



The DSA Alone Won't Save Democracy —but Its Interplay with the Rule of Law Might


| **By Daniela Alvarado Rincón,**
Digital Democracy Policy Officer at DRI

Executive Summary

The EU's Digital Services Act (DSA) has created high expectations both in the EU and globally. As enforcement ramps up, attention is turning to whether the Act can meet those expectations. The German snap elections of February 2025 provided a key test, amid concerns of potential foreign influence and the misuse of online platforms, drawing lessons from previous elections, such as Romania's presidential election in November 2024. Issues like the misuse of AI, disinformation, political propaganda, biased algorithms, and irregularities in paid political ads all came to the forefront in the German vote.

This brief maps actions taken by key actors to protect online integrity during the German elections:

- | **The European Commission.** As the primary enforcer of the DSA, it indirectly oversaw the election, through ongoing cases, soft law initiatives, and co-regulatory tools, such as the Code of Conduct on Disinformation and the Rapid Response System.
- | **Germany's Digital Services Coordinator (DSC)** facilitated roundtables and stress tests with relevant stakeholders, supported data access, and established incident response channels.
- | **The European Board for Digital Services** published a DSC Toolkit for elections and is responsible for fostering cross-border cooperation and joint investigations by DSCs. The Board will soon release an annual report on best practices for mitigating systemic risks and advises the Commission on when to activate the crisis mechanism.
- | **National administrative and judicial authorities** played a critical role, particularly in incident response, determining the justiciability of the DSA, and establishing potential benchmarks for when an election may be considered compromised on the grounds of online integrity.
- | **Executive actors** are powerful drivers of media attention, as they can play a crucial role in elevating issues, thus placing them on the political agenda.



This analysis highlights advocacy opportunities, gaps, and challenges for civil society organisations (CSOs) and other stakeholders when engaging with the regulatory landscape and protecting online integrity during elections.

Germany's Snap Elections: A Test Case for the DSA and EU Digital Regulations

Although polls leading up to Germany's snap elections on 23 February did not suggest major swings in voter support (and the polls were confirmed by the results), the campaign still drew intense national and international scrutiny.

One key reason for this was the elections' broader geopolitical significance – widely seen as an indicator of how Germany, and by extension the EU, would position itself in relation to the new administration of President Donald Trump in the United States.

The United States loomed large in the background, because an administration official, Elon Musk, used his X platform to promote the AfD party, which the German security agencies have designated as “in parts rights-wing extremist”. Musk published posts on X and an OpEd in the German daily Die Welt in favour of the party, and interviewed its leader, Alice Weidel, in a supportive conversation streamed on his platform.¹ This open support by one foreign media owner and presidential administration official marked unprecedented foreign meddling in a democratic process.

At the same time, Meta suddenly accused fact-checkers, with which it had co-operated for many years (while itself making any decision on deletions) of censorship, and terminated fact-checking programmes in the United States.² Meanwhile, high-level US officials ramped up pressure against key EU digital regulations – the DSA, DMA, and AI Act – arguing that they posed a threat to US business interests and US notions of free speech.³

Given this backdrop, Germany's elections became a critical test case for the EU Digital Regulatory Framework, particularly the DSA. Following the controversial annulment of Romania's presidential election due to allegations of foreign interference on TikTok, the ability of the DSA to safeguard a fair and transparent online debate was under intense scrutiny.

- 1 Alima de Graaf, [“Fact check: How Elon Musk meddled in Germany's elections”](#), *DW*, 21 February 2025.
- 2 Csongor Körömi, Pieter Haeck & Daniella Cheslow, [“Zuck goes full Musk, dumps Facebook fact-checking program”](#), *Politico*, 7 January 2025.
- 3 Ramsha Jahangir, [“Tracking recent statements on the enforcement of EU Tech Laws”](#), *Tech Policy.Press*, 13 March 2025.



In this brief, we reconstruct the mechanisms through which different authorities worked to safeguard the online integrity of the German elections, mainly under the DSA framework.

We aim here to support other organisations working at the member-state level in advocating for stronger protections during elections. We also highlight key challenges and gaps – ultimately addressing a fundamental question: Is the DSA enough to tackle the online platform-related risks to elections?

The “Menu” Available in the DSA — and Beyond — to Protect Online Integrity During Elections

We mapped actions taken by key authorities during Germany’s snap elections, including by: (i) the European Commission; (ii) Germany’s DSC; (iii) the European Board for Digital Services; (iv) other national authorities; and (v) political authorities. Our analysis highlights potential advocacy avenues provided by these authorities, along with their respective gaps and challenges.

1. The European Commission – DG Connect


1.1. Indirect enforcement through ongoing open cases against VLOPs and VLOSEs

Although the Commission did not open new DSA enforcement cases specifically related to the German elections, it leveraged existing cases to monitor the efforts by very large online platforms (VLOPs) and very large online search engines (VLOSEs) to mitigate online risks to election integrity.

For example, amid claims that Musk might also support the AfD by changing algorithmic amplification of the party’s content on the platform, the Commission expanded its ongoing investigation into X’s compliance with the DSA.⁴ On 17 January, the Commission took a number of steps, including: (i) requesting internal documentation regarding the platform’s recommender system and any recent changes; (ii) issuing a retention order for X to preserve documents related to future algorithm changes between 17 January and 31 December 2025; and (iii) seeking access to X’s API, to examine the enforcement of content moderation and the virality of accounts.⁵

⁴ Anupriya Datta & Théophane Hartmann, [“Weidel-Musk X interview legal but could influence Commission’s DSA investigation”](#), Euractiv, 6 January 2025.

⁵ European Commission, [“Commission addresses additional investigatory measures to X in the ongoing proceedings under the Digital Services Act”](#), press release, 17 January 2024.



Similarly, last year, the Commission opened a case against TikTok for potentially failing to meet its obligations to identify and mitigate systemic risks to election integrity.⁶ Although the case is linked to TikTok's role in the Romanian elections, the Commission's press release made clear that the investigation would *"focus on the platform's management of risks to elections and civic discourse"* – in particular, related to its recommender systems and political advertising policies. This suggests that the investigation has implications for all EU elections.

Further, the Commission's retention order to TikTok, requiring the platform to *"freeze and preserve data related to actual or foreseeable systemic risks to electoral processes and civic discourse within the EU"* from 24 November 2024 to 31 March 2025, explicitly covers data related to the German elections.

Facebook and Instagram are also under investigation for the proliferation of deceptive advertisements, disinformation campaigns, and coordinated inauthentic behaviour on their platforms, particularly as these issues pose risks to civic discourse, electoral processes, and fundamental rights.⁷ The investigation is not linked to a specific case, so we can assume it applies to all EU elections.

Advocacy avenues

- ▶ Adding new findings into on-going investigations is often more efficient than trying to convince the Commission to initiate new cases altogether. Researchers, CSOs, and other stakeholders should consider focusing on contributing evidence to ongoing investigations.

Gaps and challenges

- ▶ Enforcement actions against VLOPs and VLOSEs carry significant legal implications, so these cases often take considerable time to process. As a result, this advocacy avenue is long-term, and is unlikely to resolve issues or incidents quickly (e.g., before an election).
- ▶ Transparency of enforcement cases is limited. Stakeholders and the public only have access to press releases, and not to the complete reasoning behind sanctions or the specific facts of each case. Furthermore, platforms and the Commission may negotiate and reach commitments to address concerns, but CSOs are not included in these discussions.

⁶ European Commission, ["Commission opens formal proceedings against TikTok on election risks under the Digital Services Act"](#), press release, 17 December 2024.

⁷ European Commission, ["Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act"](#), press release, 30 April 2024.

1.2. Enforcement through soft-law instruments: Guidelines on electoral integrity

In the context of the 2024 European Parliament elections, the Commission issued guidelines on online electoral integrity, outlining measures for VLOPs and VLOSEs to address many of the systemic risks related to elections.⁸ These guidelines were designed as a broader framework applicable to all EU elections. By translating the general provisions of Articles 34 and 35 into more concrete terms, the guidelines provide a crucial roadmap for monitoring platforms' compliance with the DSA.

Moreover, the guidelines address risks not covered by existing regulations, or those that are not yet in force. For example, **they suggest measures to tackle issues such as transparency of political advertising and the mitigation of generative AI risks.** These topics are also addressed by the political advertising and the AI Act, but those regulations are still not fully in force. By including these measures in a DSA enforcement document, the Commission provided a mechanism for addressing risks that remain unregulated.

In other areas, the guidelines go beyond the DSA. For example, **they introduce measures on data access and third-party scrutiny, encouraging VLOPs and VLOSEs to exceed the requirements of Article 40.** These measures promote ad-hoc cooperation, including the development of tailored tools, features, visual dashboards, additional data points to existing APIs, and providing access to specific databases.

Advocacy avenues

- The guidelines on electoral integrity can help CSOs and researchers design projects that assess how online platforms identify and mitigate systemic risks for civic discourse and democracy. Aligning research with these guidelines can make findings more actionable for enforcement.

Gaps and challenges

- While the guidelines provide detailed and concrete suggestions for implementing DSA obligations, they remain non-mandatory. Platforms can choose other means for achieving the DSA's objectives. Moreover, the guidelines do not contain benchmarks against which the success or failure of the suggested measures can be evaluated.⁹

- ⁸ European Commission, "[Communication from the Commission – Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35\(3\) of Regulation \(EU\) 2022/2065](#)", Official Journal of the European Union, 26 April 2024.
- ⁹ To address this gap, the Centre on Regulation in Europe (CERRE), a think-tank, published a paper proposing [benchmarks for evaluating the management of risks to electoral processes](#). Arcom, Booking, Google, Microsoft, Ofcom, and Tencent are member organisations of CERRE.

1.3. Enforcement through co-regulatory instruments: Codes of conduct on illegal hate speech and disinformation

In the weeks leading up to the German elections, the Commission finalised the integration of the Code of Conduct on Countering Illegal Hate Speech Online+ (CoC on Illegal Hate Speech) and the Code of Practice on Disinformation (CoC on Disinformation) into the DSA framework.¹⁰ This decision, long anticipated for the DSA, carries two significant implications. First, platform commitments under these codes will now be subject to annual independent audits (Article 37[1][b] DSA). Second, compliance with these codes is explicitly recognised as a valid risk mitigation measure (Article 35[1][h]), meaning refusal by a platform to participate without valid justification could be considered as an element in determining whether there has been a breach of their obligations under the DSA (Recital 104).

While the CoC on Illegal Hate Speech applies solely to online platforms, the CoC on Disinformation also includes other key stakeholders, such as the online advertising industry, ad-tech companies, fact-checkers, and CSOs. This broader inclusion has created an important space for platforms to engage and collaborate with these diverse stakeholders.

A key aspect of this collaboration is the **Rapid Response System (RRS)**, outlined in Commitment 37 of the CoC on Disinformation, which aims to strengthen coordination and collaboration among signatories during crises or elections. Due to its importance, in its opinion on the Code, the Commission stressed that the implementation of the RRS "will be thoroughly scrutinised" (p. 9).¹¹ **The Commission also highlighted that the RRS should cover all national elections (presidential and parliamentary) in member states** and, where possible, extend to regional and local elections, as well as referendums, within the EU. Moreover, the Commission stressed that, for cooperation to be meaningful, the RRS should be activated well in advance, cover all relevant languages, include swift reviews of the information received, provide detailed feedback, and ensure necessary follow-up actions are taken promptly, adapting to the time-sensitive nature of the electoral context.

¹⁰ European Commission, Policy and Legislation, ["The Code of Conduct on countering illegal hate speech online +"](#), 20 January 2025; European Commission, Policy and Legislation, ["The Code of Conduct on Disinformation"](#), 13 February 2025.

¹¹ European Commission, ["on the assessment of the Code of Practice on Disinformation within the meaning of Article 45 of Regulation 2022/2065"](#), 13 February 2025.

Advocacy avenues

- ▶ With the integration of the CoC on Illegal Hate Speech and the CoC on Disinformation into the DSA framework, and platforms now subject to audits of their CoC commitments, it is more important than ever to monitor their compliance. CSOs, researchers, and other stakeholders can monitor platforms' reports, and advocate for clear, detailed information covering both qualitative and quantitative key performance indicators.

Gaps and challenges

- ▶ During the transition from the Code of Practice to the Code of Conduct on Disinformation, signatory platforms reduced their commitments under the CoP by 31 per cent.¹² While all areas of the Code were affected, the most significant reductions occurred in measures supporting the fact-checking community (a 64 per cent decrease), followed by measures on political advertising and empowering the research community. This signals a lack of ambition in the Code, which is likely to undermine its effectiveness in holding platforms accountable and addressing disinformation threats.
- ▶ Many CSOs and fact-checking organisations involved in the Code's RRS do this work on a pro-bono basis, which places significant resource pressure on them for a time-consuming – yet crucial – activity.

2. Germany's Digital Services Coordinator


DSCs are the single points of contact for all matters related to the DSA in EU member states. As such, Germany's DSC, the Federal Network Agency (BNetzA), played an active role during the German snap elections. On 24 January, **BNetzA hosted a roundtable** with representatives from Google, LinkedIn, Meta, Microsoft, Snapchat, TikTok, X, national authorities, and CSOs to discuss election-related trends and risk mitigation strategies by VLOPs and VLOSEs.¹³

A week later, on 31 January, **BNetzA and the European Commission conducted a stress test with the same platforms**, where authorities presented various fictitious scenarios to assess the platforms' ability to respond swiftly to potential breaches.¹⁴ These scenarios

¹² Daniela Alvarado Rincón & Michael Meyer-Resende, "[Big tech is backing out of commitments countering disinformation - What's next for the EU's Code of Practice?](#)", DRI, 7 February 2025.

¹³ Bundesnetzagentur, "[Bun-desnet-za-gen-tur hosts Round Ta-ble with on-line plat-forms](#)", 24 January 2025; European Commission, "[Digital Services Coordinator for Germany hosts roundtable with online platforms](#)", 24 January 2025.

¹⁴ Bundesnetzagentur, "[Bun-desnet-za-gen-tur tests pro-ce-dures and ac-tion for in-fringe-ments of the Dig-i-tal Services Act](#)", 31 January 2025.



included information manipulation via deepfakes, coordinated inauthentic behaviour, incitement to online violence, and the suppression of online voices through harassment.¹⁵

Roundtables and stress tests are among the tools recommended in the **Toolkit for DSCs to enhance election preparedness**.¹⁶ The Toolkit encourages DSCs to establish early connections with stakeholders, VLOPs, and VLOSEs to share knowledge and resources. DSCs should also facilitate the publication of **voter information**, provide **DSA-specific guidance** for candidates, and **promote media literacy campaigns**. Crucially, DSCs are advised to **support research and data sharing**, monitor political advertising and ad libraries, and share lessons learned in post-election reports.

DSCs also have a role in **incident response**. The Toolkit advises DSCs to create incident protocols, establish networks, and ensure key escalation channels are in place to respond swiftly to complaints. Such escalation channels should involve all relevant stakeholders, including “CSOs, academic institutions, state institutions and bodies that can be mobilised in the case of elections for monitoring and knowledge-sharing purposes”.¹⁷ Moreover, under Article 53 of the DSA, DSCs are responsible for handling user complaints about online platforms’ non-compliance with the DSA. This effectively creates another avenue for addressing incidents.

Incident response by DSCs is particularly important for holding non-VLOPs and non-VLOSEs accountable. While such platforms are not subject to due diligence obligations, they must still comply with several key DSA requirements, such as notice-and-action mechanisms, complaint and redress procedures, and recommender system transparency. As smaller platforms are not part of codes of conduct, DSC coordination of incident response for these platforms becomes even more essential.

DSCs are advised to start these activities from one to six months before the election campaign period, and to continue for at least one month after the elections. In the event of snap elections, such as in Germany in this case, the Toolkit recommends that DSCs prioritise activities strategically, by focusing, for example, on engaging with stakeholders and setting up response systems.

¹⁵ Anupriya Datta, [“Germany gives Big Tech a passing grade in elections stress test”](#), Euractiv, 3 February 2025.

¹⁶ European Board for Digital Services (EBDS), [“DSA Elections Toolkit for Digital Services Coordinators. Instruments, Best Practices, and Lessons Learnt”](#), 21 February 2025.

¹⁷ EBDS, [Toolkit](#), p. 16.

Advocacy avenues

- ▶ CSOs and researchers monitoring online speech during elections may find it valuable to engage early with their country's DSC and take part in roundtables, tabletop exercises, and stress tests. Building coalitions with other CSOs can help strengthen these efforts and enhance their impact.
- ▶ Once the Delegated Act on Data Access is approved, DSCs will play a key role in facilitating access to non-public data from online platforms. Advocating for the effective implementation of Article 40(4) of the DSA will be crucial for researchers and CSOs monitoring online platforms.
- ▶ DSCs play a crucial role in incident response, particularly during elections, by facilitating escalation channels with other state institutions for urgent content assessment. The Toolkit highlights that CSOs and other stakeholders should be involved in these responses. This avenue is particularly important for incidents coming from non-VLOPs and non-VLOSEs.
- ▶ Complaints under Art. 53 serve as a crucial advocacy and legal tool for addressing both specific incidents and broader violations of the DSA by online platforms. Currently, nine complaints are pending before the German DSC, against TikTok, Meta, Google, YouTube, and LinkedIn.¹⁸

Gaps and challenges

- ▶ During the German elections, most DSC activities focused on engaging with VLOPs and VLOSEs. Non-VLOPs and non-VLOSEs, however, such as Telegram, also play a significant role in disseminating political content. Given their influence, CSOs and other stakeholders should advocate for a more comprehensive approach that includes these online platforms in the response framework.
- ▶ To effectively carry out their responsibilities, DSCs need adequate resources, and must maintain independence and autonomy from political pressure, especially during elections. Focus groups conducted by DRI last year revealed that political factors, such as setbacks in the Rule of Law or changes in government, often impact the pace and effectiveness of DSA implementation.¹⁹ Moreover, the messaging of DSCs differs, and they may have different perceptions of their mandates. After being criticised, rightly, for initially exaggerating the intervention possibilities,²⁰ the president of BNetzA expressed caution about the DSA's powers before the German election, emphasising in interviews that it was intended solely to target the dissemination of illegal content, and could only intervene after risks had materialised²¹ In contrast, the president of Romania's DSC (Ancom) took a far more assertive stance, even calling for the suspension of TikTok in Romania following the election controversy.²²

18 [DSC Database](#), Germany, EDRi, 2025.

19 Daniela Alvarado Rincón, Miriam Candelú & Tamera Allen, ["From Policy to Practice: DSA implementation in focus across the EU"](#), DRI, 30 October 2024.

20 The Agency corrected an initially misleading statement about trusted flaggers: Bundesnetzagentur, ["Bundesnetzagentur lässt erstmalig Trusted Flagger für Online-Plattformen in Deutschland zu"](#), 1 October 2024.

21 In an [interview with Deutschlandfunk](#) on 9 January 2025, Klaus Müller, Head of the Federal Network Agency, mentioned that the DAS *"does not regulate individual statements that people post on social media – that is a matter of individual reactions. Instead, the DSA asks: Is there a systemic risk of illegal disinformation? Are illegal contents being spread?"* Then, when asked about the possibility of the DSA acting as a preventive tool, he replied *"The DSA does not provide mechanisms for preventive intervention – meaning authorities cannot act ahead of time. This is a fundamental dilemma in a constitutional democracy. I understand the concerns and the criticism. Many would like a different system that allows more proactive action. However, the EU Commission – and to a lesser extent, the national Digital Services Coordinators – must act based on what has already happened. We can review and investigate incidents after the fact, and if necessary, enforce penalties through legal procedures."* Original in German, translation by the author.

22 Jon Henley, ["Romania regulator calls for TikTok suspension amid vote interference fears"](#), The Guardian, 27 November 2025.

3. The European Board of Digital Services (EBDS)

As an independent advisory group, the EBDS supports DSCs and the European Commission in overseeing VLOPs and VLOSEs by, among other activities: i) facilitating cross-border cooperation and joint investigations by DSCs; ii) publishing an annual report outlining best practices for mitigating systemic risks (Art. 35.2); and iii) advising the Commission on when to activate the crisis mechanism (Art. 36.1).²³

To our knowledge, the EBDS has not yet facilitated any cross-border investigations. We anticipate the publication of EBDS' annual report on systemic risks later this year, which will come amid warnings from multiple actors, including the DSA Civil Society Coordination Group, that recent VLOPs and VLOSEs Risk Assessment Reports "fail to adequately assess and address the actual harms and foreseeable negative effects of platform functioning".²⁴

Advocacy avenues

- The Commission has opened opportunities for CSOs and other stakeholders to discuss gaps and failures in VLOP and VLOSE risk assessments.²⁵ These discussions, along with the EBDS's annual risk mitigation report, provide a key avenue to improve the depth and effectiveness of these reports.
-

4. National judicial and administrative authorities

While not directly responsible for enforcing the DSA, **national security agencies** play a vital role in protecting election integrity online, particularly against foreign interference. During the German elections, the country's domestic intelligence service (BfV) established a task force to increase cooperation with national and international partners and to counter foreign influence operations.²⁶ Meanwhile, the Federal Ministry of Internal Affairs Ministry of the Interior launched the Central Office for the Detection of Foreign Information Manipulation (ZEAM).²⁷ This initiative, including also the Federal Foreign Office, the Ministry of Justice, and the Press and Information Office, focused on identifying and addressing


²³ Julian Jaursch, ["More than an advisory group: The European Board for Digital Services has key roles in DSA enforcement"](#), DSA Observatory, 23 February 2025.

²⁴ DSA Civil Society Coordination Group, ["Initial Analysis on the First Round of Risk Assessments Reports under the EU Digital Services Act"](#), March 2025.

²⁵ European Commission, ["Third roundtable with Civil Society Organisations on the implementation of the Digital Services Act"](#), 12 December 2024.

²⁶ Bundesamt für Verfassungsschutz, ["Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme"](#), November 2024.

²⁷ German Federal Ministry of the Interior and Community, ["Central Office for the Detection of Foreign Information Manipulation \(ZEAM\)"](#), 2025.



foreign disinformation and other hybrid threats. The Federal Office for Information Security (BSI) oversaw cybersecurity measures.

Beyond security agencies, **electoral authorities** are central to ensuring information about the electoral process is trustworthy. In Germany, the Federal Returning Officer, responsible for overseeing elections, actively worked to identify and correct misinformation.²⁸

Political financing institutions also play a key role when **campaign financing intersects with digital political advertising**. During the German election campaign, some organisations²⁹ and political figures, including then-candidate Friedrich Merz,³⁰ argued that **Musk's support for AfD on X could constitute an illegal party donation**. Under the Political Parties Act, election advertising by third parties is considered a party donation, and donations from non-EU countries are prohibited. How this rule applies in the digital context remains, nonetheless, uncertain.

Judicial authorities are another crucial piece of the puzzle. As enforcement of the DSA evolves, litigation is likely to become a crucial tool for rightsholders – including users and researchers – to clarify and strengthen its provisions. In January, DRI, with support by its legal partner, Gesellschaft für Freiheitsrechte (GFF), filed the first-ever lawsuit against X under Article 40(12) of the DSA.³¹ The case, which is still ongoing, seeks access to publicly available data to identify systemic online risks to the German snap elections.

Judicial authorities may also have the **power of an extreme measure – the annulment of elections**. The 2024 Romanian presidential election serves as the most significant recent example. Romania's Constitutional Court annulled the election, citing irregularities in the campaign, including foreign interference through TikTok and irregular online paid political ads, and alleging that these breaches “distorted the free and fair nature of the vote, compromised electoral transparency, and disregarded legal provisions on campaign financing”.³² The Court found that the disproportionate online exposure of one candidate affected the fundamental right to run for office, significantly distorting the election process. The case has, nonetheless, generated serious controversy.

²⁸ Die Bundeswahlleiterin, [„Fakten gegen Desinformation. Die Bundestagswahl 2025“](#). 2025.

²⁹ Aurel Eschmann, [„Gespräch zwischen Alice Weidel und Elon Musk könnte illegale Parteispende sein“](#), Lobby Control, 8 January 2025.

³⁰ Nette Nöstlinger, [“Musk will face consequences for interfering in German election, says front-runner Merz”](#), 14 February 2025.

³¹ Daniela Alvarado Rincón & Ognjan Denvoksvi, [“Why we're suing Elon Musk's X for German election data”](#), EUobserver, 27 February 2025.

³² Romanian Constitutional Court, Decision No. 32, [“Regarding the annulment of the electoral process for the election of the president of Romania in 2024”](#), 6 December 2024; Elena Lazar & Joan Barata, [“Will the DSA save democracy? The test of the recent presidential election in Romania”](#), Tech Policy. Press, 27 January 2025; John Albert, [“TikTok and the Romanian elections: a stress test for DSA enforcement”](#), DSA Observatory, 20 December 2025.

All other administrative authorities in a country have competencies under Art. 9 and Art. 10 of the DSA to alert VLOPs and VLOSEs about illegal content online.

Advocacy avenues

- Mapping national institutions and their areas of responsibility is essential for understanding their roles and authority in managing platform-related processes, such as issuing orders under Articles 9 and 10 of the DSA, escalating issues, or flagging content. CSOs should also be sensitive to the risks of overblocking or disproportionate administrative or judicial decisions that threaten the rule of law and democracy.

Gaps and challenges

- There is no universally accepted, evidence-based benchmark for determining when an election has been compromised from the perspective of online integrity. A weakness of the Romanian Court ruling was that it did not even propose such a benchmark of severity, even though it is obvious that not just any amount of disinformation renders an online campaign massively unfair. Assessing the impact of influence operations – whether foreign or domestic – on election outcomes remains a highly contested issue, often leading to tensions between national authorities, and potentially eroding public trust in elections and the rule of law.
- There are also concerns about the power of authorities to flag and order the removal of illegal content, as this power could be used as an excuse in certain political contexts to censor or threaten fundamental rights.

5. European and national executive authorities

The German elections attracted significant scrutiny from political/executive authorities. In Germany, the **Bundestag's Digital Committee** invited representatives from X, Meta, and TikTok to discuss the upcoming elections, but the platforms declined, arguing they were given too short notice.³³ On 22 January, German Minister of Internal Affairs Nancy Faeser met with major tech platforms to discuss measures against targeted disinformation campaigns, including those aimed at the election process or candidates, and hate crimes.³⁴ The Ministry held similar meetings with other stakeholders, including CSOs.

At the EU level, on 30 January, 12 member-states urged the European Commission to use its powers under the DSA due to “disruptive interventions in public debates during key

³³ *Ibid.*

³⁴ Chris Powers, [“Germany's interior minister calls on social media to protect election”](#), Euractiv, 22 January 2025.

electoral events” that, according to the letter, represented a direct challenge to EU’s stability and sovereignty.³⁵

Concerns about online integrity of the German elections also reached the European Parliament. On 4 January, German MEP Damian Boeselager wrote to EU Executive Vice President Henna Virkkunen, questioning whether Musk’s use of the platform X met the transparency requirements of the DSA. Commissioner Virkkunen replied, insisting that the EC “is determined to advance with the case expeditiously and, while respecting due process, adopt a decision closing the proceedings as early as legally possible.”³⁶ Other lawmakers posted similar concerns in their own social media channels. Eventually, on 21 January, the European Parliament held a debate on the need to enforce the DSA and protect democracy “against foreign interference and biased algorithms”.³⁷

Advocacy avenues

- Executive actors are powerful drivers of media attention and can play a crucial role in elevating issues, thus placing them on the political agenda. This, in turn, could make VLOPs and VLOSEs more aware and willing to activate all relevant mitigation measures.

Gaps and challenges

- An overly politicised discourse surrounding content moderation, curation, and online integrity risks overshadowing the technical and often nuanced challenges of mitigating systemic online threats to elections. The most recent example, of course, is the deliberate misuse of free speech arguments to oppose platform regulation.

So, Can the DSA Safeguard Election Integrity?


As the first regulation of its kind addressing online platforms – extending beyond illegal content to include due diligence obligations and requiring measures to tackle legal but harmful content and platform design risks – the DSA has set high expectations.

These expectations have, however, been met with growing skepticism, following the release of the first Risk Assessment Reports from VLOPs and VLOSEs – arguably the DSA’s most significant innovation.

³⁵ [“France, Germany, others urge EU Commission to protect elections in Europe from foreign interference”, Reuters, 30 January, 2025.](#)

³⁶ Cynthia Kroet, [“Lawmakers add pressure on Commission to investigate Elon Musk’s attempt to influence EU”, Euronews, 7 January 2025.](#)

³⁷ European Parliament (Debate), [“Need to enforce the Digital Services Act to protect democracy on social media platforms”, plenary session, 21 January 2025.](#)



The reports have disappointed, including in their assessment of systemic risks to civic discourse and elections. Key concerns include inconsistencies across the reports, a lack of meaningful data or analysis on the effectiveness of mitigation measures, minimal transparency about teams handling civic discourse and electoral risks, little to no information on platform design risks, and, crucially, the absence of stakeholder consultation.³⁸ Additionally, the reports tend to focus narrowly on elections, rather than on fostering a broader, healthier political discourse online.

But the DSA does not stand alone. It is part of a broader institutional framework designed to guarantee democratic resilience against both online and offline threats.

This brief only highlights the critical role that the DSA and national institutions play in safeguarding online integrity. Many other regulations, such as the European Media Freedom Act, the Political Advertising Regulation, the Digital Markets Act, and the AI Act, also contribute to this end.

The European Union acknowledges this broader understanding of democratic resilience through, for example, the proposed **European Democracy Shield**, a plan included in Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection Michael McGrath's mission letter and the Commission's 2025 work programme.³⁹ The Shield aims to address major threats to democracy in the EU, such as rising extremism and disinformation, though with a strong focus on foreign interference.

For CSOs, researchers, and other stakeholders working to create safer online spaces during elections, engaging with the broader regulatory landscape is essential. While advocating across multiple areas can be challenging, this strengthens democratic resilience beyond just digital issues. It also reinforces the DSA's role – not as a standalone tool wrongly seen as “limiting free speech,” but as part of a wider framework for protecting democracy.

³⁸ Orsolya Reich & Sofia Calabrese, [“Civic Discourse and Electoral Processes in the Risk Assessment and Mitigation Measures Reports under the DSA”](#), March 2025.

³⁹ European Council, [“Democratic resilience: Council approves conclusions on safeguarding electoral processes from foreign interference”](#), 21 May 2024.

Date: April 2025

About Democracy Reporting International

DRI is an independent organisation dedicated to promoting democracy worldwide. We believe that people are active participants in public life, not subjects of their governments. Our work centres on analysis, reporting, and capacity-building. For this, we are guided by the democratic and human rights obligations enshrined in international law.

Acknowledgements

This brief was written by Daniela Alvarado Rincón, Digital Democracy Policy Officer (DRI). This brief is part of the Tech and Democracy project, funded by Civitates and conducted in partnership with the European Partnership for Democracy. The sole responsibility for the content lies with the authors and the content may not necessarily reflect the position of Civitates, the Network of European Foundations, or the Partner Foundations.

This brief was designed by Julieta Jimenez.



This publication is available under a Creative Commons Attribution Non-Commercial 4.0 International license.