upgrade
democracy

Impulse Series #5

August 2023

The EU Elections 2024: How to build resilience against disinformation campaigns on social platforms

Cathleen Berger, Charlotte Freihse, Vincent Hofmann,
Matthias C. Kettemann, Katharina Mosene

Alexander von Humboldt
INSTITUT FÜR INTERNET
UND GESELLSCHAFT

BertelsmannStiftung

About the Impulse Series and this Publication

In a collaboration between the Bertelsmann Stiftung's Upgrade Democracy Team and the Humboldt Institute for Internet and Society, we are organising a five-part Impulse Series on **"Digital Platforms: Design Proposals and Alternatives"** from April to September 2023. The focus of the series is an in-depth examination of current challenges and problems on existing social platforms and the identification and discussion of alternatives. Regarding the democratic design of dominant social platforms, special attention is placed on the topics of participation and platform governance as well as on questions of how to make decision-making processes more oriented towards the public common good. The individual impulses intertwine thematically and aim to develop ideas, action and policy recommendations for sustainable platform and content governance in digital spaces.

All impulses take up ideas from expert workshops, in which provocative hypotheses and central questions are discussed in small, intimate groups under Chatham House rules. Following each event, an impulse paper summarising the most important aspects of the discussion is published.

The series was conceived by Cathleen Berger, Charlotte Freihse, Matthias C. Kettemann, Katharina Mosene and Vincent Hofmann.

Participants of the discussions on 22. August 2023

Impulse giver:
- Dr. Clara Iglesias Keller, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Sabine Frank, YouTube

Experts:
- Josephine Ballon, HateAid
- Cathleen Berger, Bertelsmann Stiftung
- Irene Broer, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Stephan Dreyer, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut
- Charlotte Freihse, Bertelsmann Stiftung
- Dominik Hierlemann, Bertelsmann Stiftung
- Carla Hustedt, Stiftung Mercator
- Richard Kuchta, Democracy Reporting International
- Sami Nenno, Humboldt Institut für Internet und Gesellschaft
- Jan Rau, Leibniz-Institut für Medienforschung | Hans-Bredow-Institut

Moderation:
- Georgia Langton, Bertelsmann Stiftung

1 Electoral processes and disinformation: Strengthening digital discourse ahead of 2024

The upcoming 2024 EU elections present an important moment for digital campaigning, the governance of online discourses – and the overall future of Europe. A key challenge will come in the form of disinformation campaigns, hate speech and attempts to manipulate public debates. The risk is that citizens may turn skeptical and distrusting towards democratic processes, public discourses and Europe's political institutions. And this risk is real: Recent *forsa* surveys, commissioned by the Media Authority of North Rhine-Westphalia, delved into the influence of digital disinformation, especially in the context of elections. They found that 54 % of internet users encounter politically-driven disinformation at least occasionally. A staggering 85 % believe that such disinformation can jeopardise democratic processes. There is good news however: Contrary to popular belief, research shows that disinformation is not swaying opinions in large numbers and that users are growing increasingly successful at spotting such misleading or false content, even if they could be encouraged to report it more regularly and actively.

Efforts and initiatives that protect democratic elections, including EU elections, from information manipulation and foreign interference have significantly grown in relevance over the years. Examples from recent elections in other countries raise the question of whether we are prepared (enough): Disinformation campaigns targeting the electoral process and its legitimacy played a major role in the Brazilian riots in January 2023 and the storm on the U.S. capitol in Washington D.C. in January 2021. In both cases, the actions of social networks that were flooded with claims and accusations of election fraud or denial long before the actual rioting began, leave much to be desired. There is a need for caution as platforms continue to act too slow and without appropriate preparation. This is further exacerbated by recent widespread layoffs or staff reductions across almost all platforms, notably within teams responsible for monitoring and dealing with disinformation (often called „Trust & Safety" teams).

This is coupled with worrying trends of political actors exploiting polarising issues to mobilise voters and undermine social cohesion. Common topics prone to disinformation themes include measures taken during the COVID-19 pandemic, Russia's involvement in Ukraine, gender and climate-related topics (which we discussed in our last impulse), migration, energy prices or mobility in cities – all of which are instrumentalised to trigger emotional reactions and to hinder a constructive, public discourse with differentiated arguments. In this way, political debates are poisoned and trust in political processes and institutions is increasingly eroded. Such disinformation campaigns can be launched by foreign actors or spread deliberately by domestic actors serving short-sighted agendas. Finding appropriate countermeasures is therefore even more complex.

Admittedly, the European Union has taken various steps to counter disinformation. For instance, the so-called European Rapid Alert System for Disinformation will be fully operational in time for the 2024 EU elections. In addition, the Digital Services Act (DSA) will be put to a test on whether it effectively regulates the spread of disinformation on digital platforms. Digital platform providers, such as Meta, X (formerly Twitter) and Google have developed election integrity policies aimed at identifying and removing fake accounts and illegal content. Given both the volatility of public debates and the importance of electoral processes, however, we may find that lots more must be done.

2 Forging a resilient future: Bridging lessons learned and new ideas

A look at past elections and other political processes indicates that social media and messaging services play an increasingly influential role:

- The **2016 U.S. presidential election** for example saw significant influence exerted through social media. Russian actors were found to use platforms like Facebook, Twitter, and Instagram to disseminate disinformation, sow controversy, and polarise public opinion. The infamous Internet Research Agency (IRA) successfully orchestrated coordinated campaigns that reached millions of Americans. The election results in 2020 ultimately led to a storm on the U.S. capitol in January 2021.
- The **2016 Brexit referendum** in the United Kingdom was marked by an extensive use of social media campaigns. Both the „Leave" and „Remain" camps employed targeted advertising on platforms like Facebook to reach specific voter groups with tailored messages.
- The **Cambridge Analytica scandal**, which came to light in 2018, further revealed how personal data from millions of Facebook users were harvested without consent and used for targeted political advertising and undue influence operations.
- During the **2018 Brazilian presidential** election, social media played a significant role in shaping the discourse. Far-right candidate and ultimate leader, Jair Bolsonaro, leveraged platforms like WhatsApp to spread unverified information and conspiracies. The use of encrypted messaging apps highlighted the challenges of monitoring and countering misinformation. Elections in 2022 became a focal point for claims of fraud and denial of results amplified on social media, which erupted in violence in January 2023.
- The **2019 general election in India** witnessed a surge in social media activity, with political parties employing targeted advertising and social media campaigns to reach diverse voter segments. The 2024 elections will surely follow similar patterns.

All of these are illustrative of potentially harmful and severe repercussions. Currently most platforms have introduced transparency measures for political and issue-based advertisements. On their basis, advertisers are required to provide information on who is funding the ads and who the target audience is. Many platforms have also started collaborations with fact-checking organisations to identify and label false or misleading content. Users are further provided with additional context or warnings when interacting with such content, as widely seen during the Covid-19 pandemic. We've also seen the introduction of new rules tailored to ensuring electoral integrity, that allow for the accelerated flagging, take-down procedures or similar actions.

On the regulatory level, the EU has adopted the Digital Services Act (DSA), which targets multiple issues of digital platforms that can harm democratic elections, such as the spread of illegal content or targeted advertisement. Counter measures include, among many others, the use of trusted flaggers, fact checking, risk assessments, research access and transparency requirements. The EU has also developed a Rapid Alert System to facilitate the sharing of information and coordinated responses to disinformation threats among member states and platforms. In addition, the EU has established the European Digital Media Observatory (EDMO) to monitor and counter disinformation campaigns, aiming at fostering increased cooperation between researchers, fact-checkers, and online platforms.

Against this multifaceted and highly political background, we posed two hypotheses to start the dialogue:

1. Measures taken by large social platforms to protect electoral processes, and the multilingual EU elections, do not go far enough and lack incentives to prevent coordinated disinformation campaigns.
2. Resources for independent monitoring of disinformation campaigns and the respective (context-specific) narratives instrumentalised to influence and manipulate EU elections need to be significantly increased. Without alliances between civil society monitoring organisations and researchers, a data-based analysis of EU election resilience will not be possible.

Based on this, we raised and reflected on **three questions** during our discussion with experts:

1. What concrete measures should the EU and providers of large social platforms like Meta, Google & Co take to strengthen resilience against disinformation during the 2024 elections? And how will European regulations such as the DSA serve to support such efforts, and what are their limits?
2. What could be incentives to promote partnerships between EU member states and civil society to foster transparent and accountable political debates and to increase citizens‘ trust in European political institutions, including to counter foreign interference?
3. What other measures and innovative concepts can we propose to increase the resilience of European democracies and how do we emphasise the urgency to start preparing now?

2.1 Effectiveness and limits of platform measures and regulatory approaches to protect elections

To be able to effectively counter disinformation, it is critical to understand how influence operations and disinformation campaigns function and/or which aspects of social platforms they may exploit to their advantage. There are three broad aspects that can be instrumentalised to fuel the spread of digital disinformation:

1. **Amplification and virality:**
   Social media platforms are designed to facilitate the rapid dissemination of information. The shareability and visibility of posts, combined with engagement mechanisms such as likes, shares, and comments, contribute to the amplification of certain narratives, messages, or (their representing) candidates.
2. **Micro-targeting and paid content:**
   Social media platforms build their businesses on the ability to micro-target specific demographics and individuals. Campaigns can tailor their messages to resonate with specific voter segments, increasing the likelihood of engagement. Advanced data analytics and user profiling further allow political actors to customise content based on users‘ preferences, behaviours, and even psychological traits, creating a more personalised and persuasive communication approach. Sponsored content, presented alongside organic posts, blurs the line between informative content and paid promotion, additionally influencing users‘ perceptions.

3. **User-generated content and grassroots mobilisation:**
   Social media allows ordinary users to become or at least imitate political activists and influencers. User-generated content, including videos, memes, and posts can "go viral" (get amplified significantly) and therefore influence public discourse. Grassroots movements can quickly gain momentum, mobilise supporters, and challenge established political narratives.

Unfortunately, all three aspects can be used to increase the reach of disinformation campaigns, especially during elections. False narratives, fabricated and manipulated content or images can thus spread rapidly, often fuelled by coordinated (and automated) efforts to deceive and manipulate public opinion.

The multifaceted nature of threats that endanger election processes requires the involvement of diverse stakeholders as well as more efficient cooperation among them. The fact that the EU elections are transnational makes the implementation of measures even more complex. The following provides a broad overview of existing measures on a platform and regulatory level – indicating where and how these could and should be strengthened or scaled:

Social media platforms:

- To combat the rising tide of digital disinformation, platform operators need to take proactive measures, ensuring that users have the tools and knowledge to discern fact from falsehood. This includes strengthening content verification mechanisms to identify, flag, report and block false or misleading information; and further providing users with warning labels and/or clear information about the source of content and its accuracy rating. Based on specific policies to tackle election-related disinformation, such content can be removed with more care for the vulnerability of the democratic processes.
- Platforms have and should continue to establish dedicated rapid response teams that can swiftly identify, assess, and counter disinformation campaigns during critical periods such as elections. These teams should work to debunk false narratives and provide accurate information to the public in real-time. In support of these teams, allowing for independent researchers to access data to continuously monitor activities on platforms is key to detecting, understanding, analysing and countering disinformation campaigns. Such research is also pivotal in conducting systemic risk assessments.
- In addition, oversight and transparency of recommendation algorithms must be increased. Regular audits and transparency reports can shed light on how algorithms prioritise and display content, ensuring fairness and accuracy.
- „Prebunking" methods, which use straightforward educational texts on disinformation tactics and techniques (rather than individual content), have proven to be effective and should be rolled out at scale.
- To identify disinformation, close collaboration between platforms and independent fact-checking organisations can expedite the identification and correction of false information. Such partnerships can also help with balancing the need to swiftly remove harmful content whilst upholding the right to freedom of speech.

The general (good) news is: the accurate identification of harmful and misleading content is very much possible – if continuous monitoring and research access is ensured; reliable journalistic sources are available; technical and design features support labelling, flagging, and reporting; users possess the necessary skills to assess sources and content; and collaboration and partnerships allow for further contextualisation.

However, it is not only the platforms that hold responsibility in this.

Regulatory and legislative measures:

- The Digital Services Act (DSA) presents the most significant regulatory approach to countering illegal content in the digital space. However, when it comes to countering digital disinformation, it contains various limitations, mostly because disinformation often does not fall under illegal content – yet its effects remain harmful, including in the context of elections. This requires context-specific assessments, nuance, and cooperation, especially with civil society.
- As the DSA creates a stronger relation between Very Large Online Platforms (VLOPs) and the EU Commission, it is crucial to ensure constant multi-stakeholder processes in its implementation and execution – though all actors involved may need different levers of support to fulfil their respective roles, they heavily depend on each other.
- Furthermore, digital platforms operate globally, making it challenging to enforce EU regulations beyond its borders -- including disinformation campaigns that originate from outside of the EU. Disinformation tactics, similarly, evolve constantly, which is why regulators need to remain agile and adapt swiftly to new challenges. There must be a balance between broad wording that allows for being open to new technological developments, whilst allowing for the clear and precise interpretation of regulatory definitions – as well as a balance between new regulatory needs and collaborative outcome-driven interpretation of existing laws.
- Another regulatory approach besides the DSA is the political ads regulation. The fact that this regulation may not be ready in time for the 2024 elections is alarming, as it presents an important step in (re)gaining transparency of political parties and their candidates.
- All regulatory approaches regarding digital content rely to some extent on data-driven and evidence-based knowledge, primarily generated by researchers. Legislative measures including data-sharing agreements could therefore contribute to facilitating and bolstering social media monitoring efforts. In addition to that, the European Union needs to increase collaboration with international partners, including tech companies, non-European civil society and governments, to develop a coordinated and widespread response to disinformation campaigns that target multiple regions.

Yet again, the good news here is: regulatory mechanisms like the DSA are crucial. Their impact on the EU elections next year, however, will depend on their enforcement. Moreover, member states can and should build on structures already in place, for example when it comes to early warning systems and joint crisis response mechanisms.

2.2 Monitoring and countering disinformation during elections requires cooperation and partnerships

It is crucial to continuously invest in independent social media monitoring to allow for the detection, understanding and analysis of disinformation as a systemic risk. Only then will we be able to design effective countermeasures. Either way, disinformation campaigns won‘t just disappear -- to limit their spread and impact, all actors must play their part. We need reliable and trusting partnerships between the EU, member states, civil society organisations and platforms.

Here are just five incentives that could foster this cooperation:

- **Shared goals of democracy:** Identify actors that share a common interest in upholding democratic values and ensuring fair elections. Collaborative efforts can contribute to maintaining the integrity of democratic processes, notably if this is clearly identified as a shared goal – potentially aiding public support, credibility and trustworthiness of all.
- **Enhanced effectiveness:** Member states can benefit from the specialised knowledge and expertise that civil society organisations can provide in monitoring and countering disinformation, leading to more effective strategies. Through this, civil society can offer valuable input into policy discussions, and hence more informed and effective policies to counter disinformation.
- **Access to information and resources:** Civil society often has access to grassroots information and insights that member states might not possess. Collaboration can provide member states with a deeper understanding of disinformation issues. By combining resources, both can access a broader range of data sources, leading to more accurate analyses of disinformation campaigns.
- **Broader impact:** Effective collaboration can lead to a broader impact in countering disinformation, contributing to societal resilience against manipulation and misinformation.
- **Accountability and transparency:** Working together promotes transparency and accountability, reducing the likelihood of misinformation within the countering disinformation efforts themselves.

2.3 Recommendations: The time to prepare for 2024 is now

The challenge of countering disinformation cannot be effectively addressed by any single entity in isolation. Just as discourses themselves, there are a lot of players and normative layers, and influence vectors involved: social, legal, political, economic, technical. Rather, a collaborative approach is essential, with each actor embracing their roles and obligations.

What governments can do:

- **Ensure regulatory measures, such as the DSA, are enforced:** The Digital Services Act provides a necessary legal framework for removing illegal content, yet its impact on the 2024 elections could fall short if it is not swiftly implemented and enforced reliably. This also includes ensuring that adequate funding for civil society and researchers is available to make use of data access-related rights.
- **Foster collaboration to scale the reach of reliable sources:** Government entities should explore the potential of partnerships with digital platforms to ascertain and elevate verified sources. Depending on the context and political system, this can include support for public service broadcasters, identifying and amplifying the voices of independent fact-checking, monitoring, educational and democracy-supporting organisations, or institutional support for systemic risk assessments regarding the impact of digital disinformation.
- **Provide more resources and funding for efforts and actors strengthening democracy – online and offline:** Efforts that aim to strengthen democratic societies online and offline should be embedded within a sustainable system that allows researchers and civil society to operate efficiently. This requires sufficient funding that is reliable, flexible, and comes with low administrative burdens. In addition, our conversations highlighted that the responsibility and the role of the media in countering any kind of disinformation cannot be overestimated – this too requires that quality journalism is equipped with the necessary resources and that journalists are protected and safe when doing their work.

What platform providers can do:

- **Amplification of trustworthy sources:** To counter the spread of disinformation, there's a crucial need to elevate credible and trustworthy sources. By highlighting well-sourced and reliable information, individuals can be empowered to make informed decisions and resist the influence of misleading narratives. Providers of digital platforms can help amplify trustworthy sources, credible information about election processes etc. to contribute to that. To avoid political census, it is necessary that platforms implement multi-stakeholder processes and set up transparent frameworks indicating how credible and trustworthy information sources are identified and labelled.
- **Transparency, data access, and research collaboration:** The availability of APIs from platforms like YouTube, as well as reports on ads are important and should be implemented by all social media platforms. Access must be straightforward, reliable, and affordable in terms of data processing, storage, and analyses. Moreover, a clear outline on what data is available to platforms to allow researchers to design their questions and methodologies accordingly is critical.
- **Comprehensive approach to election integrity:** Forging a synergy of human intelligence and machine interventions proves to be essential. Quarterly released transparency blogs, a library of political ads, or dedicated election integrity policies, which outline processes, available resources and reporting mechanism may transcend legal requisites but can only prove beneficial to the efficiency of digital discourse. Civil society collaborations further present an avenue for informed actions and insights, significantly contributing to the broader landscape.

What civil society can do:

- **Draw attention and conduct awareness campaigns:** The EU lacks a unified media environment, which makes it harder to rally voters across borders, to monitor and inform citizens about potential disinformation campaigns, and to provide trustworthy sources across all EU languages. This makes it even more important that civil society organisations from all EU member states coordinate, collaborate, and amplify each other's awareness raising campaigns to allow for a strong, well-informed, and resilient voter base.
- **Provide media and digital literacy training:** Implementing digital literacy programmes that educate citizens about critical thinking, media literacy, and responsible online behaviour are an integral factor in tackling the challenges connected to disinformation in the long run.
- **Support conflict resolution and content governance through strategic litigation:** Where content laws differ per country, platforms often serve as the arbiter of what is visible where, to whom and how. Such decisions on content governance should be embedded in broad-based input mechanisms and/or civil society consultations. Where disputes cause harm, strategic litigation can serve as an effective tool to highlight and solve contradictions of laws across borders.

What political candidates and entities can do:

- **Lead by example and step up your digital security game:** Social media campaigns have become an integral part to electoral processes. It is not only important to ensure digital safety of accounts and individuals, but technical measures can also support credibility of political campaigns. Deep fakes and other forms of manipulated content are on the rise: parties and candidates should demonstrate the effective use of tools like watermarks on visuals or audio to help increase confidence in the content. Moreover, the adoption of such techniques might induce a ripple effect, prompting other stakeholders to incorporate them into their practices.

Regarding elections, our observations revealed a tendency towards measures that are short-term in nature. While this observation does not negate the importance of heightened measures during electoral

periods, we strongly suggest focussing on long-term, sustainable strategies and measures. Strategies must extend beyond electoral cycles and provide a more comprehensive approach to countering disinformation.

If you only take one thing from this: we cannot passively standby, we must act now. The effectiveness of countering disinformation is very much connected to how good actors are prepared and preventive measures are set into place. As the EU elections draw near, we therefore urge all actors to start acting – after all a resilient European society will be the most effective protection against digital disinformation during the elections in 2024.

3 Go deeper on elections, digital disinformation and democracy:

- In a recent study, the Upgrade Democracy project of Bertelsmann Stiftung took a closer look at how citizens of the European Union perceive disinformation and what kind of experiences they have had with it so far. Find the study and a summary of the results here: New Study: Attitudes and Perceptions of Disinformation in Europe – Upgrade Democracy
- A recent study by forsa for the Media Authority of North Rhine Westphalia shows how people see disinformation, how we can protect our democracies against it and which tools work with a focus on elections. You can find the full study here: Forsa-Umfrage_zum_Informationsverhalten_bei_Wahlen_2023 (medienanstalt-nrw.de)
- In a paper for the Konrad Adenauer Stiftung, Clara Iglesias Keller, Laura Schertel Mendes and Victor Fernandes deal with the Brazilian legal framework for the regulation of online content in a descriptive and prescriptive manner during the first one hundred days of the third Lula administration (January to April 2023). Read the full paper here: efdd5b2d-e5c5-6c5c-8a0c-315cef9cb65b (kas.de)
- In this article, Charlotte Freihse illustrates the behaviour of different social media platforms during the last elections in the US and Brazil, concluding that they still lack strategies how to react to electoral disinformation campaigns, contested election results and incitement to violence in connection to that. Read the analysis here: Riots Reloaded: Major social platforms are still poorly equipped to counter disinformation campaigns ahead of elections – Upgrade Democracy
- Authored by leading journalists from the BBC, Storyful, ABC, Digital First Media and other verification experts, the Verification Handbook provides tools, techniques and step-by-step guidelines for how to deal with user-generated content (UGC) during emergencies. You can find the handbook here: Verification Handbook: homepage
- Regulating disinformation is not a simple task. Freedom of expression sets clear boundaries to states. Have a look at this extensive survey of normative vectors on how to regulate social practices connected to disinformation behaviour by a team from the Leibniz Institute for Media Research: HBI_Disinformation_07112021.indd (medienanstalt-nrw.de)
- Prebunking is one approach to counter disinformation. Google subsidiary Jigsaw, social enterprise Moonshot, and six German NGOs have launched a video campaign using the „prebunking“ method in close cooperation with local experts. Learn more about the project here: Falschinformationen bekämpfen, bevor sie verbreitet werden (blog.google)
- The National Democratic Institute (NDI) has outlined approaches to addressing the threat of disinformation in the electoral context, particularly the actions citizen election observers and international observers can take to mitigate, expose, and counter disinformation. You can read the full report here: Disinformation and Electoral Integrity: A Guidance Document for NDI Elections Programs | National Democratic Institute
- In this essay, Erik C. Nisbet, Chloe Mortenson and Quin Li argue the presumed influence of misinformation (PIM) may be just as pernicious, and widespread, as any direct influence that political misinformation may have on voters. Read their essay and survey here: The presumed influence of election misinformation on others reduces our own satisfaction with democracy | HKS Misinformation Review (harvard.edu)

- In their article, Dr. Julie Posetti, Felix Simon and Nabeelah Shabbir share insights from national elections in South Africa, the Philippines, and in India where disinformation-busting strategies of three digital-born newsrooms have been tested. Read their findings here: Reporting elections on the frontline of the disinformation war | Reuters Institute for the Study of Journalism (ox.ac.uk)
- The Centre for Innovation and Technology has provided training to improve media and news literacy so that as many voters as possible are able to tell the difference between reliable news and disinformation. You can find it here: FEATURE-Zimbabwe fights fake news with lessons in spotting disinformation | Reuters
- To what extent does artificial intelligence change the disinformation landscape, and do we need to defend our elections against deepfakes and other fabricated content? The Brennan Center for Justice puts forward a few safeguards: How AI Puts Elections at Risk — And the Needed Safeguards | Brennan Center for Justice
- The EU Disinfo Lab created an overview of existing platform policies on election misinformation with comes in handy for comparisons: 20230621_ElectionsFS.pdf (disinfo.eu)
- This thought paper, commissioned by the United Nations, encourages states and platforms to join forces regarding information integrity. A proposed common agenda also looks at the vulnerability of elections: our-common-agenda-policy-brief-information-integrity-en.pdf (un.org)