Athens Journal of Mass Media and Communications 2025, 11: 1-16
https://doi.org/10.30958/ajmmc.X-Y-Z

From Fragmentation to Coordination: Regulating Social Media to Protect Electoral Integrity in the European Union

*By Adriana Mutu**

This paper investigates the evolving regulatory landscape shaping the "European approach" to addressing the role of social media platforms in amplifying systemic risks to democratic elections. Based on a qualitative methodology grounded in desk research, it examines legislative and non-legislative measures adopted over the past decade to counter threats such as election delegitimization, political propaganda, unlawful micro-targeting, and technology-enhanced campaigning. The study draws in regulatory coordination literature to explore how European frameworks and national strategies converge to address election-related disinformation. Key findings reveal that increased European cooperation has helped reduce regulatory fragmentation and foster stakeholder engagement. The analysis also highlights challenges posed by regulatory asymmetry across Member States, where divergent political priorities, institutional capacities and legal frameworks add complexity to the creation of unified responses to online disinformation. The study maps the plethora of constitutional norms, binding laws and soft law instruments underscoring the tension between safeguarding democratic integrity and protecting freedom of expression. By situating these efforts within the broader developments in digital governance, the paper contributes to scholarship on political communication and offers practical insights for policymakers aiming to strengthen cross-border coordination and enhance information integrity.

Keywords: *European Union, online disinformation, social media platforms, democracy, elections*

Introduction

On December 6, 2024, Romania's Constitutional Court invalidated the first round of the presidential election held on November 24, following the release of declassified intelligence from the Supreme Council for National Defense. The report revealed "aggressive" foreign interference, cyber-attacks targeting critical electoral infrastructure, hybrid warfare tactics, deliberate manipulation of users via the social media platform TikTok, and the opaque use of AI and digital technologies to influence voter behavior—raising serious concerns about election integrity. In response, the European Commission initiated formal proceedings against TikTok under the Digital Services Act (DSA) on December 17, 2024, citing the platform's failure to adequately assess and mitigate systemic risks related to electoral information manipulation. Additionally, on December 5, 2024, the Commission ordered TikTok to preserve data relevant to potential risks its services may pose to electoral processes across the EU,

*Assistant Professor and Head of Quality, ESIC Business & Marketing School, Spain.

covering national elections from November 24, 2024, through March 31, 2025. In the lead-up to the 2024 European elections, regulatory scrutiny intensified over social media platforms amid growing concerns about disinformation, data privacy violations, and the distortion of democratic discourse. Authorities warned that such practices could mislead voters, undermine fair competition among candidates, and compromise citizens' rights to make informed electoral choices. On April 30, 2024, the European Commission launched proceedings against Facebook and Instagram under the DSA for failing to address election-related disinformation, deceptive advertising, and biased content moderation. Shortly after, on May 31, Spain's Data Protection Agency (AEPD) imposed a temporary ban on Meta's "Election Day Information" tools, citing violations of the General Data Protection Regulation (GDPR) and the risk of intrusive data collection practices. As documented in prior research (Mutu, 2024), parallel investigations into Meta Ireland's data practices further exposed concerns over transparency and consent in behavioral advertising. Meanwhile, in the UK, the BBC's Undercover Voters Project revealed how platforms like TikTok and X were used to spread AI-generated misinformation targeting young voters, while deepfake content impersonating global leaders proliferated across networks.

Recent investigations into major social media platforms have intensified scrutiny over their compliance with European and national laws, particularly the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and the Artificial Intelligence Act (AIA). Allegations include unlawful microtargeting, profiling of sensitive personal data to fuel recommendation algorithms, and the use of addictive design features that exploit behavioral psychology to maximize user engagement (Spirit Legal, 2025). These practices have prompted a wave of legal actions and regulatory inquiries, reflecting growing concern over the platforms' influence on democratic processes and individual rights.

Democratic backsliding has emerged as a central concern in the European Union's struggle to safeguard electoral integrity in the digital age. Recent warnings from the Venice Commission (2025) underscore the gravity of this issue, pointing to the destabilizing influence of social media platforms and the effects of online disinformation on democratic participation. The erosion of informed voter engagement, influenced by widespread exposure to misleading content, poses a direct threat to the legitimacy of democratic institutions. According to the 2024 Youth Eurobarometer, 76% of young Europeans encountered fake news or disinformation in the week prior to the survey, while nearly half of EU citizens expressed concerns about personal data misuse and disinformation as significant barriers to democratic engagement (European Parliament, 2025; European Commission, 2024).

This phenomenon is critically examined in *the Regulation of Social Media and Elections in Europe* report by the Media and Journalism Research Center (Mutu, 2024), which frames digital disinformation as a catalyst for democratic backsliding. The study highlights how social media's operational architecture—particularly its capacity to amplify false or harmful content during elections—undermines democratic self-governance. Mutu (2024) synthesizes taxonomies of information disorder and reveals how disinformation is weaponized through cognitive hacking, social engineering, and the strategic use of fabricated news, contributing to what is termed "information pollution". This pollution, exacerbated by alarmist media narratives,

gendered disinformation, and disproportionate journalistic coverage, erodes public trust and weakens institutional accountability. The report identifies political disinformation campaigns—whether driven by foreign actors or domestic elites—as a form of public harm and a key driver of democratic decline. When state or state-sponsored entities exploit their power to manipulate public opinion and distort electoral outcomes, they not only compromise democratic accountability but also infringe upon citizens' rights to truthful information and free expression. These practices, embedded within broader patterns of democratic backsliding, highlight the urgent need for coordinated regulatory responses to preserve the integrity of democratic processes in the digital era.

Against this backdrop, the present study investigates the EU's coordination priorities in regulating disinformation across its Member States. It seeks to understand how divergent national legal traditions, institutional capacities, and regulatory approaches influence the Union's efforts to develop a coherent governance framework for election-related digital threats. Drawing on interdisciplinary perspectives from political science, law, media studies, and public policy, this research offers a comprehensive analysis of the challenges and opportunities involved in constructing a resilient, rights-based regulatory response.

Literature Review: The Role of Social Media Platforms in Accelerating Democratic Backsliding

Over the past decade, a growing body of research has underscored the profound impact of digital technologies on electoral processes and democratic governance. Online campaigning via social networks, precision-targeted propaganda, and coordinated cyberattacks—often accompanied by disinformation—have been systematically exploited by malicious actors engaging in Foreign Information Manipulation and Interference (FIMI) (European External Action Service, 2021). These tactics have amplified falsehoods, manipulated public opinion, and eroded trust in democratic institutions (Hanafin, 2022; United Nations, 2024; Bösch & Divon, 2024), contributing to invalid ballots, voter disengagement, and growing skepticism about the legitimacy of elections. Empirical studies (Schaewitz et al., 2020; Kessler & Zillich, 2019; Kessler, 2025) have further demonstrated that disinformation's reach extends beyond electoral contexts, affecting critical policy domains such as public health (Nielsen et al., 2021; Schmid, Altay & Scherer, 2023), national security (Pierri et al., 2023; OECD, 2022; Wenzel et al., 2024), and climate action (OECD, 2024), where it undermines consensus-building and policy effectiveness.

In response, scholars, technologists, and global institutions have raised urgent warnings about the destabilizing effects of digital disinformation. Social scientists (Turcilo & Obrenovic, 2020; Rozgonyi, 2020; Wardle & Derakhshan, 2017; Festus, 2025; Battista, 2025; Pavlik, 2023; Papanikos, 2023), alongside private sector leaders and international organizations—including the World Economic Forum, the United Nations, and the OECD—have emphasized that rising distrust in media ecosystems, coupled with the unchecked spread of false narratives and malign foreign influence, poses a direct threat to information integrity and the democratic legitimacy of elected

governments. Initiatives such as the AI Elections Accord (2024) reflect growing recognition that safeguarding democratic processes requires coordinated, multi-stakeholder action to counter digital threats and restore public confidence in electoral systems.

Automated systems and algorithmic technologies have become central to the dynamics of electoral manipulation and disinformation in the digital age. Features of computational propaganda—automation, scalability, and anonymity—are routinely exploited by social media platforms to amplify false narratives, distort public discourse, and fuel sophisticated disinformation campaigns, particularly in conflict zones (Woolley & Howard, 2019; Bösch & Divon, 2024). These systems not only facilitate the rapid dissemination of misleading content but also enable malicious actors to evade accountability. Deepfakes, misleading chatbots, and fabricated political content are increasingly used to simulate public support and manufacture political scandals, with microtargeting techniques enhancing their psychological impact on voters (Dobber et al., 2020; Riedl, 2024). As the United Nations Commission on Science and Technology for Development (2023) warns, the proliferation of fake accounts and synthetic media complicates the information landscape, making it difficult for users to distinguish between authentic and manipulated content.Beyond technical manipulation, algorithmic personalization and selective exposure contribute to societal polarization by reinforcing users' existing beliefs and limiting access to diverse viewpoints (Taddicken & Wolff, 2023; Hastall & Wagner, 2017; Cinelli et al., 2021). Political actors across Europe have strategically embraced these platforms for digital campaigning, leveraging both populist and marketing-driven communication styles to engage voters (Schmuck & Hameleers, 2020; Edelson et al., 2021; Enli & Skogerbø, 2013). In response, policy frameworks within the European Union have evolved to address the constitutional and regulatory challenges posed by election-related digital threats. Comprehensive research and legal assessments underscore the importance of coordinated national responses and the role of central electoral watchdogs in safeguarding democratic integrity and ensuring compliance with international human rights standards (Mutu, 2025). These developments reflect a growing recognition that electoral resilience in the digital era requires not only technological safeguards but also robust institutional oversight and cross-border regulatory cooperation.

Methodology

This study employs a qualitative methodology, specifically a comparative and thematic content analysis, grounded in comprehensive desk research to examine coordinated EU policy actions aimed at countering online disinformation during elections. The comparative dimension enables cross-country evaluation of institutional approaches, revealing how national strategies diverge or converge in their approach to tackle disinformation. Thematic analysis further identifies recurring regulatory concerns which shaped legislative and non-legislative measures adopted over the past decade. Central to this approach was a systematic review of primary and secondary academic literature, which provided the theoretical foundation for understanding

regulatory coordination within multilevel governance regimes. The review drew upon scientific research literature, legal frameworks and interdisciplinary studies in political communication and digital governance. To complement academic sources, the study incorporated industry reports, policy briefs, and white papers from key institutions such as the European Commission, European Parliament, the European External Action Service (EEAS), and the European Digital Media Observatory (EDMO). To triangulate findings and ensure empirical robustness, the research extended to governmental websites and national regulatory authorities' portals across EU Member States. This included the analysis of national strategies, legislative amendments, regulatory decisions, and official communications to map country-specific responses to disinformation. A core component of the study involved examining binding European legislation - such as the Digital Services Act (DSA), the European Democracy Action Plan (EDAP), and the Audiovisual Media Services Directive (AVMSD) – alongside soft law instruments such as the Code of Practice on Disinformation. Finally, the study assessed coordination mechanisms and institutional processes designed to reduce information asymmetries, including the EU´s Rapid Alert System (RAS) and intergovernmental working groups addressing disinformation and hybrid threats. The findings reveal patterns of convergence in regulatory practices and evaluate their impact on the EU´s capacity to deliver a unified response to digital disinformation threats.

The "European Approach" to Online Disinformation: Coordinated Regulatory Oversight of Platforms in Electoral Contexts

Addressing electoral interference and disinformation within national and European democratic processes demands a comprehensive and coordinated policy response. As emphasized by the Organization for Economic Co-operation and Development (2024), countering malicious actors requires systemic efforts that span Member State cooperation, diplomatic engagement, and international regulatory alignment. In response to these escalating threats, European policymakers have implemented a wide array of measures grounded in empirical research to fortify digital information ecosystems. These include restrictions and regulatory frameworks aimed at mitigating the systemic risks posed by social media platforms, particularly in the context of electoral scrutiny. The EU's evidence-based approach to disinformation governance calls for the active participation of governmental bodies, civil society, and private sector actors in developing shared policy language and contributing to informed regulatory design.

Over the past decade, this coordinated strategy has led to significant advancements in transparency, media pluralism, and democratic resilience. European initiatives have focused on curbing election-related disinformation campaigns, political propaganda, and the misuse of computational technologies in digital campaigning. By enhancing regulatory capacities and promoting inclusive information environments, the EU has sought to safeguard electoral integrity and uphold democratic norms. These efforts reflect a broader commitment to building a resilient governance framework capable of adapting to evolving digital threats while maintaining alignment with fundamental rights and international standards.

To enhance coordination on platform governance in the context of elections, the European Union has adopted a multi-level governance approach aimed at reinforcing information integrity across Member States. This "European approach" has led to the development of institutional frameworks and strategic practices that prioritize research on disinformation dynamics, societal resilience, and the creation of actionable policy guidance (OECD, 2024). Key initiatives include the EUvsDisinfo project led by the European External Action Service (EEAS), and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), which collaborates with both the EU and NATO to strengthen the capabilities of its 36 participating states. Complementary efforts such as the Action Plan on Disinformation, the European Democracy Action Plan, and the High-Level Expert Group (HLEG) on Fake News and Online Disinformation have helped establish clearer accountability for online platforms. The creation of the European Digital Media Observatory (EDMO), its 2024 elections-focused task force, and the voluntary Code of Conduct for the European Parliament elections—developed jointly by International Institute for Democracy and Electoral Assistance (International IDEA), European political parties, and the European Commission—further reflect the EU's commitment to coordinated action. These efforts are supported by mechanisms like the Transparency Center and the Permanent Taskforce, which monitor the implementation of the Code of Practice on Disinformation. Data-sharing protocols involving fact-checkers, civil society, researchers, and platforms, along with private sector commitments such as the "Tech Accord to Combat Deceptive Use of AI in 2024 Elections", underscore the broad stakeholder engagement in this regulatory ecosystem.

These multifaceted policy efforts have significantly strengthened EU-wide cooperation and stakeholder involvement in countering digital threats to electoral integrity. By establishing institutional responsibilities and promoting information-sharing, the EU has helped prevent duplication of efforts and reduce asymmetries across national governments (Cinelli et al., 2021). In response to the transformative impact of digitalization on how citizens access and interpret information, several Member States have enacted legal reforms to criminalize election-related disinformation. Countries such as Lithuania, Malta, France, Austria, Croatia, the Czech Republic, Greece, Hungary, Romania, and Slovakia have amended their Criminal Codes to make the deliberate spread of false news during elections a punishable offense. These national measures reflect a growing consensus on the need for enforceable safeguards to protect democratic processes from manipulation and digital warfare.

The European Union has developed a robust and multifaceted legal framework to address the growing risks to electoral integrity, information quality, and platform governance in the digital age. Central to this framework are the Digital Services Act (DSA) and the Digital Markets Act (DMA), which impose stringent obligations on very large online platforms (VLOPs) and search engines (VLOSEs) to mitigate systemic risks to civic discourse, electoral processes, and public security. These include content moderation duties (Articles 15, 24(1), and 42 DSA), restrictions on microtargeting (Articles 5(2) and 6(2) DMA), transparency in recommender systems (Articles 14, 23(4), and 27(3) DSA), and data-sharing requirements with authorities and researchers (Article 40(4) DSA). Platforms must also inform users about the nature and targeting of advertisements (Article 26(1) DSA), enhancing transparency and user awareness.

Complementing these horizontal regulations, the European Media Freedom Act (EMFA) addresses sector-specific challenges in the media landscape, including editorial independence, media pluralism, and protection against unjustified content removal by VLOPs. The General Data Protection Regulation (GDPR) plays a critical role in safeguarding personal data, especially in electoral contexts where political actors may rely on data brokers and analytics firms to target voters. The ePrivacy Directive (e-PD) further regulates unsolicited communications and the tracking of user behavior online. To counter foreign interference and enhance transparency in political campaigning, the Regulation on the Transparency and Targeting of Political Advertising (TTPA) introduces obligations for service providers and data controllers. Finally, the Artificial Intelligence Act (AIA) and the emerging Digital Fairness Act (DFA) address the lawful use of AI systems in elections, ensuring that algorithmic tools do not undermine democratic processes. Together, these instruments form a comprehensive legal architecture aimed at reinforcing democratic resilience and protecting citizens in the digital public sphere.

International cooperation plays a pivotal role in reinforcing the effectiveness and coherence of regulatory oversight in the digital sphere. By mitigating fragmentation, preventing regulatory arbitrage, and ensuring the continued relevance of policy frameworks, cross-border collaboration strengthens the EU's capacity to safeguard electoral integrity. Beyond the adoption of binding legal instruments, the European Union has advanced a wide array of initiatives to counter disinformation and foreign interference. These include the foundational 2018 *Code of Practice on Disinformation* and its enhanced 2022 version, as well as a series of European Parliament resolutions addressing foreign electoral interference, artificial intelligence, and industrial policy. Equally vital are capacity-building tools such as international conventions, strategic communications, and a suite of guidelines and recommendations that provide practical support for Member States and stakeholders. These instruments address systemic risks, data protection in political campaigning, and the ethical use of emerging technologies, including AI and big data.

In response to the intensifying threat of election-related disinformation, the EU has adopted a multi-level governance strategy to promote regulatory convergence and institutional resilience. Central to this approach is the European Democracy Action Plan (EDAP), which seeks to bolster democratic institutions, enhance media pluralism, and improve transparency. The Digital Services Act (DSA) complements EDAP by imposing binding obligations on digital platforms to identify and mitigate systemic risks, marking a shift from voluntary commitments to enforceable legal standards. The Rapid Alert System further supports this framework by enabling real-time information exchange among Member States, facilitating swift responses to cross-border disinformation campaigns. Together, these mechanisms aim to streamline coordination, reduce information asymmetries, and clarify institutional roles—laying the groundwork for a more unified and resilient European response to digital threats against democracy.

Shared Goals, Divergent Paths: National Strategies and Regulatory Tensions in Tackling Electoral Disinformation

The regulation of disinformation across the European Union represents a significant challenge, stemming from Member States´ institutional diversity, national sovereignty and different regulatory incentives. Important challenges can be identified in the process of harmonizing disinformation regulations across Member States.

Firstly, one central issue is the contested definition of disinformation itself. What one Member State considers harmful content (disinformation) or illegal content (such as hate speech, incitement to violence, or child sexual abuse material) may be regarded as protected speech in another (Ó Fathaigh et al., 2021). A significant gap in European legal scholarship lies in the absence of a clear, consistent, and legally binding definition of disinformation which can further obscure regulatory efforts and cross-border coordination and raise concerns about the proportionality of state interventions in the digital informational ecosystem. As Ó Fathaigh et al. (2021) highlight, existing studies do not examine in detail how disinformation is defined within EU law or whether national legislation across Member States effectively aligns with or applies to these definitions. For clarification, disinformation is defined by the European Commission as "verifiably false or misleading information that, cumulatively, is created, presented and disseminated for economic gain or to intentionally deceive the public and that may cause public harm" (European Commission, 2018). Misinformation "refers to the unintentional spread of inaccurate information shared in good faith by those unaware that they are passing on falsehoods. Misinformation can be rooted in disinformation as deliberate lies and misleading narratives are weaponized over time, fed into the public discourse and passed on unwittingly" (United Nations, 2024). The High-Level Expert Group on fake news and online disinformation (European Commission, Directorate-General for Communications Networks, Content and Technology, 2018, p.3) defined disinformation as encompassing "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit". Finally, one of the prominent definitions of misinformation, disinformation and malinformation was developed by Wardle and Derakhshan (2017). Misinformation happens "when false information is shared, but no harm is meant"; disinformation happens "when false information is knowingly shared to cause harm", while malinformation occurs "when genuine information is shared to cause harm, often by moving what was designed to stay private into the public sphere".

As mentioned, Ó Fathaigh et al. (2021) clarified how these definitions diverge in scope and emphasis. The authors argued that although all definitions acknowledge the falsity or misleading nature of information, they vary in their treatment of verifiability, with the European Commission emphasizing "verifiably false" content and the High-Level Expert Group including "inaccurate" information. These definitional nuances have profound implications for freedom of expression, especially if such terms were to be codified into law rather than remain policy tools. A second major tension arises from how these definitions conceptualize harm and intent. As Ó Fathaigh et al. (2021) highlighted, Wardle and Derakhshan adopt a broad view of harm, encompassing individuals, groups, and nations, while the European Commission and High-Level Expert Group focus narrowly on public harm, particularly threats to democratic

processes and public goods. The European Commission's definition allows for disinformation to be identified even if harm is only potential, whereas the other two require harm as a material condition. This distinction influences how intent is framed: Wardle and Derakhshan and the High-Level Expert Group link intent directly to causing harm, while the European Commission defines intent as the act of deceiving the public, thereby broadening the scope of what qualifies as disinformation. Additionally, all three definitions overlook the complexity of actor intent in networked environments, where disinformation may be produced and disseminated by multiple, intersecting actors with varying motivations. This oversimplification risks undermining regulatory effectiveness and raises questions about accountability in digital ecosystems.

Additional regulatory tensions emerge from the varied ways in which EU Member States have criminalized disinformation, false news, or the dissemination of false information. As outlined by Mutu (2024), national legal frameworks differ significantly in scope, terminology, and enforcement mechanisms, creating discrepancies across the Union. For example, Lithuania addresses disinformation under Article 19 of its Law on the Provision of Information to the Public, while Malta criminalizes false news through Article 82 of its Criminal Code. France applies Article 27 of the Law on Freedom of the Press, and Croatia enforces penalties under Article 16 of the Law on Misdemeanours against Public Order and Peace. Similar provisions exist in Cyprus (Criminal Code, Article 50), the Czech Republic (Section 357), Greece (Article 191), and Slovakia (Section 361). Although Hungary, Romania, and Austria also have relevant legislation, their approaches vary in terms of legal thresholds and definitions. These discrepancies reflect broader tensions between national sovereignty and EU-level harmonization, raising concerns about legal fragmentation, inconsistent enforcement across jurisdictions and potential infringements on freedom of expression. The criminalization of election-related falsehoods – adopted in Malta, Hungary and Austria – raises concerns about proportionality and the risk of such laws being misused to suppress legitimate political discourse. Enforcement practices also vary widely across jurisdictions, influenced by legal cultures and institutional capacities. In more illiberal contexts, disinformation regulations may be weaponized against opposition parties, civil society actors, or independent media, thereby undermining the credibility of EU-wide efforts and complicating the balance between effective regulation and the protection of democratic standards.

Digitally advanced countries possess more developed regulatory infrastructures, allowing them to implement and enforce oversight mechanisms for online content and platform governance. Some Member States perceive disinformation as a national security issue, such as Lithuania or France, which have faced targeted disinformation campaigns by hostile foreign actors. To safeguard the integrity of democratic processes, the French government enacted two laws on 22 December 2018 (Organic Law No. 2018-1201 of 22 December 2018 Regarding the Fight Against Information Manipulation) aimed at curbing the manipulation of information during election periods. These laws introduced emergency procedures that allow authorities to halt the spread of false or misleading claims disseminated at scale, particularly when such content is deliberately amplified through artificial or automated means on public online platforms. Under these regulations, major digital platforms are required to inform users about how to report disinformation and must submit annual reports to the national media regulator,

Arcom. These reports must detail actions taken to ensure algorithmic transparency, manage sponsored content related to public interest news, regulate advertising, promote media literacy, and counter the spread of false information (Mutu, 2024). Additionally, the national audiovisual regulator is empowered to suspend the broadcast of television services operated by foreign states if they are found to undermine France's core national interests, especially by spreading disinformation that disrupts institutional stability in the three months leading up to a national election. These measures are reinforced by existing legal provisions, including the 1881 Law on Freedom of the Press and Article L.97 of the Electoral Code, both of which explicitly prohibit the dissemination of false news capable of influencing electoral outcomes. In Germany, the Network Enforcement Act – NetzDG (Bundesgesetzblatt, 2017), which came into force in January 2018, imposes strict obligations on social media which are required to swiftly block, filter, and remove illegal content, including "violating content," within tight timeframes or risk substantial fines. The law was introduced to address the growing concerns around hate speech, online radicalization, and the spread of fake news. Under NetzDG, social media companies must respond to user complaints about unlawful content that falls under eighteen specific provisions of the German Criminal Code (Strafgesetzbuch, 1998). They are also required to submit biannual transparency reports and ensure that false or misleading content, often labeled as "fake news", is removed within 24 hours of notification. In Austria, the dissemination of false information during an election is considered a criminal offense under Article 264 of the Criminal Code (Criminal Code, Austria). Specifically, it is illegal to publicly spread false claims that could either prevent eligible voters from casting their ballots or manipulate their voting decisions, particularly when such claims are made at a time when a corrective statement cannot be effectively circulated. Violators may face penalties of up to six months in prison or fines equivalent to 360 daily rates. The law imposes stricter consequences if the false information is supported by forged or falsified documents intended to enhance its credibility, in which case the maximum penalty increases to three years of imprisonment.

The study by the European Audiovisual Observatory (Cabrera Blázquez et al., 2022) examines how national governments across Europe are responding to the challenge of online disinformation by promoting user and citizen empowerment. It highlights that many measures are designed to protect citizens and consumers by enhancing the quality and accessibility of reliable information. These user-focused initiatives aim to help individuals identify and resist disinformation, for example, by reducing the visibility of false content and improving access to trustworthy sources and diverse viewpoints. The study shows that in addition to targeting users directly, governments are also placing increased responsibilities on online platforms. These include requirements for greater algorithmic transparency, obligations for self-regulation, and tools that enable users to participate in content moderation. Platforms may also be mandated to de-prioritize, block, or remove certain types of harmful content and websites. Furthermore, regulatory efforts extend to journalists, media outlets, and political actors, with measures such as mandatory transparency in online political advertising and the promotion of fact-checking during election periods. Together, these strategies reflect a multi-stakeholder approach to combating disinformation and strengthening democratic resilience.

The European Audiovisual Observatory's 2022 study (Cabrera Blázquez et al., 2022) highlights Italy's evolving legislative approach to online disinformation, which has focused more on institutional inquiry and user empowerment than on direct regulatory enforcement. The Italian bill No. 1900 (Committee of Inquiry into the Dissemination of False Information, 2021), approved in its first reading by the Chamber of Deputies, did not introduce binding legal measures to counter the spread of fake news. Instead, it aimed to establish a parliamentary committee tasked with investigating large-scale disinformation activities, particularly during sensitive periods such as electoral campaigns. The committee's mandate included examining the origins, financing (including foreign sources), intended impact, and strategic objectives of disinformation, as well as assessing the adequacy of platform procedures for content removal. This bill was considered alongside Senate Act No. 1549 (Senate Act No. 1549 XVIII Legislature, 2021) and Chamber Bill No. 470 presented on 25 October 2022, both of which proposed the creation of similar parliamentary commissions to investigate the serial and massive dissemination of illegal or false content via digital platforms. In parallel, as the European Audiovisual Observatory's 2022 study clarified, user empowerment was addressed through broader legislative instruments, notably the European Delegation Law No. 53/2021, which authorized the transposition of the AVMS Directive 2018/1808 into national law. This law emphasized the need for media service providers, including social platforms, to inform users about harmful content, such as misleading advertising, and to implement safeguards against identity misuse and manipulation of public discourse. It also called for the promotion of digital literacy. These principles were operationalized in Legislative Decree No. 208/2021 (the new AVMS Code), which introduced specific obligations for video-sharing platform (VSP) services. Article 42 of the Code requires VSPs to include clear terms and conditions, provide transparent and accessible complaint mechanisms, and implement media literacy tools to raise user awareness.

Discussion and Conclusions

The study shows that the European Union's response to election-related disinformation reflects a dynamic and evolving regulatory landscape shaped by coordinated policy efforts. Recognizing the threat posed by malicious actors and digital interference operations, EU institutions and Member States have embraced a systemic approach that combines legislative innovation, multi-level governance, and cross-sector collaboration. Initiatives such as the European Democracy Action Plan, the EUvsDisinfo project, and the establishment of EDMO and its election-focused task force illustrate the EU's commitment to reinforcing information integrity and democratic resilience. These efforts are further supported by international cooperation, transparency mechanisms, and voluntary codes of conduct, which engage both public institutions and private stakeholders, including technology companies addressing deceptive AI content. Importantly, the criminalization of election-related disinformation in several Member States signals a growing consensus on the need for enforceable safeguards against digital manipulation. While challenges remain in harmonizing national approaches and balancing regulation with fundamental rights, the EU's

multifaceted strategy demonstrates a robust commitment to protecting democratic processes in the digital age.

As noted, a fundamental challenge in addressing disinformation across the European Union lies in the absence of a legally binding definition. As Ó Fathaigh et al. (2021) emphasized, what constitutes harmful or illegal content varies significantly between Member States, with some forms of expression considered criminal in one jurisdiction and protected speech in another. This definitional ambiguity not only complicates regulatory coherence but also undermines cross-border coordination, raising critical concerns about the proportionality and legitimacy of state interventions in the digital information ecosystem.

Despite persistent challenges, the benefits of coordinated disinformation regulation within the European Union remain substantial. Harmonization across Member States can reduce duplication and contradictions in national approaches, streamline compliance for digital platforms operating transnationally, and reinforce the EU's normative leadership in global digital governance. Coordinated action also enables the exchange of best practices and fosters consistency in enforcement, increasing the likelihood that platforms will adhere to EU standards. Moreover, unified regulatory efforts enhance the EU's geopolitical influence as a champion of responsible, rights-based digital regulation. To further strengthen this coordination, a series of actionable recommendations emerge from recent scientific research and policy studies (Mutu, 2024; Mutu, 2025), particularly those examining the impact of disinformation on electoral processes.

Key among these recommendations is the urgent need to enhance media pluralism and digital literacy. Policymakers should prioritize initiatives that empower users to critically navigate digital environments and assess the credibility of the information they encounter. Regulatory frameworks must incentivize transparency and accountability among online platforms, promote adherence to journalistic and academic standards, and support innovation in news media. This includes financial backing for independent reporting and fact-checking initiatives, as well as the development of news literacy programs and coordination mechanisms to monitor misinformation and promote the lawful use of communication technologies. Ahead of elections, governments and election management bodies should invest in capacity-building efforts focused on digital campaigning, data protection, disinformation, and generative AI. Future research should explore how demographic shifts influence news consumption and information-sharing behaviors. Legislative and regulatory instruments must aim to create secure, inclusive, and trustworthy digital ecosystems, while safeguarding freedom of expression and opinion in line with international human rights standards.

Ultimately, fostering international, cross-sectoral, and multi-stakeholder cooperation is essential to address the complex challenges posed by social media in electoral contexts. Reinforcing information integrity and coordinating platform governance will strengthen societal resilience, rebuild public trust, and ensure a harmonized and effective response to disinformation. This approach not only protects democratic processes within the EU but also offers a model for policy design and implementation beyond its borders. In conclusion, the European Union faces a fundamental coordination dilemma: balancing national sovereignty and institutional

diversity with the imperative for a unified response to rapidly evolving digital threats. Success will depend on pragmatic harmonization, strategic investment in regulatory infrastructure, and a shared commitment to upholding democratic values in the digital age.

References

AI Elections Accord. (2024). A tech accord to combat deceptive use of AI in 2024 elections. https://www.aielectionsaccord.com/

Battista, D. (2025). The evolution of digital communication: Zelensky and the use of Instagram in wartime. *Athens Journal of Social Sciences, 12*(1), 43–58.

Bösch, M., & Divon, T. (2024). The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. *New Media & Society, 26*(9), 5081–5106. https://doi.org/10.1177/14614448241251804

Bundesgesetzblatt. (2017). *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

Cabrera Blázquez, F. J., Cappello, M., Talavera Milla, J., & Valais, S. (2022). User empowerment against disinformation online. *IRIS Plus*. European Audiovisual Observatory. https://rm.coe.int/iris-plus-2022en3-user-empowerment-against-disinformation/1680a963c4

Ciampaglia, G. L. (2018). Fighting fake news: A role for computational social science in the fight against digital misinformation. *Journal of Computational Social Science, 1*, 53–60.

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences of the United States of America, 118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

Committee of Inquiry into the Dissemination of False Information. (2021). *Istituzione di una Commissione parlamentare di inchiesta sulla diffusione massiva di informazioni false*. https://www.senato.it/leg/18/BGT/Schede/Ddliter/53197.htm

Criminal Code, Austria. (n.d.). *Strafgesetzbuch*. https://www.jusline.at/gesetz/stgb/paragraf/264

Darius, P., Drews, W., Neumeier, A., & Riedl, J. (2024). The EUDigiParty data set. *Harvard Dataverse*. https://doi.org/10.7910/DVN/U6UWPN

Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2020). Do (microtargeted) deepfakes have real effects on political attitudes? *The International Journal of Press /Politics, 26*(1), 69–91. https://doi.org/10.1177/1940161220944364

Edelson, L., Nguyen, M.-K., Goldstein, I., Goga, O., McCoy, D., & Lauinger, T. (2021). Understanding engagement with US (mis)information news sources on Facebook. In *Proceedings of the 21st ACM Internet Measurement Conference* (pp. 444–463). ACM. https://doi.org/10.1145/3487552.3487859

Enli, G. S., & Skogerbø, E. (2013). Personalized campaigns in party-centered politics. *Information, Communication & Society, 16*(5), 757–774. https://doi.org/10.1080/1369118X.2013.782330

European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT 'Digital Decade' Unit). (2024). *Special Eurobarometer 551 on the digital decade*. https://europa.eu/eurobarometer/surveys/detail/3174

European Commission: Directorate-General for Communications 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). *Code of practice on disinformation*. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

European Commission. (2024). *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act.* https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European External Action Service (EEAS). (2021). *Tackling disinformation, foreign information manipulation and interference: Stratcom activity report*. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interfer ence_en

European Parliament. (2019). *Report on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)) (2021/C 202/06).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019IP0031%2801%29

European Parliament. (2021). *European Delegation Law (Law No. 53/2021) of 22 April 2021: Legislative delegation for the transposition of EU directives and other acts into the Italian framework*. http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2021-04-22;53!vig=2021-05-082019-2020

European Parliament. (2025). *Youth survey 2024*. https://europa.eu/eurobarometer/surveys/detail/3392

Festus, E. (2025). War propaganda and correspondents: Updating UN Covenant and media ethics principles. *Athens Journal of Mass Media and Communications, 11*(1), 9–18.

French Executive Committee. (2018). *Organic Law No. 2018-1201 of 22 December 2018 regarding the fight against information manipulation*. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847556

Hanafin, N. (2022). *Strategic guidance: Information integrity – Forging a pathway to truth, resilience and trust*. United Nations Development Programme. https://www.undp.org/publications/information-integrity-forging-pathway-truth-resilience-and-trust

Hastall, M. R., & Wagner, A. J. M. (2017). Enhancing selective exposure to health messages and health intentions: Effects of susceptibility cues and gain–loss framing. *Journal of Media Psychology, 30*(4), 217–231. https://doi.org/10.1027/1864-1105/a000197

Italian Chamber of Deputies. (2021). *House Act No. 470: Establishment of a Parliamentary Commission of Inquiry into the serial and massive dissemination of illegal content and false information through the Internet*. https://www.camera.it/leg19/126?tab=&leg=19&idDocumento=470&sede=&tipo=

Italian Government. (2021). *Legislative Decree No. 208/2021: Implementation of Directive (EU) 2018/1808 amending Directive 2010/13/EU (AVMS Directive).* https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:DECRETO.LEGISLATIVO:2021-11-08;208!vig=5

Kessler, S. H. (2025). Misinformation on social media: Individual reception and the importance of self-directed internet search for rebuttal. *SCM Studies in Communication and Media, 1*, 140–202. https://doi.org/10.5771/2192-4007-2025-1-140

Kessler, S. H., & Zillich, A. F. (2019). Searching online for information about vaccination: Assessing the influence of user-specific cognitive factors using eye-tracking. *Health Communication, 34*(10), 1150–1158. https://doi.org/10.1080/10410236.2018.1465793

Lejla, T., & Obrenovic, M. (2020). *Misinformation, disinformation, malinformation: Causes, trends, and their influence on democracy.* Heinrich Böll Stiftung. https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_ENG.pdf

Mutu, A. (2024). *Regulation of social media and elections in Europe.* Media and Journalism Research Center (MJRC).

Mutu, A. (2025). *Monitoring the ballot: Election supervision, monitoring and observation.* Media and Journalism Research Center (MJRC).

Nielsen, R. K., Schulz, A., & Fletcher, L. (2021). An ongoing infodemic: How people in eight countries access news and information about coronavirus a year into the pandemic. *Reuters Institute report*. https://reutersinstitute.politics.ox.ac.uk/ongoing-infodemic-how-people-eight-countries-access-news-and-information-about-coronavirus-year

Organisation for Economic Co-operation and Development (OECD). (2022). *Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses*. https://www.oecd.org/en/publications/disinformation-and-russia-s-war-of-aggression-against-ukraine_37186bde-en.html

Organisation for Economic Co-operation and Development (OECD). (2024). *Facts not fakes: Tackling disinformation, strengthening information integrity.* OECD Publishing. https://doi.org/10.1787/d909ff7a-en

Ó Fathaigh, R., Helberger, N., & Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review, 10*(4). https://doi.org/10.14763/2021.4.1584

Papanikos, G. T. (2023). The Greek newspaper coverage of the Ukrainian war: The pre-invasion phase and the day of the invasion. *Athens Journal of Mass Media and Communications, 9*(4), 363–382.

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think.* Penguin.

Pavlik, J. V. (2023). Introduction: An inclusive scholarly perspective on media and the war in Ukraine. *Athens Journal of Mass Media and Communications, 9*(4), 223–228.

Pierri, F., Luceri, L., Jindal, N., & Ferrara, E. (2023). Propaganda and misinformation on Facebook and Twitter during the Russian invasion of Ukraine. In *Proceedings of the 15th ACM Web Science Conference 2023* (pp. 65–74). ACM. https://doi.org/10.1145/3578503.3583597

Politov, A., Bogdanova, V., & Gerganov, A. (2025). *Unraveling influence: Social and collective drivers of foreign information manipulation and interference.* Center for the Study of Democracy.

Riedl, M. (2024). Political deepfakes and misleading chatbots: Understanding the use of genAI in recent European elections. *Center for Media Engagement*. https://mediaengagement.org/research/generative-artificial-intelligence-and-elections

Rozgonyi, K. (2020). Disinformation online: Potential legal and regulatory ramifications to the right to free elections – policy position paper. In F. Loizides, M. Winckler, U. Chatterjee, J. Abdelnour-Nocera, & A. Parmaxi (Eds.), *Human computer interaction and emerging technologies: Adjunct proceedings from the INTERACT 2019 workshops.* https://doi.org/10.18573/book3.g

Schaewitz, L., Kluck, J. P., Klosters, L., & Kramer, N. C. (2020). When is disinformation (in)credible? Experimental findings on message characteristics and individual differences. *Mass Communication and Society, 23*(4), 484–509. https://doi.org/10.1080/15205436.2020.1716983

Schmid, P., Altay, S., & Scherer, L. D. (2023). The psychological impacts and message features of health misinformation. *European Psychologist, 28*(3), 162–172. https://doi.org/10.1027/10169040/a000494

Schmuck, D., & Hameleers, M. (2020). Closer to the people: A comparative content analysis of populist communication on social networking sites in pre- and post-election periods. *Information, Communication & Society, 23*(10), 1531–1548. https://doi.org/10.1080/1369118X.2019.1588909

Senate of the Italian Republic. (2021). *Senate Act No. 1549 XVIII Legislature: Establishment of a Parliamentary Commission of Inquiry into the serial and massive dissemination of illegal content and false information via the Internet, social media, and other digital platforms.* https://www.senato.it/leg/18/BGT/Schede/Ddliter/52384.htm

Spirit Legal. (2025). *Press release: Class actions filed against TikTok and X in Germany – A test for the DSA, GDPR, and AI Act.* https://www.spiritlegal.com/en/news/details/press-release-class-actions-filed-against-tiktok-and-x-in-germany-a-test-for-the-dsa-gdpr-and-ai-act.html

Strafgesetzbuch. (1998). *Criminal Code.* http://perma.cc/X8TS-UCBK

Taddicken, M., & Wolff, L. (2023). Climate change-related counter-attitudinal fake news exposure and its effects on search and selection behavior. *Environmental Communication, 17*(7), 720–739. https://doi.org/10.1080/17524032.2023.2239516

United Nations Commission on Science and Technology for Development. (2023). *Issues paper on data for development.* https://unctad.org/system/files/information-document/CSTD2023-2024_Issues01_data_en.pdf

United Nations. (2024). *UNRIC library backgrounder: Combat misinformation – Selected online resources on misinformation, disinformation and hate speech.* https://unric.org/en/unric-library-backgrounder-combat-misinformation/

Venice Commission. (2025). *Urgent report on the cancellation of election results by constitutional courts (CDL-PI(2025)001).* European Commission for Democracy through Law. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-PI (2025)001-e

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27). Council of Europe. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

Wenzel, M., Stasiuk-Krajewska, K., Macková, V., & Turková, K. (2024). The penetration of Russian disinformation related to the war in Ukraine: Evidence from Poland, the Czech Republic and Slovakia. *International Political Science Review, 45*(2), 192–208. https://doi.org/10.1177/01925121231205259

Woolley, S. C., & Howard, P. N. (2019). *Computational propaganda worldwide: Executive summary (Working Paper 2017.11).* Project on Computational Propaganda.

World Economic Forum. (2024). *The global risks report.* https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf