DSA elections guidelines – CMS contribution

1. Elections-specific risk mitigation measures

Q3: Do you agree with the recommended best practices in this section?
Yes.

Q4: What additional factors should be taken into account by providers of VLOPs and VLOSEs when detecting systemic risks related to electoral processes?
Based on the recent experience with the Slovak elections, it seems appropriate to consider adding media (providers) to the list of elements to be considered for the election-specific risk profile. Currently, the list of elements focuses on political entities, which are, however, often aided by various media providers. While media providers are to be offered protection against unwarranted removal of content by VLOPSEs, as per art. 17 EMFA, they may pose a significant risk to electoral processes and civic discourse (e.g. by inciting violence or spreading hate speech). As such, media providers generally have larger followings, which allows them to reach a substantial number of potential voters and significantly alter ongoing political discussions. Including media providers in risk profiles allows VLOPSEs to identify potentially problematic behaviour early on and appropriately tailor the subsequent risk mitigation measures with respect to fundamental human rights and media freedom standards.

Q5: Are there additional mitigation measures to be considered as best practices on the basis of their proven effectiveness mitigating risks to electoral processes?

Drawing on the practice of regulating linear media, it seems appropriate that VLOPSEs observe and are compliant with the electoral silence periods established by national legislation. Some EU Member States impose a silence period during which political campaigning, including the dissemination of partisan messages, is prohibited, to give voters a chance to reflect and decide ahead of Election Day (period of reflection), and to ease the campaign pressure on them before they cast their vote. Theoretically, all electoral activities during the silence period are banned, as is the dissemination of the results of public opinion polls relating to the elections. As most VLOPSEs offer the possibility of paid promotion of political content, it is appropriate to consider VLOPSEs subject to national legislation prohibiting any such activities online.

Additionally, the current version of the guidelines does not mention the implicit protection from terms of service and/or community content moderation standards enforcement enjoyed by verified users. Even though we consider the verification of users a useful risk mitigation measure, it seems that content moderation standards applied by all major VLOPSEs are constructed in a way that protects verified users from much of content moderation, especially when the content in question is published by a prominent political figure and features harassment or incitement to violence against another politically active entity. Even when reported, and otherwise removed or downranked, the content stays online with VLOPSEs claiming the protection of freedom of expression. It seems appropriate to recommend that VLOPSEs adapt their terms and service and/or community content moderation standards as well as their enforcement to tackle the misuse of their services during electoral periods.

Additionally, VLOPSEs should strive to enhance the integrity and transparency of their political advertising. For one, prior investigations revealed notable deficiencies in the verification processes employed by VLOPSEs, particularly concerning political ad transactions. For this, we recommend that VLOPSEs intensify their efforts to authenticate the identities of both sponsors and political advertising publishers.

Second, there is a pressing need to implement a more transparent labelling system for political advertising. While ads on VLOPSEs are commonly labelled as such, there remains a conspicuous absence of clear references to their political nature. Enhancing the visibility and clarity of these labels ensures that users can readily identify and discern political from commercial content.

With regard to addressing the proliferation of disinformation, VLOPSEs must establish collaborations with local source-rating organisations and integrate robust brand safety tools into their systems. This collaborative effort will curb the financial incentives for disseminators of disinformation, thereby mitigating its adverse impacts on public discourse and electoral processes.

Finally, considering the recent restrictions on data access for independent researchers coupled with the absence of a delegated act on data access under the DSA, it seems appropriate to consider a temporary scheme under which VLOPSEs share data with independent researchers and/or the DSCs. While recognising the importance of safeguarding user privacy and data security, allowing limited and regulated access to specific data sets pertaining to elections via licensed tools can significantly help detect and mitigate any potential risks related to electoral processes.

Q6: How should providers of VLOPs and VLOSEs measure effectiveness of their risk mitigation measures in a reliable and conceptually valid way for electoral processes?

An effective and timely review of the adopted risk mitigation measures is key when safeguarding a series of elections or elections occurring across the EU. Taking into account prior experience with VLOPSEs' reporting on their commitments under the Code of Practice on Disinformation or their bilateral agreements on safeguarding elections with national authorities, there is a clear need for a regular, comprehensive and granular exchange of data between national authorities (e.g. the DSCs) and VLOPSEs. Inferring from our findings from the 2023 Slovak general elections, we recommend VLOPSEs report relevant data at the MS level and include both qualitative and quantitative results (i.e. impact) of their risk mitigation measures, such as media literacy campaigns and information panels (e.g. reach, engagement, impressions, share rate, etc.)

2. Mitigation measures linked to generative AI

Q7: Do you agree with the recommended best practices in this section?
Yes

Q8: Which risks of generative AI for electoral processes should additionally be considered in this section?

In addressing the risks posed by generative AI to electoral processes, it is essential to consider the nuanced challenges associated with the inauthentic and authentic dissemination of manipulated media, particularly deepfakes, within VLOPSEs. One such risk involves the propagation of only segments or altered versions of original deepfake content, a tactic observed during the 2023 Slovak general elections. Our experience underscores a concerning trend wherein deepfakes, upon initial publication, are swiftly manipulated into various forms—such as screenshots, partial excerpts of the video or audio, or even phone recordings capturing the content displayed on a separate screen. These tactics serve to circumvent the conventional safeguards implemented by platforms for AI-generated content, as they often result in the loss of metadata crucial for content moderation purposes.

This method of disseminating manipulated deepfakes poses significant challenges to effective content moderation on VLOPSEs. By fragmenting and altering the original deepfake content, perpetrators exploit gaps in existing moderation systems, rendering traditional detection methods less effective. The absence of preserved metadata further complicates the task of identifying and mitigating the spread of manipulated media, as it hampers efforts to trace the origin and authenticity of the content.

Q10: What additional evidence-based best practices on risk mitigation for electoral processes related to the dissemination of generative AI content should be considered?

Drawing on our experience tackling terrorist content following the 2022 Bratislava shooting, we recommend VLOPSEs use hashing to prevent the re-upload of content that violates either their terms of service or national legislation pertaining to illegal content online. It seems, however, that VLOPSEs use hashing only for either extremely gruesome content or well-known terrorist materials and are unable to react quickly to content going viral in the days preceding the elections. Additionally, it is important that VLOPSEs engage in good faith with other providers of intermediary services and address the problem of cross-platform sharing of manipulative and/or illegal AI-generated content jointly by, for example, taking part in hash-sharing initiatives (e.g. GIFCT's hash sharing database for terrorist content).

In the context of the 2023 Slovak parliamentary elections, we have noted that despite pre-bunking and prompt statements by the Police Force, independent fact-checkers and experts on AI, VLOPSEs still allowed users to view, comment or share the viral piece of manipulative AI-generated content (although VLOPSEs did remove or label individual pieces of the said content, but the response is to be considered piecemeal and not systemic). For this, we consider hashing, cross-platform cooperation, and sufficient platform/search engine resources to be key to tackling the harms emanating from the dissemination of generative AI content.

When developing policies and measures tackling the creation and dissemination of potentially harmful AI-generated content, it seems appropriate to suggest that such measures take into account not only their impact on fundamental human rights but also their impact on other areas, such as education. For this, we recommend VLOPSEs design their policies and measures in a way that does not preclude creators from using AI-generated content for educational or commercial purposes.

Q11: What are best practices for providers of VLOPs and VLOSEs to ensure that their risk mitigation measures keep up with technological developments and progress?

VLOPSEs' risk mitigation measures ought to be scrutinised both internally, by the provider itself, as well as by the public, including researchers and civil society experts. To achieve this, we suggest VLOPSEs set up dedicated internal units dedicated to reviewing the risk mitigation measures after every election, including a rigorous analysis of their impact and technical feasibility (e.g. scalability of a particular risk mitigation measure). The reviews should be organised systematically, and frequently and contain quantitative and qualitative inputs.

As with all risk mitigation measures, VLOPSEs could set up dedicated information channels to foster an effective exchange of information between the VLOPSE and civil society organisations/DSCs, as these organisations will be at the very forefront of emerging issues concerning the dissemination of generative AI.

3. Cooperation with national authorities, independent experts and civil society organisations

Q12: Do you agree with the recommended best practices in this section?
Yes.

Q13: What other mechanisms should be considered to foster more effective collaboration with relevant stakeholders, such as national authorities and civil society organisations?

While timely communication and meetings concerning the electoral processes are of paramount importance for VLOPSEs to effectively mitigate any risks stemming from the design and functioning of their services, it seems appropriate, especially in light of the recent general elections in Slovakia, to recommend that VLOPSEs' dedicated units, or the already recommended points of contact, remain in touch and meet regularly in the days preceding and following the election day. Evidence suggests that the days preceding and immediately following the election day tend to be the source of potential risks to electoral processes. For this, it is necessary that the exchange of information between VLOPSEs and national authorities intensifies during this period so as to allow for a prompt response to any unforeseeable situations.

Taking into account the upcoming EU elections, it is necessary that VLOPSEs cooperate not only with the designated DSCs and competent authorities but also engage with the relevant prospective DSCs (the so-called proto-DSCs). Given the current state of designations, it is highly unlikely that all member states will have designated DSCs by June 2024. For this, it is necessary that effective collaboration between national authorities and VLOPSEs is ensured and no member state is left without an effective response mechanism (i.e. VLOPSE's point of contact).

Given the importance of local contexts, it seems appropriate that the draft guidelines recognise the pivotal role of the European Commission's Network of Electoral Authorities (ECNE) and the European Regulators Group for Audiovisual Media Services (ERGA) as key stakeholders, safeguarding the integrity and fairness of electoral processes.

Q14: Are there any additional resources that could help providers of VLOPS and VLOSEs identify relevant organisations/experts at the national level?

In order to assist providers of VLOPSEs in identifying relevant organisations and experts at the national level, several valuable resources from Slovakia are available. These publications offer insight into the processes and activities undertaken by state and CSO actors supporting election integrity. Furthermore, they provide a comprehensive analysis of the roles played by state actors in countering hybrid threats, not only in connection to elections:

Report by CMS: Monitoring of Platform Functionalities in Relation to the 2023 Elections to the National Council of the Slovak Republic: This report provides a detailed examination of platform functionalities during the 2023 elections, offering valuable observations and recommendations for platform providers.

https://www.rpms.sk/sites/default/files/2024-02/Monitoring%20of%20platform%20functionalities%20in%20relation%20to%20the%202023%20Elections.pdf

Report by CCHT: Analysis of the Dissemination of Misleading and Deceptive Content Related to the 2023 Elections to the National Council of the Slovak Republic: This analysis delves into the dissemination of misleading and deceptive content surrounding the 2023 elections, shedding light on the tactics employed and their impact on public perception.
https://www.hybridnehrozby.sk/wp-content/uploads/2023/11/Zaverecna-analyza-k-doveryhodnosti-volieb-%E2%80%93-EN-1.pdf

Report by CCHT: In-Depth Vulnerability Analysis of Selected State Administration Bodies to Hybrid Threats: This in-depth analysis examines the vulnerability of selected state administration bodies to hybrid threats, offering a comprehensive overview of potential risks and vulnerabilities. VLOPSEs can leverage the findings of this report to identify key stakeholders and experts in the field of hybrid threats, fostering collaboration and knowledge-sharing initiatives to bolster resilience against such threats.

https://www.hybridnehrozby.sk/wp-content/uploads/2023/10/Hlbkova-analyza-EN.pdf

4. During an electoral period

Q15: Do you agree with the recommended best practices in this section?
Yes.

Q16: Are there any additional measures that providers of VLOPs and VLOSEs should take specifically during an electoral period?

Evidence shows that electoral periods provide users with a plethora of highly divisive and polarising content. Its polarising nature incites borderline behaviour that often becomes illegal. It is thus foreseeable that an increase in such incidents is proportional to an increase in user reports concerning illegal content. For this, it is essential that VLOPSEs review their Notice and Action mechanisms (established under art. 16 DSA) and prioritise their user-friendly design and accessibility. This includes ensuring that these mechanisms are available in the national language of each Member State, thereby facilitating easy and efficient reporting for all users alike. By addressing such shortcomings and enhancing accessibility, VLOPSEs empower users to report electoral malpractices and effectively participate in safeguarding the electoral processes.

Drawing on the practice of regulating linear media, it seems appropriate that VLOPSEs observe and are compliant with the electoral silence periods established by national legislation. Some EU Member States impose a silence period during which political campaigning, including the dissemination of partisan messages, is prohibited, to give voters a chance to reflect and decide ahead of Election Day (period of reflection), and to ease the campaign pressure on them before they cast their vote. Theoretically, all electoral activities during the silence period are banned, as is the dissemination of the results of public opinion polls relating to the elections. As most VLOPSEs offer the possibility of paid promotion of political content, it is appropriate to consider VLOPSEs subject to national legislation prohibiting any such activities online.

Q17: How can rapid response mechanisms be improved for handling election- related incidents on VLOPs or VLOSEs?

The recommended incident response mechanism has the potential to significantly enhance the integrity of electoral processes. For one, such a mechanism facilitates quick identification of potential elections-related risks, such as FIMI, and allows for the prompt adoption of risk mitigation measures by VLOPs. Additionally, this mechanism would also facilitate the coordination and communication between national authorities and VLOPs.

Effectively, the incident response mechanism represents a two-way means of communication as it not only allows national authorities to report elections-related incidents but provides VLOPSEs with meaningful channels for DSA compliance (i.e. outlining what steps have been taken to safeguard the integrity of electoral processes).

Q18: What other mechanisms should be considered to foster more effective collaboration with national authorities and civil society organizations?

See response to Q10.

Q19: Are there any additional resources that help providers of VLOPS and VLOSEs identify relevant organisations/experts at the national level?

See response to Q14.

5. After an electoral period

Q20: Do you agree with the recommended best practices in this section?

Yes.

Q21: What elements should be included in voluntary post-election review by providers of VLOPs or VLOSEs to assess the effectiveness of their risk mitigation strategies?

Based on our experience overseeing the compliance of VLOPSEs with the DSA during the 2023 Slovak general elections, we consider early bilateral meetings with VLOPs crucial to maintaining electoral integrity. In June 2023, CMS held bilateral meetings with representatives of the most widely used VLOPs and presented them with a set of “asks” pertaining to the elections. These requirements respected the current European and national legislation and took into account their commitments under the Code of Practice on Disinformation. These requirements were presented to the VLOPs in the form of a questionnaire that the VLOPs submitted in the weeks following the election day. These questionnaires, covering 5 areas of interest, significantly narrowed down the scope of oversight conducted by the national regulatory authority and facilitated the setting up of targeted and measurable metrics for post-election review.

Additionally, as part of the post-election review process, VLOPSEs should provide a list of actors, stakeholders and organisations with which they cooperated during the elections so as to allow for an independent impact review. As part of this process, VLOPSEs should share with the DSCs the key metrics pertaining to the performance of each engagement with national actors (e.g. impact, reach, impressions, interactions, etc.).

6. Specific guidance for the elections to the European Parliament

Q22: What are your views on the best practices proposed in this section?

Overall, we welcome the best practices highlighted in this section and have complemented them throughout our contribution (see, for example, our responses to Q6 and Q14). From the regulatory perspective, it is important that VLOPSEs maintain close contact with prospective DSCs and share relevant information with national authorities.