

Code of Conduct on
Disinformation – Report of
Democracy Reporting
International for the period
1 January 2026 –
30 June 2026

Table of Contents

Executive summary	2
Key Findings and Actions during the Reporting Period:	3
Reporting on the service's response during an election	3
Threats observed or anticipated at time of reporting:.....	4
Mitigations in place – or planned – at time of reporting:	6

Executive summary

Democracy Reporting International's (DRI) Digital Democracy Programme Unit focuses on identifying trends in online discourse and potential threats to the integrity of information during political events and electoral periods across Europe and beyond. Our Digital Democracy team monitors and audits key elements of the online information space (social media platforms, consumer AI products) and formulates policy recommendations for various stakeholders in the technology and society ecosystem, including lawmakers, tech platforms, and civil society organisations.

During the reporting period, DRI identified multiple threats to electoral integrity, centred on Hungary's 2026 parliamentary elections. These included unlabelled AI-generated political content and weak platform governance of it, cross-border coordinated inauthentic behaviour on X, and coordinated inauthentic news networks operating on Telegram outside the DSA's systemic risk obligations. Barriers to platform data access persisted throughout. These threats risked misleading voters, amplifying manipulation, and letting coordinated campaigns evade regulatory oversight. In response, DRI combined research, stakeholder engagement, advocacy, legal action, and public awareness to strengthen compliance with EU digital regulations and safeguard civic discourse.

Key Findings and Actions during the Reporting Period:

- **AI-Generated Content and Platform Governance:** DRI assessed how Meta, TikTok, and YouTube govern AI-generated content in political contexts across five dimensions. None of the three mandate political accounts to label such content. During Hungary's elections, we identified 2,043 posts from 22 accounts focused on Hungarian politics. Nearly three quarters contained AI-generated content, and 37.5 per cent of that content was left unlabelled. We reported 199 unlabelled posts to TikTok for non-compliance. We also provided comments to Meta's oversight board on the use of generative AI during the Hungarian elections.
- **Coordinated Inauthentic Behaviour on X:** A Berlin Court of Appeal ruling in February 2026 secured DRI's API access to X, which made pattern detection at scale possible. We first identified 46 cryptocurrency-themed accounts that pivoted to Hungarian political content, one amplified post tracing to the Russian Storm-1516 campaign. We also uncovered a larger network of 337 coordinated accounts based in Serbia, amplifying pro-Orbán content and disinformation about the opposition.
- **Inauthentic Networks on Telegram:** Using a replicable cross-platform dissemination methodology that we developed, we uncovered a coordinated network of 19 inauthentic news channels during Hungary's elections, operating across many languages with clear signatures of automation and shared branding.
- **Stakeholder Engagement and Awareness:** DRI convened more than 35 researchers, regulators, and fact-checking experts to sharpen detection and attribution methods and surface the regulatory gaps around Telegram and other non-VLOP platforms. We carried this further in an op-ed making the case for stronger Telegram accountability under the DSA.
- **Data Access:** DRI raised awareness about barriers to platform data access under the DSA. Through an EU DisinfoLab webinar on our litigation against X under Article 40(12). We shared practical lessons for researchers and civil society actors considering similar action.

Reporting on the service's response during an election

Reporting on the service's response during an election

Threats observed or anticipated at time of reporting:

1. AI-generated content in electoral contexts: policy and enforcement gaps

During the reporting period, DRI assessed how VLOPs govern AI-generated content in political contexts, as generative AI reshapes political communication and lets political actors create and spread synthetic content at scale and speed. VLOPs increasingly distribute this content, yet their policies remain inconsistent, opaque, and weakly enforced. We examined Meta, TikTok, and YouTube across five dimensions: actors, behaviours, content, degree, and effect. None of the three platforms mandate official political accounts to label AI-generated content, even though parties, candidates, and government actors reach larger audiences and carry greater authority than ordinary users. Most platforms do not treat AI-generated manipulative political content as a distinct electoral risk. TikTok addresses it under its integrity guidelines, but Meta and YouTube fold it into broader manipulated-media and misinformation frameworks. Automatic detection and labelling are applied inconsistently, with no clear triggers, leaving significant gaps in coverage.

We tested these gaps empirically during Hungary's 2026 elections. Using TikTok's search function and election-related hashtags, we identified 2,043 posts from 22 accounts that reached over 50 million views and either posted predominantly AI-generated content or presented as AI-generated personas, focused on Hungarian politics. Nearly three quarters of the posts (71.6 per cent) contained AI-generated content, and 37.5 per cent of that content was left unlabelled by the user or the platform. We reported 199 unlabelled posts to TikTok for non-compliance with its Edited Media and AI-Generated Content labelling requirements. The company removed 19 videos and one account and restricted the visibility of two posts. The remaining 177 posts stayed unlabelled despite our flagging.

Additionally, we submitted comments to Meta's Oversight Board on generative AI use during the elections. We argued that Meta's labelling standard sets a higher bar than the DSA Electoral Integrity Guidelines and called on Meta to align with the guidelines, cover the full electoral cycle, and sanction non-disclosure.

- [The governance gap: How online platforms are falling behind on addressing AI-Generated content during elections](#) | 06.05.2026
- [DRI's submission to Meta's Oversight Board on AI-generated political content in the Hungarian elections](#) | 13.05.2026
- [Beyond the Label: Generative AI on TikTok and the Limits of Platform Governance in Hungary's 2026 Elections](#) | 19.05.2026

2. Cross-border amplification and inauthentic networks on X

DRI investigated inauthentic behaviour on X in the context of Hungary's 2026 parliamentary elections. This research was made possible by a Berlin Court of Appeal ruling in February 2026, which required X to grant DRI data access through its API. Querying data at scale is what allowed us to detect patterns of coordination that manual browsing could not surface. Our initial observations identified 46 suspicious cryptocurrency and NFT-themed accounts commenting on Hungarian election posts. These accounts otherwise posted in English about crypto but switched to Hungarian to criticise opposition leader Péter Magyar and support Prime Minister Orbán and his Fidesz party. They amplified two posts attacking Magyar, one of which traced to the Russian Storm-1516 disinformation campaign. X's moderation response was inconsistent: when we reported 13 of the accounts, the platform stated they were not in violation of its rules, yet 45 of the 46 accounts were later suspended.

We subsequently identified a larger, higher-confidence network of 337 accounts based in Serbia. All were created in 2026 and amplified content promoting Orbán and Fidesz while spreading disinformation about Magyar, whose Tisza party ultimately won the election. The network showed clear automation signals: bulk account registration, mathematically regular posting intervals, duplicate messaging, and concentrated burst activity between 9 and 11 April. In several cases, these accounts made

up over 30 per cent of a post's reposts, quote tweets, or replies. The network appeared primarily focused on Serbian domestic politics and switched to Hungary only temporarily, pointing to cross-border amplification.

- [Initial Observations: 46 Suspicious Crypto Accounts on X Commenting on Hungarian Elections](#) | **02.04.2026**
- [Amplification across borders: Serbian networks promoted Orban on X in the leadup to Hungarian elections](#) | **28.05.2026**

3. Cross platform Information dissemination and Inauthentic Networks on Telegram

During the reporting period, DRI developed a replicable methodology to measure how coordinated information manipulation moves across platforms. FIMI campaigns increasingly operate across several services at once, exploiting regulatory gaps and evading detection. Messaging apps sit at the centre of this, with Telegram often serving as the coordination hub where narratives form before spreading to mainstream platforms. We piloted the methodology during the Dutch snap parliamentary elections of October 2025, tracing how Telegram content surfaced on Facebook and TikTok.

We applied this Telegram focus directly to Hungary's 2026 elections, where we uncovered a coordinated network of 19 inauthentic news channels operating across many languages, including most official EU languages, with a combined subscriber base of 167,000. The channels shared clear signatures of automation and coordination. Most relied on the same contact bot, posted at fixed intervals, and published within the same minute of one another.

- [Narratives in Motion: Measuring Cross-Platform Dissemination in a FIMI Context](#) | **15.01.2026**
- [Inauthentic news networks on Telegram: What we found during Hungary's 2026 elections](#) | **28.07.2026**

Mitigations in place – or planned – at time of reporting:

1. Code of Conduct on Disinformation

DRI continued its reporting efforts under the Rapid Response System of the Code of Conduct on Disinformation, actively collaborating with signatories. Between January and February 2026, DRI helped shape new [transparency guidelines](#) for the Rapid Response System under the Code. Co-chairing the Working Group on Elections alongside TikTok, we led negotiations for the non-platform signatories, producing a public Q&A on how the system works and internal guidelines on how signatories may display the content they report.

2. Raised awareness about threats and built networks with relevant stakeholders

On 16 July 2026, DRI hosted an [online roundtable](#) on countering FIMI and accountability gaps regarding Telegram. The event brought together more than 35 participants, including researchers, regulators, and fact-checking experts, to exchange approaches to detection and attribution and to examine regulatory gaps and enforcement challenges. The first session focused on detecting and attributing coordinated inauthentic behaviour on Telegram, drawing on collaboration with CeMAS (Center für Monitoring, Analyse und Strategie) and GLOBSEC. Discussion centred on how researchers surface coordination through signals such as matching channel names, synchronised posting, and improbable channel growth, and on the constraint that platform-level data access continues to place on this work. The second session brought together the European Fact-Checking Standards Network (EFCSN) and the Belgian and Slovak Digital Services Coordinators to examine accountability and the regulatory gaps around Telegram and other non-VLOP platforms. A recurring theme was that Telegram's lack of VLOP designation lets it escape the systemic risk obligations that would otherwise apply under the DSA.

We developed this argument further in an op-ed, drawing on our research into a multilingual Telegram network spreading Kremlin-aligned disinformation. We argued that Telegram's reach in the EU warrants closer scrutiny of its reported user numbers, and that VLOP designation would require it to assess and mitigate the systemic risks tied to coordinated manipulation.

- [What a Growing Telegram Disinformation Network Reveals About the DSA](#) | 31.07.2026

3. Communicating continued data access challenges

DRI continued to raise awareness about barriers to platform data access under the DSA. On 25 June 2026, we participated in a [webinar](#) hosted by EU DisinfoLab on our litigation against X to obtain platform data under Article 40(12) of the DSA. We shared how the legal process unfolded and what the ruling means for platform accountability and independent research. We also offered practical lessons for researchers and civil society actors considering similar action, at a moment when the European Commission had itself found X non-compliant on related grounds.