The use of AI in electoral campaigns: key issues and remedies*

Giuseppe Muto

Abstract

The expanding influence of artificial intelligence in electoral campaigns presents substantial challenges, particularly as it becomes a tool for generating and propagating disinformation, thereby undermining democratic principles. The following observations relate to the legal frameworks of the United States and the European Union that address such concerns. Within the United States, the utilization of artificial intelligence for the manipulation of public opinion has given rise to reinterpretations of the First Amendment, whereas the European Union has introduced legislative reforms. Alongside these normative developments, the paper also considers the initiatives undertaken by major private sector entities, such as Google and Meta, to prevent the misuse of AI technologies in political advertising and the dissemination of false information. It argues for a comprehensive approach – encompassing legislative measures, regulatory oversight, and private sector cooperation – to protect electoral integrity and uphold democratic values in the digital era.

Il crescente sfruttamento dell'intelligenza artificiale nelle campagne elettorali pone sfide significative, soprattutto per la sua capacità di creare e diffondere disinformazione. Ciò mette a rischio i principi democratici. Queste brevi note descrivono gli atti normativi adottati dagli Stati Uniti e dall'Unione Europea per affrontare tali problematiche. Negli Stati Uniti, la manipolazione dell'opinione pubblica mediante l'uso dell'IA sta conducendo a nuove interpretazioni del Primo emendamento, mentre nell'Unione Europea sono state introdotte norme specifiche per contrastare il fenomeno. L'analisi considera, inoltre, le iniziative intraprese dai grandi attori del settore privato, come Google e Meta, volte ad arginare l'uso improprio delle tecnologie di IA nella pubblicità politica e nella diffusione delle notizie. Emerge la necessità di un approccio articolato che integri misure legislative, regolatorie e la cooperazione del settore privato, al fine di salvaguardare l'integrità elettorale e i valori democratici nell'era digitale.

* This text incorporates, with necessary modifications, the discussions held during a panel orga-nized within the ICON•S Annual Conference, which took place in Madrid from 8 to 10 July 2024.

Summary

Keywords

elections – AI – democracy – disinformation – European Union

1. Introduction

2024 was the year of elections.[1] In that year, countries home to nearly half of the world's population held elections, marking a first in history. These include seven of the world's ten most populous nations: Bangladesh, India, the United States, Indonesia, Pakistan, Russia, Mexico and the European Union. Within concerns about the decline of democracies worldwide, these elections represented a crucial year for democracy itself. Despite threats to democracy, such as increased ethnic violence and attempts to weaken judicial checks on executive power, the popularity of democracy remains high. In this unstable context, generative AI represented a novel challenge in this historic election year.

It has become clear that artificial intelligence have played an increasing role in the production of disinformation and manipulation of information, an issue that had been relevant in that pivotal year for democracy.[2] Evidence from Newsguard, a database that collects and catalogues false information on the web, demonstrates a concerning trend: in the period between 1 January 2021 and 30 May 2024, Newsguard had identified that 5.48% of false information was produced by means of AI. This percentage is particularly concerning given the sharp rise over a relatively short period: in 2021, only 0.78% of false information was attributed to AI, and this figure had risen to 8.5% by 2024.[3]

[1] S. Shamim – A. Lodhi, *The year of elections – Is 2024 democracy's biggest test ever?*, in *aljazeera.com*, 4 January 2024.

[2] C. Vaccari – A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, in *Social Media + Society*, 6, 1, 2020.

[3] More information is available here at *newsguardtech.com*. On this topic, see O. Pollicino, *Disinformazione e intelligenza artificiale: un cocktail esplosivo?*, in *Rivista della Corte dei Conti*, *forthcoming*.

2. AI, disinformation and the world outside the window

The proliferation of disinformation necessitated heightened attention, particularly in the context of crucial democratic functions. This is not merely an abstract concern, but a matter of demonstrable harm. Disinformation campaigns can be used to manipulate public opinion, undermine trust in legitimate institutions, and sow discord among citizens. These effects can have a direct and detrimental impact on elections, referendums, and other democratic processes.[4] A pertinent example is provided by the recent annulment of the presidential elections in Romania. In light of allegations of foreign interference, particularly from Russia, involving both disinformation and misinformation, the Romanian Constitutional Court's decision to invalidate the first round of elections has ignited considerable debate regarding the ramifications for democratic governance.[5] Critics argue that this ruling not only undermines the voices of millions of voters but also raises critical questions about the role of the judiciary in electoral processes.[6] This issue of constitutional relevance highlights the delicate balance that must be maintained to protect democratic principles while ensuring the integrity of elections, emphasizing the need for transparent mechanisms that safeguard both electoral outcomes and fundamental freedoms.

Therefore, the interplay between disinformation and democratic processes takes on heightened significance within the current geopolitical climate, characterized by ongoing international conflicts, particularly in Russia and the Middle East. In such an environment, disinformation can be weaponized to exacerbate existing tensions, destabilize fragile governments, and even serve as a precursor to armed conflict.[7] For example, malicious actors may use disinformation to create a false narrative justifying military intervention, or disrupt diplomatic efforts.[8]

Artificial intelligence has emerged as a potent weapon in the arsenals of modern warfare, surpassing its role in simply enhancing the precision of traditional weaponry. Often operating with minimal human oversight, AI-powered autonomous weapon systems (AWS) raise a multitude of legal and ethical concerns regarding proportionality, accountability, and the blurring of lines between combatants and civilians.[9] Furthermore, AI serves as a formidable tool for both domestic and international propaganda campaigns. State actors demonstrably utilize deepfakes, face swaps, lip-syncing, text-to-speech, and voice conversion to fabricate narratives that diverge significantly

[4] M. Kelly – E. Samuels, *How Russia weaponized social media, got caught and escaped consequences*, in *washingtonpost.com*, 18 November 2019.

[5] A. L. Solea, *Why Romania's election was annulled – and what happens next?*, in *The Conversation*, 16 December 2024

[6] A. Carrozzini, *Shooting Democracy in the Foot?*, in *Verfassungsblog*, 13 December 2024.

[7] See A.R. Di Maggio, *Fake News as Propaganda: The Bush and Obama Years*, in *Fake News in America: Contested Meanings in the Post-Truth Era*, Cambridge, 2023.

[8] J. Buchheim – G. Abiri, *The War in Ukraine, Fake News, and the Digital Epistemic Divide*, in *verfassungsblog.de*, 12 May 2022.

[9] It is not a case that Pope Francis during the session of G7 in Apulia concerning AI claimed that «no machine should choose to take the life of a human being», as reported by S. Cernuzio, *G7, il Papa: nessuna macchina dovrebbe scegliere se togliere la vita a un essere umano*, in *vaticannews.va*, 14 June 2024.

from reality.[10] A prime illustration of this is the now-debunked video, released in February 2022, purporting to show Ukrainian President Volodymyr Zelensky urging his citizens to give up.[11]

The nexus between AI-fueled disinformation, foreign propaganda, and the manipulation of democratic processes has been demonstrably established, even in relatively peaceful periods. For instance, in 2022, a group of British Members of Parliament lodged a complaint with the European Court of Human Rights against the Russian Federation.[12] Their claim centered on alleged violations of art. 3 of the First Additional Protocol to the European Convention on Human Rights (the right to free elections)[13], since they argued that Russia employed a sophisticated AI-powered disinformation campaign to influence the outcomes of the 2014 Scottish independence referendum, the 2016 Brexit referendum, and the 2019 UK general election. These campaigns reportedly involved the use of deepfakes, social media bots, and targeted online advertising to spread misinformation, sow discord, and erode public trust in democratic institutions.[14] Similarly, in the United States, many reports detailed extensive evidence of Russian interference in the 2016 presidential election, with suspected use of AI-powered tactics to manipulate social media algorithms and target swing voters with misleading content.[15] In these particular instances, AI has been utilised as a social bot or as a potent instrument for the organisation of online content. Social bots, which are essentially counterfeit accounts managed either automatically or semi-automatically, have the objective of disseminating material of a "polluting" nature. Moreover, AI assumes a significant role in the content recommendation systems that are present on the feeds of various platforms, playing a fundamental role in the propagation of information and the shaping of public consciousness. They have the capacity to influence and structure user preferences, guiding decisions at both the individual and collective levels, with a particular emphasis on political choices. This underscores the profound impact that AI has on our digital society.

Hence, considering the significantly deteriorated geopolitical framework compared to the past when such interference occurred, it appears necessary and fitting to adopt

[10] For an deepen analysis of the different type of deepfakes, consider O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *federalismi.it*, 12, 2024.

[11] M. Holroyd, *Deepfake Zelensky surrender video is the 'first intentionally used' in Ukraine war*, in *euronews.com*, 16 March 2022.

[12] ECtHR, *Bradshaw et al v. Regno Unito*, app. 15653/22 (2022).

[13] Art. 3 of the First Additional Protocol to the European Convention on Human Rights, according to which «Right to free elections. The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature».

[14] J. Grierson, *MPs take Russian election interference case to human rights court*, in *theguardian.com*, 29 March 2022.

[15] Among the others, M. Rodriguez, *Disinformation Operations Aimed at (Democratic) Elections in the Context of Public International Law: The Conduct of the Internet Research Agency During the 2016 US Presidential Election*, in *International Journal of Legal Information*, 47, 3, 2019. On the same point, see also *(U)Report of the Select Committee on Intelligence United States Senate on Russian Active Measure Campaigns and Interference in the 2016 U.S. Election*, available at intelligence.senate.gov; S. Lynch, *U.S. Justice Dept. asks watchdog to check for political motivations in FBI Russia probe*, in *reuters.com*, 21 May 2018.

suitable measures to ensure the free and fair conduct of electoral competitions in this 'super' election year. The most crucial challenge confronting legislators on both sides of the Atlantic is to discern the thin line that separates a justified and reasonable restriction on freedom of expression from detestable censorship. This task, while delicate, is of utmost importance in preserving the integrity of our democratic processes.[16] Indeed, the ongoing war in Ukraine, appropriately labeled the «first social media war»[17], has presented a unique challenge in balancing freedom of expression with the need to counter foreign disinformation. This tension appears to have been recognized by the Tribunal of the European Union.[18] In a landmark case, the Tribunal upheld the legitimacy of sanctions imposed on a French television channel that broadcasted Russian propaganda messages. The Tribunal justification rested on the principle of proportionality – the restriction on the channel's freedom of expression was deemed necessary to counteract a significant threat posed by foreign disinformation. This decision finds its constitutional foundation in the principles expressed in the Charter of Fundamental Rights of the Union, that provide a legal framework for navigating the complex interplay between free speech and the need to combat information manipulation in the digital age.[19]

3. The USA

3.1. A new reading of the First Amendment

In response to the increasing power and influence of AI tools, both the United States and the European Union implemented a range of measures to prevent the exploitation of these technologies in the context of the 2024 elections.
The non-regulation approach, which generally characterises the US's style to digital regulation, has, allegedly, led to unauthorised influences on the 2017 election results. This has highlighted the need for «a narrow law prohibiting the use of AI to deceptively undermine our elections through fake speech».[20] While the First Amendment[21] safeguards the «free marketplace of ideas»,[22] it cannot be construed as providing con-

[16] On this topic, see O. Pollicino, *General Report: Freedom of Speech and the Regulation of Fake News*, in O. Pollicino (edited by), *Freedom of Speech and the Regulation of Fake News*, Cambridge, 2023; G. Pitruzzella, O. Pollicino, *Disinformation and Hate Speech: A European Constitutional Perspective*, Milan, 2020.

[17] P. Suciu, *Is Russia's Invasion Of Ukraine The Firs Social Media War?*, in *Forbes*, 1 March 2022.

[18] GC, T-125/22, *RT France v. Council* (2022).

[19] P. Dunn, *Il contrasto europeo alla disinformazione nel contesto della guerra in Ucraina: riflessioni a margine del caso* RT France, in *Rivista di diritto dei media*, 1, 2023.

[20] Congress of the United States of America - Senate Rules and Administration, S.Hrg. 118-130 – AI and the Future of our Elections, 27 September 2023.

[21] Constitution of the United States of America, First Amendment: «Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances».

[22] This definition was elaborated in a 1997 judgement of the American Supreme Court (*Reno v. Aclu*, 521 US 844 (1997)), recalling a famous expression formulated in the very important dissenting opinion

stitutional protection for those who intentionally defraud voters.

3.2. Who has the legitimacy for the protection of free elections?

It may be argued that the Federal Election Commission (FEC) possesses the legislative legitimacy to enact a regulation that restricts the use of certain AI tools during elections. This regulation, to be enforceable, would need to survive judicial review under the strict scrutiny test[23] established by the Supreme Court. This test is the most demanding standard applied by courts to evaluate restrictions on First Amendment rights. To pass this test, the FEC would need to demonstrate that the regulation is narrowly tailored to achieve a compelling governmental interest. In this case, the compelling interest would be safeguarding the integrity of the electoral process from being undermined by AI-powered tools capable of generating entirely fabricated realities and convincing voters. In this context, the forthcoming judgments of the Supreme Court in the TikTok case may offer crucial insights into the limitations of governmental authority to restrict access to digital platforms under the First Amendment.[24]
Therefore, the FEC, as the federal agency tasked with overseeing campaign finance and election administration, seems to be well-positioned to craft regulations that address this specific threat. However, this approach also faces challenges.[25] Indeed, in a recent statement,[26] the FEC clarified that while it lacks the authority to create new regulations specifically targeting AI,[27] the current provisions of the Federal Election Campaign Act (FECA) are applicable to deceptive AI-generated communications. This acknowledgment came after a petition from Public Citizen, which sought clarification on how these laws pertain to AI-generated ads. The FEC's interpretation indicates that any AI-generated content that constitutes fraudulent misrepresentation, as defined under FECA, is already prohibited by existing regulations. However, the agency emphasized that not all AI-generated content is inherently misleading, and it cannot regulate de-

of Justice Holmes in 1919 (*Abrams v. United States*, 250 US 616 (1919).

23 Among the others, R.H. Fallon, *Strict Judicial Scrutiny*, in *UCLA Law Review*, 54, 1267, 2007.

24 The recent ruling by the Court of Appeals for the D.C. Circuit in the TikTok case (*TikTok Inc. v. Garland*, No. 24-1113 (D.C. Cir. 2024)) marks a pivotal moment in the ongoing debate over the regulation of digital platforms and the application of strict scrutiny regarding freedom of expression. The court upheld the constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act, which imposes a ban on TikTok in the United States, asserting that the law does not violate the First Amendment or the equal protection rights guaranteed by the Fifth Amendment. This case is now subject to expedited appeal before the Supreme Court, where it will be determined whether the scope of strict scrutiny may be significantly reduced. Such an outcome could have profound implications for online free speech and the government's authority to restrict access to foreign platforms.

25 D. Young – J. Gardner – M. Block, *FEC Interpretive Rule on AI in Political Ads*, in *Policy Backgrounders*, 25 September 2024.

26 Federal Election Commission, *Concurring Statement of Chairman Sean J. Cooksey on Notification of Disposition of Reg 2023-02: Artificial Intelligence in Campaign Ads*, 19 September 2024, available at *fec.gov*.

27 C. Mcisaac, *FEC Makes the Right Call on AI Regulation in Federal Elections*, in *R Street Institute*, 16 September 2024.

ceptive practices beyond the narrow confines of the law as it currently stands.

4. The European Union

On the other side of the Atlantic, in Europe, there has been a growing recognition of the need to address the shortcomings of the 2018 Code of Practice on Disinformation. This Code was found to be disappointing due to its over-reliance on self-regulation, a trait it shares with the regulatory approach in the United States. This excessive dependence on self-regulation has been identified as a weakness, as it often fails to adequately address the complex and evolving challenges posed by disinformation.
Consequently, the EU has implemented a diverse set of tools specifically designed to counteract the malicious use of artificial intelligence during elections. These measures aim to provide a more comprehensive and proactive response to disinformation, surpassing the constraints inherent to self-regulation.

4.1. The Action Plan for European Democracy

By the year 2020, the European Commission had developed a keen understanding of the amplified effectiveness of online propaganda tools. This understanding was explicitly articulated in the Communication on the Action Plan for European Democracy.[28] The document underscored how online campaign tools have gained increased force by harnessing a combination of elements[29]:

- Personal data: The capacity to collect and utilise extensive quantities of personal data facilitates a profound comprehension of individual users. This data can include demographic information, online behaviour, preferences, and more, painting a detailed picture of each user.[30]
- Artificial intelligence: AI algorithms can scrutinise this data and discern patterns, thereby enabling the generation of highly targeted and personalised message. These algorithms can predict user behaviour and preferences with remarkable accuracy, making the messages more relevant and engaging.
- Psychological profiling: By gaining an understanding of user behaviour and preferences, AI can create messages that resonate with individual psychology. This could potentially exploit emotional vulnerabilities, making the propaganda more effective.[31]
- Complex micro-targeting techniques: These systems permit the precise delivery of customised messages to specific user segments, maximising the impact of the

[28] Communication COM/2020/790 final from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan.

[29] Communication COM/2020/790 final, cit., 3.

[30] Communication COM/2020/790 final, cit., 21.

[31] Communication COM/2020/790 final, cit., 2.

propaganda. By ensuring that the right message reaches the right user at the right time, these techniques can significantly enhance the effectiveness of online propaganda campaigns.

4.2. The 2022 Strengthened Code on Disinformation and the DSA

The Strengthened Code on Disinformation of 2022 recognizes the potential for recommender systems to distort users' access to information. While it acknowledges that users can theoretically adjust settings to influence the content they see, the Code highlights the limitations of this approach. Recommender systems can be highly sophisticated, and users may not fully understand the algorithms that shape their online experience. This creates a situation where users might believe they have control over their information diet, while recommender systems can still subtly manipulate what they see.[32]

In terms of systemic risk assessment and mitigation obligations, arts. 34 and 35 of the Digital Services Act[33] mark a significant shift from self-regulation to co-regulation. These articles mandate that providers of very large online platforms (VLOPs) and search engines actively identify and address systemic risks within their services. This includes any algorithmic systems that may contribute to the spread of disinformation. Indeed, artt. 34 and 35 specifically mention «recommendation systems and advertising systems» as areas of particular scrutiny. These algorithmic systems are known to play a significant role in shaping user exposure to content, both positive and negative. The DSA compels VLOPs to assess how these systems might amplify misleading or deceptive content, even if it originates outside the platform itself. In addition, VLOPs are required to conduct regular risk assessments. This involves evaluating how their platform design, features, and algorithms contribute to the spread of disinformation. Based on this assessment, VLOPs must develop and implement mitigation strategies. These strategies could involve changes to algorithms, increased transparency around content moderation practices, or partnerships with fact-checking organizations.

The Strengthened Code on Disinformation of 2022 serves as a valuable tool within this co-regulatory framework. While not mandatory itself, the Code outlines the best practices for tackling disinformation that align with the obligations laid out in the DSA. By adhering to the Strengthened Code, VLOPs can demonstrate a proactive approach to content moderation and gain valuable insights into areas where their platforms might be susceptible to manipulation by spreaders of disinformation. This compliance with the Code can then be used as evidence towards fulfilling the legal requirements of the DSA.

In essence, the co-regulatory approach embodied by the DSA and the Strengthened Code pushes VLOPs beyond a self-regulatory model. It establishes a framework for

[32] The 2022 Strengthened Code on Disinformation, cit., 18.

[33] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

accountability and transparency in how these platforms handle the spread of disinformation.

4.3. The European Commission's Communication on defending democracy

The European Commission's recent Communication on defending democracy[34] builds upon the foundation laid by the 2020 European Democracy Action Plan. This commitment to a healthy democratic environment informs a new Recommendation focused on ensuring the integrity of European Parliament elections of 2024.[35] This Recommendation emphasizes the crucial role of political parties and political organizations in upholding fair elections. Furthermore, the Recommendation sheds light on the critical link between AI and the quality of online information available during elections.[36] Malicious use of AI systems could exacerbate the spread of disinformation and undermine public trust.

It calls for them to adopt voluntary pledges and codes of conduct that promote responsible campaigning and protect democratic values. These pledges and codes should address several key areas:

- promoting inclusive discourse: campaigns should encourage respectful debate and avoid tactics that divide or marginalize voters.
- combating manipulation: pledges should commit to avoiding tactics like spreading disinformation, using "deep fakes," or employing misleading or hateful content to influence voters. Additionally, manipulative tactics designed to amplify political messages are explicitly discouraged.
- transparency: financial contributions, including gifts and loans, along with campaign spending (especially donations exceeding set limits) must be transparent. The same goes for political advertising – its sources and content should be clearly identifiable.
- cybersecurity: campaigns should take steps like regular cybersecurity checks to protect against attacks that could disrupt elections.
- independent oversight: the Recommendation encourages independent observation of how well campaigns uphold their pledges and codes of conduct. This ensures accountability and strengthens public trust in the electoral process.

By advocating for these measures, the Commission aims to safeguard the integrity and efficiency of elections, fostering a democratic environment where citizens can make informed choices based on accurate information and respectful debate.[37]

[34] Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament.

[35] Commission Recommendation (EU) 2023/2829, cit., para. 1.

[36] Commission Recommendation (EU) 2023/2829, cit., para. 13.

[37] Commission Recommendation (EU) 2023/2829, cit., Whereas no. 39.

4.4. The Regulation on the transparency and targeting of political advertising

The recently adopted Regulation on the transparency and targeting of political advertising[38] recognizes the inherent tension between AI-powered user profiling and a healthy democratic information environment. By allowing political campaigns to target users with laser-like precision based on their data profiles, AI can effectively create echo chambers, limiting exposure to diverse viewpoints and potentially amplifying disinformation that resonates with pre-existing biases. The Regulation's emphasis on transparency serves as a crucial first step in addressing these concerns.[39] Indeed, when personal data is processed using targeting or ad-delivery techniques, controllers are required to adhere to certain provisions, that supplements Regulation (EU) 2016/679[40] and Regulation (EU) 2018/1725[41]. One of the key requirements is that controllers must provide additional information alongside the indication that a given piece of content is a political advertisement. This information is intended to help the individual to understand the logic and main parameters of the techniques used. It should clarify whether an artificial intelligence system has been used to target or deliver the political advertisement, and whether any additional analytical techniques have been employed. They seek to empower individuals with the knowledge and understanding of how their data is being used, who is being targeted, and why certain parameters are chosen.[42] This, in turn, can help individuals make informed decisions about their engagement with such advertisements.

[38] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

[39] Regulation (EU) 2024/900, cit., Whereas no. 4.

[40] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[41] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

[42] Regulation (EU) 2024/900, cit., art. 19, para. 1, lit. c., according to which: «When using targeting techniques or ad-delivery techniques in the context of online political advertising involving the processing of personal data, controllers shall, in addition to other requirements laid down in this Regulation and to the requirements laid down in Regulations (EU) 2016/679 and (EU) 2018/1725, comply with the following requirements: […] provide, together with the indication that it is a political advertisement, additional information necessary to allow the individual concerned to understand the logic involved and the main parameters of the techniques used, including whether an artificial intelligence system has been used to target or deliver the political advertisement and any additional analytical techniques, and including the following elements: (i) the specific groups of recipients targeted, including the parameters used to determine the recipients to whom the advertising is disseminated; (ii) the categories of personal data used for the targeting techniques or ad-delivery techniques; (iii) the targeting goals, mechanisms and logic including the inclusion and exclusion parameters, and the reasons for choosing those parameters; (iv) meaningful information on the use of artificial intelligence systems in the targeting or ad delivery of the political advertising; (v) the period of dissemination of the political advertisement and the number of individuals to whom the political advertisement is disseminated; (vi) a link to or a clear indication of where the policy referred to in point (a) can be easily retrieved».

4.5. The European Media Freedom Act

The European Media Freedom Act[43] acknowledges a user's right to have content personalized by platforms, a process often achieved through the use of AI and algorithms. However, the EMFA expresses a significant concern: such personalization can inadvertently create echo chambers and exacerbate political polarization.

The core of the issue lies in how AI tailors content to a user's existing preferences. By analyzing past behavior and interactions, AI algorithms can predict which information a user is most likely to engage with. While this can lead to a more convenient user experience, it can also lead to a situation where users are primarily exposed to content that reinforces their existing beliefs. This "filter bubble" effect limits exposure to diverse viewpoints and potentially fuels confirmation bias, where users favor information that confirms their pre-existing biases and disregard information that contradicts them. In a healthy democracy, informed debate requires exposure to a variety of perspectives. If users only encounter information that aligns with their existing political convictions, it hinders their ability to critically evaluate different viewpoints and engage in constructive discourse. The EMFA highlights this potential danger of AI-driven personalization, emphasizing the need for safeguards that ensure users have access to a diverse range of information and are not confined to echo chambers that limit their understanding of complex issues.

4.6. The private actors

In this pivotal 'super election year', private entities were not just bystanders but active participants in safeguarding the democratic process. They took significant improvements to prevent the misuse of AI from casting a shadow over the integrity of elections. A landmark event in this regard was the Munich Security Conference held in February 2024. Here, a consortium of tech giants, including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok, and X, undertook to combat the dissemination of content that could potentially undermine electoral processes.

This pact was not merely a statement of intent but included eight concrete commitments:[44]

The development and implementation of technologies to mitigate the risks associated with deceptive election content created with AI systems, including those that are open-source.

The assessment of AI models under the agreement to understand the potential dangers they may pose in relation to the production of deceptive election content.

The detection and monitoring of the distribution of such materials on their platforms.

The implementation of measures to manage deceptive information distributed on

[43] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

[44] For more information, visit *securityconference.org*.

their services appropriately.
The promotion of an intersectoral response to deceptive election content, fostering collaboration across different sectors.
The continued engagement with academics and civil society organizations, ensuring a multi-stakeholder approach.
The support of efforts to encourage awareness, media literacy, and societal resilience, empowering individuals to navigate the digital landscape.
An example of these efforts is the partnership between Meta and the European Commission.[45] They had joined forces to create a platform that offered users swift access to real-time content and information related to the European Parliament elections, which took place in June 2024. This platform aggregated posts on Facebook and Instagram made by candidates from each member state of the Union. It also included posts from pages and accounts that contain specific keywords, as well as institutional posts published by parties. This initiative has been a testament to the proactive steps being taken to ensure transparency and uphold the integrity of the electoral process. It underscored the crucial role of technology in fostering a healthy democratic discourse.

5. Conclusion

Election year 2024 presented unprecedented challenges to global democracy, exacerbated by the misuse of AI for the purposes of spreading disinformation and manipulating public opinion. The proliferation of fake AI-generated content highlighted the growing ability of malicious actors to undermine democratic processes. Faced with this threat, both the United States and the European Union took measures to safeguard the integrity of their elections.
The United States reconsidered its traditional non-regulatory approach in light of past election interference, considering new interpretations of the First Amendment and the potential role of the Federal Election Commission.
The European Union took a more proactive approach, as evidenced by a series of legislative and self-regulatory initiatives aimed at regulating the use of AI, promoting transparency and combating online disinformation. These measures included the strengthened Code of Conduct on Disinformation, the Digital Services Act, the European Commission Communication on the Defence of Democracy and the European Media Freedom Act.
Equally important was the proactive engagement of the private sector in countering election disinformation. Leading technology companies, including Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI, TikTok and X, have committed to mitigating the risks posed by AI by prioritising the detection, management and transparency of misleading content. Initiatives such as the partnership between Meta and the European Commission to provide real-time information during the European Parliament elections further demonstrated these efforts.
In conclusion, protecting democratic processes in the digital age requires a multifac-

[45] *2024 European Parliamentary Elections | Live Displays*, in *help.crowdtangle.com*, June 2024.

eted approach involving governments, regulators, the private sector and civil society. The goal is not to stifle freedom of expression, but to promote a fairer and more transparent information ecosystem where citizens can exercise their right to vote based on facts, not falsehoods.