Code of Practice on Disinformation – Report of Democracy Reporting International for the period 1 January 2024 – 31 December 2024

Table of Content

Executive summary

Democracy Reporting International's (DRI) Digital Democracy Programme Unit focuses on identifying trends in online discourse and online harms during political events and electoral periods across Europe and beyond. Our Digital Democracy team conducts social media monitoring and formulates policy recommendations for various stakeholders in the technology and society ecosystem, including lawmakers, tech platforms, and civil society organizations.

Key Findings and Actions during the Reporting Period:

- Research into Murky Accounts: DRI's Digital Democracy Programme Unit researched how VLOPs and VLOSEs address tactics like inauthentic accounts, fake followers, and political impersonation. We published eight reports on "Murky Accounts" —accounts of questionable affiliation that present themselves as official government, politician, or party accounts when, in fact, they are not. Murky accounts do not declare themselves as fan or parody pages, and can be interpreted as attempts to promote, amplify, and/or advertise political content.
  We identified the systematic use of Murky Accounts in the 2024 European Parliament, French, and Romanian elections. We recommended that TikTok strengthen policies to prevent fan account abuse, improve enforcement of their policies to identify and address impersonation, require verified badges for political accounts, and enforce consistent guidelines, including pre-election reviews.

- Social Media Monitoring (SMM): DRI also conducted detailed analyses of online discourse during the EP Elections in eight member states uncovering instances of toxic speech and disinformation threats targeting historically marginalised groups and the integrity of elections. Our techniques included keyword searches, sentiment analysis, and advanced computational methods to glean a nuanced understanding of online discourse during both electoral periods.

- AI System Analysis and Recommendations: DRI continued its monitoring of generative AI risks, particularly from LLM-powered chatbots, through regular audits assessing their impact on elections. While some genAI systems (e.g., Gemini) implemented safeguards, others (e.g., Copilot, ChatGPT-4) still generated misleading electoral information, highlighting the need for consistent safeguards. We also track the use of AI-generated content during the 2024 EP Elections and formulated policy recommendations to address potential misuses. During the reporting period we also published a guide on auditing approaches for LLM risks and a report analysing chatbot alignment with human rights-based pluralism.

- Policy Recommendations, Engagement and Advocacy: DRI actively participated in the Rapid Response System under the Code of Conduct on Disinformation, advocating for the robust implementation of the DSA's risk mitigation framework and data access provisions. We worked directly with platforms to develop strategies for minimising online harms and pushed for greater transparency in content recommendation and moderation practices. Additionally, we engaged with EU stakeholders through roundtables, workshops, and conferences, fostering awareness and action on the DSA and broader digital governance issues.

IV. Integrity of Services

Commitment 14

In order to limit impermissible manipulative behaviours and practices across their services, Relevant Signatories commit to put in place or further bolster policies to address both misinformation and disinformation across their services, and to agree on a cross-service understanding of manipulative behaviours, actors and practices not permitted on their services. Such behaviours and practices, which should periodically be reviewed in light with the latest evidence on the conducts and TTPs employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework, include:

The following TTPs pertain to the creation of assets for the purpose of a disinformation campaign, and to ways to make these assets seem credible:

- 1. Creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts)
- 2. Use of fake / inauthentic reactions (e.g. likes, up votes, comments)
- 3. Use of fake followers or subscribers
- 4. Creation of inauthentic pages, groups, chat groups, fora, or domains
- 5. Account hijacking or impersonation

The following TTPs pertain to the dissemination of content created in the context of a disinformation campaign, which may or may not include some forms of targeting or attempting to silence opposing views. Relevant TTPs include:

- 6. Deliberately targeting vulnerable recipients (e.g. via personalized advertising, location spoofing or obfuscation)
- 7. Deploy deceptive manipulated media (e.g. "deep fakes", "cheap fakes"...)
- 8. Use "hack and leak" operation (which may or may not include doctored content)
- 9. Inauthentic coordination of content creation or amplification, including attempts to deceive/manipulate platforms algorithms (e.g. keyword stuffing or inauthentic posting/reposting designed to mislead people about popularity of content, including by influencers)
- 10. Use of deceptive practices to deceive/manipulate platform algorithms, such as to create, amplify or hijack hashtags, data voids, filter bubbles, or echo chambers
- 11. Non-transparent compensated messages or promotions by influencers
- 12. Coordinated mass reporting of non-violative opposing content or accounts

Measure 14.1	*Relevant signatories will adopt, reinforce and implement clear policies regarding impermissible manipulative behaviors and practices on their services, based on the latest evidence on the conducts, tactics, techniques and procedures (TTPs) employed by malicious actors, such as the AMITT Disinformation Tactics, Techniques and Procedures Framework.*

QRE 14.1.1 Relevant Signatories will list relevant policies and clarify how they relate to the threats mentioned above as well as to other disinformation threats.	**Murky accounts as a systemic threat to elections in the EU** In 2024, the DRI's Digital Democracy Programme Unit conducted research on how VLOPs and VLOSEs address TTPs, including the creation of non-automated inauthentic accounts, the use of fake followers or subscribers, and the impersonation of political candidates and parties. As part of this effort, we published **a total of eight reports** analysing the phenomenon of Murky Accounts on TikTok in the context of the 2024 *European Parliament Elections,* the *French snap elections*, the *Saxony and Thuringia regional elections in Germany*, and the *Romanian elections.* We argued that these accounts pose a serious risk to civic discourse and EU elections by misleading voters, distorting perceptions of political support, and bypassing TikTok's stricter policies on political accounts. A list of all Murky Accounts reports can be found in QRE 14.2.1. Across all reports, we recommended TikTok to strengthen their policies to prevent fan account abuse, introduce features to stop impersonation, require verified badges for political accounts in the EU, conduct pre-election reviews, and ensure consistent enforcement of their community guidelines. We met with TikTok representatives in Berlin on 12 August to discuss our findings and recommendations. **Social media monitoring (SMM) of elections** Through DRI's SMM across Europe and beyond we also identified trends in online discourse and detect instances of online harms, including disinformation, hate speech and toxic content. The following is a list of DRI's efforts in 2024 to detect impermissible online content, behaviours, and practices relevant to Commitment 14, as well as those polices recommended to mitigate the spread of such content. Outside of the European context, DRI also conducts social media monitoring in South America, the Middle East, and North Africa: - New Report: Anti-immigrant hate speech, AI solutions, detecting online violence against women and regional strategies | 23.01.2024 - From Engagement to Enmity: Toxicity and Key Narratives in EP Elections 2024 | 24.06.2024 - AfD v. RN: A Comparative Analysis of Far-Right Political Campaigning on X | 12.07.2024 - European Parliament Dashboard | 14.07.2024 - Local Insights, European Trends: Case Studies on Digital Discourse in the 2024 EP Elections | 13.08.2024

	• Election Integrity in the Digital Age: Online Risks and Recommendations for the Brazilian Municipal Elections | 05.2024 • Climate Crisis at the Polls: How Porto Alegre’s Mayoral Candidates Address Environmental Challenges | 20.09.2024 • Click Here for Controversy: Disinformation Narratives on YouTube During the 2024 EP Campaign | 25.09.2024 • Gender-Based Violence on X and YouTube in the São Paulo Mayoral Election | 16.10.2024 • Decoding politicians' social media campaigns in Rio de Janeiro and Recife | 11.11.2024 • Brazilian Municipal Elections 2024 Dashboard | 14.11.2024 • Understanding Digital Threats in Brazil: Media and Democracy Meta-Analysis | 12.2024 • Social Media Monitoring and Election Integrity in Brazil | 19.12.2024
Measure 14.2	*Relevant Signatories will keep a detailed, up-to-date list of their publicly available policies that clarifies behaviours and practices that are prohibited on their services and will outline in their reports how their respective policies and implementation address the above set of TTPs, threats and harms as well as other relevant threats. Such information will also be reported in the Transparency Centre. The list of TTPs will serve as the base for the TTPs to be reported upon and relevant Signatories will work within the permanent Taskforce to further develop and refine related indicators on the impact/effectiveness of their related actions. Relevant Signatories will also develop further metrics to estimate the penetration and impact that fake/inauthentic accounts have on genuine users and report at the Member State Level (including trends on audiences targeted; narratives used etc).*
QRE 14.2.1 Relevant Signatories will report on actions taken to implement the policies they list in their reports and covering the range of TTPs identified/employed, at the Member State level.	As part of the Rapid Response System, DRI identified 231 Murky Accounts, leading TikTok to take action on 159 for impersonation or inauthentic behavior. You can find all eight reports here: • Inauthentic Behaviour on TikTok - Concerning Accounts Supporting the AfD and Rassemblement National | 07.05.2024 • TikTok accounts with unclear affiliation supporting political parties and political candidates in the EU | 11.06.2024 • The big loophole (and how to close it): How TikTok's policy and practice invites murky political accounts | 22.07.2024 • Fourth report: Impersonation and inauthentic TikTok Accounts (French Elections) | 04.07.2024 • Disinformation Concern: Inauthentic TikTok Accounts that Support Political Parties | 24.05.2024 • Germany: TikTok only acts on Pro-AfD accounts when pushed to do so | 25.10.2024 • Manufactured Support: How Inauthentic Activity on TikTok Bolstered the Far-Right in Romania | 28.11.2024

	- Skirting the Rules: The Romanian far-right continues to enjoy inauthentic and prohibited support on TikTok | 04.12.2024

SLI 14.2.1		
TTP OR ACTION 1 [replicate for number of TTPs or actions reported]		
	SLI 14.2.1	
	Nr of instances of identified TTP	Nr of actions taken by type
Data	*We reported 231 Murky Accounts to TikTok*	*TikTok acted on 159 accounts*

IV. Integrity of Services

Commitment 15

Relevant Signatories that develop or operate AI systems and that disseminate AI-generated and manipulated content through their services (e.g. deep fakes) commit to take into consideration the transparency obligations and the list of manipulative practices prohibited under the proposal for Artificial Intelligence Act.

Measure 15.1	*Relevant Signatories will establish or confirm their policies in place for countering prohibited manipulative practices for AI systems that generate or manipulate content, such as warning users and proactively detect such content.*
QRE 15.1.1 *In line with EU and national legislation, relevant Signatories will report on their policies in place for countering prohibitive manipulative practices for AI systems that generate or manipulate content.*	Throughout 2024, DRI's Digital Democracy Programme Unit continued its monitoring of generative AI, conducting regular audits to assess the risks LLM-powered chatbots pose to elections and voters. We also provided guidance on the recently enforced AI Act, analysing its implications for elections and democracy. We tracked the use of AI-generated content by political parties in the EU during the EP Elections, compiling our findings into a report and dashboard. These insights were later presented at the European Parliament to EU stakeholders and Microsoft, where we advocated for stronger policies to prevent potential misuse.

During the reporting period, we also published a guide evaluating different auditing approaches for identifying and mitigating risks associated with large language models (LLMs), supporting researchers in conducting similar analyses. Additionally, we released a report assessing how well LLM responses align with our human rights-based definition of pluralism and their representation of different political perspectives.

Building on our findings on chatbots' ability to deliver accurate election-related information across multiple languages and regions, we developed policy recommendations examining the role of AI-generated content in the 2024 European elections.

Below is a list of DRI reports published during the reporting period related to these efforts:

- Are Chatbots Misinforming Us About the European Elections? Yes. | 11.04.2024
- When Misinformation Becomes Disinformation: Chatbot Companies and EU Elections | 07.06.2024
- AI Act Comes into Force: What It Means for Elections and DRI's Next Steps | 01.08.2024
- Ensuring AI Accountability: Auditing Methods to Mitigate the risks of Large Language Models | 14.10.2024
- Are AI Chatbots Reliable? Insights from Tunisia's 2024 Presidential Race | 02.12.2024
- The GenAI Factor at the Ballot Box | 12.12.2024
- An AI-Powered Audit: Do Chatbots Reproduce Political Pluralism? | 27.12.2024

Our research over the past year indicates that while some of the most widely used publicly available generative AI systems (e.g., Gemini) have implemented safeguards to mitigate misinformation—such as refusing to answer election-related questions—following our risk notifications, others, including Copilot and ChatGPT-4/4o, have yet to adopt a consistent approach. As a result, largely used language models continue to generate false or partially inaccurate electoral information.

IV. Integrity of Services

Commitment 16

Relevant Signatories commit to operate channels of exchange between their relevant teams in order to proactively share information about cross-platform influence operations, foreign interference in information space and relevant incidents that emerge on their respective services, with the aim of preventing dissemination and resurgence on other services, in full compliance with privacy legislation and with due consideration for security and human rights risks. [change wording if adapted]	
Measure 16.1	*Relevant signatories will share relevant information about cross-platform information manipulation, foreign interference in information space and incidents that emerge on their respective services for instance via a dedicated sub-group of the permanent Task-force or via existing fora for exchanging such information.*
QRE 16.1.1 *Relevant signatories will disclose the fora they use for information sharing as well as information about learnings derived from this sharing.*	• All identified TTPs, including murky accounts and ads violating TikTok's community guidelines on political advertising, **were flagged under the Rapid Response System of the Code of Conduct on Disinformation**. Additionally, in July 2024, we engaged in discussions with TikTok about their policies on impersonation and verified badges for political accounts, fostering collaboration and informing future enforcement measures. • **We directly shared our findings with relevant signatories to push for platform improvements.** For example, on 30 September we shared with Google our YouTube report on disinformation during the EP Elections, highlighting the platform's failure to use basic fact-checking tools like information panels and source indicators, despite its commitment to Measure 22.7 of the Code of Practice. Participating in and establishing fora for sharing information on the tools, tactics, and narratives deployed by disinformation actors is a key facet of DRI's Digital Democracy work. The following is a list of working groups, webinars, conferences, and roundtables attended during the reporting period, with DRI in the role of either organiser or presenter: • **Risk Assessment Roundtable. Anticipating the Storm: Mapping Digital Threats to the EP Elections | 04.04.2024.** DRI held an online exchange with participants from across EU institutions, platforms, international organisations and NGOs to assess risks to the information space before the EP elections. Participants were encouraged to share their thoughts, observations, and predictions about each topic in the context of the EP elections. • **EP Elections Social Media Monitoring Hub | March – June 2024.** In the lead-up to the EP Elections, DRI brought together a team of eight researchers from across the European Union to collaborate on social media monitoring. This group met regularly to discuss major risks and key narratives at the member state level. Each researcher contributed with an in-depth case study analysis.

	• Artificial Intelligence, Democracy and Elections **| 21.05.2024.** DRI presented at the International Seminar on Artificial Intelligence, Democracy and Elections alongside experts, academics, professionals and leaders to discuss the challenges and opportunities that the intersection between artificial intelligence, democracy and elections represents for the future of global democratic society. • Separating Voice from Noise: Insights from the 2024 EP Elections **| 24.06.2024.** The 2024 European Parliament elections took place against the backdrop of an evolving EU legal framework designed to address digital threats, though its mechanisms and impacts were still unfolding throughout the campaign period. In the aftermath of the elections, understanding the complexities of these digital battlegrounds became even more critical. Key questions emerged: How did political campaigns evolve online? Which political actors and media outlets shaped public discourse? What role did generative AI play in the electoral process? To explore these pressing issues, we provided comprehensive insights and analysis, examining the influence of digital platforms on election narratives, the spread of disinformation, and the challenges of mitigating hate speech. These findings were further discussed in our post-election webinar, where we unpacked the latest trends and their implications for policymakers, civil society, and digital platforms. • Webinar on Innovative Uses of AI by Civil Society in Europe **|26.06.2024.** On June 26, GLOBSEC hosted an online discussion highlighting the innovative uses of AI by civil society organizations in Europe, exploring tools and technologies from leading tech companies designed to support these initiatives, and addressing the ethical challenges and concerns associated with AI in civil society. DRI attended to share their researching findings. • SEEDS Webinar on Joint Lessons from the 2024 EP Elections **|24.09.2024.** In this webinar, the SEEEDS partners provide insights into the 2024 European Parliament elections based on the findings of civil society organisations and initiate the discussion on the way forward regarding future European electoral reforms and strengthening democratic processes at the EU level. • Focus groups with Digital Services Coordinators **| 27 September – 02 October 2024.** DRI held three focus groups between 27 September and 2 October 2024 with key DSA implementation stakeholders, including 3 CSO representatives, 1 academic, and 8 DSC representatives from 6 small-to-medium member states. We focused on DSA implementation status, challenges DSCs face, their collaboration plans with external stakeholders, particularly CSOs, and citizens' awareness of DSCs and digital rights.

- **Denver Democracy Series and Summit: 21st Century Elections: Technology, Disinformation/Misinformation & AI | 11.10.2024.** DRI joined the Josef Korbel School of International Studies-organised event, where DRI shared its research findings from the European Parliament elections.

- **Expert roundtable: Kick-Off for the Circle of Friends | 07.11.2024.** After nine months of DSA enforcement, the DSA Research Network's Circle of Friends held its inaugural meeting, taking stock of the DSA-related areas in need of further academic research. DRI attended to share their position on emerging topics around the DSA, identify needs for scientific insight and explore different methods to fill those gaps.
- **Delegated Act Roundtable| 25.11.2024.** Following the European Commission's released draft Delegated Act on Data Access, DRI hosted a roundtable for DSA stakeholders. In this roundtable, joined by 23 participants, including European Commission representatives, we presented DRI's position on the draft and gathered feedback and insights from other CSOs to build a shared understanding of the Delegated Act's implications for civil society research. This resulted in a joint submission of feedback for the EC. DRI thereby also contributed to policy formulation as lead organisation of this submission of feedback.

- **Distinguindo Vozes de Ruídos: Reflexões sobre as Eleições Municipais de 2024 | 03.12.2024.** The 2024 Brazilian municipal elections marked a new phase in online political communication, with AI risks overshadowed by the ongoing spread of disinformation, hate speech, and hostility toward traditional institutions. This webinar, organized by DRI in partnership with FGV Comunicação Rio, FGV Direito Rio, and Agência Lupa, supported by the EU, gathered experts to discuss disinformation, hate speech, online gender-based violence, and the impact of digital platforms on political campaigns and democracy.

- **The GenAI Factor in the 2024 Elections Report Event | 11.12.2024.** DRI attended the Kofi Annan Launch event at the European Parliament, sharing key insights from the report with relevant EU stakeholders.

- **From Posts to Polls - Lessons from the 2024 European Elections on Strengthening Young People's Engagement Through Effective Social Media Strategies | 12.12.2024.** This two-hour lunch event presented key findings from the policy study *From Posts to Polls: Lessons from the 2024 European Elections* on strengthening youth engagement through social media. The study examines young voters' preferences, behaviours, and motivations, alongside political parties' campaign strategies. The event featured panel discussions with academics, policymakers, and

<table>
<tr><td></td><td colspan="3">youth organizations, exploring the study’s implications for the next European Political Institutions' mandate, with a focus on the EU’s upcoming Youth Agenda.
• **Are AI Chatbots Reliable? Insights from Tunisia’s 2024 Presidential Race |12.2024.** DRI's Tunisia office presented in December their findings from their report into how chatbots answer electoral questions in the country. The Digital Democracy team attended and presented our findings from our earlier audits concerning the European Parliament elections and the importance of testing LLM responses.
• **DRI Media Coverage| 2024.** Our research and advocacy efforts garnered significant attention, with our reports and analysis being referenced by leading media outlets such as *Politico*, *Euronews*, *Forbes*, *EUobserver*, *Euractiv*, and many more. This media coverage furthers the impact of our work, shaping public discourse and informing key stakeholders—including policymakers, civil society, and the broader public—we continue to drive meaningful conversations on critical issues.</td></tr>
<tr><td rowspan="2">**SLI 16.1.1 – Numbers of actions as a result of information sharing** [change wording if adapted]</td><td colspan="3">Methodology of data measurement [suggested character limit: 500 characters]</td></tr>
<tr><td>Nr of actions taken (total)</td><td>Type of detected content</td><td>Other relevant metrics</td></tr>
<tr><td>**Data**</td><td></td><td></td><td></td></tr>
</table>

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. **Impersonation and inauthentic TikTok political accounts and political ads violating TikTok's policies**

European Parliament and French snap Elections: DRI submitted the first RRS notification under the newly created system drawing TikTok's attention to "murky accounts", a term we coined for accounts with unclear affiliations and questionable authenticity actively distributing and promoting politician and party content. Between May and July, we sent four RRS notifications flagging 116 TikTok accounts from 31 candidates/political parties across 15 EU member states. We looked at accounts supporting parties from across the political spectrum. 79.31% of the flagged accounts supported far-right candidates and political parties. As of September 2024, TikTok had removed 53 out of the 116 accounts we flagged.

- **Fourth report: Impersonation and inauthentic TikTok Accounts (French Elections) | 04.07.2024**
- **TikTok accounts with unclear affiliation supporting political parties and political candidates in the EU | 11.06.2024**
- **Disinformation Concern: Inauthentic TikTok Accounts that Support Political Parties | 24.05.2024**
- **Inauthentic Behaviour on TikTok - Concerning Accounts Supporting the AfD and Rassemblement National | 07.05.2024**

Romanian Elections: Across our two reports, we identified a total of 114 TikTok accounts violating the platform's rules on impersonation and/or displaying signs of coordinated inauthentic behaviour or fake engagement, all linked to candidate Călin Georgescu.

We also analysed TikTok's Commercial Content Library, which is intended to list all active ads on the platform. Despite TikTok's policy prohibiting political advertising—including ads that reference, promote, or oppose candidates or solicit votes—we uncovered 49 political ads supporting Călin Georgescu.

- **Manufactured Support: How Inauthentic Activity on TikTok Bolstered the Far-Right in Romania** | 28.11.2024
- **Skirting the Rules: The Romanian far-right continues to enjoy inauthentic and prohibited support on TikTok** | 04.12.2024

2. **Chatbots misinforming about the EP Elections, and prevalence of generative AI in the campaign**

After asking four chatbots ten questions in ten different EU languages (a total of 400 questions), DRI showed that chatbots are less reliable than search engines in providing users with electoral information. We asked ChatGPT 3.5 & 4, CoPilot and Gemini common questions about the European elections and all of them provided some totally or partially incorrect answers. This research brief was covered by Politico and Euronews, as well as other outlets. A follow-up study showed that Google adapted its Gemini chatbot which refused to answer election-related questions instead of giving wrong responses. The chatbots of OpenAI and Microsoft continued to provide wrong responses. We also examined the use of generative AI in political campaigns across eight EU countries.

- **When Misinformation Becomes Disinformation: Chatbot Companies and EU Elections | 07.06.2024**
- **Are Chatbots Misinforming Us About the European Elections? Yes. | 11.04.2024**
- **The GenAI Factor at the Ballot Box | 12.12.2024**

3. **Toxicity in political speech, disinformation narratives, and far-right online campaigning**

DRI monitored social media ahead of the European elections to track trends in online debates and identify country-specific instances of toxic content, disinformation, and manipulation. Through our Social Media Monitoring Hub, eight researchers analysed posts from political figures across Facebook, Instagram, X, and TikTok. We also explored WhatsApp activity across German public groups during the months leading up to the elections and examined political campaigns by AfD and RN on X. Our findings were shared via an interactive dashboard, three election briefs, and a final report.

- Local Insights, European Trends: Case Studies on Digital Discourse in the 2024 EP Elections **| 13.08.2024**
- AfD v. RN: A Comparative Analysis of Far-Right Political Campaigning on X **| 12.07.2024**
- From Engagement to Enmity: Toxicity and Key Narratives in EP Elections 2024 **| 24.06.2024**
- Unveiling the Surface: A Snapshot from Political Content on German Public WhatsApp Groups **| 04.07.2024**
- European Parliament Elections 2024, Dashboard **| 2024**

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

1. **Provided evidence to enforcement authorities on identified threats**

We provided the European Commission with our research and findings as evidence for ongoing enforcement processes. We shared our chatbot audits to support investigations into VLOPs and VLOSEs regarding their policies and enforcement of regulations on generative AI.

2. **Urged platforms to revise and strengthen their terms and conditions to effectively combat the identified threats.**

DRI published a brief elaborating on the policy implications of impersonation and inauthentic political accounts on TikTok, highlighting their threat to civic discourse and EU elections by misleading voters, distorting perceptions of support, and bypassing TikTok's stricter policies on political accounts. We recommended that TikTok and other VLOPs update their policies to prevent fan account abuse, implement features to stop impersonation, mandate verified badges for political accounts in the EU, conduct pre-election reviews, and ensure consistent enforcement of guidelines. Following the brief, we met with TikTok representatives in Berlin on 12 August to discuss our findings and recommendations.

The big loophole (and how to close it: How TikTok's policy and practice invites murky political accounts| 22.07.2024

3. **Raised awareness about threats and built networks with relevant stakeholders through webinars and roundtables**

Throughout our monitoring of the EP elections, we worked closely with key stakeholders. A key initiative was establishing the Social Media Monitoring Hub, staffed by eight researchers from France, Germany, Spain, Poland, Hungary, Italy, Sweden, and Romania, to track relevant country-specific issues and online threats in the months leading up to the election. We also raised public awareness about these threats through webinars and events. In April, DRI organised a 90-minute online exchange with 34 participants from EU institutions, platforms, and NGOs to assess risks ahead of the European Parliament elections. Breakout groups discussed emerging online threats, sharing insights and identifying potential risks. We continued these efforts with a post-election webinar to review how campaigns unfolded, identify opinion leaders, and explore the use of generative AI in the elections.

- **Separating Voice from Noise: Insights from the 2024 EP Elections | 24.06.2024**
- **Anticipating the Storm: Mapping Digital Threats to the 2024 European Parliament Elections | 18.04.2024**
- **DRI is Investigating Online Political Posts Surrounding the 2024 EU Elections | 25.04.2024**
- **Wie war das mit Desinformation bei der Europawahl? FAZ, 6.07.2024**