Digital Democracy in CEE:

Things to Watch For in 2024 European Parliament Elections

CEE Digital
Democracy Watch

Report by **CEE Digital Democracy Watch. 2024**
Registered as: **Fundacja Obserwatorium Demokracji Cyfrowej**

Contact us at: info@ceeddw.org

CONTENTS

POLITICAL CULTURE

DEEP FAKES

DISINFORMATION

POLITICAL ADVERTISING

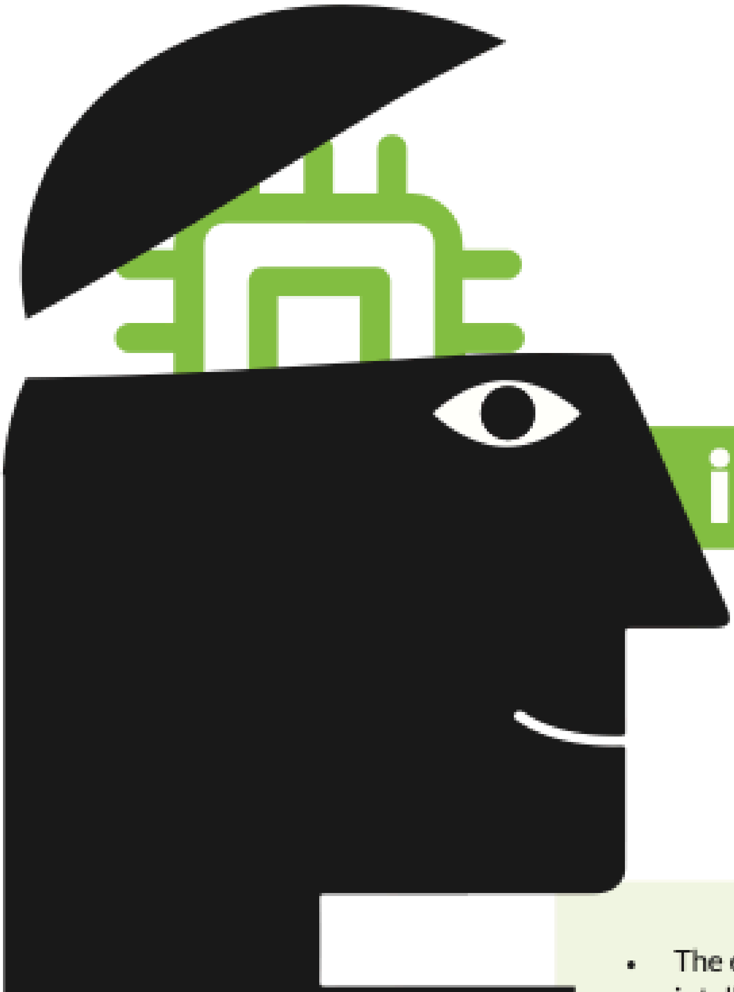
FOREIGN INTERFERENCE

PLATFORMS APPROACH

Paulina Szkoła

Digital Forum Director in Union of Entrepreneurs and Employers

CEE Digital
Democracy Watch



Role of Tech Companies in Safeguarding Voter Trust

Disinformation supported by the latest advancements in AI technology is currently the biggest threat to the integrity of democratic elections. Misinformation campaigns and deepfakes are targeting various communities with the aim of creating suspicion, swaying voters' opinions, and potentially jeopardising their representation in the voting process. To address this issue, organisations responsible for managing elections must focus on building and sustaining public confidence in the fairness of the voting process. Technology companies can play an essential role in helping to achieve this goal.

- The emergence of content generated by artificial intelligence has sparked significant worries regarding disinformation in the context of elections, especially with major global electoral events on the horizon.
- Around 64 countries are gearing up for elections this year, with many taking place in Europe. These include the all-important European Parliament elections in June, which come at a time when the Old Continent faces significant challenges in areas such as defence, expansion, migration, and internal reforms. In light of this, digital platforms and tech companies have pledged to combat misinformation.
- They are taking several measures such as complying with content moderation law Digital Services Act, increasing transparency, collaborating with academic institutions and non-profit organisations, and promoting media literacy.
- However, for these efforts to be effective, tech firms must be adaptable and work closely with government agencies and international civic organisations. This will help them prepare for future elections in which more than half of the global population is expected to participate.

Disinformation – new election tool

Technology has had a significant impact on elections worldwide since the introduction of the internet in politics in 1996. The influence of digital technology and technology firms on electoral integrity is a critical area of concern in modern politics. Campaigning has shifted from traditional mediums to the digital realm over the past two decades, with the 2008 Obama campaign being a pivotal moment in leveraging social media for electoral advantage (Aaker and Chang, 2009).

This set a precedent for digital mobilisation strategies that have evolved significantly since then. Social media platforms have democratised access to political discourse, making information and discussions about elections more accessible to wider segments of society. However, this transition has also led to a surge in disinformation campaigns that threaten the very fabric of democratic processes. Since the 2016 US presidential race, the issue of misinformation in elections has become significant, with Russian entities discovering cost-effective methods to disseminate false information through social networks. The open economy has made it easier for "troll farms" and other harmful entities to trade and spread false information internationally. They take advantage of areas with weak regulations and insufficient protections. In 2021, researchers estimated that over $60 million has been spent on outsourced digital propaganda since 2009 (Bradshaw, Bailey and Howard, 2021) . And the war in Ukraine raises the stakes even higher. It is expected that Russia will use the upcoming European elections as a sort of testing ground to assess the effectiveness of their strategies and tactics of disinformation and "troll farms" in elections more broadly, swaying public opinion in favour of the Kremlin and undermining support for Ukraine.

Today, the swift advancement of AI has heightened concerns even further. And the upcoming elections will be a tsunami of AI-generated disinformation, posing a significant challenge to electoral integrity. Commissioner Thierry Breton urges companies to "spare no effort" to counter the spread of misinformation, while the World Economic Forum targets AI-generated disinformation as a major threat in the upcoming European elections (Li, 2024). The threat is real, and the examples prove it. In the past years, deep fakes have surged, with 900% more online content in 2020 than in 2019 (World Economic Forum, 2023) .

In recent times, there have been instances where artificial intelligence (AI) has been used to create fake audio and video clips to mislead people in political campaigns. For example, an AI-generated audio clip of a fake Joe Biden was created to discourage voters in the New Hampshire primaries, while a manipulated video of Muhammad Basharat Raja, a participant in Pakistan's elections, was altered to urge voters to abstain from voting (Adami, 2024). These incidents highlight the potential dangers of AI technology being misused for political propaganda and disinformation.

Joint efforts

The spread of false information has become the biggest obstacle to maintaining the trustworthiness of European Parliament elections in June. This has altered the fundamental responsibilities of those overseeing elections. It is no longer enough to simply ensure that elections are technically sound, open, and fair. Instead, the main objective has shifted towards emerging focus on disinformation that targets and has a clear focus in undermining the idea of election integrity (Neubert, 2024). The duty to tackle this issue goes beyond just the election authorities. Lawmakers, political parties, contenders, news outlets, and non-governmental organisations all have crucial roles to fulfil. Similarly, tech companies are essential participants in this shared mission.

To address this challenge, it is essential to adopt a multi-faceted strategy that integrates legislative action, civic education, and technological interventions. One notable effort in this regard is the European Commission's action plan against disinformation, launched in December 2018. The Action Plan recommends engaging the private sector to combat disinformation. In September 2018, significant online platforms, social media services, and advertising firms made a landmark move by endorsing a self-regulatory Code of Practice on Disinformation (Cabrera Blázquez, Cappello, Talavera Milla and Valais, 2022). The Code intends to achieve the Commission's goals, as outlined in its 2018 Communication, by carrying out a comprehensive range of commitments. These commitments involve enhancing transparency in political advertising, terminating fake accounts, and putting an end to revenue streams for those who spread false information. The overhaul of its revision commenced in June 2021, and following the formal endorsement and unveiling of the updated Code on 16 June 2022, the new CoP is set to integrate into a more expansive regulatory landscape. This integration will occur alongside legislation pertaining to the Transparency and Targeting of Political Advertising and the Digital Services Act (Jackson, Adler, Dougall and Jain, 2023).

Two reports from CoP-affiliated online platforms present the initial assessments of the initiative. In January 2023, Adobe, Google, Microsoft, Meta, TikTok, Twitch, Twitter (which later exited the CoP in May 2023), and Vimeo submitted the first round of reports. By July 2023, Google, Meta, Microsoft, and TikTok had all submitted follow-up reports (Lai and Yadav, 2023). A database was created to track the occurrence of interventions, the reporting of actions, the impressions made, and the impact of each intervention, and to suggest potential impact metrics for future reports.

Some platforms shared specific metrics that detailed the impact of their anti-disinformation efforts. Google and Microsoft presented data on click-through rates and the financial consequences for pages and domains that had been demonetised, highlighting the economic effects of policy violations. These insights represented important steps in quantifying the impact of interventions on user behaviour.

Reports faced criticism for not providing sufficient data to compare across platforms and offering information of minimal utility. Going forward, there's an emphasis on fostering cooperation between corporations and policymakers to standardise reporting practices.

However, these actions highlight the significance of a collaborative approach involving all stakeholders in the democratic process to combat misinformation. It is imperative to guarantee that citizens have access to reliable and trustworthy information, that media and civil society institutions are empowered to detect and address disinformation, and that online platforms and advertisers are responsible for their conduct. This way, we can establish a truthful, transparent, and reliable information system that is indispensable for the integrity of elections and the operation of democratic societies.

Pledge to prevent AI election interference

Another crucial aspect of the collaboration lies in the companies' willingness to pledge commitments and align with policies related to technology and democracy. Online platforms companies are often misused by malicious individuals to spread false information. However, it is reassuring to know that some of these corporations have acknowledged their responsibility in addressing this problem. They have set up special teams for elections and have voluntarily pledged to limit the dissemination of AI-generated disinformation content pertaining to the 2024 elections.

In February 2024, twenty major technology firms came together under the 'A Tech Accord to Combat Deceptive Use of AI in 2024 Elections' initiative to show their commitment to fight against AI-generated misinformation during electoral processes. Their primary focus is on deepfakes - manipulated audio, visuals, and images that falsely represent important figures in democratic elections or disseminate incorrect voting details (Cerulus, Roussi and Volpicelli, 2024). The signatories of this agreement include renowned names such as Microsoft, Meta, Google, Amazon, IBM, Adobe, and the chip designer Arm. Along with these, AI startups such as OpenAI have also joined the initiative.

Even the biggest technology companies cannot handle every aspect of the technological infrastructure involved in creating AI-generated content. However, the Tech Accord initiative illustrates how platforms can enhance openness regarding their interactions with governments, thereby rebuilding public trust in efforts to counter disinformation during elections. Platforms need not delay for governmental transparency reforms, instead, they can proactively reveal discussions related to content, similar to the way they currently disclose government requests for access to personal data, and they are doing so.

Ecosystem of enforcement structures

The European Union has recently released new guidelines to mitigate the risks associated with elections, such as the spread of false information and coordinated campaigns by Russian bots or fake media. These guidelines include a robust set of protective measures that start with the Digital Services Act's explicit due diligence regulations. These guidelines require stringent measures against the spread of falsehoods, with potential fines up to 6% of a company's global revenue for non-compliance. The DSA's requirements include transparent political advertising, clear labeling of AI-generated content, and the establishment of specialised teams to monitor threats.

The EU has gained over five years of experience in collaboration with platforms through the Code of Practice Against Disinformation. Additionally, upcoming regulations under the AI Act will introduce transparency labelling and AI model marking rules. But even with adequate surveillance and regulations, tracking electoral misinformation online proves difficult. As we navigate the complexities of AI-generated disinformation, collaborative efforts between technology companies and policymakers must also enhance public awareness, promote digital literacy, and media education.

LINK TO THE FULL REPORT

CEE Digital
Democracy Watch