing threats to public security or contributing to the spread of disinformation and the serious risks associated with it. The recitals associated with the Article 17 (Recitals 47–49) highlight the specific practical expertise of media authorities in protecting the internal market from activities of media services originating outside the EU that target or reach audiences within the EU and may threaten or endanger public security. Such risks include systematic international campaigns involving foreign information manipulation and interference, aimed at destabilizing the EU or any Member State.

To address these threats, the legislation aims to coordinate national measures that can be adopted to counter risks to public security posed by media services originating outside the EU, or established outside but targeting EU audiences. In this context, the legislation proposes the creation of a criteria list by the European Board for Media Services, as established under the EMFA, to assist national regulatory authorities or bodies when a media service provider seeks jurisdiction in a Member State, or when a media service provider under a Member State's jurisdiction presents a serious public security risk.

REGULATION ON THE TRANSPARENCY AND TARGETING OF POLITICAL ADVERTISING

In its Communication on the European Democracy Action Plan, published in December 2020, the European Commission, recognizing the threats posed by online platforms and social media sites, in particular to the electoral process, expressed its determination to adopt a comprehensive set of rules to ensure the visibility and transparency of political advertising for the 2024 European

Parliament elections (COM(2020) 790 final). As a first element of this commitment, in November 2021, the Commission published a draft regulation on rules of the transparency and targeting of political advertising (COM(2021) 731 final). The need for legislation was already expressed by several stakeholders before the draft was presented, in particular in the light of research findings based on information available in social networking sites' advertising directories (Dommett and Bakir, 2020). The proposal was intended as a response to the fragmentation of regulation in the EU Member States, but the increasing role of social platforms in election campaigns has undoubtedly led to calls for common EU regulation. The RPA was finally adopted in spring 2024.

The legislator has recognized the potential for misinformation through political advertising, stressing that this can occur in particular when the message is not overtly political, comes from outside the EU or, for example, uses targeted techniques (Recital 4). In principle, as the title of the legislation also indicates, the RPA lays down transparency requirements for political advertising services, such as identification (Article 7), retention and transmission of specific data on advertisers and advertisements (Articles 9–10 and 16–17). The other main part of the legislation deals with the targeting techniques and ad-delivery techniques of online political advertising, requiring political advertisers and political advertising solvers to comply with certain data protection conditions when using targeting or ad-delivery techniques (Articles 18–20).

It is important to note that the RPA does not affect the substantive content of political advertising in the legislation of each Member State. Another principle of the RPA that concerns the issue of responsibility for content posted on platforms is the prohibition of a general monitoring obligation, similar to the provision in Article 8 of the DSA (Recital 54); social networking sites should "merely" provide a suitable reporting platform and mechanism for users to report political advertising that does not comply with the rules of the RPA, or the persons who commission it (Article 15).

CRITICAL EVALUATION

Current approaches to the regulation of information reflect both progress and challenges. On the one hand, the EU has taken some significant steps in tackling fakes news in the European public sphere by introducing and modifying the Code of Practice on Disinformation, as well as the DSA. Experts agree that those documents have provided frameworks to improve so-much needed transparency, especially in political advertising. Moreover, they hold platforms accountable and – to some extent – empower users and researchers to combat disinformation. On the other hand, there is consensus that actions taken by the EU are

not enough to eradicate disinformation from the public sphere. Self-regulation measures, such as the aforementioned Code of Practice, have established voluntary commitments from social media platforms, but they lack binding enforcement mechanisms. This is why there is a growing political push for the Code to move swiftly with its conversion into a Code of Conduct under the DSA (Article 45).

Unsurprisingly, critics argue that this voluntary nature has allowed Facebook, Amazon and other large tech companies to remain blurred in their efforts, limiting the impact of these measures. Part of the problem is the very nature of the EU, which has limited competences in areas, such as internet and media policies. These are traditionally left for member states to regulate.

The 2022 Russian invasion of Ukraine has proven that dissemination of fake news is part of the contemporary warfare that may cause as much harm as traditional weaponry. What is lacking, apart from coherent legislation at a national and European level is coordination between member states and the EU when it comes to tackling disinformation. Despite some progress in this matter, there is still much to do in order to establish a successful system.

To end the evaluation, we propose that the emergence of instruments in the EU's anti-disinformation agenda is not only a rational response mechanism but also a structural necessity arising from the dispersed nature of both the problem and the Union's competences. This issue stems from a rather trivial polemic; disinformation cuts across economic, communicative, and democratic spaces, while the EU's authority is – still – fragmented between internal market, audiovisual, and electoral domains. Hence, no single act could adequately address its complexity. The Code and the Regulations, therefore, represent interlocking layers of governance that together form a composite regulatory ecosystem. In this "onion-like" layering, the principle-related foundation, lies the Code as it enables voluntary cooperation between platforms, advertisers, and civil society under the Commission's guidance. The DSA transforms this "soft" coordination into enforceable obligations by embedding the principles of transparency, accountability, and the necessity to ensure users' safety within broader risk-management architecture while the EMFA intervenes upstream by reinforcing the independence and plurality of the media sector. Lastly, the RPA targets the electoral interface, curbing opaque micro-targeting and foreign influence in political advertising.

It is also crucial to mention that the connection among these instruments is thus functional and sequential. Each act occupies a distinct but complementary regulatory space, whether it be soft law/self-regulatory, horizontal, structural, or sector-specific, all collectively seeking to transform the EU's approach into a systemic resilience-building against disinformation. Subsequently, in essence, the multiplicity of legal norms also mirrors the multidimensionality of the threat. Where earlier regimes focused on takedowns and liability, the current framework emphasizes transparency, accountability, and coordination and

in this context, the Code-DSA-EMFA-RPA quart-partite nexus demonstrates the EU's progressive understanding that combating disinformation requires much more than a single prohibitive instrument and proposes a network of mutually reinforcing mechanisms addressing different stages of information production, dissemination, and influence.

CONCLUSION

To conclude, we invite the readers to revisit the initial question: Can disinformation be regulated?

As seen from our above analysis, despite the efforts made, these instruments are solely legal *tools* but not *solutions*. Constrained by their reactive nature and the evolving tactics of disinformation campaigns, these initiatives are designed to address "symptoms" rather than the systemic causes of disinformation. We propose that the solution does not lie *solely* in regulation but in a more holistic approach that does not just include but rather promotes strengthening media literacy, enhancing cross-border collaboration, and developing adaptive and progressive strategies to fight disinformation.

In order to substantiate the above, we wish to outline a few recommendations – which should also be taken as an invitation for other scholars, policy-makers, and stakeholders to find a common solution. Our premise, in terms of suggestions, is that the path forward tackling disinformation on the EU level requires a set of complementary mechanisms that translate the normative ambition into operational capacity. First, the Union should consider establishing an entity that manages information integrity with interdisciplinary lenses. Adding to this, secondly, the EU must invest more decisively in structured digital literacy and professional training. For this, we also propose allocating cross-border scholarly funds as well so that experts and scholars could work on region-specific and sector-specific issues. Furthermore, given the generous scholarly funding schemes in the EU (such as the European Research Council grant), we also propose that projects related to disinformation and media literacy should be obliged to perform practical outputs that can be implemented on local or EU-wide layers. Lasty, we recommend – in accordance with Wardle's (2023) line of thinking – that these projects can and shall not be executed in "silos".

While the change in the framework of public discourse has placed limits on the effectiveness of legal regulation, it has not questioned its necessity. However, while regulating platforms, at least as much emphasis should be placed on promoting digital literacy; without public awareness, legal regulation of platforms and strict enforcement of rules will not be able to produce visible results. Successfully combating disinformation is a necessity for democratic societies.

Effective regulation, then, must be part of a broader societal response that involves both proactive governance and empowered citizens, recognizing that the battle against disinformation is not a finite one, but an ongoing challenge.

REFERENCES

Al-Zaman, M. S. (2021). Covid-19-related social media fake news in India. *Journalism and Media*, *2*(1), 100–114. https://doi.org/10.3390/journalmedia2010007

Argemi, M., & Fine, G. A. (2018). Faked news: The politics of rumour in British World War II propaganda. *Journal of War and Culture Studies*, *12*(2), 176–193. https://doi.org/10.1080/17526272.2018.1495905

Barragán-Romero, A. I., & Bellido-Pérez, E. (2019). Fake News durante la Primera Guerra Mundial: Estudio de su representatividad en las portadas de la prensa española (ABC Madrid). *Historia y Comunicación Social*, *24*(2), 433–447. https://doi.org/10.5209/hics.66288

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B., & De Vreese, C. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, *14*(1), 82–96. https://doi.org/10.18352/ulr.420

Bovet, A., & Makse, H. A. (2019). Influence of fake news in Twitter during the 2016 US presidential election. *Nature Communications*, *10*, 7. https://doi.org/10.1038/s41467-018-07761-2

Brennen, B. (2017). Making sense of lies, deceptive propaganda, and fake news. *Journal of Media Ethics*, *32*(3), 179–181. https://doi.org/10.1080/23736992.2017.1331023

Broda, E., & Strömbäck, J. (2024). Misinformation, disinformation, and fake news: Lessons from an interdisciplinary, systematic literature review. *Annals of the International Communication Association*, *48*(2), 139–166. https://doi.org/10.1080/23808985.2024.2323736

Cauffman, C., & Goanta, C. (2021). A new order: The Digital Services Act and consumer protection. *European Journal of Risk Regulation,* 12(4), 758–774. https://doi.org/10.1017/err.2021.8

Code of practice on disinformation. (2023, September 22). Disinfocode. https://disinfocode.eu/wp-content/uploads/2023/09/code-of-practice-on-disinformation-september-22-2023.pdf.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling online disinformation: a European Approach. (COM(2018) 236) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan. (COM(2020) 790 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN

Dobber, T., Ó Fathaigh, R., & Zuiderveen Borgesius, F. J. (2019): The regulation of online political micro-targeting in Europe. *Internet Policy Review*, *8*(4), https://doi.org/10.14763/2019.4.1440

Dommett, K. (2023). The 2024 election will be fought on the ground, not by AI, *Political Insight, 14*(4), 4–6. doi.org/10.1177/20419058231218316a

Dommett, K., & Bakir, M. E. (2020): A transparent digital election campaign? The insights and significance of political advertising archives for debates on electoral regulation. *Parlamentary Affairs*, *73*(1), 208–224. https://doi.org/10.1093/pa/gsaa029

Espaliú-Berdud, C. (2024). The EU Code of Practice on Disinformation. *VISUAL REVIEW International Visual Culture Review / Revista Internacional De Cultura Visual*, *16*(2), 95–109. https://doi.org/10.62161/revvisual.v16.5217

European Commission (2018). A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation, Directorate-General for Communication Networks, Content and Technology

(2018). A multi-dimensional approach to disinformation: report of the independent High level Group on fake news and online disinformation. Publications Office. https://data.europa.eu/doi/10.2759/739290

European Commission, (2018). Recommendation of 12 September 2018 on electoral cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament (C(2018) 5949) https://cyberpolicy.nask.pl/wp-content/uploads/2018/09/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf

European Commission: Third Meeting of the European Board for Digital Services https://digital-strategy.ec.europa.eu/en/news/third-meeting-european-board-digital-services

Fowler, E. F., Franz, M. M., & Ridout, T. N. (2022). The challange of online advertising. In *Political advertising in the United States* (2nd ed., pp. 63–75). Routledge. https://doi.org/10.4324/9781003165712-4

Fowler, E. F., Franz, M. M., & Travis N. (2022). Buying and Targeting Political Advertising. In *Political advertising in the United States* (2nd ed., pp. 93–114). Routledge. https://doi.org/10.4324/9781003165712-6

Gosztonyi, G. (2023). Content Management or Censorship? In *Censorship from Plato to Social Media* (Ser. Law, Governance and Technology Series, vol 61., pp. 7–19). Springer. https://doi.org/10.1007/978-3-031-46529-1_2

Husovec, M. (2024). The Digital Services Act's red line: What the Commission can and cannot do about disinformation. *Journal of Media Law*, *16*(1), 47–56. https://doi.org/10.1080/17577632.2024.2362483

Ilves, L. K., Evans T. J., Cilluffo F. J., & Nadeau, A. A. (2016). European Union and NATOglobal cybersecurity challenges: A way forward. *PRISM*, 6(2), 126–141. http://www.jstor.org/stable/26470452

Kirk, N., & Teeling, L. (2021). A review of political advertising online during the 2019 European Elections and establishing future regulatory requirements in Ireland, *Irish Political Studies*, *37*(1) doi.org/10.1080/07907184.2021.1907888

Leerssen., P., Dobber, T., Helberger, & N., de Vreese, C. (2021). News from the ad archive: how journalists use the Facebook Ad Library to hold online advertising accountable. *Information, Communication and Society*, *26*(7), 1381–1400. https://doi.org/10.1080/1369118X.2021.2009002

Leiser, M. (2023). Reimagining digital governance: The EU's Digital Service Act and the fight against disinformation. http://dx.doi.org/10.2139/ssrn.4427493 7

Nannini, L., Bonel, E., Bassi, D., & Maggini, M. J. (2025). Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act. *AI and Ethics, 5.* https://doi.org/10.1007/s43681-024-00467-w

Pagoto, S. L., Palmer, L., & Horwitz-Willis, N. (2023). The Next Infodemic: Abortion Misinformation. *Journal of Medical Internet Research*, *25*, e42582. https://doi.org/10.2196/42582

Palomino-Flores, P., Cristi-López, R., & Paul, D. (2024). Unraveling the truth: investigating the spread of fake news on Facebook during the COVID-19 Crisis. In Ibáñez, D.B., Castro, L.M., Espinosa, A., Puentes-Rivera, I., & López-López, P.C. (eds), *Communication and Applied Technologies. ICOMTA 2023.* (Ser. Smart Innovation, Systems and Technologies, vol 375, pp. 223–233). https://doi.org/10.1007/978-981-99-7210-4_21

Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising (COM/2021/731 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0731

Shattock, E. (2021). Self-regulation 2:0? A critical reflection of the European fight against disinformation. *Harvard Kennedy School Misinformation Review*, *2*(3). https://doi.org/10.37016/mr-2020-73

Shrestha, A., & Spezzano, F. (2021). Characterizing and predicting fake news spreaders in social networks. *International Journal of Data Science and Analytics*, *13*(4), 385–398. https://doi.org/10.1007/s41060-021-00291-z

Strowel, A., De Meyere, J. (2023). The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 14*(1), 66–82.

The Sounding Board's Unanimous Final Opinion on the so-called Code of Practice. (2018). https://www.euractiv.com/wpcontent/uploads/sites/2/2018/10/3OpinionoftheSoundingboard-1.pdf.

Török, B. (2024). Free speech principles to consider when restricting disinformation. *Információs Társadalom, 24(*2), 115–128. https://doi.org/10.22503/inftars.XXIV.2024.2.7

Van Duyn, E., & Collier, J. (2018). Priming and fake news: The effects of elite discourse on evaluations of news media. *Mass Communication & Society*, *22*(1), 29–48. https://doi.org/10.1080/15205436.2018.1511807

Vicente, D. M. (2023). Protection against disinformation on the internet: A Portuguese perspective. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law 14*(3), 453–461.

Warde, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe report DGI(2017)09.

Wardle, C. (2017). Fake news. It's complicated. January 27, 2019 from https://fi rstdraftnews. com/fake-news-complicated/.

Wardle, C. (2023). Misunderstanding misinformation. *Issues in Science and Technology*, *39*(3), 38–40. https://doi.org/10.58875/ZAUD1691

Wasilewski, K. (2021). Fake news and the Europeanization of cyberspace. *Polish Political Science Yearbook, 50*, 61–80. https://doi.org/10.15804/ppsy202153

Wood, A. K. (2020). Facilitating Accountability for Online Political Advertisements, *Ohio State Technology Law Journal, 16*(2), 520–557.