CEE Digital Democracy Watch

Protecting Digital Civic Space in the EU

CEE Digital
Democracy Watch

Protecting Digital Civic Space in the EU

Authors:
Konrad Kiljan, Jakub Szymik

Publisher:
Fundacja Obserwatorium Demokracji Cyfrowej
Karmelicka 3c/19, 00-149 Warszawa
www.ceeddw.org

After years of headlines and debates, 2025 is emerging as a pivotal point for how we understand digital spaces and their profound effects on our social and political climates.

This year marks the beginning of the Digital Services Act era in practice – a moment when EU member states must grapple with its implications. What does it truly mean to hand governments more authority over online content? How do we enforce regulations in the political superstorm? And, perhaps most critically, can this ambitious EU framework genuinely protect the vulnerable voices and safeguard national election systems from digital interference? These questions are no longer theoretical; they are urgent and unavoidable.

The DSA's global ambitions are also being put to the test. The United States, home to the majority of the communication platforms the Europeans use, is pushing back against Europe's efforts to set global digital standards. JD Vance's infamous remarks on "free speech" have become emblematic of this resistance, while platforms have made abrupt decisions to sideline fact-checkers – moves that have sent shockwaves through the European community and beyond. The transatlantic tension underscores a larger question: can Europe's vision for digital regulation transcend borders, or will geopolitical realities clip its wings?

Yet Europe is not retreating. The European Commission is doubling down, by expanding the Digital Services Act framework through new guidelines and complementary initiatives like the European Democracy Shield and the Digital Fairness Act. These efforts are an attempt to keep on providing the "golden standard" for global digital regulations. At the same time, the rapid rise of AI-driven technologies has thrown policymakers into a dilemma: how to strike the delicate balance between fostering innovation and imposing necessary guardrails? It's a pendulum swing that could define Europe's role in the global tech race.

To better understand this moment, we hit the road in late 2024 and early 2025, speaking with over 60 stakeholders across Warsaw, Prague, Budapest, and Bucharest. Our goal was simple: to take the temperature on how effective these new approaches seem to be, what challenges remain unresolved, and what role national governments should play in the fast-moving digital environment.

This report offers an imperfect picture but an essential one. It amplifies voices that are often overlooked in EU discussions from organisations from Central and Eastern Europe that deserve a seat at the table as Europe charts its digital future. We are looking to continue to amplify those perspectives for better, stronger EU tech landscape.

Jakub Szymik,
Founder at CEE Digital Democracy Watch

Executive Summary: The Future of EU Democracy in Digital Times

This report examines five key areas that will shape the future of EU democracy in the digital age. Its findings are based on extensive discussions with experts from organisations across five countries, aimed at identifying shared priorities for strengthening the digital civic space.

EU Introduces: Election Integrity

The first area of focus is election integrity in the digital age, which is being introduced as part of the Digital Services Act framework, Transparency and Targeting of Political Advertising Regulation and the European Democracy Shield package. While their objectives are commendable, they face significant challenges due to the varying electoral standards among Member States and the complexities of defining the European Commission's competences in relation to national sovereignty. Achieving a harmonised framework that balances national autonomy with effective EU-wide enforcement will be critical.

Strengthening Trust in Regulatory Bodies

Ensuring apolitical and objective decision-making is an ongoing challenge, with continued debate over which institutions are best suited to handle sensitive cases. Balancing independence with accountability remains a complex issue. Institutional reforms are needed to enhance impartiality and public trust while providing clear mandates and safeguards against political interference.

AI on the Rise New Tools & Tactics

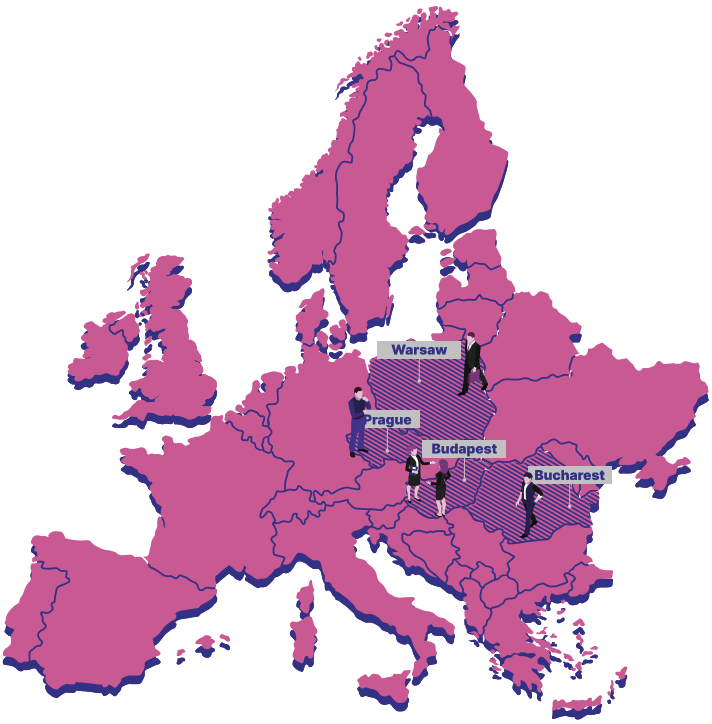
The rise of AI-powered tools present both opportunities and risks for EU democracy. While these tools can drive positive change, civic society actors often face exclusion from adoption due to restrictions on political content. At the same time, bad-faith actors exploit vulnerabilities in existing protection systems, undermining democratic processes. Inclusive policies must be developed to enable civic groups to leverage AI tools effectively while implementing adequate safeguards to prevent misuse by malicious actors.

Access to Communications for Social Groups

Many civic organisations face unpredictability in how their content is distributed, particularly when addressing sensitive topics such as healthcare access, minority rights, or political campaigns. Shifting platform policies and regulatory whirlwind have led to increased restrictions on political content, creating additional barriers for these groups. Ensuring consistent policies that protect equitable access to communication channels is essential for fostering an inclusive digital civic space.

Content Moderation Remains a Pickle

Transparency in how platforms moderate content is insufficient, as new tools and techniques often outpace existing trust and safety frameworks. Platforms frequently adjust their approaches to political content without clear accountability, and infringement proceedings against non-compliant platforms have shown limited progress. Addressing these issues requires stronger oversight mechanisms and clearer standards to ensure accountability and compliance.



About this report

At the turn of 2024 and 2025, we organised four meetings with over 60 representatives from NGOs, government agencies, diplomatic missions, universities and industry associations from Central and Eastern Europe.

CEE Digital Democracy Watch team met with international participants in Warsaw, Prague, Budapest, and Bucharest to gather their perspectives on shared challenges. Each session began with a briefing on the current state of affairs, followed by an open discussion.

All meetings were complemented by a structured workshop designed to collect insights on key issues, stakeholders, and potential solutions. While the process followed a systematic approach, the findings remain subjective, as they were synthesised after the meetings and do not fully reflect the positions of any single participating organisation. The discussions were not recorded.

The series of events were supported by Google.

This report is written with the goal of amplifying the voices of the underrepresented Central and Eastern European community. The 2024 Draghi report on Europe's competitiveness generated significant interest but was also criticised for lacking input from experts representing countries that joined the EU in the last 20 years. A Europe-wide policy developed without these perspectives risks failing to harness the region’s full potential and is bound to increase skepticism in Eastern European countries.

With this report, we aim to address that gap.

WARSAW
27.11.2024

PRAGUE
05.12.2024

BUDAPEST
10.12.2024

BUCHAREST
21.01.2025

State of play:

In 2024 The Commission has opened, but not resulted yet the infringement procedures on political content against Meta[1] and X[2], and requested more information on political content from Google, Snapchat and TikTok[3]. The TTPAR has launched partially with the main launch expected by November 2024[4]. Commission has also issued the Guidelines for systemic risks on electoral behaviour, specifying how XYZ is considered[5].

Digital Services Act is being rolled out across Central and Eastern Europe with varying level if implementation – Poland has not appointed the Digital Services Coordinator yet[6], Romanian ANCOM has been thrown on choppy waters with managing potential elections infringements[7] with the use of digital tools. In many cases it is still a growing pain of how regulatory bodies should be restructured, which new institutions should be created, and how responsibilities should be divided and coordinated between the European and national levels.

This did not limit the attempts of foreign manipulation and potential election interference, with most obvious examples in Romania, Germany, and Slovakia. Most of them are connected to Russian aggression in the region and dubbed as „hybrid warfare tools" by the political leaders [8][9].

While the 2024 European Parliament elections were officially assessed by the Commission as free from serious security threats, worrying incidents still occurred. These included abuses of political advertising frameworks[10], untrue deepfake videos[11] shared in sensitive campaign moments, AI-driven disinformation[12], and violations of sanctions on Russian content[13].

Political Guidelines by the 2024-2029 European Commission for the new term of office include focus on election integrity and fighting foreign interference in the European Democratic Shield, regulation of the scope of influencer activities in the Digital Fairness Act and stronger enforcement of Digital Services Act to protect the fundamental rights.

1 https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373
2 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709
3 https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-youtube-snapchat-and-tiktok-recommender-systems-under-digital
4 https://www.consilium.europa.eu/en/press/press-releases/2024/03/11/eu-introduces-new-rules-on-transparency-and-targeting-of-political-advertising/
5 https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes
6 https://dig.watch/updates/poland-fails-to-appoint-dsa-regulator-after-eu-deadline
7 https://www.euronews.com/next/2025/03/26/tiktok-meta-google-and-x-invited-to-romanian-election-stress-test
8 https://cepa.org/article/making-russia-pay-for-hybrid-attacks/
9 https://neweasterneurope.eu/2025/04/04/poland-is-defending-europe-from-russias-hybrid-war/
10 https://www.accessnow.org/eu-political-ad-rules-wont-protect-european-elections/
11 https://www.reuters.com/technology/few-ai-deepfakes-identified-eu-elections-microsoft-president-says-2024-06-03/
12 https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-threat-analysis-2024-uk-and-european-elections
13 https://pism.pl/publications/eu-needs-better-monitoring-to-enforce-sanctions-on-russian-disinformation-online

Main topics and findings:

EU Introduces: Election Integrity

Why this issue?

Safeguarding election integrity is essential for maintaining citizens' trust in democratic systems, especially in Eastern European countries, which are particularly vulnerable to Russian disinformation campaigns.

Through the Digital Services Act (DSA) and initiatives addressing Foreign Information Manipulation and Interference (FIMI), the influence of the internet on election integrity has become a critical pan-European issue.

Countries are adopting varying approaches, delegating Digital Services Act implementation to differently organised bodies. Drawing lessons from their recent experiences, The European Commission is addressing this matter through Guidelines on election integrity, measures targeting platform abuses and development of election stress-tests and Member States roundtables. The issue is also under continuous discussion in the European Parliament, as evidenced by multiple sessions on January 15.

European institutions also provided regulation for online political advertising that is growing and extending its influence on elections rapidly. During the 2024 European Parliament campaign, CEE Digital Democracy Watch monitored spending in Eastern Europe and revealed major differences within the region. These differences were driven more by political than economic factors, with spending reaching almost €4 million in Hungary, €2.8 million in Romania, and €1 million in Poland.[14] The influence of online advertising on election outcomes is undeniable, as research shows that exposure to political ads from a specific party significantly increases the likelihood of voting for a given party, especially among people with less political knowledge and online literacy[15].

Critics say that lack of consistent framework across Europe creates opportunities for politicians to exploit regulatory gaps – running ads in the "grey sphere" (for example, on lifestyle profiles that appear apolitical), bombarding citizens with targeted messages, and using increasingly provocative language.

Unlike traditional media, oversight of digital platforms in most countries is fragmented, leading to inconsistencies and vulnerabilities.

Several non-governmental organisations have raised concerns regarding a recent emergency ordinance adopted by the Romanian government, which establishes the presidential election schedule and sets new rules for the electoral campaign. The main concern is the labeling of political materials in a way that could affect the fundamental right to freedom of expression. Under the new regulations, activities such as a private individual's personal post on a social network or a personal photo with a preferred candidate could be restricted, severely limiting the freedom of expression of ordinary citizens on social media. Civic organisations argue that the ordinance was

14 https://ceeddw.org/info-ponad-cztery-miliony-na-reklamy-polityczne-w-sieci-finisz-wolnej-kampanii-do-parlamentu-europejskiego-moze-byc-goracy/

15 Chu, X., Vliegenthart, R., Otto, L., Lecheler, S., de Vreese, C., & Kruikemeier, S. (2023). Do Online Ads Sway Voters? Understanding the Persuasiveness of Online Political Ads. *Political Communication*, *41*(2), 290–314. https://doi.org/10.1080/10584609.2023.2276104

enacted without public consultation and contains provisions that could infringe upon fundamental rights, particularly freedom of expression. Expert Forum emphasized that the ordinance was developed and discussed non-transparently, without involving key stakeholders, and bypassed the mandatory public debate stage[16]. They highlight that the draft was neither subjected to public consultation nor reviewed by the Economic and Social Council, as required by current legislation.

Civic organisations monitoring elections express concerns about allowing technology platforms to regulate political advertisements. Leaving the definition and final decision over what constitutes political advertisement to these businesses already results in several issues. First, these definitions are often tailored to suit the platforms' business models rather than establishing universal standards, creating loopholes that can be exploited. Second, inconsistent reporting across platforms hinders transparency, making it difficult to compare data between platforms and countries. Additionally, questions arise about which accounts should be monitored and held accountable.

Some of the public bodies indicated that the absence of a national representative is becoming increasingly problematic. There is a growing need for improved transparency in public spending, particularly regarding election campaigns. Politicians often believe that their online activities may go unchecked, which contributes to the lack of accountability. A notable example of this is when a Romanian politician publicly stated that they spent €0 on their online campaign, despite the clear impact digital platforms have on modern political campaigning[17]. This type of statement highlights the challenges in ensuring transparency in online political activities and the need for better oversight.

While campaign periods are certainly crucial, most participants emphasized that a significant portion of the issues surrounding electoral integrity and disinformation emerge during the pre-campaign phase. The early stages of an election cycle are increasingly being used to shape narratives and target voters in ways that may not be immediately apparent. It is important to recognize that disinformation is not solely the result of foreign influence. Politicians themselves contribute to the spread of false or misleading information, intentionally or otherwise. Therefore, combating election-related disinformation requires a more comprehensive approach that goes beyond identifying foreign interference and addresses the role of domestic actors as well.

> **The challenges related to the impact of technology on democratic processes are particularly evident in the context of elections, including online election campaigning. In today's electoral landscape, not only politicians and their audiences play important roles, but so does a range of intermediaries, including corporations that control access to and the dissemination of information. Ensuring that the electoral process remains both transparent and fair for all parties is increasingly difficult when not all actors in the online space have equal access to content processing.**

16 https://expertforum.ro/oug-alegeri-2025/

17 https://apnews.com/article/romania-raids-election-georgescu-1095e-5a6420af8c25208971a8855d664

Digital policy in Europe should therefore strive for the standardization of rights and management of access to the digital sphere. It is especially important to ensure access to online content for civil society organisations, researchers, and fact-checkers, who play a crucial role as guardians of democracy. Additionally, national electoral bodies should be equipped with the necessary tools to oversee compliance with the principles of fairness and equality in elections, including in the online space.

Sonia Horonziak PhD,
Institute of Public Affairs
(Poland)

Recommendations:

With the objective of securing an equal standard of protection across the entire EU, it is essential to establish a clear delineation of the European Commission's competencies versus those of member states. To achieve this, the following actions are crucial:

- **A more distinct division of responsibilities** between the EU and national governments is needed, alongside raising the threshold for independent disinformation/FIMI efforts.
- **Within the framework of the European Democracy Shield**, continuous support and broader promotion should be provided to the Code of Practice on Disinformation. Avoiding the overlap with existing digital regulations is key to the success of new legislation.
- **As national electoral organisations struggle to keep pace**, there is an increasing need for broader support in facilitating the exchange of regional best practices.
- **By combining enhanced platform accountability** with strengthened institutional capacity, the current political advertising framework should continue to grow in transparency and open access to spending data.

Content Moderation: *Why this issue?*

Digital Services Act promises a new age in transparency of content moderation. Still, a year after entering into force, some issues remain.

Local languages remain significantly underrepresented in social media content moderation policies. Major platforms prioritize widely spoken languages, often neglecting those with smaller user bases. This reluctance to invest in local-language moderation creates a fundamental gap in the enforcement of community standards, leaving harmful content unchecked while also failing to protect legitimate speech. Some platforms continue to automate these processes and lower the numbers of human moderators, with the notable example of X reaching 1 human moderator for every 297,458 users[18].

The consequences extend beyond the digital space – such disparities reinforce inequalities between larger and smaller linguistic communities, exacerbating democratic vulnerabilities. Without systemic change, this will contribute to a two-speed Europe, where certain countries benefit from robust content moderation while others are left to navigate an unregulated or inconsistently policed online environment.

A related concern is the disproportionate and arbitrary removal of content important for vulnerable groups, e.g. related to LGBTQ rights and abortion access. In the United States, Amnesty International has documented cases where Meta's platforms – Facebook and Instagram – have censored such content, including by blurring, blocking, or deleting advertisements from abortion pill providers[19]. Some suppliers had their accounts suspended or made less visible in search results and recommendations. These actions raise serious concerns about bias in automated enforcement mechanisms and the broader impact on access to essential information. When marginalised communities and vital healthcare resources face undue suppression, the problem extends beyond policy enforcement failures - it becomes a matter of fundamental rights and freedoms.

Such challenges have serious implications for public discourse. Misinformation campaigns distort public understanding of critical issues, while unchecked hate speech disproportionately affects vulnerable communities. Moreover, blanket demotion of political content risks silencing legitimate voices, particularly from marginalized or opposition groups, instead of targeting truly harmful content like active hate campaigns. Without clear and transparent guidelines, platform actions can inadvertently undermine free expression and erode trust in digital governance.

Even tech-savvy and empowered users often remain unaware of the mechanisms available for flagging harmful content, highlighting a critical gap in platform transparency. The lack of clarity around how automated moderation functions further exacerbates the issue, leaving users uncertain about when and how their reports are processed. Governments must take an active role in fostering open consultations with citizens, ensuring that moderation systems are both effective and understandable. Without such efforts, the fight against harmful content remains inefficient, undermining user trust and the integrity of online spaces.

18 https://www.socialmediatoday.com/news/x-has-significantly-fewer-moderation-staff/714650/

19 https://www.amnesty.org/en/latest/news/2024/06/united-states-social-media-companies-removal-of-abortion-related-content-may-hinder-access-to-accurate-health-information/

A local case study by The Panoptykon Foundation and Helsinki Foundation For Human Rights raised concerns about a proposal by Poland's Ministry of Digital Affairs to expand the powers of the President of the Office of Electronic Communications (UKE) to order the blocking of illegal online content. While intended to combat harmful material, the proposal lacks safeguards, risking excessive censorship and violations of free speech. Under the plan, UKE would have up to 21 days to decide on blocking requests, with immediate enforcement required. Although a procedure for restoring wrongly removed content exists, it only applies to legal violations, not platform policy breaches, leaving many users unprotected.

Discussion:

Discussions on online harms consistently highlight that minors and women are among the most affected groups. They are particularly vulnerable to harmful content, often facing severe emotional and psychological consequences. Exposure to online hate can lead to significant distress, damaging their self-esteem and well-being. In many cases, relentless criticism and targeted attacks push them to withdraw from public life, silencing their voices and limiting their participation in digital spaces. This not only harms individuals but also weakens diversity and inclusivity in online discourse, reinforcing the need for stronger protections against hateful content.

At the same time, news feeds and comment sections on political issues are flooded within seconds after publication with automated anti-democratic and anti-science opinions. Such campaigns are heavily funded in Eastern countries on which Russia is focusing its cognitive warfare, sometimes with the help of national governments, as seen in Hungary[20]. With the aim of undermining informed discourse, it distorts public opinion by creating the illusion of Eurosceptic majority stance[21]. Fake profiles are a pervasive issue in the digital ecosystem, often serving as tools for spreading disinformation, amplifying divisive narratives, and manipulating public opinion. Coordinated campaigns using fake identities can distort electoral outcomes, polarize societies, and erode trust in democratic institutions. Proliferation of such practices undermines the integrity of public discourse, leaving individuals and organisations vulnerable to misinformation.

20 https://www.tandfonline.com/doi/full/10.1080/09662839.2025.2468943?src=#abstract

21 https://www.euractiv.com/section/tech/news/fake-climate-news-thriving-as-politics-and-ai-turbocharge-disinformation-crisis/?fbclid=IwZXh0bgNhZW0CMTEAAR2p4ZzhNWLC1eXTc5ILwvpYHtG8EFAZdIk49WDQb-71sCo8m_cpaYxr3RNM_aem_2vIPMWYFune3e9u2Hgtlog

One major challenge is the sheer scale and sophistication of fake profile operations. As early as 2020, a report by Political Capital highlighted the urgent need to strengthen the resilience of critical infrastructure against attacks from non-human sources such as bots and trolls[22]. A 2025 investigation by the Atlantic Council revealed how the Russia-funded global Pravda network is leveraging advanced technologies to evade detection and exploit platform vulnerabilities by running influence campaigns and even altering seemingly neutral websites like Wikipedia[23]. Additionally, the challenges in consistent cooperation between platforms and regulators across Europe hinder efforts to address these threats effectively. Civic organisations working to expose and counter disinformation often face resource constraints, limiting their ability to match the scale of the problem.

Stakeholders, including civic organisations and policy experts, are voicing concerns about the current lack of transparency in platform regulations. They argue that platforms often prioritize business interests over societal responsibilities. A recent example of this complexity is the Oversight Board's 2025 decision to overturn Meta's initial choice to keep up reported posts criticizing a government's handling of a migrant crisis. The Board found that specific terms used in the post qualified as hate speech under Meta's rules and recommended their removal[24]. Key questions remain unanswered: How are harmful messages defined? What mechanisms exist to challenge platform decisions? And how are these decisions communicated to the public? The absence of clear answers creates an environment of uncertainty.

To address these issues, implementing transparent regulatory practices is essential. Platforms should adopt clear policies that define what constitutes harmful content, with a focus on targeting active hate speech rather than silencing political opposition. This would ensure that regulatory measures do not hinder democratic dialogue. Additionally, introducing a robust right-to-appeal process that includes human oversight is crucial. Automated systems, while efficient, often lack the nuance required to assess complex content, making human involvement indispensable for fair outcomes.

During election periods, the urgency of combating disinformation increases, highlighting the need for clear rules on collaboration with independent fact-checking organizations. Platforms' preference for Community Notes weakens the ability of transparent, internationally recognized fact-checking institutions to swiftly identify and correct political misinformation. Additionally, election-related content moderation requires fast-track decision-making processes and the involvement of independent monitoring bodies. The still under-promoted experiences with the Rapid Response System of the Code of Conduct integrated into the Digital Services Act framework, demonstrate the potential of bodies composed of experts with deep knowledge of local languages, social contexts, and electoral regulations, ensuring a nuanced approach to content moderation. Some argue that to safeguard democratic processes, independent bodies should be complemented by a judicial system capable of issuing final rulings on content legality. A rapid, expert-led response during elections is critical to preventing the manipulation of public debate while maintaining a fair and open digital environment.

Defining levels of harm in a standardised and transparent manner would enable platforms to better differentiate between misinformation, hate speech, and

22 https://politicalcapital.hu/pc-admin/source/documents/pc_defense_of_critical_communication_infrastructures_against_bot_and_troll_armies_in_cee_policy_recommendations_20200327.pdf

23 https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/

24 https://www.oversightboard.com/decision/bun-lj939ea3/

legitimate political expression. This approach would provide civic organisations and the public with clear benchmarks for accountability. By combining these measures, platforms can create a more inclusive, fair, and transparent regulatory environment.

”

The challenges posed by election integrity, content moderation transparency, regulatory impartiality, and AI governance require a nuanced approach that considers the region’s specific political landscape. Given that autocratisation poses a significant threat to free speech and that disinformation often originates from far-right and populist actors, as well as malign foreign actors such as Russia or China, supporting fact-checking initiatives, independent media, and civil society organisations could enhance democratic resilience. Policymakers must ensure that regulatory frameworks do not inadvertently suppress democratic voices but instead empower them to counter digital threats both at the European and Central European levels.

Lorant Gyori,
Political Capital
(Hungary)

Recommendations:

Ensuring fair and effective content moderation is essential to maintaining a safe and open digital space. While automated systems play a crucial role in combating harmful content, concerns over transparency, accountability, and public trust remain central to the debate. The scope that will be set by the Digital Fairness Act will face the harsh realities of complex implementation and technical challenges. To foster a content moderation system that is both effective and publicly trusted, the following measures should be prioritised:

- **Platforms should improve the clarity** of their content moderation decisions, ensuring users understand the reasoning behind removals or restrictions. Effective and politically impartial enforcement of the Digital Services Act is key to holding platforms accountable and reinforcing users’ rights.
- **While automated tools seem indispensable** in detecting and mitigating bot-driven disinformation, human users must be afforded clear and

accessible appeal mechanisms. Strengthening human oversight, expanding user support in smaller languages, and ensuring direct contact options are critical to maintaining fairness in moderation.

- **Policies should place those most affected** – such as minorities, women, and victims of online hate – at the core of content moderation strategies. Addressing the harms caused by fake profiles and hate speech will not only offer much-needed protection but also help build broad political consensus. Regular evaluations of these measures will ensure continuous learning and improvement.
- **As content moderation increasingly intersects with political discourse**, clear definitions and rules regarding political content are necessary to prevent accusations of censorship. Establishing transparent guidelines is the only way to maintain public trust, avoid political polarization, and ensure sustained support for content moderation policies.

Trust in Regulatory Bodies: *Why this issue?*

The process of enforcing European digital regulations is still evolving, with national and European bodies building expertise and, at times painfully, learning how to maintain citizens' trust. While acknowledging the issue in previous years, the EU favored a cautious approach to balance regulation and freedom of expression. A 2021 European Parliament Think Tank study highlighted the importance of strengthening civil capacity and supporting bottom-up initiatives, rather than solely relying on regulatory measures, in addressing disinformation[25].

Lack of consensus within the European Commission was clearly demonstrated by the reactions to Thierry Breton's 2024 letter to Elon Musk. While Breton emphasized the EU's focus on how content is managed and amplified, rather than regulating the content itself, a spokesperson revealed that the letter's timing and wording were not coordinated with other commissioners, which highlighted internal disagreement[26].

Moreover, the Commission has faced criticism for its transparency, especially in the case of political ads linked to von der Leyen's campaign that failed to disclose their connections, thus violating EU rules on political advertising[27]. Such incidents underscore the EU's struggles to balance transparency, internal coordination, and adherence to its regulatory frameworks, weakening public trust in its actions.

In some countries, doubts have arisen about the quality of disinformation research, with notable examples of departments within state-funded agencies being used to support party narratives through their analytical insights[28]. While there is broad support for blocking businesses profiting from fake news, public funding for fact-checkers remains less favored[29]. Eroding trust in regulatory bodies is also a part of a Russian strategy to undermine democratic capabilities. A report focused on security aspects recommends going beyond disinformation monitoring, advocating for more structured information flow between public institutions and more transparent cooperation with the media to ensure public awareness[30].

Discussion:

Trust is a two-way street, particularly when it comes to the relationship between regulators and civil society. Civic organisations often feel that state institutions are not up to date and lack the political will to foster resilience and fully grasp the emerging issues. Most criticism focuses on the slow pace and misguided action, especially regarding serious issues like hate speech and online violence. For organisations dedicated to tackling sensitive matters, limited mutual respect and recognition for their work results in a sense of alienation.

The discontent is evident in public calls for broader openness and citizen participation in the policy-

25 Colomina, C., Sánchez Margalef, H., & Youngs, R. (2021), The impact of disinformation on democratic processes and human rights in the world, European Parliament, https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653635

26 https://www.euractiv.com/section/platforms/news/civil-society-criticises-commissioner-bretons-approach-to-eu-digital-rulebook/

27 https://www.politico.eu/article/ursula-von-der-leyen-online-ad-campaign-eu-transparency-rules-european-commission-president-google-violation/

28 https://www.money.pl/gospodarka/wszystko-jasne-zapadla-decyzja-ws-finansow-pis-7065268486388256a.html

29 https://www.gov.pl/web/rcb/disinfo-radar

30 Report of the Disinformation Team, Commission for the Examination of Russian and Belarusian Influence on Internal Security and the Interests of the Republic of Poland in the Years 2004–2024, https://www.gov.pl/web/sprawiedliwosc/raport-zespolu-ds-dezinformacji-komisji-ds-badania-wplywow-rosyjskich-i-bialoruskich

-making process, where frustration grows over the direction of reforms and the insufficient coordination between various state institutions. Civil society is particularly concerned with the lack of expertise within governmental bodies, especially those tasked with addressing issues in the online space. While some progress is being made, there is a growing demand for more political will and strategic foresight to modernize regulatory frameworks.

Across the region, the shortcomings in governance and regulatory actions are evident in widely recognized cases. In Hungary, the government's takeover of media outlets and its failure to be held accountable for the content in the public space have undermined trust in regulatory institutions. In Romania, the inability to facilitate communication and coordination between different authorities, such as electoral committees, ministries, and media regulators, has exacerbated governance challenges. Poland, meanwhile, has faced controversies around state interventions in traditional media, particularly regarding campaigns using hate speech against minorities[31]. These examples reflect the broader issue: state authorities being not adequately equipped to address the complexities of digital governance.

In many Eastern European countries, bodies like electoral committees lack the resources and expertise to handle the complexities of monitoring digital political advertisement. This highlights the need for the governments to take more responsibility for their role in monitoring the spending, which should be supported by capacity building to enhance the efficiency of electoral oversight bodies. The establishment of stable, long-term positions for IT experts, as well as specialized training for staff, is crucial to ensure that oversight bodies are able to manage the challenges of the digital age effectively. By combining platform accountability with the development of institutional capacity, a more transparent and fair political advertising system can be created, thereby protecting democratic processes.

> **Even if properly enforced, the Digital Services Act's fines alone aren't enough to safeguard election integrity. Authorities must also implement robust data access and transparency requirements, allowing researchers and civil society to hold platforms accountable for misinformation campaigns that threaten democratic processes.**

Anda Bologa
Center for European Policy Analysis (Romania)

Recommendations:

To ensure trust in regulators, it is crucial that the public understands the rules and sees that public bodies adhere to them. We recommend the following actions:

- **Securing apolitical decision-making** – only ensuring that decision-making processes by the Commission and DSA implementation bodies remain free from political influence will grant citizens confidence that decisions are based on impartial and fair criteria, rather than political agendas.

31 https://oko.press/skarga-do-komisji-europejskiej-za-homofobie-tvp

- **More transparency in disinformation classification** – providing clear rules for classifying disinformation and fostering closer cooperation with the media is essential for showing regulators commitment to accuracy and fairness in managing online content.
- **Adequate funding for public bodies** – proper funding enables public bodies to be responsive and efficient in handling citizen concerns, improving their ability to take swift action and thereby enhancing trust in their effectiveness and accountability.

Communication Quality:

Prompt / why this issue:

Just like businesses, civic organisations and public institutions are heavily using the commercial online platforms to communicate with citizens. The example of Czech firefighters relying on X during the 2024 flood crisis to inform the public about the latest developments and security protocols highlights the nature of the problem. On the surface, being active on platforms which citizens already are actively using seems like the best way to ensure quick and efficient two-way communication. However, this approach leads to several issues, most notably reliance on algorithm preferences and uneven spread of information, excluding citizens who are less fluent in technology. The resulting dependence on private platforms also contributes to the neglect of local media and reduces direct human contact, which is crucial for maintaining public trust in institutions.

Several civic organisations encountered issues with overmoderation, particularly in cases where progressive content has been blocked. While the European Commission has initiated proceedings on such matters, their outcomes remain ambiguous, offering no clear resolution. This regulatory uncertainty leaves organisations vulnerable to arbitrary enforcement by platforms, which often fail to differentiate between harmful content and legitimate civic discourse. As a result, critical discussions on social and political issues face unjustified restrictions, limiting public access to diverse perspectives.

Beyond individual cases of moderation, platforms impose overarching restrictions on political content, shaping the visibility of civic debate. Sensationalized and aggressive content is amplified, while more nuanced or constructive political discussions struggle to gain traction.

Political advertising rules further complicate the landscape, as civic organisations - including humanitarian groups - are subjected to the same restrictions as political parties. This leads to unjust barriers for nonpartisan actors seeking to engage the public, as platforms frequently classify their activities as political in an inconsistent and arbitrary manner. The result is a digital environment where visibility is dictated not by the value of discourse but by the platforms' opaque enforcement practices.

Discussion:

Digital platforms wield significant power over the flow of information, affecting millions of users daily. However, problems with raging misinformation, inadequate protection of vulnerable groups and demoting content arbitrarily labeled as political highlight significant

gaps in current platform regulations. As we heard on numerous examples, one of the most pressing concerns is the arbitrary demotion of content classified as political, which disproportionately affects organisations engaged in political transparency and humanitarian aid. These restrictions limit their ability to reach audiences, communicate critical information, and hold politicians accountable. Meanwhile, platform algorithms operate without clear criteria, creating an opaque system where harmful narratives may thrive while legitimate civic engagement is suppressed.

Moreover, blanket demotion of political content can silence marginalized and opposition voices rather than curbing genuinely harmful material, such as hate campaigns. Without transparent and consistently enforced guidelines, platforms risk reinforcing biases and applying a "double standard" in defining hate speech. This lack of clarity not only weakens trust in digital governance but also allows bad actors to exploit loopholes while legitimate discourse is penalized. To prevent this, platforms must establish clearer definitions and enforcement mechanisms that prioritise accuracy and fairness over arbitrary restrictions.

Beyond platform policies, the demand for low-quality political content presents a broader societal challenge. Many organisations argue that addressing this issue requires a stronger focus on media literacy and civic empowerment rather than purely algorithmic solutions. Educating citizens on how to critically engage with digital content can reduce the impact of misinformation and foster a more informed electorate. To achieve this, public policy and NGO funding should prioritize long-term investments in media literacy programs, ensuring that organisations have both stability and flexibility to adapt their strategies and effectively engage the public.

Recommendations:

To enable quality exchange of ideas online, it is crucial to address over-moderation, enhance platform accountability, and reduce reliance on dominant digital intermediaries. The following actions are essential:

- **Safeguarding minority, NGO, and civic voices** – platforms must ensure that advocacy and transparency-focused initiatives are not arbitrarily classified as political content. Strengthening appeal mechanisms and involving civil society in moderation decisions can prevent undue restrictions.
- **Enhancing transparency in content promotion and labeling** – clear, publicly accessible rules on content visibility, labeling, and algorithmic ranking are needed. Independent oversight and regular transparency reports can help prevent bias and ensure consistent enforcement.
- **Reducing dependence on dominant platforms** – greater investment in media literacy programs and support for independent and local media is needed to diversify information sources. Regulatory incentives should encourage decentralized digital spaces and reduce structural reliance on a few major platforms.

AI and New Tools & Tactics:

Why this issue:

AI tools have been one of the biggest technological sensations in recent years, with still-unclear consequences for the job market. Their rapid development has drawn heavy investment, opened new commercial opportunities, and captured the public imagination.

In civic discourse, AI applications are expanding just as quickly. Some are deployed as solutions to moderation challenges – TrollWall, for instance, enables users to block harmful content. However, most commentators highlight the risks associated with these fast-evolving technologies, which are being leveraged both for aggressive market gains and for interference in public debate. The scale of these risks remains difficult to measure, but some cases have already proven deeply concerning and outright harmful.

These concerns have been reflected in early EU regulations, such as the AI Act, which introduced a four-tier risk classification each tool should be ascribed to: minimal, limited, high, and unacceptable. CEE Digital Democracy Watch pointed out during General-Purpose AI Code of Practice consultations that the current clause is overly vague and risks unintended harm to fundamental rights by relying on subjective terms, which may lead to overreach and misuse, particularly by governments seeking to suppress dissent. Without clear, objective definitions, the clause could disproportionately affect civic groups, minority voices, and legitimate political discourse, undermining democratic engagement. The challenge now is to determine where new applications fit within this framework and what regulatory action is necessary.

A particularly troubling development is the rapid rise of deepfake technology, with freely available tools making high-quality forgeries accessible to anyone. Some deepfake videos, often indistinguishable from satire, fabricate politicians' statements. Without clear labeling, such materials can mislead the public and distort political discourse. Even more alarming is the increasing prevalence of deep-fake pornography. These doctored images are frequently weaponized against women – especially female politicians – yet they continue to circulate widely on major platforms such as X, reaching millions[32].

Meanwhile, internet influencers have become a growing source of concern, operating with minimal oversight. While most creators avoid political content and focus on commercial activities, some play an active role in shaping civic discourse. A notable example is Hungary's Megafon, an influencer agency known for its substantial financial support of pro-government narratives. It has become one of Hungary's largest social media spenders, particularly during election campaigns, promoting content that aligns with Prime Minister Viktor Orbán's government. The Polish Office of Competition and Consumer Protection (UOKiK) has come under scrutiny for its failure to regulate political promotions by influencers like Filip Zabielski, despite growing concerns over transparency and accountability in political content on social media. Given the lack of transparency requirements and the strong influence of digital personalities on public opinion, similar outsourced political campaigning tactics are likely to emerge in other countries as well.

Discussion:

The rise of AI-generated content and influencer-driven political narratives presents an urgent regula-

32 This topic was covered in our policy report "Non-Consensual Sexualising Deepfakes – Threats and Recommendations for Legal and Societal Action" https://ceeddw.org/wp-content/uploads/2025/04/NCII_DeepFakes_ThreatsRecommendations.pdf

tory challenge. While digital tools offer new opportunities for civic engagement, they also create vulnerabilities that can be exploited to manipulate public discourse. The increasing use of deepfakes, voice cloning, and AI-generated propaganda threatens democratic integrity, yet enforcement mechanisms remain insufficient.

As political figures themselves engage in or tacitly endorse the spread of manipulated content, it becomes nearly impossible to convince the broader public that such practices are unacceptable. Unfortunately, politicians across the spectrum frequently use manipulated edits of their opponents without much reflection. Resulting erosion of trust not only weakens democratic debate but also undermines the legitimacy of electoral processes. A clear and enforceable policy on AI-generated content – whether through mandatory labeling or outright bans in political contexts – is necessary to prevent further deterioration of public trust.

At the same time, the unequal access to AI tools exacerbates existing disparities in civic participation. While well-funded organisations and political actors can harness sophisticated digital strategies to amplify their influence, smaller NGOs and independent watchdogs struggle to keep pace. The digitization of civil society requires more than just technological infrastructure; it demands stable funding, skilled personnel, and regulatory clarity to ensure fair access to digital tools. Without these measures, AI risks becoming another instrument of power consolidation rather than a tool for democratic empowerment. If regulators fail to address this imbalance, public discourse will increasingly be dictated by those who can afford to leverage emerging technologies at scale.

Ensuring the effective enforcement of the Digital Services Act in relation to AI tools and influencer activity requires both strong institutional oversight and broad public awareness. Clear guidelines, consistent monitoring, and sufficient resources must be allocated to national and European authorities to hold platforms accountable. Civic organisations and regulators play a crucial role in ensuring compliance, but they need dedicated funding and transparent enforcement mechanisms to do so effectively. Equally important is educating users about their rights and responsibilities regarding new technologies. Laws alone are insufficient if they are not accompanied by widespread education on digital literacy and media accountability. Public education campaigns, school curricula, and community initiatives can empower individuals to critically assess online content and engage more effectively with new tactics.

Developers of AI promise a transformative technology, which can be both a grave threat and amazing opportunity. In the hands of fraudsters or foreign influence operations, it can overwhelm us with misinformation. If utilized by public institutions and civil society, it can serve as a protective tool.

In any event, there is no easy way to limit the use of AI. No safety feature will fully prevent bad actors from utilizing current AI models after they are released, and we may soon get to the point where (to paraphrase an old quote) the only thing that stops a bad guy with an AI is a good guy with an AI.

Petr Gongala, Demagog (Czechia)

Recommendations:

As artificial intelligence increasingly shapes the digital public sphere, it is crucial to establish clear policies that ensure AI tools serve the public good rather than distort democratic processes. To maintain transparency, accountability, and democratic integrity, the following measures should be prioritized:

- **Expanding access to AI for monitoring and transparency** – AI-driven tools can expose disinformation and track harmful narratives, but access to them should not be limited to well-funded entities. Smaller civic organisations need support to use these tools effectively, ensuring they can monitor online spaces without facing resource barriers.
- **Ensuring transparency in the influencer economy** – influencers play a growing role in public debate but often operate without oversight, allowing hidden sponsorships to shape opinions. Those engaging in political discourse should be required to disclose financial ties, similar to political advertising rules. Balancing this with a focus on not infringing on political voices would prevent covert manipulation and help audiences assess credibility.
- **Setting limits on AI in political campaigns** – AI-generated content in politics risks large-scale manipulation and deception. While AI can enhance communication, it also enables deepfakes and micro-targeted persuasion. Policymakers must decide whether to ban AI-generated political content or at least enforce strict labeling and transparency requirements


AI