MJRC
MEDIA&JOURNALISM RESEARCH CENTER

Maharat

Funded by the European Union
بتمويل من الاتحاد الأوروبي

Regulation of Social Media and Elections in Europe

By Adriana Mutu

2024

Project Brief

This publication is within the project entitled "**Media Reform to Enhance Freedom of Expression in Lebanon**", implemented by Maharat Foundation, Legal Agenda and the Media and Journalism Research Center (MJRC) with the support of the Delegation of the European Union to Lebanon.

The project aims at enhancing Freedom of Expression in Lebanon through the promotion of media law reform as a priority on the national agenda and improvement of the environment for media coverage on the transparency and accountability of elections process.

The project supports the publication of background papers produced by Maharat Foundation on the local Lebanese context and by MJRC on the European standards and best fit recommendations for Lebanon.

The papers cover **eight** main themes:
protection of journalists and their sources, associations of journalists, decriminalization of free speech, incentives and innnovation among journalistic startups, regulation, co-regulation and self-regulation opportunities for the media, modernization of media regulation, regulation of social media and elections, and grounds for elections supervision and monitoring.

Funded by the European Union
بتمويل من الاتحاد الأوروبي

Disclaimer:

Author

Adriana Mutu

Adriana Mutu is a University Professor in the Departments of Humanities and Market Research at ESIC Business & Marketing School in Barcelona, where she also serves as the Head of Academic Quality. She holds a Ph.D. in Political Science from the Autonomous University of Barcelona and a MA in Journalism and Communication Sciences from the University Alexandru Ioan Cuza of Iasi, Romania. She has conducted research at the University of Pennsylvania and the University of Helsinki. Adriana is founding member of MEDEA (Mediterranean Europe and Africa) and provides expertise to the Council of Europe and the European Commission.

Editors: Marius Dragomir and Theodore Southgate

Published by

Media and Journalism Research Center (MJRC)

MJRC is an independent media research and policy think tank that seeks to improve the quality of media policymaking and the state of independent media and journalism through research, knowledge sharing and financial support. The center's main areas of research are regulation and policy, media ownership and funding, and the links between tech companies, politics and journalism.

Maharat Foundation

Maharat Foundation is a women-led freedom of expression organization based in Beirut dedicated to campaigns grounded in research and strengthening connections between journalists, academics, and policy makers. It advances and enables freedom of expression, quality information debate and advocates for information integrity online and offline. Maharat promotes innovation and engages the journalistic community and change agents within Lebanon and the wider, MENA region to promote inclusive narratives and debates and to counter misinformation, disinformation, and harmful content.

Table of contents

1. Executive summary

Social media platforms have now become important venues for shaping public debate, public opinion, and voter behavior.[1] Access to reliable information related to the electoral ecosystem is a core prerequisite for informed decision-making, open deliberation, and citizen participation, fostering confidence in the democratic process. The rise of social media platforms as the main preferred source of information[2] among the populace has renewed both interest and concern over the potentially destabilizing impact of such platforms in the electoral context. They facilitate widespread falsehoods and boost users' exposure to misinformation, disinformation, and inflammatory content, inciting and exacerbating societal divisions and giving rise to fragmentation, polarization, and populism. Distorted information disseminated via social media platforms finds a conducive setting in a divided electorate, eroding democratic principles and leading to distrust in political institutions.

Over the last several years, the impact of social media platforms in elections has driven heightened legislative and regulatory oversight of digital platforms, given their potential to amplify systemic risks that could harm the democratic process of elections. Protecting elections from disinformation is crucial, since 2024 is described as "the biggest election year in recorded history" with 4 billion people worldwide going to the polls[3]. Scientists, technologists and policymakers have expressed concerns regarding the heightened risk to election integrity caused by the proliferation of fake news. The strategies employed amount to election delegitimization, the unlawful processing of personal data for political micro-targeting and profiling, foreign interference campaigns, synthetic and manipulated media through new technologies such as generative Artificial Intelligence, threats of violence against election officials, and the proliferation of illegal hate speech online and (violent) extremist content. There is an increasing recognition of the need for policies that ensure election fairness and integrity, as well as the effective regulation of social media platforms. These measures are essential to maintain public confidence in electoral processes and to provide voters with an environment where they can make informed decisions based on access to fair and balanced information.

[1] European Commission. (2024). Commission Guidelines C/2024/2537. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024XC03014
[2] Reuters Institute for the Study of Journalism. (2024). Digital News Report. University of Oxford. https://reutersinstitute.politics.ox.ac.uk/news/how-ai-generated-disinformation-might-impact-years-elections-and-how-journalists-should-report
[3] Nature. (2024). How online misinformation exploits 'information voids' — and what to do about it. https://www.nature.com/articles/d41586-024-00030-x

Based on this background, this report provides a comprehensive overview of constitutional, legal and regulatory frameworks enforced in the European Union, examining the responses of different Member States as they seek to mitigate the risks related to electoral manipulation on social media and tackle election information digital warfare. The central research question explores how social media platforms are regulated during elections within the European Union. This is examined from multiple perspectives, considering both legislative and non-legislative measures implemented across Europe, along with complementary legal tools. These perspectives include the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) and Digital Markets Act (DMA), the Audiovisual Media Services Directive (AVMSD), the e-Privacy Directive (e-PD), the Regulation on the Transparency and Targeting of Political Advertising (TTPA), the Artificial Intelligence Act (AIA), measures against disinformation, EU Parliament resolutions and communications, as well as sector-specific regulations. The analysis also draws on case law from the European Court of Human Rights under the Council of Europe. The assessment is guided by a set of criteria/key issues identified based on a systematic review of relevant academic and policy research, which concentrate on the potential impact and risks of social media platforms for election integrity. A background context is provided as to why social media platform regulation is needed, based on an overview of the current state of the art regarding the regulation of social media platforms during elections, and the challenges posed by the integrity standards of these platforms to democratic legitimacy.

For the purposes of the present report, the term “digital platform” refers to the description provided by the European Commission: online platforms “cover a wide range of activities including online marketplaces, social media, creative content outlets, app stores, price comparison websites, platforms for the collaborative economy, as well as search engines”[4]. The report incorporates the working definitions provided by United Nations entities and the European Commission, as follows:

- “Disinformation is understood as false information that is disseminated intentionally to cause serious social harm and misinformation as the dissemination of false information unknowingly”.[5]Disinformation is described 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”[6].

- “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. In practice, the distinction between mis- and disinformation can be difficult to determine”[7].

[4] European Commission. (2024). Shaping Europe’s digital future: online platforms. https://digital-strategy.ec.europa.eu/en/policies/online-platforms.
[5] OHCHR. (2021). Disinformation and freedom of opinion and expression. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/085/64/PDF/G2108564.pdf?OpenElement.
[6] European Commission. (2018). Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[7] 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/

- The term “hate speech” is understood as “any kind of communication in speech, writing or behavior that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is often rooted in, and generates intolerance and hatred and, in certain contexts, can be demeaning and divisive”[8].

The taxonomy of information disorder developed by Wardle and Derakhshan (2017)[9] is also considered in the report:

- Misinformation: when false information is shared, but no harm is meant.
- Disinformation: when false information is knowingly shared to cause harm.
- Malinformation: when genuine information is shared to cause harm, often by moving what was designed to stay private into the public sphere.

The methodology for the study consisted of comprehensive desk research based on an extensive review of interdisciplinary primary and secondary academic literature, industry reports, and governmental websites, along with relevant European enforced legislation, national strategies, and official documents.

The report is structured as follows. The background context sets out the criteria used to assess the challenges, opportunities, and risks associated with the use of social media platforms during elections. It starts with the premise that social media platforms play a dual role in the electoral process and that the reliability of online information is crucial during elections. Fair elections cannot take place without an environment that promotes access to transparent and trustworthy information that inspires public confidence, shaping public perception of the legitimacy of the electoral process. A detailed discussion of the potential risks to election integrity and social media platforms is provided in Sections III and IV, based on analysis of extant evidence-based interdisciplinary research. Of particular interest are the efforts of the European Union to protect the electoral process from the dangers of disinformation without infringing upon freedom of opinion and expression. The legal and regulatory responses of the European Union are outlined in Section V. Section VI focuses on specific case studies which introduce more detailed evidence for the observations and claims made in the report and examine regulatory and legislative arrangements in the countries under review. The subsequent sections provide conclusions and recommendations for Lebanon.

[8] United Nations. (2019). Strategy and Plan of Action on Hate Speech. https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf
[9] Claire Wardle & Hossein Derakhshan. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking (Vol. 27). Council of Europe Strasbourg. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

2. Introduction

On April 30 2024, the European Commission launched formal proceedings[10] against Facebook and Instagram under the **Digital Services Act (DSA)** amid concerns over both platforms' failure to act regarding online targeted disinformation campaigns ahead of the elections to the European Parliament and other elections in various Member States. The charges included a multitude of shortcomings for failing to flag illegal content, dissemination of deceptive advertisements, handling of political advertising, demoting political content in the algorithm systems of Instagram and Facebook, and a failure to assess and mitigate risks to civic discourse and electoral processes.

The aftermath of this proceeding placed the spotlight on the ecosystemic issue of online disinformation on social media platforms. To uphold electoral integrity, on May 31 2024 the Spanish Data Protection Agency (AEPD) ordered a temporary ban on the launch of the "Election Day Information" and "Voter Information Unit" tools on Meta's social media platforms in Spain, as a precautionary measure against Meta's plan to collect users' information about the EU elections. The AEPD reasoned that the data processing planned by Meta (collection of basic demographic data, username, IP address, or information on how users interact with the election tools) would entail a "disproportionate interference in the rights and freedoms of data subject", contrary to the **General Data Protection Regulation (GDPR)**. In addition, it "would put the rights and freedoms of Instagram and Facebook users, who would see an increase in the volume of information Meta collects about them, at serious risk, allowing for more complex, detailed and exhaustive profiling, and generating more intrusive processing"[11]. This adds to current concerns[12] about Meta Ireland Limited's processing of personal data for behavioral advertising purposes and several alleged unlawful infringements of the GDPR in Europe. Its conduct is characterized by a lack of transparency, inadequate information, and lack of valid consent in ad personalization.

[10] European Commission. (2024). Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373
[11] Spanish Data Protection Agency. (2024). Press and Communication. https://www.aepd.es/en/press-and-communication/press-releases/the-agency-orders-precautionary-measure-prevents-meta.
[12] On November 10, 2023, the Irish Data Protection Authority (IE DPA) imposed a ban on Meta Ireland Limited (Meta IE) for processing personal data for behavioral advertising, following a binding decision by the European Data Protection Board (EDPB). This decision was prompted by the Norwegian Data Protection Authority, citing risks to user rights under GDPR. Similar legal actions targeting privacy violations include lawsuits against TikTok in the UK (2020-2021) and the Netherlands (2021) for unlawfully collecting children's data. TikTok was previously fined $5.7 million in 2019 by the US FTC, and WhatsApp Ireland was fined €225 million in 2021 for GDPR violations.

In the UK, BBC journalists uncovered how social media networks influence young people on TikTok, feeding misleading election news and shaping narratives about the democratic process and political candidates. The BBC's Undercover Voters Project revealed that “Young voters in key election battlegrounds are being recommended fake AI-generated videos featuring party leaders, misinformation, and clips littered with abusive comments”[13]. In May 2024, the BBC discovered misleading URLs trending on X, fueled by hundreds of fake accounts using the names of London mayoral election candidates, which redirected to the Russian government’s website[14]. A study[15] published by the Reuters Institute for the Study of Journalism at the University of Oxford provided a snapshot of the recent deepfakes circulating on social media impersonating the former UK Prime Minister Rishi Sunak, the US president Joe Biden, the pop star Taylor Swift, the head of government in Mexico City, and Ukraine’s President Volodymyr Zelensky, among others. Other examples of politically motivated election-related disinformation cases are compiled in the Disinfo Bulletin[16], an initiative of the **European Digital Media Observatory (EDMO) Task Force On 2024 European Elections.** Major incidents relate to the spread of false narratives alleging fraud and irregularities in voting procedures, pushing citizens to abstentionism. Examples include a false story on a “Ukraine Solidarity Tax” forging anti-Ukrainian sentiments to sow discord toward European institutions, disinformation narratives about the assassination attempt of the Slovak Prime Minister Robert Fico, and false claims about migrants in Europe, portraying them as criminals. Le Monde reported on how India’s general election has been impacted by deepfakes, “ranging from the broadcast of personalized messages addressed to voters to the most outlandish disinformation montages”[17], while WhatsApp, “India's most popular messaging platform, has become a vehicle for misinformation and propaganda”[18].

These recent events highlight the prominence of the effect of social media platforms on the electoral process and the perceived need for public scrutiny and regulatory oversight. The European Commission has recognized the consumption of online disinformation as a significant societal threat[19]. Specifically, intentional disinformation targeting elections and immigration policies has been identified through extensive consultations with citizens and stakeholders, as the categories most likely to cause harm[20].

[13] Marianna Spring. TikTok users being fed misleading election news. 2 June 2024. BBC. https://www.bbc.com/news/articles/c1ww6vzll81o
[14] Yasmin Rufo. London mayor election: Bots, misleading URLs cause voter confusion. 1 May 2024. BBC. https://www.bbc.com/news/uk-england-london-68923015.
[15] Marina Adami. How AI-generated disinformation might impact this year’s elections and how journalists should report on it. 15 March 2024. England: Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/news/how-ai-generated-disinformation-might-impact-years-elections-and-how-journalists-should-report.
[16] European Digital Media Observatory. (2024). EU Elections - Disinfo Bulletin. https://ec.europa.eu/newsroom/edmo/newsletter-archives/53807.
[17] Sophie Landrin. India's general election is being impacted by deepfakes. 21 May 2024. Le Monde. https://www.lemonde.fr/en/pixels/article/2024/05/21/india-s-general-election-is-being-impacted-by-deepfakes_6672168_13.html.
[18] Kevin Poniah. WhatsApp: The 'black hole' of fake news in India's election. 6 April 2019. BBC. https://www.bbc.com/news/world-asia-india-47797151.
[19] European Commission. (2018). Tackling online disinformation: a European Approach. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236
[20] European Commission. (2018). Summary report of the public consultation on fake news and online disinformation. https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation.

Concerns about social media's role in political polarization and misuse of personal data are growing, as the European Parliament's Spring 2024 Eurobarometer revealed ahead of the June elections. Survey data reported that 81% of European citizens recognize the importance of voting in the current geopolitical climate. Europeans view democracy as their most valued principle, which the European Parliament should prioritize defending[21]. The increasing reliance on digital technologies for democratic participation and access to news significantly impacts people's lives, particularly considering EU legislation regulating online platforms, as outlined in the European Commission's 2024 Special Eurobarometer on 'the digital decade.' In July 2024, EU citizens identified personal data misuse (46%) and fake news and disinformation (45%) as having the greatest personal impact. Other concerns include inadequate protection for minors (33%), untrustworthy online sellers (27%), hate speech (22%), inappropriate advertising (18%), non-transparent content moderation (12%), and unjustified content removal (9%). Looking ahead to 2030, digital technologies are expected to enhance public engagement in democratic life (74%), as well as improve cybersecurity and protection of online data (79%). Respondents from Sweden and Hungary (both 88%), Croatia, Italy and the Netherlands (all 81%) were most likely to consider that digital technologies will be important in engaging in democratic life, while respondents least likely to think so were in Romania (61%), Estonia (69%), Slovenia (66%) and France (67%)[22].

Given that social media represents the primary source of news across the world[23], in the new information economy, the electorate's exposure to propaganda-driven falsified news and harmful information[24] raises concerns over the impact of large-scale disinformation endangering democratic institutions and fundamental human rights[25]. Adding to this level of concern, the Digital News Report 2024 of the Reuters Institute for the Study of Journalism at the University of Oxford revealed that social media use is the fastest-growing source of news across 47 markets, with only "around a fifth of respondents (22%) identify(ing) news websites or apps as their main source of online news"[26]. Most people view "platforms including social media, search, or aggregators as their main gateway to online news" and their attention is captured by partisan commentators, influencers, and young news creators, especially on YouTube and TikTok. YouTube is used for news by 31% of people globally each week, WhatsApp by 21%, and TikTok (13%) has surpassed X (10%). This reflects a growing trend of video as a key source of online news, particularly among younger audiences. Most news video consumption (72%) occurs on online platforms, while only 22% happens on publisher websites. 59% of respondents specify that they are concerned about the rise of online fakes on platforms such as TikTok and X. Some of the countries holding elections in 2024 show higher levels of concern, with South Africa at 81%, the United States at 72%, and the UK at 70%. In contrast, Northern and Western European nations, such as Norway (45%) and Germany (42%), report lower levels of concern.

[21] European Commission, Directorate-General for Communications Networks, Content and Technology (DG CNECT 'Digital Decade' Unit). (2024). Special Eurobarometer *551* on 'the digital decade' 2024. https://europa.eu/eurobarometer/surveys/detail/3174
[22] European Commission. (2024) Special Eurobarometer *551*..., *cit*.
[23] Marina Adami. (2024). How AI-generated disinformation..., *cit*.
[24] Kristina Rozgonyi. (2020). Disinformation online: potential legal and regulatory ramifications to the right to free elections – policy position paper. In Fernando Loizides, Marco Winckler, Usashi Chatterjee, Jose Abdelnour-Nocera, Antigoni Parmaxi. (2019). Human Computer Interaction and Emerging Technologies: Adjunct Proceedings from the INTERACT 2019 Workshops. DOI: https://doi.org/10.18573/book3.g.
[25] United Nations. (2021). Our Common Agenda – Report of the Secretary-General. https://www.un.org/en/content/common-agenda-report/.
[26] Reuters Institute for the Study of Journalism. (2024). Digital News..., *cit*.

To conclude, social media platforms play a dual role in the electoral process. They can act as a tool facilitating information exchange, public scrutiny, and citizens' engagement and association, "strengthening the discourse that lies at the heart of a democratic system of government"[27]. On the other hand, social media platforms also pose a significant threat to democracy[28] as they can be used to destabilize and erode trust in the electoral process, reduce citizen participation, amplify voter confusion, spread fake news, and enhance extremism with the proliferation of echo-chambers. This results in radicalization, exacerbation of social divisions, suppression of political participation, and marginalization of women and minority groups. This in turn undermines trust in election management bodies and decreases governmental accountability and transparency.

The advent of new digital technologies poses challenges and opportunities for the exercise of free elections, as they can be used to affect the outcome of democratic elections and public confidence in electoral scrutiny. This is achieved through personalized political advertisements, microtargeting techniques, algorithmic filtering of social media news feeds, and the ability to influence voters' decision-making processes through artificial intelligence (AI) via deepfakes or the artificial intelligence-manipulated media. These issues emerge as global risks ranked by severity over the short and long term, as they "may radically disrupt electoral processes in several economies over the next two years"[29]. According to the 2024 Global Risks Report released by the World Economic Forum, based on a survey of 1,400 experts, policymakers, and the private sector, growing distrust in the media coupled with the widespread use of misinformation and disinformation on social networks might undermine the "the legitimacy of newly elected governments" across the world, "a vicious cycle that could trigger civil unrest and possibly confrontation"[30].

[27] Yasmin Dawood. (2020). Protecting elections from disinformation: a multi-faceted public private approach to social media and democratic speech. The Ohio State Technology Law Journal, 1, 640-668.
[28] Niamh Hanafin. (2022). Strategic Guidance. Information Integrity: Forging a pathway to Truth, Resilience and Trust. Envisioning comprehensive and effective responses to information pollution. The United Nations Development Programme. https://www.undp.org/publications/information-integrity-forging-pathway-truth-resilience-and-trust
[29] World Economic Forum. (2024). The Global Risks Report. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.
[30] World Economic Forum (2024). The Global..., *cit*.

3. Context for the study: the social media challenge for election integrity

Democracies "rely on well-informed and politically educated citizens" who "participate in various ways in making informed voting decisions"[31]. The notion of "post-truth" defines the post-truth society "which is based on the information disorder – either on fake news (misinformation, disinformation, and/or malinformation) or alternative facts (true or partly true information framed in a specific context) – to which the public reacts emotionally rather than rationally"[32]. The lack of credible information, distortion of the truth, manipulation of the public using emotional rhetoric, and the proliferation of sensationalist content and partisan information affects ordinary citizens and influences them to "not elect those who will represent them in their best interest, but rather those who are better manipulators"[33]. Research shows that the prominence of source information does not significantly impact people's ability to detect fabricated news, manipulated images, or false headlines, and that individuals' reliance on intuition over analytical thinking is a strong factor in why people fall for fake news[34]. Social networking sites (SNS) as "alternative discursive platform" are proven to be forums for populist communication[35] adopted by populist politicians who use discursive framing and stylistic elements such as emotionality, negativity, us-them-rhetoric, people-centrism, anti-elitism, and popular sovereignty to engage with voters during elections. Quantitative content analysis of Facebook and X posts of 13 leading candidates of parliamentary parties in Austria and the Netherlands in 2017 revealed that populist statements with negative tonality are more prevalent before election periods, which suggests that populist political communication is used strategically as a tool to maximize votes during elections[36]. Social media platforms are recognized for fostering personalization, serving as spaces where candidates are portrayed as individuals[37]. This occurs regardless of whether candidates adopt dialogue-driven or marketing-focused campaigning styles[38]. Empirical data[39] reveals that European parties actively leverage social media platforms for digital campaigning, with Facebook as the most adopted social medium and TikTok emerging as a relatively new platform.

[31] Lejla Turcilo & Mladen Obrenovic. (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
[32] Lejla Turcilo & Mladen Obrenovic. (2020). Misinformation, Disinformation..., *cit*.
[33] Lejla Turcilo & Mladen Obrenovic. (2020). Misinformation, Disinformation..., *cit*.
[34] Matthew Groh, Aruna Sankaranarayanan, Nikhil Singh, Dong Young Kim, Andrew Lippman & Rosalind Picard. (2024). Human detection of political speech deepfakes across transcripts, audio, and video. Nature Communications, 15, 7629. https://doi.org/10.1038/s41467-024-51998-z
[35] Desirée Schmuck & Michael Hameleers. (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. DOI: 10.1080/1369118X.2019.1588909
[36] Desirée Schmuck & Michael Hameleers. (2020). Closer to the people..., *cit*.
[37] Liesbeth Hermans & Maurice Vergeer (2012). Personalization in e-campaigning: A cross-national comparison of personalization strategies used on candidate websites of 17 countries in EP elections 2009. New Media & Society, 15(1), 72–92. DOI:10.1177/1461444812457333.
[38] Gunn Enli S. & Eli Skogerbø. (2013). Personalized campaigns in party-centered politics. Information, Communication & Society, 16(5), 757–774. doi:10.1080/1369118X.2013.782330
[39] Philipp Darius, Wiebke Drews, Andreas Neumeier, and Jasmin Riedl. (2024). The EUDigiParty data set. Harvard Dataverse. DOI: 10.7910/DVN/U6UWPN.

Psychological factors driving virality of content sharing and video-based misinformation on social media include characteristics that divert people's focus from accuracy, such as high-arousal emotions, whether positive (surprise, novelty) or negative (anger, anxiety, fear, or disgust)[40]. This encapsulates what scholars call "moral contagion", expressions of moral emotion, a phenomenon that helps explain how social media platforms capture attention and drive engagement by sharing morally and emotionally evocative content, amplifying political polarization, propaganda, and disinformation in the digital era[41]. Researchers show that "social media often acts like an accelerant for existing moral dynamics—amplifying negative facets of morality such as outrage, harassment, status seeking, and intergroup conflict as well as some positive aspects of morality, such as social support, prosociality, and collective action"[42]. Evidence[43] suggests that people are motivated by group identity to share moral-emotional content, which tends to capture attention more effectively. Additionally, the design of social media platforms enhances these natural cognitive and motivational tendencies, making it easier for such content to spread.

Even though online media and digital platforms have become widely debated in the context of fake news dissemination, it is worth noting that disinformation is not only spread by online social networks, but also by state controlled or captured legacy media. "Closed authoritarian regimes are systems in which the state itself – that is, the political elites – controls the media systems (traditional media) and limits opportunities for access to online platforms. As a result, these elites continue to be the primary actors who spread disinformation and propaganda. In contrast, in more democratic systems, media and online platforms are freer and more open for various actors that can spread fake news. This creates a political environment that is not considered as democratic, but rather influenced by political manipulation, political propaganda, and populistic narratives"[44]. Information disorder cannot be attributed only to "technology or malicious actors", but also to "a struggling legacy media sector, challenged by digital transformation and competition from online platforms and threatened by state pressure in some parts of the world; the absence of robust public information regimes; low levels of digital and media literacy among the general public; and the frustrations and grievances of a growing number of people, fueled by decades of economic deprivation, market failures, political disenfranchisement and social inequalities, which make some individuals more susceptible to manipulation"[45].

[40] Jonah Berger & Katherine Milkman. (2012). What Makes Online Content Viral? Journal of Marketing Research, 49(2), 192-205. https://doi.org/10.1509/jmr.10.0353
[41] William Brady, M.J. Crockett & Jay J Van Bavel. (2020). The MAD Model of Moral Contagion: The Role of Motivation, Attention, and Design in the Spread of Moralized Content Online. Perspectives on Psychological Science, 15(4), 978-1010. https://doi.org/10.1177/1745691620917336
[42] Jay J. Van Bavel, Claire E. Robertson, Kareena del Rosario, Jesper Rasmussen & Steve Rathje. (2024). Social Media and Morality. Annual Review of Psychology, 75:311–40. https://doi.org/10.1146/annurev-psych-022123-110258
[43] William Brady, M.J. Crockett & Jay J Van Bavel. (2020). The MAD Model..., *cit*.
[44] Lejla Turcilo & Mladen Obrenovic. (2020). Misinformation, Disinformation..., *cit*.
[45] OHCHR. (2021). Disinformation..., *cit*.

Much of the recent research on risks associated with the social media operations apparatus of spreading false or harmful information during elections has centered around the dangers of "data voids of misinformation and disinformation"[46] to democratic self-government and democratic legitimacy. Taxonomies of information disorder are put forward addressing how the diffusion of propaganda through deceptive AI-generated content or large-scale data collection by digital platforms enables micro-targeting of segmented groups of voters[47]. Disinformation is defined in prior research as "information intentionally created to trigger, mislead or generate decision errors, manipulate belief systems of individuals and deceive humans", while misinformation stems from "misrepresented information that causes confusion and are not always intentionally created"[48]. Online disinformation "is used for cognitive hacking, in social engineering and human-factors exploitation schemes, to persuade individuals to fall into targeted attacks like spear phishing and malware installation or in the creation and dissemination of "false news" and hoaxes"[49]. Information pollution as an "existential risk to humanity"[50], injections of false information into political discourse and political campaigning, misinformation as "a moral panic"[51], alarmist discourses, gendered disinformation, out of proportion journalistic reporting, and media emphasis on misinformation prevalence are shown to provoke democratic backsliding, undermining government accountability and eroding trust in the media[52].

Another strand of research addresses the role of search engines in computational propaganda, as information gatekeepers shape the digital information environment and become a "de facto infrastructure" for democratic processes. Technology can be exploited to influence political outcomes; search engine optimization (SEO) strategies are used to amplify disinformation, political propaganda, and junk news[53]. Junk news domains are websites created to spread conspiracy theories, counterfeit professional news brands, and mask partisan commentary as news. They rely on Google Search for discoverability and monetization via optimization and keyword strategies. An analysis[54] of 29 junk news domains and their SEO keyword strategies between January 2016 and March 2019 shows that junk news producers generate profit particularly around major political events, and that technology can be subverted for political and economic outcomes.

[46] Nature. (2024). How online misinformation..., *cit*.
[47] Renée DiResta & Josh Goldstein. (2024). How spammers and scammers leverage AI-generated images on Facebook for audience growth. Harvard Kennedy School (HKS) Misinformation Review, *5*(4), 1-19.
[48] Alisson Puska, Lara Piccolo & Roberto Pereira. (2020). DisMiss False Information: A Value Matter. In Fernando Loizides, Marco Winckler, Usashi Chatterjee, Jose Abdelnour-Nocera, Antigoni Parmaxi. (2019). Human Computer Interaction and Emerging Technologies: Adjunct Proceedings from the INTERACT 2019 Workshops. DOI: https://doi. org/10.18573/book3.g.
[49] Alisson Puska, Lara Piccolo & Roberto Pereira. (2020). DisMiss..., *cit*.
[50] Niamh Hanafin. (2022). Strategic Guidance. Information Integrity..., *cit*.
[51] Matt Carlson. (2020). Fake news as an informational moral panic: The symbolic deviancy of social media during the 2016 US presidential election. Information, Communication & Society, 23(3), 374 388. https://doi.org/10.1080/1369118X.2018.1505934.
[52] Elizabeth Harris, Stephanie DeMora, & Dolores Albarracín. (2024). The consequences of misinformation concern on media consumption. Harvard Kennedy School (HKS) Misinformation Review, *5*(3), 1-21.
[53] Samantha Bradshaw. (2019). Disinformation optimised: gaming search engine algorithms to amplify junk news. Internet Policy Review, 8(4). DOI: 10.14763/2019.4.1442
[54] Samantha Bradshaw. (2019). Disinformation optimised..., *cit*.

Scholars suggest that mitigation measures must be undertaken by policymakers to counteract systemic risks and the excessive power of big tech platforms undermining the functioning of democratic societies. Various countries have taken on legislative challenges in battling digital information disorder, holding online platform providers accountable[*55*]. Legislative efforts, policies, strategies, and regulatory responses must counter digital information disorder, enabling affordable, accessible, trusted, and secure digital ecosystems, without infringing upon the freedom of opinion and expression. The impact of digital platforms in elections and potential regulatory solutions must address issues such as technological design, governance and policy decisions, advertising infrastructure, algorithms, and user agreements that support social networking technologies. Stakeholders must curb and mitigate the potential harm of hate speech, misinformation and disinformation, and in accordance with human rights and international law, correct the regulatory vacuum created by the advent of generative AI technologies, ensuring "information integrity", a newly coined term utilized in the United Nations system. "Information integrity" is determined by "the accuracy, consistency, and reliability of the information content, processes and systems to maintain a healthy information ecosystem"[56]. As opposed to "information integrity", "information pollution" has a negative impact on the information ecosystem, including "reduced public access to accurate and reliable news, increased use of alternative information sources, spread of junk news stories on- and offline", "increased gender targeted trolling, harassment and cyberviolence, stifling of activists and opposition voices", and "regulation curtailing rights to information, freedom of expression and opinion, legislation restricting civic space and dissenting voices, growth of "disinformation industry"[*57*].

[*55*] During the 2022 Brazilian elections, the Superior Electoral Court of Brazil took action to counter disinformation by ordering social media platforms to halt payments to specific individuals and pages disseminating disinformation, prohibiting platforms from suggesting political content through algorithms and requiring them to implement reverse tracking mechanisms to trace the origin of posts. See https://globalfreedomofexpression.columbia.edu/cases/the-case-of-disinformation-demonetization-on-brazilian-social-media/

[56] Niamh Hanafin. (2022). Strategic Guidance. Information Integrity…, *cit*.

[57] Niamh Hanafin. (2022). Strategic Guidance. Information Integrity…, *cit*.

4. Online platforms and the distortion of democratic elections: key policy issues

4.1 The spread of online disinformation, misinformation and propaganda

Digital disinformation and misinformation as "viral deceptions" represent systematic risks to election integrity, jeopardizing electoral processes, intensifying political polarization, and diminishing social trust and cohesion. An overview of systemic challenges provoking power imbalances in the data economy, namely data accessibility, economic constraints, and digital illiteracy, owing to the dominance of tech giants in the global platform economy, is presented in an Issue "Paper on Data for Development"[58] prepared by the United Nations Commission on Science and Technology for Development. The report shows that "While disinformation is not a new problem, data-enabled technologies such as social media platforms, artificial intelligence (AI), and Big Data analytics have created new avenues for false or manipulated information to be created, disseminated, and amplified at a scale, speed, and reach never known before"[59]. Users' confirmation biases are enabled by exposure to "content that aligns with their political affiliation and personal beliefs" which is generated by digital platforms' "large-scale data collection of users' online activities, including their browsing activity, purchasing history, location data, and more, to provide users with content they are most likely to engage with, in turn, spending more time on the platforms, which converts to more advertising revenue for the platform"[60]. Platform design choices, algorithmic content curation through platform recommendations, algorithmic filtering, and micro-targeting of users with specific content hinder exposure to plural and diverse sources of information, inhibiting "the capacity of an individual to reflect on their values, motivations, and decision-making involved in engaging with content", which "allows the spread and cementing of misinformation"[61].

[58] UNCTAD Secretariat. (2023). United Nations Commission on Science and Technology for Development Inter-sessional Panel 2023-2024. https://unctad.org/system/files/information-document/CSTD2023-2024_Issues01_data_en.pdf
[59] UNCTAD Secretariat. (2023). United Nations..., *cit*.
[60] UNCTAD Secretariat. (2023). United Nations..., *cit*.
[61] UNCTAD Secretariat. (2023). United Nations..., *cit*.

Automated systems are shown to influence collective human behavior, including the spread of misinformation[62], voting behavior[63], social movements[64], sexist and racist harassment[65], public safety, and extremism[66]. Recent human-algorithm behavior experiments[67] demonstrate that collective human behavior can also influence algorithm behavior. A study exploring whether encouraging readers to fact-check unreliable sources impacts news aggregation algorithms showed that prompting readers to fact-check led to increased human fact-checking and lower average vote scores for those articles. In a large-scale experiment involving 1,104 discussions, the fact-checking efforts resulted in the algorithm reducing the visibility of unreliable sources by up to 25 rank positions[68].
The formation of "filter bubbles" or "echo chambers" enabling confirmation bias has been studied in prior research[69] examining how online polarization may foster misinformation and the way social media platforms influence information spreading. Feed algorithms, which prioritize content based on users' preferences and behaviors, play a significant role in shaping which information gains visibility. This shift has influenced how people form social perceptions and frame narratives, which can impact policymaking, political discourse, and public debates, particularly on divisive topics. Online, users often gravitate towards content that aligns with their existing beliefs while ignoring opposing viewpoints, leading to the formation of polarized groups around shared narratives. High levels of polarization can also foster an environment where misinformation spreads rapidly. Selective exposure heavily influences how content is consumed on social media, and the dynamics can vary significantly across different platforms[70].

The key characteristics of each platform, such as their data practices, policies, algorithms, intermediation, and network effects, as well as their black box systems, serve as hidden mechanisms of authority that influence, regulate, and facilitate freedom of speech, political engagement, and access to information. "The design of these systems engenders a range of civic issues, including fair political campaigning and election integrity, regime transformation and political mobilization, changing patterns of information consumption, or issues at the intersection of democracy and security, including data security, foreign influence operations, and trolling and harassment"[71].

[62] Giovanni Luca Ciampaglia. (2018). Fighting fake news: A role for computational social science in the fight against digital misinformation. J. Comput. Soc. Sci. 1, 5360.
[63] Eli Pariser. (2011). The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think. Penguin; Robert Epstein & Ronald Robertson. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. Proc. Natl. Acad. Sci. 112, E4512.
[64] Helen Margetts, Peter John, Scott Hale & Taha Yasseri. (2015). Political Turbulence: How Social Media Shape Collective Action. New Jersey: Princeton University Press.
[65] Adrienne Massanari. (2017). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. New Media & Society, 19(3), 329-346; Gina Neff. (2016). Talking to bots: Symbiotic agency and the case of Tay. Int. J. Commun. 10, 4915.
[66] Kari Paul. It Let White Supremacists Organize: The Toxic Legacy of Facebook's Groups. 4 Feb 2021. The Guardian.https://www.theguardian.com/technology/2021/feb/04/facebook-groups-misinformation
[67] J. Nathan Matias. (2023). Influencing recommendation algorithms to reduce the spread of unreliable news by encouraging humans to fact-check articles, in a field experiment. Sci Rep 13, 11715. https://doi.org/10.1038/s41598-023-38277-5
[68] J. Nathan Matias (2023). Influencing recommendation..., *cit*.
[69] Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi & Michele Starnini. (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
[70] Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi & Michele Starnini. (2021). The echo chamber..., cit.
[71] Samantha Bradshaw. (2019). Disinformation optimised..., *cit*.

In liberal democracies, online platforms self-regulate user-generated content, incentivized by limited liability regimes that exempt them from responsibility for third-party content. In exchange, platforms cooperate with government requests to remove illegal content, generally through a notice-and-takedown approach rather than ongoing monitoring. Increasingly, platforms proactively remove certain content, mainly targeting extremist and terrorist speech[72]. Most social media platforms offer advice on online security, including how to identify misleading news and disinformation, as well as how to report online harassment, threats, and abuse. X provides general safety guidelines, quick access to account security tips, and instructions for reporting offensive content and abuse. Parties and candidates can report abusive material directly via email. Facebook, which owns Instagram and WhatsApp, offers general online safety advice and specific support for individuals running for office, including detailed instructions on reporting abusive behavior. Google, which owns YouTube, provides guidance to protect users from digital attacks and resources to promote reliable election information.

4.2 Digital information warfare, state sponsored disinformation and foreign election interference

The intersection of political disinformation and internet platform technologies has drawn significant public attention, particularly as social media has emerged as a battleground in cyberwarfare following the perceived influence by foreign actors in both the Brexit referendum and the U.S. presidential election in 2016. The risks associated with foreign electoral interference and disinformation sparked Meta's September 2024 decision[73]to ban RT, Rossiya Segodnya, and other Russian state media outlets from its platforms, including Instagram, WhatsApp, and Threads. Meta cited the outlets' use of deceptive tactics in covert online influence operations. This move follows charges by US authorities against two RT employees for money laundering related to attempts to influence the 2024 US elections, with the US Secretary of State calling for RT to be treated as a covert intelligence operation rather than legitimate journalism.

Political disinformation campaigns constitute a "public harm regardless of the propagators"[74] and can be labeled as threat intelligence. Threat intelligence has been defined as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."[75]

[72] Yasmin Dawood. (2020). Protecting elections..., *cit*.
[73] Katie Paul. Meta bans Russian state media for 'foreign interference'. 17 September 2024. Reuters. https://www.reuters.com/business/media-telecom/meta-bans-rt-other-russian-state-media-networks-2024-09-17/
[74] Dipayan Ghosh & Ben Scott. (2018). #DIGITALDECEIT The Technologies Behind Precision Propaganda on the Internet. https://www.newamerica.org/documents/2077/digital-deceit-final-v3.pdf
[75] Gartner Inc. (2013). Definition: Threat Intelligence. www.gartner.com/en/documents/2487216

The role played by disinformation campaigns led by State or State-sponsored actors (governmental bodies, political parties and other elite actors) within or outside their borders is another critical phenomenon attracting scholarly interest. Part of a "larger process of democratic backsliding"[76], disinformation campaigns orchestrated by domestic stakeholders constitute "an abuse of the legitimate power of the state", hindering democratic accountability and depriving citizens of their right to information and freedom of expression[77]. Their aim is to shape public opinion to influence political processes and electoral outcomes, increasing electoral vulnerability.

The multifaceted process of "deceiving citizens for political gains" is extensively scrutinized in the book titled "State-Sponsored Disinformation Around the Globe"[78]. State-sponsored disinformation is defined as "the systematic and coordinated effort by state actors and elite collaborators to intentionally spread false or misleading information on a large scale. This effort is coordinated because it puts the state at the center of broader elite power circuits that foster environments conducive to disinformation. The ultimate goal of state-sponsored disinformation is to gain political and economic dominance by controlling public discourse and opinions"[79]. Deceptive practices and features of intentional state-sponsored disinformation include strategic planning, privileged access to material and symbolic resources, sophistication, perceived legitimacy, abuse of institutional power, and corporate and media collusion. Various actors are involved in this destabilizing process, including corporate stakeholders, security agencies, captured media organizations, "think tanks that emerge during elections to later disappear"[80], and private sector proxy organizations, among others. Social media and messaging apps are tools for disinformation operations, enabling datafication, algorithmic targeting, segmentation, source impersonation, and harnessing users' demographic and behavioral data.

Precision propaganda employs industry-standard digital advertising and marketing tools that can be adapted by both domestic and foreign malicious actors. Its toolbox includes behavioral data collection, digital advertising platforms, search engine optimization, social media management software, and algorithmic advertising technology, all used by internet-based advertising and social media platforms[81]. Interference operations during electoral processes often involve targeting information consumption, undermining voter participation, attacking candidates and political parties, eroding trust in democratic institutions, and compromising election-related infrastructure. These actions exemplify foreign actors' deliberate attempts to engage in Foreign Information Manipulation and Interference (FIMI). The 2nd European External Action Service (EEAS) Report on FIMI Threats documents these threats from a comprehensive, risk-based perspective. FIMI, also labeled as "disinformation"[82], represents a growing political and security challenge for the European Union.

[76] Alexander Schmotz. (2019). Hybrid regimes. In Wolfgang Merkel, Raj Kollmorgen & Hans-Jürgen Wagener. (2019). The handbook of political, social, and economic transformation. England: Oxford University Press. DOI: 10.1093/oso/9780198829911.003.0053
[77] Martin Echeverría, Sara García Santamaría & Daniel Hallin. (2025). State-sponsored disinformation around the globe: How politicians deceive their citizens. Routledge.
[78] Martin Echeverría, Sara García Santamaría & Daniel Hallin. (2025). State-sponsored disinformation..., *cit*.
[79] Martin Echeverría, Sara García Santamaría & Daniel Hallin. (2025). State-sponsored disinformation..., *cit*.
[80] Martin Echeverría, Sara García Santamaría & Daniel Hallin. (2025). State-sponsored disinformation..., *cit*.
[81] Dipayan Ghosh & Ben Scott. (2018). #DIGITALDECEIT..., *cit*.
[82] 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-interference_en

FIMI "describes a mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory"[83]. The 2021 report analyzes 33 FIMI incidents concerning elections held between 2017-2023 across EU Member States, the US, and Africa, and reveals a plethora of risks associated with specific FIMI threats[84]. Threat actors seek to control the flow of information and set the agenda on key topics during electoral periods by targeting information consumption. A common tactic involves discrediting traditional or mainstream media, creating narratives that foster distrust in official sources and widely used communication channels. This manipulation undermines confidence in information shared by democratically elected officials, encouraging the public to rely on unverified sources instead. Targeting citizens' ability to vote seeks to both encourage voter abstention and promote invalid votes. The associated risk is that segments of society may reject the legitimacy of election results, potentially leading to violent reactions, protests, and civil unrest.

Threat actors also engage in FIMI to target political parties or individual candidates, aiming to polarize citizens by either supporting or attacking specific political positions or promoting particular political agendas. This can involve undermining political adversaries, specific minorities, or alternative political views. The risk is that such tactics may discourage candidates from running for office or speaking out on key issues, with personal and public repercussions that could damage their political careers and impair their ability to effectively represent voters' interests. Targeting trust in democracy seeks to erode faith in the democratic system and diminish public support for it. The motives behind these efforts can be geopolitical, economic, or political, or simply aimed at creating confusion and instability. The risks include higher rates of voter abstention, protest votes, invalid ballots, low voter turnout, sustained protests, and a general perception that elections are not truly democratic.

Targeting election-related infrastructure involves cyber-enabled operations aimed at both physical and digital election systems, often reinforcing the broader objectives of threat actors. In the context of FIMI, cyberattacks may be accompanied by disinformation campaigns, forming a hybrid attack strategy. These attacks can have real consequences by undermining critical election infrastructure, potentially interfering with or invalidating election results. Even when the attacks have no direct impact, the perceived risks can foster insecurity and fuel doubts about the integrity of the electoral process, further eroding trust. To sum up, these risks threaten the integrity of democratic societies and institutions, undermining fundamental rights and freedoms, the rule of law, security, economic wellbeing, and the principle of sovereignty.

[83] European External Action Service (EEAS). (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en
[84] European External Action Service (EEAS) (2024). 2nd EEAS..., *cit*.

Tackling interference operations requires comprehensive policy measures against malicious users of technology, and diplomatic actions and international agreements. Recital 19 of **Regulation (EU) 2024/900 on the transparency and targeting of political advertising** highlights the serious threat that unlawful interference in European elections by third-country entities or nationals poses to democracy. The **European Parliament Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes**[85] emphasizes that foreign interference can manifest in various ways, such as disinformation campaigns on social media aimed at shaping public opinion, the dissemination of online political adverts, cyber-attacks on critical electoral infrastructure, and both direct and indirect financial support for political actors (Paragraph C).

Some countries are taking steps to prevent foreign influence in their national elections. Under French law, a judge can mandate actions required to halt the online spread of misleading information within the three months leading up to an election. Additionally, during this period, foreign television broadcasts may be suspended if they broadcast false information. The **German Network Enforcement Act (NetzDG law)** was introduced in recognition that self-regulatory initiatives of online platforms were insufficient to tackle fake news and foreign election tampering in electoral periods. In the United States, the National Defense Authorization Act (NDAA) includes measures intended to address deepfakes and 'digital content forgeries' by foreign states. The "Countering Foreign Propaganda and Disinformation Act of 2016"[86] serves as the key legal framework for tackling misinformation and malicious foreign activities. It mandates the establishment of a Center for Information Analysis and Response, which is tasked with coordinating the sharing of information among various government agencies about foreign information warfare efforts, developing processes that integrate insights on foreign propaganda and disinformation into national strategies, enhancing the government's ability to combat deceptive information and protect democratic processes.

[85] 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
[86] House – Foreign Affairs. (2016). H.R.5181 - Countering Foreign Propaganda and Disinformation Act of 2016.https://www.congress.gov/bill/114th-congress/house-bill/5181/text

4.3 Blockchain technology, dissemination of false information and political campaign finance in the age of cryptocurrencies

Blockchain technology as a game changer in the fight against disinformation is a relatively novel theme that has consistently gained scholarly attention[87]. A blockchain consists of a decentralized database shared across a network of computers, characterized by transparency, immutability, traceability, and accountability[88]. Blockchains can be public, private, or consortium. Transactional trust is a feature of blockchain technology, as it "promises to supply a kind of digital trust between complete strangers"[89], generating transaction records that are simultaneously stored across a network of computers, making them immutable by any single party. Scholars have examined the propagation of cyber currencies and use of blockchain technology in e-government operations[90], transatlantic relations and international economics[91], international development in fragile states[92], EU technological sovereignty and global AI governance[93], political activism, digital insurgencies, and national security threats[94], raising awareness of personal data privacy concerns[95] and highlighting the technological and political challenges[96] that may hinder the wider adoption of blockchain solutions[97]. These include the immaturity of the technology, the lack of regulatory oversight, and threats to governmental monetary control[98].

[87] Petros Iosifidis. (2025). Theoretical understanding of State-Sponsored Disinformation. In Martin Echeverría, Sara García Santamaría & Daniel C. Hallin, State-Sponsored Disinformation Around the Globe. How Politicians Deceive their Citizens. Routledge Studies in Media, Communication, and Politics, 21-36; Ana Mutu & Álex Vallejo Blanxart. (2024). Blockchain applications for professional journalists: a preliminary qualitative assessment. International Conference on Communication and Applied Technologies; Don Tapscott & Alex Tapscott. (2016). Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. New York: Penguin.
[88] Don Tapscott & Alex Tapscott. (2016). Blockchain revolution..., *cit*.
[89] Harry Collins, Robert Evans, Martin Innes, Eric B Kennedy, Will Mason-Wilkes and John McLevey. (2022). The Face-to-Face Principle Science, Trust, Democracy and the Internet. Wales: Cardiff University Press.
[90] F. Rizal Batubara, Jollen Ubacht & Marijn Janssen. (2018). Challenges of blockchain technology adoption for e government: a systematic literature review. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, 76 .https://doi.org/10.1145/3209281.3209317; Teogenes Moura & Alexandre Gomes. (2017). Blockchain Voting and its effects on Election Transparency and Voter Confidence. Proceedings of the 18th Annual International Conference on Digital Government Research, 17. http://dx.doi.org/10.1145/3085228.3085263; Michal Pawlak, Jakub Guziur & Aneta Poniszewska-Marańda. (2019). Voting Process with Blockchain Technology: Auditable Blockchain Voting System. Advances in Intelligent Networking and Collaborative Systems. http://dx.doi.org/10.1007/978-3-319-98557-2_21
[91] Nicola Bilotta. (2024). Technological Sovereignty: Italy, the EU and the US. Instituto Affari Internazionali. https://www.jstor.org/stable/resrep60159
[92] Willem van den Berg. (2018). Blockchain for fragile states: the good, the bad and the ugly. Clingendael Institute, Netherlands Institute of International Relations. https://www.jstor.org/stable/resrep17341; Nir Kshetri. (2023). Fourth Revolution and the Bottom Four Billion. Michigan: University of Michigan Press; Daivi Rodima-Taylor. (2023). The Cryptopolitics of Digital Mutuality. New York: Berghahn Books.
[93] Raluca Csernatoni. (2024). Charting the Geopolitics and European Governance of Artificial Intelligence. Carnegie Endowment for International Peace. https://www.jstor.org/stable/resrep58111.6
[94] Noam Unger, Austin Hardman & Ilya Timtchenko. (2023). Analyzing the Role of Blockchain Technology in Strengthening Democracies. Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep53851; Armin Krishnan. (2020). Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations. Journal of Strategic Security 13(1), 41-58. https://scholarcommons.usf.edu/jss/vol13/iss1/3
[95] Guy Ziskind, Oz Nathan & Alex Sandy Pentland. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE CS Security and Privacy Workshops.
[96] Nathan Schneider. (2024). Governable Spaces: Democratic Design for Online Life. Oakland: University of California Press.
[97] Omkar Mahajan. (2023). Note-the advent of campaign finance: a dilemma regulating blockchain technology and cryptocurrency while balancing free speech interests. Cornell Journal of Law and Public Policy, 31:355-388. https://community.lawschool.cornell.edu/wp-content/uploads/2023/02/Mahajan-note-final.pdf
[98] F. Rizal Batubara, Jollen Ubacht & Marijn Janssen. (2018). Challenges of blockchain..., *cit*.

Advocates of digital technologies claim that the cryptographic security of blockchain technology can improve the detection of fake media, creating ecosystems to support fact-based information[99], thereby enhancing public trust during high-stakes events such as elections. This technology allows for the validation of media authenticity and the tracing of digital content back to its source. By recording original media documents on the blockchain, it becomes possible to expose forgeries and manipulation, as the data is rendered mathematically immutable, preventing any tampering or destruction[100]. Social media users dissatisfied with censorship of content look "towards new platforms that are censorship-free" including blockchain-based solutions and decentralized online communications services[101].

Fact Protocol (FACT), a US-based community-governed web3 protocol aggregating fact-checks around the world, offers insights on blockchain technology as a tool to detect and combat the spread of fake news. Blockchain applies mathematical algorithms for encrypting and decrypting data[102] to establish a decentralized, cross-referenced, secure ledger (immutable and public database) that transparently records transactions, making them verifiable at any time and resistant to manipulation or tampering. Once the news or information is stored on a blockchain it becomes a permanent, traceable and immutable record serving as a reliable reference for verifying the authenticity of news and information, making it easier to track and identify the author spreading false information. Because blockchain is decentralized, it allows multiple participants to collaborate to fact-check and verify information in a transparent manner, allowing the public to track and see the source of the content. Smart contracts, secure, tamper-proof, and transparent self-executing agreements recorded on a distributed ledger are increasingly being adopted in the context of combating fake news, to enforce rules and standards for sharing and distributing information. There is some evidence that blockchains and smart contracts can be used for deepfake detection, analyzing the metadata within a video back to the original computer source, determining whether the video is real or fake[103].

Criticism[104] of blockchain technologies has been put forward, highlighting their association with fraudulent pseudo-banks, financial collapses, investment and commodities violations, money laundering, illegal gambling, tax evasion, theft, embezzlement, mail and wire fraud, and ransomware attacks on public infrastructure, often linked to attempts to evade regulatory oversight.

[99] Ben Gregori & Chris Doten. How could blockchain power government services and uplift citizen voices? 29 April 2021. New America. https://www.newamerica.org/digital-impact-governance-initiative/blockchain-trust-accelerator/around-the-blockchain-blog/how-could-blockchain-power-government-services-and-uplift-citizen-voices/
[100] Tomicah Tillemann, Allison Price, Glorianna Tillemann-Dick & Alex Knight. (2019). The Blueprint for Blockchain and Social Innovation. The Blockchain Trust Accelerator at New American. The Blueprint for Blockchain and Social Innovation (newamerica.org).
[101] Armin Krishnan. (2020). Blockchain Empowers..., *cit*.
[102] FACT Protocol. (2023). Blockchain technology as a tool to detect and combat fake news. https://fact.technology/learn/blockchain-technology-to-combat-fake-news/
[103] Haya Hasan, & Khaled Salah. (2019). Combating deepfake videos using blockchain and smart contracts. IEEE Access, 7, 41596–41606. DOI: 10.1109/ACCESS.2019.2905689; Adam G Lee. (2024). Deepfake It Til You Make It: How To Make A Short Film. Illinois: Olivet Nazarene University.
[104] Nathan Schneider. (2024). Governable Spaces..., *cit*.

These risks represent strong incentives for governments to regulate cryptocurrencies in the context of political campaigning to prevent malicious foreign influence and safeguard national self-determination. The lack of regulatory oversight in this area is concerning, as cryptocurrency donations in political campaigns, crowdfunding, and micro-credits can easily bypass existing regulations on donations and electoral fundraising[105]. Technology scholars agree that using blockchain technology during political campaigns can create transparent and tamper-proof records of political parties' funding sources and expenditures (cryptocurrencies cannot be counterfeited or double spent), which could help minimize the risk of anonymous donations and foreign interference[106] and curb the spread of misinformation regarding campaign finances[107]. In the US, the Political Reform Act[108] establishes obligations for reporting cryptocurrency contributions for political purposes, while the Federal Election Commission[109] forbids anonymous donations and has strict disclosure policies regarding the identity of donors. In Europe, the **Regulation on Markets in crypto-assets**[110] approved by the European Parliament on May 31 2023 lays down a harmonized regulatory framework for the issuance, distribution, and trading of crypto-assets in the European Union.

4.4 Microtargeting, algorithmic filtering, and the uses of Generative Artificial Intelligence for online election interference

Personalization in political advertising and microtargeting relies on the collection and aggregation of data to either rally support for a candidate or suppress political engagement during elections. Anonymity is established through design choices made by platforms during the registration process, along with their data collection policies. Algorithmic curation plays a crucial role in sorting, ranking, and delivering content based on individual user data, aggregate trends among similar users, and reputation systems that assess information quality. This algorithmic approach can lead to disputes regarding how news and information are prioritized and presented to users, raising concerns about whether algorithms promote a diversity of viewpoints or reinforce narrow perspectives, potentially steering users towards extreme or polarizing sources of information.

[105] Omkar Mahajan. (2023). Note-the advent..., *cit*.
[106] Kristian Hernández. How Cryptocurrency is Sneaking into State Elections. 26 October 2018. The Center for Public Integrity. https://archive.publicintegrity.org/politics/state-politics/how-cryptocurrency-is-sneaking-into-state-elections/#:~:text=As%20more%20than%203%20billion%20people%20worldwide
[107] FACT Protocol. (2023). Blockchain technology..., *cit*.
[108] The Political Reform Act is contained in Government Code Sections 81000 through 91014. The regulations of the Fair Political Practices Commission are contained in Sections 18104 through 18998 of Title 2 of the California Code of Regulations.
[109] Federal Election Commission. (2024). How to report Bitcoin contributions. https://www.fec.gov/help-candidates-and-committees/filing-reports/bitcoin-contributions/
[110] European Parliament. (2023). Regulation (EU) 2023/1114. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02023R1114-20240109

The Disinformation and Freedom of Opinion and Expression Report of the Human Rights Council highlights that targeting "is politically motivated against institutions and individuals in vulnerable situations and affects a wide range of human rights, including economic, social, cultural, civil and political rights"[111]. Microtargeting technologies used in political campaigning to segment groups of voters, donors, and supporters undermine the right to free and fair elections, "chilling free speech, reducing the level of trust in the public sphere as a space for democratic deliberation, amplifying anti-democratic narratives, driving polarization and promoting authoritarian and populist agendas"[112]. As the 2023 United Nations Commission on Science and Technology for Development Report suggests, "the technology enabling these practices ranges from relatively simple computer programs, such as bots that operate fake social media accounts, to more advanced technologies like machine learning algorithms capable of generating realistic-looking profile pictures and deepfakes. These technologies can be used to amplify specific narratives, manipulate public opinion, and even spread disinformation. The proliferation of fake accounts and deepfakes complicates the information landscape, making it challenging for users to discern between authentic and manipulated content"[113].

Democratic systems facilitate empowered inclusion in debates and collective decision-making[114]. These core democratic functions can be weakened by the misuse of digital technologies, which can fuel destabilization, information warfare[115], and political subversion, and create "epistemic threats" and "epistemic harms"[116]. Election-related deepfakes have a detrimental effect on democratic processes, reducing "trust in elected representatives and the legitimacy of collective decisions"[117]. AI misused for political manipulation, and the role of social media as the main distribution platform of fake news, is discussed in the 2020 Report "Deep Fakes. On the Threat of Deep Fakes to Democracy and Society"[118]. This report discusses how democratic elections can be disrupted by deep fakes or machine-learning technologies used to augment influence campaigns. Examples of low-quality deepfakes include the 2019 British parliamentary elections, where political manipulation targeted the Liberal Democrats' leader and a Labour politician, and two altered videos of the former US House Speaker Nancy Pelosi, which Facebook refused to remove despite being flagged as manipulated content.

[111] OHCHR. (2021). Disinformation..., *cit*.
[112] OHCHR. (2021). Disinformation..., *cit*.
[113] 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.
[114] Maria Pawelec. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. Digital Society, 1:19. https://doi.org/10.1007/s44206-022-00010-6
[115] Maria Pawelec. (2022). Deepfakes and Democracy..., *cit*.
[116] Don Fallis. (2020). The epistemic threat of deepfakes. Philosophy & Technology, 1–21. https://doi.org/10.1007/s13347-020-00419-2
[117] United Nations Commission on Science and Technology for Development. (2023). Issues Paper..., *cit*.
[118] Hany Farid & Hans-Jakob Schindler. (2020). Deep Fakes: On the Threat of Deep Fakes to Democracy and Society. The Konrad-Adenauer-Stiftung. https://www.kas.de/en/single-title/-/content/on-the-threat-of-deep-fakes-to-democracy-and-society

The technological breakthrough fueled by AI as a “catalyst of democracy” [119] has attracted both positive and negative attention. On the one hand, AI has the potential to enhance democratic and policymaking processes, helping citizens better understand political issues and facilitating their inclusion in democratic discussions. Politicians can connect more closely with the voters, allowing them to represent their constituents more effectively. Conversely, concerns[120] surrounding the use of AI in politics primarily revolve around its potential to generate disinformation and wide-scale deception, disrupting democratic processes through deepfakes, botnets, targeted misinformation campaigns, and synthetic identities and fake accounts. Additional worries include privacy violations from the leakage or inference of personal information, the development of malicious software, and the creation of personalized scams and fraud. Noteworthy highlights from a report on political deepfakes and misleading chatbots used in recent European elections[121] reveal that chatbots often provide inaccurate or fabricated information. Right-wing political parties, such as Alternative for Germany and France’s National Rally, employed AI personas to generate fake online support. High-profile politicians, including German Chancellor Olaf Scholz and UK Prime Minister Keir Starmer, were targeted by deepfakes, some with satirical elements. Additionally, Russian actors have leveraged large language models (LLMs) to promote pro-Russia narratives, attempting to influence public opinion. While the direct impact on election outcomes is uncertain, AI is increasingly seen as a threat to democratic integrity.

A comprehensive overview of the deceptive deployment of Generative Artificial Intelligence (GenAI) for online election interference is provided in prior research[122]. Malicious actors can manipulate digital information and disrupt electoral processes. Deepfake technology enables the generation of realistic political figures used “to spread false information, damage reputations, and even blackmail individuals” while AI-powered botnets are programmed to coordinate and amplify divisive content, “creating the illusion of widespread support or opposition to certain political ideas”[123]. Examples of deepfakes include fake celebrity endorsement, political smear campaigns, and pornographic deepfakes, while AI-powered botnets coordinate disinformation campaigns during elections, amplifying low-credibility and inflammatory content. Pornographic deepfakes are considered hate speech, encouraging discrimination and discouraging societal groups from participating in the public sphere[124].

[119] European Parliamentary Research Service. (2023). Artificial intelligence, democracy and elections. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)751478
[120] OECD. (2023), AI language models: Technological, socio-economic and policy considerations. OECD Digital Economy Papers, No. 352, OECD Publishing. https://doi.org/10.1787/13d38f92-en.
[121] Martin Riedl. (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
[122] Emilio Ferrara. (2024). Charting the Landscape of Nefarious Uses of Generative Artificial Intelligence for Online Election Interference. University of Southern California. https://ssrn.com/abstract=4883403
[123] Emilio Ferrara. (2024). Charting the Landscape…, *cit*.
[124] United Nations Commission on Science and Technology for Development. (2023). Issues Paper…, *cit*.

On the other hand, Large Language Models (LLMs) can be used to generate fake news content and personalized propaganda disseminated on social network platforms, suppressing legitimate political discourse and facilitating targeted misinformation campaigns. Synthetic identities and fake accounts are designed to exploit and weaponize social divisions and infiltrate online communities, altering public perceptions and viewpoints. Evidence shows that election interference operations enabled by AI or bots has occurred in various countries during election periods: UK, USA, Brazil and the Philippines in 2016, France, Spain, Germany in 2017, and Italy in 2018, among others[125]. Digital watermarking and forensic techniques that can help detect the authenticity of digital content represent technological solutions that could mitigate AI-generated misinformation. Related research provides evidence that people's ability to distinguish between real political speeches and political deepfakes is influenced by perception of visual and auditory cues[126]. People rely more on the way something is said than on the actual content of the speech itself when trying to discern authenticity. Combining auditory and visual information leads to more accurate identification of deepfakes compared to relying on text alone. These findings are especially important for designing content moderation systems aimed at flagging misinformation on social media.

[125] United Nations Commission on Science and Technology for Development. (2023). Issues Paper..., *cit*.
[126] Matthew Groh, Aruna Sankaranarayanan, Nikhil Singh, Dong Young Kim, Andrew Lippman & Rosalind Picard. (2024). Human detection..., *cit*.

5. European standards on regulating social media platforms during elections

The European Union is closely examining the challenges posed by large-scale online election-related disinformation, the unlawful micro-targeting of voters, and the risks associated with technology-enhanced political campaigning. Both legislative and non-legislative measures have been implemented across Europe, along with complementary legislative tools to address these issues effectively. Applicable international legal frameworks and policies related to the identified key issues identified in Section IV of the report must be assessed in relation to the right to freedom of expression and the right to freedom of opinion set out in the **Universal Declaration on Human Rights, Article 19 and the International Covenant on Civil and Political Rights (ICCPR) Article 19**[127]. The European Court of Human Rights interprets that "it is necessary to consider the right to freedom of expression under Article 10 in the light of the right to free elections protected by Article 3 of Protocol No. 1 to the Convention [Convention for the Protection of Human Rights and Fundamental Freedoms[128]]" and that "free elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system"[129].

The tradeoff between protecting freedom of speech in the digital sphere and applying human rights to social media platform regulation is addressed in a United Nations Report[130] on the overlaps and differences between hate speech, misinformation, and disinformation from the perspective of international human rights law and international humanitarian law. There is a need to safeguard freedom of expression, a fundamental human right. The three categories of harmful speech, hate speech, misinformation and disinformation, are "considered protected under international human rights law, which upholds freedom of expression. Responses to this protected speech must be carefully designed and implemented to avoid unintended consequences, such as increased censorship. However, ignoring the potential harms of protected speech can, over time, lead to incitement to discrimination, hostility, or violence"[131]. On the other hand, it is essential to counteract these types of harmful speech and address systemic risks that undermine trust in international norms, destabilize political environments, and increase the potential for election-related violence. On the other hand, it is essential to counteract these types of harmful speech and address systemic risks that undermine trust in international norms, destabilize political environments, and increase the potential for election-related violence.

[127] United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[128] European Convention on Human Rights. https://www.echr.coe.int/european-convention-on-human-rights
[129] Bowman v the United Kingdom (1998). EctHR 24839/94. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-58134%22]}
[130] Claire Wardle. (2024). A Conceptual Analysis of the Overlaps and Differences between Hate Speech, Misinformation and Disinformation. Department of Peace Operations Office of the Special Adviser on the Prevention of Genocide, United Nations. https://peacekeeping.un.org/sites/default/files/report_-_a_conceptual_analysis_of_the_overlaps_and_differences_between_hate_speech_misinformation_and_disinformation_june_2024_qrupdate.pdf
[131] Claire Wardle. (2024). A Conceptual Analysis..., *cit*.

The pressing need for comprehensive legal intervention and regulatory oversight of social media platforms has led to various provisions across different jurisdictions, including mandatory user identification on social networking and messaging platforms, limitations on user communications and data storage, content moderation as a responsibility of internet service providers, and platform transparency obligations. Critically important facets in the governance of political campaigning is the protection of users' personal data, revision of rules and regulations on political advertising, and enhanced accountability for internet intermediaries, which enhances quality journalism and voter empowerment[132]. Targeted legislative frameworks undertaken to counteract the dissemination of false information exist in the European Union, as described in the following subsections.

5.1 Tackling large-scale online election-related disinformation

During the past decade, states introduced legal restrictions to counter online disinformation and 'false news', a trend intensified by the Covid-19 pandemic. The International Press Institute documented the battle against "online misinformation" or "fake information" in 17 countries showing that these initiatives have been weaponized against critical journalists, enabling a "chilling effect" on newsrooms[133] and enforcing state censorship of dissenting voices. In the absence of a clear definition of what constitutes fake news or disinformation, "many of these 'false news' laws fail to meet the three-pronged test of legality, necessity, and legitimate aims set out in article 19 (3) of the International Covenant on Civil and Political Rights" which is contrary to UN human rights bodies that "have made it clear that criminalizing disinformation is inconsistent with the right to freedom of expression"[134].

The European Commission has several initiatives to combat disinformation[135]. The "European approach" to addressing online disinformation is outlined in **the Communication from the European Commission on April 26, 2018**[136]. This non-binding framework offers guidance on the principles and objectives necessary for effectively combating online disinformation.

[132] Kristina Rozgonyi. (2020). Disinformation online..., *cit*.
[133] Jamie Wiseman. Rush to pass 'fake news' laws during Covid-19 intensifying global media freedom challenges. 3 October 2020. International Press Institute. https://ipi.media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/
[134] Andrei Richter. International Standards and Comparative National Approaches to Countering Disinformation in the Context of Freedom of the Media. 1 July 2019. Organization for Security and Cooperation in Europe. https://www.osce.org/representative-on-freedom-of-media/424451
[135] European Commission. (2018). Tackling online disinformation. https://digital-strategy.ec.europa.eu/en/policies/online-disinformation
[136] European Commission. (2018). Tackling..., *cit*.

These focus on enhancing transparency regarding the source, production, and dissemination of information to empower citizens against manipulation, promoting a pluralistic information ecosystem through support for quality journalism and media literacy, fostering credibility by improving the trustworthiness and traceability of content, and developing inclusive, long-term solutions that involve collaboration between public authorities, online platforms, advertisers, and media organizations. Online platforms are called to act "swiftly and effectively to protect users from disinformation", while checkers and academic researchers are encouraged to monitor, detect, report, and share knowledge and public awareness about disinformation. Member States and competent national authorities must ensure secure and resilient elections by identifying, mitigating, and managing cyberattacks and disinformation.

Other initiatives to tackle online disinformation include the **Action Plan on Disinformation** focusing on strengthening EU cooperation and capabilities in combating disinformation, the **European Democracy Action Plan** establishing accountability and the responsibilities of online platforms in tackling disinformation, the **2022 Strengthened Code of Practice on Disinformation** and its first version in 2018, and establishing an independent **European Digital Media Observatory (EDMO)**.

In January 2018, the European Commission established a **High-Level Expert Group (HLEG) on Fake News and Online Disinformation** to provide policy recommendations and best practices. On March 12 2018, the HLEG released its report[137] proposing a multi-dimensional approach consisting of five key pillars: enhancing the transparency of online news through data sharing; promoting media and information literacy to help users navigate digital environments; developing tools to empower users and journalists in combating disinformation; protecting the diversity and sustainability of the European news media ecosystem; and promoting ongoing research into disinformation in Europe to inform and adjust policy responses. As part of its short-term measures, the HLEG suggested creating a Code of Practice as a self-regulatory tool involving a structured engagement process with multiple stakeholders, including online platforms, news media organizations, journalists, fact-checkers, independent content creators, and the advertising industry. The EU-wide Code of Practice on Disinformation, proposed by the European Commission, builds on these recommendations.

The 2018 Code of Practice on Disinformation and its strengthened 2022 version[138] represents a self-regulatory framework for tackling online disinformation and protecting the core EU democratic values. It includes 44 commitments and 128 specific measures for Signatories[139] (online platforms, emerging and specialized platforms, players in the advertising industry, fact-checkers, research, and civil society organizations) to cut financial incentives and demonetize the dissemination of disinformation.

[137] European Commission. (2018). A multi-dimensional approach to disinformation. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271
[138] European Commission. (2022). The 2022 Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[139] Full list of signatories available at https://disinfocode.eu/signatories-archive/

It aims to ensure transparent political advertising, scrutinize ad placements, empower users, strengthen cooperation with-fact checking organizations, and empower the research community, setting up a Transparency Center and the creation of a Permanent Taskforce to monitor the correct implementation of the Code. On September 24 2024, major online platforms including Google, Meta, Microsoft, and TikTok, released reports on efforts to combat online disinformation, focusing on the June European elections. These reports, available on the Transparency Centre, highlight cooperation among platforms to protect electoral integrity, including their use of the Code's Rapid Response System. Accompanying these reports are Structural Indicators that offer insights into the prevalence and engagement levels of disinformation during the election period across four EU countries. The platforms also detail actions taken to prevent the creation and spread of disinformation via generative AI.

For the purposes of the illustration, for the 2024 EU Parliamentary elections Google[140] engaged in a range of activities to support democracy and combat disinformation. It launched a prebunking initiative, using short video ads on social media in France, Germany, Italy, Belgium, and Poland to educate the public on disinformation techniques such as decontextualization and scapegoating. The videos were available in multiple EU languages, as well as Arabic, Russian, and Turkish. Google and YouTube also contributed €1.5 million to the European Fact-Checking Standards Network (EFCSN), supporting Elections24Check, a coalition of 40+ fact-checking organizations working across Europe. This initiative created a database of election-related disinformation and provided real-time fact-checking. Additionally, Google Search launched a weekly EU Google Trends Elections Newsletter analyzing search trends related to political topics and candidates. Other initiatives to combat disinformation focused on managing AI-generated content.

Google expanded its Political Content Policies, requiring election advertisers to disclose any use of synthetic content that misrepresents real people or events. YouTube enhanced its misinformation policies by labeling AI-generated or manipulated content, particularly in sensitive election-related materials, to help users clearly identify altered media. To mitigate risks associated with generative AI, Google restricted election-related queries in its AI products, such as Gemini, as part of its broader commitment to responsible AI use. Additionally, the 'About This Image' feature was introduced to give users more context and credibility checks for images found online. Google also advanced digital watermarking through its SynthID tool, which embeds watermarks in AI-generated images, text, audio, and video to ensure transparency. Finally, Google collaborated with the C2PA coalition and pledged, alongside other tech companies, to the Tech Accord, which aims to prevent deceptive AI-generated content from influencing elections.

[140] Google Report. (2024). Transparency Center. https://disinfocode.eu/reports-archive/?years=2024

Through Google Search, Google partnered with the European Parliament to create a “How to Vote” and “How to Register” feature, offering comprehensive voting details from electoral authorities across all 27 EU member states. This included information on ID requirements, registration, deadlines, and various voting methods. On YouTube, election-related content from trusted sources was prominently featured in search results, on the homepage, and in “Up Next” panels, with information panels providing context on candidates and parties. Google ensured transparency in election ads, requiring advertisers to verify their identity and disclose who paid for the ads. In response to the heightened cybersecurity risks during elections, Google enforced the Advanced Protection Program and Project Shield offering cyber protection and defense against Distributed Denial of Service (DDoS) attacks. Google partnered with organizations like IFES, Possible, and Deutschland sicherim Netz (DSIN) to provide account security training and tools, such as Titan Security Keys, to protect against phishing attacks.

Meta’s report[141] for January to June 2024 highlights its initiatives to combat disinformation and ensure election integrity during the European Parliament elections. Key actions included engaging users with Voter Information Units and Election Day Information, which saw 41 million interactions on Facebook and 58 million on Instagram. Meta onboarded 23 national election authorities and 13 Digital Services Coordinators (DSCs) to dedicated reporting channels, responded to reports within 24 hours, and organized 34 training sessions across 21 countries on policies and products ahead of the election with government organizations, political parties, electoral institutions, and civil society organizations. In terms of media literacy, Meta collaborated with EFCSN, training over 200 fact-checkers and supporting media literacy campaigns. Between January and June 2024, over 4.4 million ads were removed, including 170,000 for violating misinformation policies, and 1 million ads were labeled with “paid for by” disclaimers. Meta also dismantled six networks for Coordinated Inauthentic Behavior (CIB) and took action against 1.8 billion fake accounts globally.

Microsoft[142] has undertaken various initiatives to address the risks of deceptive AI in elections, including training sessions on election security and AI, cybersecurity, and information security, dedicated to political groups and election authorities in the European Parliament. It partnered with Oren Etzioni’s non-profit, True Media, to provide resources such as AI classifiers and data to help governments, civil society, and journalists identify manipulated images or videos. Additionally, Microsoft launched the “Microsoft-2024 Elections” platform in February, enabling national and federal election candidates to report deceptive AI content found on Microsoft services, providing a 24/7 response tool for addressing such issues.

[141] Meta Report. (2024). Transparency Center. https://disinfocode.eu/reports-archive/?years=2024
[142] Microsoft Report. (2024). Transparency Center. https://disinfocode.eu/reports-archive/?years=2024

Ahead of the European elections, TikTok introduced several measures, which included setting up a Mission Control Centre to monitor and address potential election-related issues in real-time, and actively participating in the Code's Rapid Response System, which facilitates swift information sharing between civil society organizations, fact-checkers, and digital platforms. TikTok also ensured that fact-checking was available in at least one official language of each EU Member State and launched localized media literacy campaigns to educate users about identifying misinformation and understanding the election process. According to the September 2024 report[143], during the EU elections TikTok did not observe any significant threats. In the four weeks leading up to and during the elections (from May 6 to June 9 2024), the platform removed over 2,600 pieces of content for breaching civic and election integrity policies and an additional 43,000 pieces for misinformation violations. TikTok reported no detection of covert influence operations specifically aimed at the EU elections during this period. Furthermore, TikTok received five notifications through the COPD Rapid Response System, which were promptly addressed, leading to account bans, geo-blocking, and the removal of content for Community Guideline violations.

Twitch[144] did not identify any misinformation, hateful conduct, harassment, or violence-related threats during the EU election period. In the first half of 2024, Twitch only had to enforce misinformation policies twice globally, a significant decrease compared to 10 cases in 2023.

Alongside the Code of Practice on Disinformation, the **Digital Markets Act**[145] (DMA) and the **Digital Services Act**[146] (DSA) are the cornerstone of the EU's digital strategy and introduce measures for very large online platforms (VLOPs) and very large online search engines (VLOSEs) to tackle systemic risks (the dissemination of illegal content; negative impacts on fundamental rights, particularly human dignity; harmful effects on civic discourse, electoral processes, and public security; risks related to gender-based violence; threats to public health and minors; and serious adverse consequences for individuals' physical and mental well-being). They also aim to introduce content moderation obligations to prevent abuse, illegal hate speech, disinformation and other societal risks, bans on targeted advertising to children (Articles 26(3) and 28(2) and (3) of the DSA), stringent rules for micro-targeting of citizens based on profiling using special categories of personal data such as political opinions (Articles 5(2) and 6(2) of the DMA), options for users to opt out of recommender systems (Articles 14, 23(4), Article 27(3) and Recital 70 DSA), and increased data sharing with authorities and researchers (Article 40(4) DSA). Online platforms are required to publish reports on content moderation activities (Articles 15, 24(1), and 42(1)-(3) of the DSA), provide data on average monthly active users (Article 24(2)-(4) DSA), and inform users about specific features of advertisements, including the main factors determining ad targeting and how users can adjust those parameters (Article 26(1) DSA).

[143] TikTok Report. (2024). Transparency Center. https://disinfocode.eu/reports-archive/?years=2024
[144] Twitch Report. (2024). Transparency Center. https://disinfocode.eu/reports-archive/?years=2024
[145] European Parliament. (2022). Regulation (EU) 2022/1925. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925
[146] European Parliament. (2022). Regulation (EU) 2022/2065. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Providers of very large online platforms or search engines that display advertisements must maintain a public repository of published advertisements which should contain details of the primary targeting criteria for one year after the advertisement was last shown. They must ensure that no personal data of service recipients who viewed or might have viewed the advertisement is included (Article 39 DSA). Online disinformation represents a category of risk that can have "negative effects on democratic processes, civic discourse and electoral processes, as well as public security" (Recital 82 of the DSA). Social media providers must comply with EU law and the law of any Member State in tackling the "dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate" (Recital 9 of the DSA) and may have to implement notice and takedown mechanisms (Article 16 DSA on action mechanisms for illegal content). Article 34 of the DSA stipulates that VLOPs and VLOSEs must identify, analyze, and assess systemic risks within the EU related to their service design, operation, and algorithmic systems. They should also evaluate how factors such as algorithm design, content moderation, advertising systems, and data practices influence these risks.

The European Commission Guidelines on the mitigation of systemic risks for electoral processes[147] introduces guidance for providers of VLOPs and VLOSEs, helping these providers mitigate systemic risks associated with electoral processes. When implementing measures to reduce negative impact, VLOPs and VLOSEs must prioritize the protection of fundamental rights, such as human dignity, respect for private and family life, personal data protection, freedom of expression and information, media pluralism, freedom of association, and the right to conduct business. Election-specific risk mitigation measures involve VLOPs and VLOSEs strengthening their internal procedures to identify and mitigate any current or potential risks arising from election-related information accessed, shared, or searched through their platforms. This includes, but is not limited to, information about political parties or candidates, their programs and manifestos, details related to organizing events like demonstrations or rallies, campaigning, fundraising, and other political activities. Other risk mitigation measures include providing access to official electoral information and implementing media literacy initiatives to educate users. Additionally, platforms should offer more contextual information regarding the content and accounts users interact with, enhance their recommender systems, and enforce transparency in political advertising. Political ads must be clearly labeled in a direct and unambiguous manner in real time, enabling users to recognize that the content they are viewing is political advertising. Influencers must also disclose whether their content includes political advertising, providing details such as the identity of the sponsor, the duration of the advertisement's publication, and the total value of benefits received from political advertising services.

[147] European Commission. (2024). Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024XC03014.

Other risk mitigation strategies include the demonetization of disinformation content and ensuring service integrity, where VLOPs and VLOSEs must establish procedures for the timely detection and disruption of any manipulation identified as a systemic risk. Furthermore, these platforms should be subject to third-party scrutiny, research, and data access. Additional measures must address risks associated with generative AI and involve collaboration with national authorities, independent experts, and civil society organizations to enhance overall electoral integrity.

A voluntary **Code of Conduct for the 2024 European Parliament Elections**[148] was jointly developed by the International Institute for Democracy and Electoral Assistance (International IDEA) in collaboration with European political parties and the European Commission. The Code of Conduct was signed on 9 April 2024 and aims to promote integrity, transparency, privacy, safety, fairness, and a level playing field in the elections. Signatories "commit to the principles of truth and accuracy in their communication strategies and to countering mis- and disinformation in elections. The signatories are committed to preventing the deliberate deception of the public, including through the use of artificial intelligence, strengthening the integrity of European elections, and supporting trust in democracy. The pledges help to safeguard European elections against undue interference or manipulation by setting minimum standards for ethical campaigning, increasing public access to relevant campaign information, and improving cybersecurity and digital hygiene measures throughout internal party mechanisms"[149].

On a side note, leading technology companies have committed to combating deceptive AI content in the 2024 elections, as announced at the Munich Security Conference on February 16 2024. The **"Tech Accord to Combat Deceptive Use of AI in 2024 Elections**[150]" includes major firms like Adobe, Amazon, Google, and OpenAI. These companies recognize the risks posed by AI-generated misinformation and will collaborate on tools to detect and address such content, conduct educational campaigns, and enhance transparency. For this accord, Deceptive AI Election Content refers to convincing audio, video, and images generated by AI that misrepresent or alter the appearance, voice, or actions of political candidates, election officials, and other key figures in a democratic election. It also includes misinformation about when, where, and how voters can legally cast their ballots. The Accord outlines eight commitments aimed at developing technology to mitigate risks, assessing AI models, detecting and addressing deceptive content, and fostering public awareness and media literacy.

[148] International Institute for Democracy and Electoral Assistance. (2024). Code of Conduct for the 2024 European Parliament Elections.Code of Conduct for the 2024 European Parliament Elections (idea.int)
[149] International Institute for Democracy and Electoral Assistance (2024). Code of Conduct..., *cit*.
[150] AI Elections Accord. (2024). A Tech Accord to Combat Deceptive Use of AI in 2024 Elections. https://www.aielectionsaccord.com/

5.2 Data-driven politics, micro-targeting of voters and campaign technologies in Europe

The proprietary nature of platform architecture, digital techniques used to manipulate search engine algorithms, and the use of social media as a distribution channel for political microtargeting campaigns based on data processing techniques are all currently under scrutiny. The regulatory vacuum surrounding political advertising, along with the ecosystem of political news and junk information, raises concerns about digital political campaigning and the opaque, unaccountable commercialization of technologies used for psychographic profiling to micro-target specific audiences with disinformation or political propaganda. Data-driven political campaigning allows political parties to democratize political fundraising and mobilize electorates, and mediate political discussions and digital deliberation, while also selectively amplifying and spreading disinformation via digital advertisements. The organizational ecosystem behind political campaigning is both complex and opaque, shaped by a multitude of cross-country regulations. These include provisions on freedom of expression, information, and association, as well as election law, the constitutional status of political parties, campaign and party financing laws, telemarketing rules, advertising codes, and regulations on unsolicited communications.

Amid growing pressure from regulators, the advertisement-driven business model based on systematic collection of data about users' activities online and targeted advertising is considered to potentially violate users' rights to freedom of opinion under article 19 (1) of the International Covenant on Civil and Political Rights, as highlighted in the 2021 UN Report on Disinformation and freedom of opinion and expression: "The lack of transparency with which companies automatically curate content online also points towards an unacceptable level of intrusion into individuals' right to form their ideas free from manipulation and right to privacy. By designing their products with highly personalized content to encourage addictive engagement, companies further promote a system that significantly undermines people's agency and choice in relation to their information diet"[151].

The EC Communication from September 2018, focused on securing free and fair European elections[152], highlights the importance of regulating Member States' cooperation in tackling hybrid threats against electoral infrastructure and campaign information systems. Non-transparent political communication and concealed political advertising targeting citizens covertly undermine legitimate democratic debate, while the unlawful processing and misuse of voters' personal data - collected from their online activities - along with cyberattacks targeting electoral processes, campaigns, political party infrastructure, candidates, or public authorities, can severely compromise the integrity of elections.

[151] OHCHR. (2021). Disinformation..., *cit*.
[152] European Commission. (2018). Communication from the Commission Securing free and fair European elections. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0637

Legislative and non-legislative action was taken in Europe to tackle risks borne of technologically enhanced political campaigning[153]. Political parties adopting data driven campaign technology in the electoral cycle, intermediary services, and content providers must comply with stringent data processing regulations, transparency obligations, and risk management requirements under the **General Data Protection Regulation (GDPR), the e-Privacy Directive (e-PD), the Digital Services Act (DSA), the Regulation on the Transparency and Targeting of Political Advertising (TTPA) and the Artificial Intelligence Act (AIA)**[154]. Content creation, engagement optimization, AI-driven micro-targeting, and sentiment analysis are strictly regulated in Europe, particularly due to the controversy surrounding online political micro-targeting and behavioral advertising. These practices gained heightened scrutiny following the Cambridge Analytica scandal.

The Commission Guidance on the application of GDPR in the electoral context[155] outlines key obligations for all stakeholders involved in the electoral process. It specifically addresses situations where political parties collect data from various sources and use services from data brokers or analytics companies to target voters on social media platforms. Under the General Data Protection Regulation[156] (GDPR), political parties qualify as data controllers and must choose the appropriate legal basis for data processing, which could include consent, legitimate interest, or tasks carried out in the public interest, particularly when dealing with sensitive data like political opinions. When using automated decision-making, strict conditions apply, including obtaining explicit consent. Data access should be clearly defined, and technical and organizational security measures must be implemented, with protocols in place to report data breaches. Additionally, contracts with data processors such as analytics companies should clearly outline obligations, and data must be deleted once it is no longer necessary for its original purpose. Under these provisions, it is unlikely that political campaigners can legitimately use personal information and images of others to create and spread false information aimed at misleading voters without obtaining consent from the affected individuals. Deliberately sharing inaccurate third-party personal data with the intent to mislead voters, particularly when aware of previous data protection violations, could also be considered unlawful[157].

On the other hand, social media companies qualify as data controllers, and they are obliged to ensure the accuracy of information (Article 5(1)(d) GDPR). As a result, social media providers must select the appropriate legal basis for processing data, which could include contracts with individuals, consent, or legitimate interest; for sensitive data, processing is permissible only with explicit consent or if the data is publicly available.

[153] Maja Brkan. (2022). The regulation of data-driven political campaigns in the EU: from data protection to specialized regulation, Yearbook of European Law, 41, 348–373.
[154] European Parliamentary Research Service. (2024). The arrival of e-voting and campaign technologies in Europe: Promise, perils and preparedness. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762321
[155] European Commission. (2018). Commission guidance on the application of Union data protection law in the electoral context. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638
[156] European Parliament. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). http://data.europa.eu/eli/reg/2016/679/2016-05-04
[157] European Parliamentary Research Service. (2024). The arrival of..., *cit*.

Platforms should utilize only the data necessary for the specified purpose and conduct a data protection impact assessment to identify potential risks. They may need to establish notice and takedown mechanisms for illegal content. Under Article 17 of the GDPR, data subjects have the right to request erasure from the platform, which must be carefully balanced against the right to freedom of expression and information (Article 17(3)(a), Article 16 GDPR). The fairness principle in Article 5(1)(a) GDPR likely prohibits the processing of behavioral data aimed at manipulating users, particularly when such data is used in advertising services that are susceptible to misuse for that purpose. Additionally, platforms must adhere to specific conditions for automated decision-making, such as obtaining explicit consent and implementing suitable safeguards. They should ensure the security of data processing through technical and organizational measures and have mechanisms in place to report any data breaches. Lastly, platforms must provide individuals with controls to effectively exercise their rights, including the right not to be subject to decisions based solely on automated processing or profiling.

The ePrivacy Directive[158] is part of the regulatory framework for electronic communication, completes the Union data protection framework, and is relevant in the electoral context as its scope includes rules on the electronic sending of unsolicited communications. Article 13 stipulates that Member States must ensure that unsolicited communications for direct marketing are only allowed with the consent of subscribers or users, or if they have not opted out of receiving such communications, with the specific approach determined by national legislation. This process must be free of charge for users. Additionally, the practice of sending direct marketing emails that disguise the sender's identity, violate Article 6 of Directive 2000/31/EC, lack a valid address for opting out, or encourage visits to websites that violate the directive, is strictly prohibited. The e-Privacy Directive establishes regulations regarding the storage of information and access to already stored data, including cookies that may track a user's online behavior on devices like smartphones or computers (Article 14).

The Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns[159] serve as a practical tool for Member States in regulating the "political influence industry" enabling political microtargeting of narrow segments of voters. Data-driven elections must guarantee democratic pluralism and individual autonomy by applying the data protection principles contained in the Protocol amending the **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)**[160] which stipulates the protection of "every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy", (Article 1, Convention 108+).

[158] European Parliament. (2002). Directive 2002/58/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219
[159] Council of Europe. (2022). Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data by and for Political Campaigns. https://rm.coe.int/guidelines-on-data-proetction-and-election-campaigns-en/1680a5ae72
[160] Council of Europe. (2018). Convention for the Protection of Individuals with Regard to the Processing of Personal Data. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Data protection laws apply to all stakeholders involved in political campaigning during and between election periods ("permanent campaigning"), including political parties and political candidates, data brokers, voter analytical and marketing services, digital platforms, behavioral and micro-targeted advertising companies, social media networks, and messaging applications that process user personal data. The unlawful use of digital technologies in elections can undermine democracy by creating filter bubbles and echo chambers, fostering voter discrimination and chilling political engagement and participation. It also contributes to increased polarization, erodes meaningful democratic debate, and weakens the integrity of elections.

The lawful processing of personal data is also stipulated in the **Recommendation CM/Rec(2021)8 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling**[161]. The general principles emphasize that profiling must respect fundamental rights, including human dignity, privacy, and freedom of expression, and promoting social justice, cultural diversity, and democracy. Profiling should respect the principles of fairness and non-discrimination, with relevant data used and human oversight maintained, especially in automated decision-making systems based on AI technologies. Member States should promote privacy protection from the design stage (privacy by design) and prevent privacy-invasive technologies. Profiling must not lead to discrimination or manipulation, and individuals should have the choice to opt in with clear understanding of the consequences. Profiling must be proportionate to its risks, with strict oversight for high-risk activities, and shared responsibilities should be clearly defined among actors, particularly in cases of data sharing.

The Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[162] provide recommendations for the lawful use of computational technologies in various sector-specific applications.

The European Data Protection Board (EDPB) has adopted various statements regarding the use of personal data collected by social media platforms in the course of political campaigns. Statement 2/2019[163] adopted on 13 March 2019 provides clarification on the processing of personal data for political purposes. Personal data that reveals political opinions falls under special category data under the GDPR (Article 9). As a general rule, the processing of such data is prohibited unless it meets certain narrowly defined conditions. One of the key exceptions is when individuals provide their explicit, specific, fully informed, and freely given consent.

[161] Council of Europe. (2021). Recommendation of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling. https://search.coe.int/cm?i=0900001680a46147
[162] Council of Europe. (2017). The Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. https://rm.coe.int/16806ebe7a.
[163] European Data Protection Board. (2019). Statement 2/2019 on the use of personal data in the course of political campaigns. https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_en

Solely automated decision-making, including profiling, is restricted when it has legal or similarly significant effects on the individual subject to the decision. Profiling linked to targeted campaign messaging may, in certain cases, produce such "similarly significant effects" and is generally only lawful with the valid, explicit consent of the data subject. When targeting voters, adequate information must be provided, explaining why they are receiving a particular message, who is responsible for it, and how they can exercise their rights as data subjects. The European Data Protection Board notes that, under the law of some Member States, there is also a transparency requirement regarding payments for political advertisements.

The EDPS Opinion 1/2022 on the Proposal for Regulation on the transparency and targeting of political advertising[164] stresses the need for stricter rules to combat disinformation, voter manipulation, and electoral interference. Key recommendations include a full ban on microtargeting for political purposes and introducing further restrictions on the personal data categories used in political advertising, including targeting and amplification, and suggests prohibiting targeted ads based on pervasive tracking.

The EDPB Guidelines 8/2020[165] on the targeting of social media users adopted on 13 April 2021 highlight the risks of targeting individuals in political discourse and electoral processes (Paragraph 13). Unlike traditional offline political campaigning, which delivers broadly accessible and verifiable messages, online targeting allows political parties to tailor messages to specific voters based on their needs, interests, and values. This approach can sometimes involve disinformation or distressing content designed to provoke certain emotions or reactions. When polarizing or misleading messages are directed at individuals without sufficient context or exposure to alternative viewpoints, these targeting techniques can undermine the democratic electoral process.

Adopted on 13 March 2024, **the Regulation on the Transparency and Targeting of Political Advertising**[166](TTPA) harmonizes rules and due diligence obligations for online service providers to ensure that political advertising fully respects fundamental rights. Political advertising distributed through online platforms, websites, mobile apps, computer games, and other digital interfaces poses significant regulatory and enforcement challenges, particularly due to the risks of information manipulation and election interference. Political advertising can become a vector for disinformation, especially when it fails to disclose its political nature, originates from sponsors outside the EU, or employs targeting and ad-delivery techniques. Ensuring a high level of transparency is essential to uphold open and fair political debate, support democratic elections or referendums, and prevent manipulation and unlawful interference, including from foreign entities. Transparency allows voters to better understand when they are being shown political ads, who is sponsoring them, and the methods behind their targeting, enabling more informed decision-making.

[164] European Data Protection Board. (2019). EDPS Opinion on the Proposal for Regulation on the transparency and targeting of political advertising. https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-transparency-and_en
[165] European Data Protection Board. (2021). Guidelines 8/2020 on the targeting of social media users. https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf
[166] European Parliament. (2024). Regulation (EU) 2024/900. https://eur-lex.europa.eu/eli/reg/2024/900/oj

Chapter II of the TTPA establishes extensive transparency obligations for providers of political advertising services, including publishers. Advertisements must be clearly labeled (Articles 11 and 19 TTPA) and accompanied by details on the targeting and ad delivery methods used (Article 12 TTPA). Additionally, these advertisements must be submitted to a public repository for online political ads (Article 13 TTPA). Data controllers face further transparency requirements related to targeting and ad delivery (Article 19 TTPA). Moreover, specific data must be made available to interested parties, such as vetted researchers, civil society members, and journalists, upon request (Articles 17 and 20 TTPA). Recital 6 clarifies that targeting methods and ad delivery techniques employed by large online platforms use opaque algorithms to deliver ads to tailored audiences based on personal data and ad content. The potential misuse of personal data through advanced targeting techniques, such as microtargeting, poses risks to the public interest, including fairness, equal opportunities, and transparency in the electoral process, as well as fundamental rights like freedom of expression, privacy, data protection, and non-discrimination. Chapter III, Articles 18, 19, and 20 outline specific responsibilities for controllers (as defined in Article 4, point 7, of Regulation (EU) 2016/679) who collect personal data using targeting or ad delivery techniques in the context of online political advertising. These obligations focus on ensuring transparency and sharing relevant information about targeting and ad delivery with other interested entities. To combat manipulative microtargeting, Recital 75 requires controllers to safeguard individual decision-making by preventing the use of dark patterns, i.e. tactics that intentionally or effectively distort or impair autonomous, informed choices. This includes avoiding pre-ticked boxes, biased techniques, and other non-transparent practices that prompt individuals toward decisions they may not have otherwise made. Common issues in the online advertising industry, such as unclear consent agreements, misleading information, and insufficient time to review terms and conditions, further complicate individuals' ability to access clear information and exercise control over their data. Media literacy should also be promoted to help individuals effectively utilize the transparency provided in political advertising. To tackle disinformation in political advertising, online platforms are encouraged to implement specific policies and engage in broader efforts to reduce the financial incentives for disinformation.

The lawful use of artificial intelligence (AI) systems and the mitigation of risks arising from their potential adverse effects on democracy and the rule of law, particularly when used to influence elections or voter behavior, are regulated under **the Artificial Intelligence Act** (AI Act)[167] adopted on 13 June 2024. Recital 62 of the Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence classifies AI systems designed to interfere with voting rights or undermine democratic processes as high-risk, recognizing their potential to harm democracy and the rule of law.

[167] European Parliament. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

This classification underscores the importance of regulating such AI systems to prevent misuse in electoral contexts. Recital 110 highlights the systemic risks posed by general-purpose AI models, including foreseeable negative impacts on democratic processes, public and economic security, and the spread of illegal, false, or discriminatory content. Additionally, AI models can facilitate disinformation or infringe on privacy, posing threats to democratic values and human rights. Providers of very large online platforms and search engines are required to identify and mitigate systemic risks arising from the dissemination of artificially generated or manipulated content (Recital 120, 136).

AI-generated deepfakes pose significant risks to the integrity of the information ecosystem, amplifying misinformation, manipulation, fraud, impersonation, and consumer deception. To counter these threats, it is mandatory to label AI-generated or manipulated content, clearly disclosing its artificial origin (Recital 134, Article 50(2) AIA). This requirement particularly affects providers of very large online platforms and search engines, who must identify and mitigate systemic risks associated with the spread of such content, including its potential impact on democratic processes, civic discourse, and elections, especially through disinformation (Recital 136). The obligation to label AI-generated content under this Regulation complements, but does not affect, the obligations outlined in Article 16(6) of Regulation (EU) 2022/2065, where hosting service providers must address notices regarding illegal content. Providers of AI systems must publicly share a detailed summary of the data used to train their models (Article 53(1)(d) AIA) and must implement technical solutions that will help identify content generated or manipulated by AI rather than by humans. These techniques include watermarks, metadata identification, cryptographic methods to verify provenance and authenticity, logging methods, and fingerprints. When political chatbots interact with individuals, users must be informed that they are engaging with AI (Article 50(1) AIA). Deployers using AI biometric systems are obligated to inform individuals about the operation of any emotion recognition or biometric categorization systems (Article 50(3) AIA).

5.3 Legislation targeting the misuse of technology for political manipulation

In Europe, the relevant legal framework for tackling the risks associated with deepfake technologies include the AI Act, the GDPR, Copyright law, image rights, the DSA and DMA package, AMVSD, the measures against disinformation, and the EU Parliament resolutions related to deepfakes[168]. Article 50(4) of the AI Act states that deployers of AI systems generating or manipulating image, audio, or video content constituting a deepfake must disclose that the content is artificially created. Similarly, those deploying AI to generate or alter text for public dissemination on matters of public interest must disclose its artificial origin. Recital 134 further emphasizes that AI-generated deepfakes resembling real people, objects, places, or events must be clearly labeled as artificially created or manipulated. The report on Tackling deepfakes in European policy[169] explores the use of personal data by deepfake creators in light of the GDPR. Deepfakes typically involve processing personal data, such as voice fragments, photos, or videos that can identify an individual. Under the GDPR, any handling of such personal data, including the training of deepfake software, is subject to privacy regulations. The GDPR requires a Data Protection Impact Assessment (DPIA) for services that create deepfakes and provides six legal grounds for processing personal data, with only "informed consent" or "legitimate interest" being relevant for deepfakes. If claiming legitimate interest, the creator must ensure it doesn't override the rights of the individual depicted. The GDPR thus governs not only the development of deepfake software but also the creation, use, and distribution of deepfakes. It provides mechanisms for victims to correct or delete unlawful content, offering significant protection against unauthorized deepfake use.

Various European parliamentary documents specifically address concerns about deepfakes and the harmful or negligent use of AI, highlighting the potential risks they pose to democracy and fundamental rights, including the distortion of election outcomes. To mitigate such threats, there are proposals to require labels for producers of deepfake or synthetic video content. For instance, the European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics[170]urges the European Commission to create a framework that penalizes manipulative practices. This would apply when personalized content or news feeds evoke negative emotions or distort perceptions of reality, potentially influencing election results or shaping public opinion on social issues like migration (Paragraph 1.2.(10)).

[168] European Parliamentary Research Service. (2021). Tackling deepfakes in European policy. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039
[169] European Parliamentary Research Service (2021). Tackling deepfakes..., *cit*.
[170] European Parliament. (2019). Resolution 2018/2088. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html

The call for the introduction of strict limits or other protective measures such as thorough investigations into hostile campaigns on the use of deepfakes in the context of elections can be found in the **European Parliament recommendation of 13 March 2019** two years after the EP report on **EU strategic communication to counteract propaganda against it by third parties**[171] (2018/2115(INI)). Paragraph L of the European Parliament recommendation of 13 March 2019 emphasizes the need to safeguard elections from hostile propaganda in the form of misinformation, disinformation, and propaganda campaigns targeting the EU and its neighbors. It highlights the use of various tools to spread disinformation, including tactics such as leveraging multiple low-level websites, private messaging apps, search engine optimization, manipulated media (sound, images, video), AI, online news portals, and TV stations. These methods are often used by opinion leaders and state-controlled or state-funded institutions to disseminate key narratives, particularly those appealing to authoritarian actors, which can be classified as state disinformation. The recommendation also addresses the harmful use of bots, algorithms, AI, trolls, deepfakes, and fake accounts in political campaigns, along with concerns about recent algorithmic developments on large social networks that may amplify false information or hate speech. These actions are seen as undermining the ability of independent democratic societies to make sovereign political decisions (Paragraph ag). Furthermore, Member States are urged to adapt their electoral rules for online campaigning and to monitor the transparency measures related to political advertising introduced by online platforms.

Paragraph 76 of the **European Parliament resolution of 20 January 2021 on artificial intelligence**[172], which addresses the interpretation and application of international law concerning the EU in both civil and military contexts, calls for mandatory labeling of all deepfake content or any other realistically produced synthetic videos as “not original” by their creators. It also advocates for strict limitations on the use of such materials in electoral processes, with strong enforcement measures. This comes in response to growing concerns about the potential misuse of deepfake technology. These technologies could be exploited for blackmail, the production of fake news, or the erosion of public trust, and have the potential to spread disinformation, destabilize countries, and manipulate elections.

The European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture, and the audiovisual sector[173] calls on the European Commission to assess the impact of AI in the creation of deepfakes and to establish appropriate legal frameworks to regulate their creation, production, or distribution for malicious purposes. It also urges the Commission to propose recommendations to counter AI-driven threats to free and fair elections and democracy (Paragraph 91).

[171] European Parliament. (2019). Resolution 2018/2115. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019IP0187
[172] European Parliament. (2021). Resolution 2020/2013. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021IP0009
[173] European Parliament. (2021). Resolution 2022/C 15/04. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0238

As new techniques emerge, the detection of false and manipulated content, like deepfakes, is becoming more challenging. Malicious actors are developing advanced algorithms capable of evading detection, which poses a serious threat to democratic values. The resolution emphasizes the need to raise awareness about the risks of deepfakes, improve digital literacy, and promote the development of better detection technologies. It also calls for greater transparency regarding the content displayed to users on digital platforms, empowering users to have more control over the information they receive. Paragraph 77 further stresses that recommendation algorithms and personalized marketing should be explainable and transparent, allowing audiovisual media consumers to fully understand how these processes work and ensuring that personalized services are not discriminatory. The resolution calls on the Commission to examine how content moderation algorithms are designed to engage users and propose ways to increase user control over the content they see. This includes ensuring users can opt out of recommended and personalized services. Additionally, it underscores the need to inform consumers when they are interacting with automated decision-making processes, and that these processes should not limit users' choices. The use of AI for commercial surveillance must be regulated in line with fundamental rights and the GDPR, even when applied to "free services". Lastly, any regulatory changes should consider the impact on vulnerable consumers.

Across the Atlantic, legislation targeting the misuse of technology for political manipulation and politically motivated audio or visual media exists in California[174] (Assembly Bill No. 730 in 2019), the first law to ban fakes from being used with malice in political campaigns. The Bill temporarily prohibited distributing materially deceptive audio or visual media of political candidates within 60 days of an election, if done with malice and intent to deceive voters or damage reputations. The bill mandates a clear disclosure if media content is manipulated, with exceptions for satire, news broadcasts, and certain publications. Candidates can seek legal relief or damages if harmed by such media. "Materially deceptive audio or visual media" is defined to mean "an image or audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that the image or audio or video recording would falsely appear to a reasonable person to be authentic and would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording". The law was in effect until January 1 2023, when previous rules regarding campaign material manipulation were restored.

[174] California Assembly. (2019). AB 730, Elections: deceptive audio or visual media. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730

Section 5709 of the National Defense Authorization Act for Fiscal Year 2020[175] passed by the US Congress in 2019 mandates the Director of National Intelligence to assess the national security impacts of deepfake technology, focusing on foreign governments' use of machine-manipulated media. Annual reporting obligations include an evaluation of the technical capabilities of China and Russia regarding deepfakes and their use for disinformation, influence operations, or political interference. Additionally, it calls for identifying counter-technologies that the US government or private sector could develop to detect, deter, or attribute deepfake-based attacks. The Director of National Intelligence is required to notify Congress when foreign entities use these tactics to influence US elections or political processes.

[175] US Congress. (2019). National Defense Authorization Act for Fiscal Year 2020. https://www.govinfo.gov/content/pkg/BILLS-116s1790enr/pdf/BILLS-116s1790enr.pdf

5.4 Member States Initiatives. Targeting false information and disinformation during elections

Challenges of defining disinformation in EU legislation are addressed by researchers[176], who distinguish between harmful content (disinformation) versus illegal content (such as hate speech, incitement to violence, or child sexual abuse material) and their prohibition under **Member States' criminal codes**. Countries that have national laws criminalizing disinformation, false news, and false information include: Lithuania (Article 19 of the Law on the Provision of Information to the Public), Malta (Article 82 of the Criminal Code), France (Article 27 of the Law on Freedom of the Press), Austria, Croatia (Article 16 of the Law on Misdemeanours against Public Order and Peace), Cyprus (Criminal Code, Article 50), the Czech Republic (Criminal Code, Section 357), Greece (Article 191 of the Criminal Code), Hungary, Romania, and Slovakia (Section 361 of the Criminal Code).

Aiming at protecting the integrity of the democratic processes, on 22 December 2018 the French government adopted two laws[177] to combat the manipulation of information, containing provisions for enforcing emergency procedures to stop the dissemination of "inaccurate or misleading allegations or statements" during election campaigns, "disseminated on a massive scale in a deliberate, artificial or automated manner via an online public communication service"[178]. Large-scale online platform operators must provide users with information on how to flag fake information and adhere to annual reporting obligations to the national media authority Arcom, disclosing the measures related to algorithmic transparency, sponsored content of public interest news, advertising, media and information literacy, and measures undertaken to combat the dissemination of fake information. The national audiovisual media regulatory authority is entrusted with the power to suspend the distribution of television services controlled by a foreign state that "harm the fundamental interests of the nation, including the smooth functioning of its institutions - particularly by disseminating false information" during the three months preceding a national election. Provisions of the **1881 Law on Freedom of the Press**[179] and Article L.97 of the **Electoral Code** [180] also prohibit the spread of fake news that could affect elections.

[176] Ronan Ó Fathaigh, Natali Helberger & Naomi Appelman. (2021). The perils of legally defining disinformation. Internet Policy Review, 10(4). https://doi.org/10.14763/2021.4.1584
[177] 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;jsessionid=3EA914DFE69980E3FBB01324A666B5D1.tplgfr22s_1?cidTexte=JORFTEXT000037847556&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037847553
[178] Amélie Blocman. IRIS Legal Observations of the European Audiovisual Observatory. 2019. IRIS Merlin.
https://merlin.obs.coe.int/article/8446
[179] French Executive Committee. (1881). Loi du 29 juillet 1881 sur la liberté de la presse
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006070722&dateTexte=vig.
[180] French Executive Committee. (2002). Code electoral. https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070239&idArticle=LEGIARTI000006353232

In Germany, the **Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, NetzDG**[181]) came into effect in January 2018 and introduced obligations for profit-making telemedia services providers, "internet platforms which are designed to enable users to share any content with other users or to make such content available to the public (social networks)", to take measures blocking, filtering and taking down illegal content, and removing the "violating content" within a short period of time, or face heavy fines[182]. The law was designed to combat hate speech, radicalization, and fake news online. Social media companies must handle complaints about unlawful content related to eighteen provisions of the German criminal code[183]. They also have biannual reporting obligations and must comply with removal requirements of "fake news" on social media networks within twenty-four hours. The law was controversial and concerns about freedom of expression and online intermediaries' responsibility in regulating content were raised by the UN Special Rapporteur David Kaye: "I am concerned with the lack of judicial oversight with respect to the responsibility placed upon private social networks to remove and delete content. Any legislation restricting the right to freedom of expression and the right to privacy must be applied by a body which is independent of any political, commercial, or unwarranted influences in a manner that is neither arbitrary nor discriminatory. The liability placed upon private companies to remove third party content absent a judicial oversight is not compatible with international human rights law"[184].

In the United Kingdom, the **Online Safety Act**[185] (the OSA) was first introduced in 2017 and received Royal Assent on 26 October 2023. The Act introduces an extensive regulatory framework to counter digital harms and obliges "user-to-user service" providers (large tech companies and online platforms) to take measures to protect children and users of online service providers, preventing the proliferation of illegal and harmful content, regulating consensual and non-consensual pornographic content, and countering fraudulent advertising. Providers of regulated user-to-user and search services are subject to duties regarding Illegal content risk assessment, content reporting, complaints procedures, freedom of expression and privacy, and record-keeping and review. The Office of Communications (Ofcom) has regulatory powers to enforce sanctions.

In Austria, the Criminal Code makes it an offense to disseminate 'false news' during an election if it is likely to influence voters. Article 264[186] provides that anyone who publicly spreads false information that could prevent voters or those eligible from casting their vote, or influence their voting behavior in a certain way, at a time when a counterstatement can no longer be effectively disseminated, may face imprisonment of up to six months or a fine of up to 360 daily rates. Furthermore, if a person uses a false or forged document to make the false information appear credible, the penalty increases to imprisonment of up to three years.

[181] Bundesgesetzblatt. (2017). Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken.
[182] Office of the United Nations High Commissioner for Human Rights. (2017). Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.
https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-DEU-1-2017.pdf
[183] Strafgesetzbuch. (1998). Criminal Code. http://perma.cc/X8TS-UCBK.
[184] Office of the United Nations High Commissioner for Human Rights. (2017). Mandate of the..., *cit*.
[185] Online Safety Act UK. (2023). https://www.legislation.gov.uk/ukpga/2023/50/enacted
[186] Criminal Code, Austria. https://www.jusline.at/gesetz/stgb/paragraf/264

6. Conclusions

The electoral process is undergoing a structural transformation due to the emergence of digital technologies and social media platforms as tools connecting political parties and individual voters. Technology influences how citizens access and consume information, which begs the question of how to enhance users' protection against information disorder. The privatization of the online public sphere, and how private platforms increasingly shape democratic functions by controlling the flow of information and political communication, pose challenges and opportunities for the exercise of free elections[187]. With globalization and technological innovation, these platforms assume roles traditionally held by state authorities, creating policies that influence freedom of speech and participation. Researchers' concerns[188] over platforms' gatekeeping of political content and their decision-making systems, through algorithms or human moderation (often described as opaque and unpredictable "black boxes"), could potentially lead to disputes over electoral legitimacy.

As the report shows, social media platforms play a dual role in elections. They can enhance democracy by facilitating information exchange, public debate, and citizens' engagement, while also posing risks by spreading misinformation, deepening polarization, and undermining trust in the electoral process. Over the past decade, legislative and non-legislative measures have been implemented in the European Union to mitigate the challenges posed by large-scale online election-related disinformation and the risks associated with technologically enhanced political campaigning. This study provides an analysis of the patchwork of European laws, regulations and guidelines governing social media platforms in the electoral context. The overarching themes in regulating social media involve the challenge of balancing various regulatory objectives with the concerns surrounding freedom of speech and access to information.

[187] Samantha Bradshaw. (2019). Disinformation optimised..., *cit*.
[188] Samantha Bradshaw. (2019). Disinformation optimised..., *cit*.

The analysis has showcased that the regulatory landscape for social media platforms consists of a complex mix of constitutional norms, along with a range of binding and non-binding regulations at both the EU and Member State levels. At the European level, the key policy directions and regulatory frameworks include the Artificial Intelligence regulatory framework, the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act, the Audiovisual Media Directive, the e-Privacy Directive, the Regulation on the Transparency and Targeting of Political Advertising, the Copyright law, the Code of Practice on Disinformation, the Action Plan on Disinformation, and the Democracy Action Plan. Various European parliamentary documents, resolutions, guidelines, and communications specifically address concerns about the effects of social media platforms, highlighting the potential risks they pose to democracy and fundamental rights, including the distortion of election outcomes. In line with prior research, the report shows that various countries have taken different approaches to tackle online disinformation, which are significantly shaped by each nation's unique political, economic, and sociocultural characteristics[189]. It also highlights that applicable international legal frameworks must be assessed in relation to the right to freedom of expression.

[189] Marius Dragomir, José Rúas-Araújo & Minna Horowitz. (2024). Beyond online disinformation: assessing national information resilience in four European countries. Humanit Soc Sci Commun 11, 101. https://doi.org/10.1057/s41599-024-02605-5.

7. Recommendations for reform in Lebanon

- Leveraging the European Union's frameworks and expertise in the oversight and regulation of technology platforms during election cycles, Lebanese lawmakers and policymakers should adhere to international standards and consider introducing both legislative and non-legislative measures for the regulation of digital platforms to tackle the challenges and risks associated with the use of social media platforms in electoral scrutiny. Legislative efforts, policies, strategies, and regulatory responses must counter digital information disorder, enabling affordable, accessible, trusted, and secure digital ecosystems, without infringing upon freedom of opinion and expression. Lebanon could adopt similar obligations for technology platforms based on applicable international legal frameworks and policies that must be assessed in relation to the right to freedom of expression and the right to freedom of opinion set out in the Universal Declaration on Human Rights Article 19 and the International Covenant on Civil and Political Rights (ICCPR) Article 19.

- Modernized legislation should address and establish clear rules for issues such as digital campaigning, electoral advertisements, political advertising, microtargeting, algorithmic filtering, data privacy, content moderation, recommender systems, gendered disinformation, political ad spending by candidates, parties, and third-party entities, and AI-manipulated media and deepfake campaigns. These topics are policy priorities in the European Union, and Lebanon could adopt similar obligations for technology platforms, drawing on examples from the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), the Audiovisual Media Services Directive (AVMSD), the e-Privacy Directive (e-PD), the Regulation on the Transparency and Targeting of Political Advertising (TTPA), and the Artificial Intelligence Act (AIA).

- Data privacy legislation should be advanced based on consultations with relevant stakeholders and interested parties, drawing on the example of the General Data Protection Regulation (GDPR).

- Legislation should strictly define disinformation and misinformation, as well as prohibited or illegal content, such as hate speech and incitement to hatred and violence. Penalties should be imposed for creating or spreading disinformation, particularly during election campaigns, to ensure transparency and accountability and protect democratic integrity.

- To combat information disorder in electoral contexts, Lebanese lawmakers and policymakers should build oversight mechanisms for detecting and mitigating domestic and foreign electoral interference that could impact public trust in electoral scrutiny. Systematic monitoring, independent audits, and human rights impact assessments of technology platforms should be required by policymakers, based on international standards and the available indicators promoted by European Union frameworks. Lebanon could adopt systemic risk assessments through regulations, drawing on the example of the Digital Services Act (DSA). While preventing online abuse and safeguarding freedom of expression, regulatory structures should monitor, enforce accountability, and apply sanctions for violations.

- Independent research and access to platform data should be supported by Lebanese lawmakers and policymakers, drawing on the example of Article 40 of the Digital Services Act (DSA) which stipulates that technology platforms must provide access to their data for the purpose of conducting research that contributes to the detection, identification, and understanding of systemic risks.

- To reduce the dissemination of electoral falsehoods and the creation of disinformation campaigns at scale, social media monitoring should be enforced through revised platform self-regulation policies and codes of conduct, drawing on the example of the European Commission's multi-dimensional approach to disinformation.

- Lebanese lawmakers and policymakers should enforce mechanisms for election cybersecurity, encouraging innovation in deepfake detection and voting disinformation campaigns, drawing on the example of the Artificial Intelligence Act (AIA). Establishing an AI Safety Institute or a Digital Infrastructure Authority, with support from the European Commission, could help create a supportive policy environment. This would strengthen the ability to monitor AI, manage systemic risks from AI-manipulated media, and address the threats posed by deepfake campaigns.

- Government officials, legislators, and election management bodies should actively promote media and information literacy programs, enforcing public service announcements that may improve social media users' discernment, along with capacity-building initiatives focused on digital campaigning, data privacy, online disinformation, and generative AI. By advocating for education on electoral integrity and democracy, they can help close the digital skills gap faced by key stakeholders.

- Financial support for independent fact-checking initiatives to counteract misinformation and disinformationin community and local media outlets should be provided to strengthen the role of the media, validating the credibility of journalists as professional gatekeepers.

- Government officials, political parties, election management bodies, and other interested stakeholders could develop a Social Media Code of Conduct for Elections, drawing on the example of the voluntary Code of Conduct for the 2024 European Parliament Elections developed by the International Institute for Democracy and Electoral Assistance (International IDEA) in collaboration with European political parties and the European Commission. The Social Media Code of Conduct for Elections could establish grounds for fair elections, setting standards for ethical political campaigning.

- Lebanese lawmakers and policymakers should promote international, cross-sectorial (National Media Regulatory Authority, Advertising Authority, Data Protection Authority, Competition Authority) and multi-stakeholder cooperation to tackle the social media challenge for election integrity, coordinating platform governance in an electoral context.

Media and Journalism Research Center

Legal address
Tartu mnt 67/1-13b, 10115,
Tallinn, Harju Maakond, Estonia

Postal address
6 South Molton St, London,
W1K 5QF, United Kingdom

Academic affiliation
Universidade de Santiago de Compostela (USC)
Colexio de San Xerome, Praza do Obradoiro s/n,
CP 15782 de Santiago de Compostela.

Contact
www.journalismresearch.org
mjrc@journalismresearch.org

Cover photo: Canva Pro

Artificial Intelligence (AI) Disclosure Statement
No AI tools were used in the creation of this report, which was written entirely by MJRC experts and editors.

MJRC
MEDIA&JOURNALISM RESEARCH CENTER

Maharat

Funded by the European Union
بتمويل من الاتحاد الأوروبي