DEM DEBATE
building an enabling environment for DEMocratic Debate

Mapping Report D2.1: European regulatory frameworks on election disinformation applicable to community-governed platforms

January 2025

Partners: WIKIMEDIA EUROPE, UNIVERSITY OF AMSTERDAM, eurecat Centre Tecnològic de Catalunya

Supporter: European MEDIA AND INFORMATION Fund Managed by Calouste Gulbenkian Foundation

Authors: Ronan Fahy (University of Amsterdam), Iris Toepoel (University of Amsterdam), and Joris van Hoboken (University of Amsterdam)

January 2025

1. Introduction

The DEM-Debate project (Building an Enabling Environment for Democratic Debate: Insights from community-governed platforms to cultivate a resilient election information ecosystem in Europe), seeks to examine how to increase resilience in the online information ecosystem to safeguard informed civic participation. It offers an interdisciplinary and transnational research of how certain community-governed platforms tackle disinformation, based on a case study of Wikipedia during the 2024 European Parliament elections. In particular, the DEM-Debate project seeks to develop new policy approaches to contribute to ensuring the information ecosystem surrounding elections in the EU is sufficiently insulated from the harmful effects of disinformation, with the research seeking to contribute to building an "enabling environment" for democratic debate.[1]

Previous legal research has mainly focused on the role of large commercial online platforms, operating a centralized-governed model (TikTok, Instagram, YouTube, and X), in the dissemination of disinformation during elections, and current legal policy is mainly focused on these online platforms.[2] However, there has been less in-depth legal analysis given to examining (non-commercial) community-governed platforms, and how they tackle disinformation during elections, and how disinformation regulation applies to these platforms. Building on work by scholars such as Grimmelmann,[3] Rozenshtein,[4] and Seering,[5] community-governed platforms broadly encompass those online platforms where content moderation is *generally* not undertaken

[1] See Council of Europe Steering Committee for Media and Information Society, *Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner* (Council of Europe, 2023), p. 35, https://edoc.coe.int/en/internet/11885-guidance-note-on-countering-the-spread-of-online-mis-and-disinformation-through-fact-checking-and-platform-design-solutions-in-a-human-rights-compliant-manner.html.

[2] See, for example, OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity* (2024), https://www.oecd.org/en/publications/2024/03/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_ff96d19f.html; M. Husovec, "The Digital Services Act's red line: what the Commission can and cannot do about disinformation" (2024) *Journal of Media Law*, 16(1), 47; S. Galantino, "How Will the EU Digital Services Act Affect the Regulation of Disinformation?" (2023) SCRIPTed, 20(1), 89; A. Strowel and J. De Meyere, "The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?" (2023) 14 JIPITEC 66; and J. van Hoboken and R. Ó Fathaigh, "Regulating Disinformation in Europe: Implications for Speech and Privacy" (2021) 6 UC *Irvine Journal of International, Transnational, and Comparative* Law 9.

[3] J. Grimmelmann, "The Virtues of Moderation" (2015) 17 *Yale Journal of Law and Technology* 42.

[4] A. Rozenshtein, "Moderating the Fediverse: Content Moderation on Distributed Social Media" (2023) *Journal of Free Speech Law* 217.

[5] J. Seering, "Reconsidering Self-Moderation: the Role of Research in Supporting Community-Based Models for Online Content Moderation", (2020) *Proceedings of the ACM on Human-Computer Interaction*, Vol. 4, 1. See also, J. Seering & S. Kairam, "Who Moderates on Twitch and What Do They Do?: Quantifying Practices in Community Moderation on Twitch", Proceedings of the ACM on Human-Computer Interaction, Vol. 7, 1.

in a centralised "top-down" approach, but rather, is "user-led moderation" undertaken by a community of users of the platform in a generally decentralised manner.[6]

The DEM-Debate project aims to address this gap by examining one such community-governed platform - Wikipedia – as a case study, and examining how it addresses disinformation during European elections, and how the European legal framework on election disinformation applies to such community-governed platforms. This is an opportune time to engage in this study, given that Wikipedia was recently designated as a so-called Very Large Online Platform (VLOP) under a new landmark piece of EU legislation, which addresses the risks associated with online disinformation, namely, the Digital Services Act (DSA).[7] Indeed, Wikipedia is the only non-profit community-governed platform designated under DSA, alongside the main commercial online platforms, including TikTok, Instagram, Facebook, YouTube, and X.[8]

The DEM-Debate project's legal research proceeds in four phases: first, a mapping of the existing and upcoming EU regulatory frameworks on online disinformation during elections that are applicable to community-governed platforms; second, a critical examination of Wikipedia, its policies on tackling disinformation during elections, and its designation as a VLOP under the DSA; third, a critical assessment of the application of EU regulatory frameworks on disinformation during elections to community-governed platforms, using Wikipedia as a case study; and fourth, developing policy recommendations for specific legislative and regulatory reforms of the EU regulatory framework to better counter disinformation during elections, building upon the findings of previous phases in relation to community-governed platforms' approach to disinformation.

This current Mapping Report (D2.1) forms part of the first phase of legal research. The purpose of this Report is to map the European regulatory frameworks on online disinformation during elections that are applicable to community-governed platforms. This is an essential step in understanding which regulatory frameworks on election disinformation exist in Europe, and how they might apply to community-governed platforms.

---

[6] A. Rozenshtein, "Moderating the Fediverse: Content Moderation on Distributed Social Media" (2023) *Journal of Free Speech Law* 217.

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). See generally, J. van Hoboken et al., Putting the DSA into Practice (Verfassungsbooks, 2023), https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf.

[8] See, European Commission, "DSA: Very large online platforms and search engines", https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

Notably, this first phase of the legal research is not designed to tease out the exact legal obligations for certain community-governed platforms, such as Wikipedia, or other decentralised community-governed platforms (such as Reddit, Mastodon), under election disinformation regulation; nor to address complex questions dependent on specific circumstances and platform structure, such as, should individual Mastodon "instances" be treated as distinct online platforms under the DSA; or does Wikipedia engage in "content moderation" under the DSA's definition of content moderation.[9] These are complex questions which require an in-depth analysis of the operation of a community-governed platform, which can vary widely in operation. Indeed, Wikipedia itself is a distinct type of community-governed platform, being mainly a user-edited online encyclopaedia. As such, the purpose of this current Mapping Report is to map the European regulatory frameworks on online disinformation during elections that are applicable to community-governed platforms. Crucially, in subsequent phases of the research, the practices of Wikipedia and its policies on tackling disinformation during elections (Task 2.3) will be reviewed; and then, the application of EU regulatory frameworks on disinformation during elections to community-governed platforms, using Wikipedia as a guiding lens, will also be assessed (Task 2.4).

The Report is structured as follows: first, in Section 2, some introductory concepts are set out. In Section 3, the regulatory frameworks on election disinformation under European Union (EU) law will be examined, including the landmark DSA, and regulatory guidance issued pursuant to the DSA, namely the 2024 Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes.[10] In addition, co-regulatory initiatives, such as the EU's 2022 Strengthened Code of Practice on Disinformation, will be discussed.[11] Further, the EU's 2024 Regulation on Political Advertising,[12] and the European Media Freedom Act 2024,[13] and also set out, as both have important provisions on disinformation. Next, Section 4 sets out the current Council of Europe legal framework on disinformation during elections, including case law of the European Court of Human Rights, and relevant Council of Europe standard-setting instruments.[14] While Section 5 sets out selected EU Member State national laws regulating disinformation during elections. Finally, Section 6

[9] See, DSA, Article 3(t).

[10] 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) 2022/206.

[11] The Strengthened Code of Practice on Disinformation 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[12] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising.

[13] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

[14] See, Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 5.

concludes. Through this examination, this research aims to contribute valuable insights into the evolving regulatory landscape surrounding online disinformation, specifically within the context of elections, ultimately enhancing our understanding of its implications for community-governed platforms within the EU.

2. The European legal framework, election disinformation, and community-governed platforms

Before setting the European legal framework applicable to election disinformation, it is important to set out what the notion of "disinformation" entails, and particularly, with regard to disinformation related to elections. First, and as recognised by various European and international bodies, the dissemination of online disinformation has been used to "undermine free and fair elections", can affect the "integrity of elections," and makes it more difficult to "protect the democratic process from manipulation".[15] Indeed, in the run-up to the 2024 European Parliament elections, the European Commission emphasised how the operation of online platforms in particular had given rise to a "heightened risk to election integrity" stemming from the proliferation of disinformation;[16] with the Commission being of the view that the growth of online platforms had made it "more difficult" to maintain the integrity of elections, and protect democratic processes from "disinformation and other manipulation".[17] Notably, government-spread disinformation is a distinct feature of election disinformation, with the Council of Europe's Committee of Ministers noting how online disinformation is spread through foreign governments' online "strategies and manipulation" to undermine free and fair elections.[18]

For example, the European Commission's Report on the 2019 European Parliament elections very much focused on foreign-government disinformation, and emphasised that foreign governments were "an important source of disinformation", with "manipulative efforts recurrently focused on

[15] Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns, 6 April 2022, https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2022)12.

[16] European 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, C/2024/3014, 26 April 2024, section 1.1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403014.

[17] European Commission, Communication on the European democracy action plan, COM(2020) 790 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790,

[18] Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns, 6 April 2022, p. 1, https://search.coe.int/cm/Pages/result_details.aspx?Reference=CM/Rec(2022)12.

politically sensitive topics and targeted EU audiences ahead of the elections".[19] However, the Report did conclude that "no large-scale covert interference operation in the 2019 elections ha[d] been identified."[20] And while further case-study research will be undertaken in later phases of this DEM-Debate project on the 2024 European Parliament election, for present purposes, it should be noted that the European Board for Digital Services' post-election report on disinformation during the 2024 European Parliament election stated there had been an "increase" in "EU-related-disinformation" in the run-up to the European Parliament elections, which amounted to 15% of the total detected disinformation in the month before the vote", which was "compared to 11% two months before the elections".[21] However, the initial assessment was that there were "no major or systemic incidents that disrupted the conduct of the European elections".[22] Similarly, the European Digital Media Observatory (EDMO) Task Force on 2024 European Elections "did not detect any major disinformation incidents during the elections."[23]

However, in late 2024, disinformation during elections in the EU came very much to the fore. In particular, during the presidential and parliamentary elections in Romania, the European Commission issued a landmark order under the Digital Services Act against TikTok, ordering the platform to "freeze and preserve data" related to "systemic risks its service could pose on electoral processes and civic discourse in the EU" from 24 November 2024 to 31 March 2025.[24] The Commission noted that it had received information "pointing to foreign interference from Russia" in the Romanian presidential elections, and the European Digital Media Observatory had "identified several disinformation narratives and tactics such as violation of electoral law, unmarked political content (including through influencers) and suspicion of coordinated inauthentic behavior".[25] Indeed, on 17 December 2024, the European Commission opened formal

[19] European Commission, Report on the 2019 elections to the European Parliament, COM/2020/252 final, p. 19, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0252.
[20] European Commission, Report on the 2019 elections to the European Parliament, COM/2020/252 final, p. 19, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0252.
[21] European Board on Digital Services, Report on the European Elections, p. 7, https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections. See, J. Albert, "TikTok and the Romanian elections: A stress test for DSA enforcement", DSA Observatory, 20 December 2024, https://dsa-observatory.eu/2024/12/20/tiktok-and-the-romanian-elections/.
[22] European Board on Digital Services, Report on the European Elections, p. 7, https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections.
[23] European Board on Digital Services, Report on the European Elections, p. 7, https://digital-strategy.ec.europa.eu/en/library/european-board-digital-services-publishes-post-election-report-eu-elections.
[24] See, European Commission, "Commission, online platforms and civil society increase monitoring during Romanian elections", 5 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243.
[25] See, European Commission, "Commission, online platforms and civil society increase monitoring during Romanian elections", 5 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243.

proceedings against TikTok for a "suspected breach" of the DSA, for failing to "properly assess and mitigate systemic risks linked to election integrity, notably in the context of the recent Romanian presidential elections on 24 November [2025]".[26] The European Commission President stated that "following serious indications that foreign actors interfered in the Romanian presidential elections by using TikTok".[27] How this investigation by the European Commission proceeds will be an important consideration during the later parts of the DEM-Debate research, especially the implications of any regulatory decision under the DSA for the regulation of elections disinformation generally.

The second point to address is what exactly is meant by disinformation. Crucially, and as will be discussed further below, there is no legal definition of disinformation under EU legislation. However, there are policy definitions that are used by EU institutions and regulatory bodies, such as the European Commission. And for the purposes of this Mapping Report, a widely-adopted definition is that of the European Commission, which defines disinformation as "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm".[28] This definition is also used in the 2022 Strengthened Code of Practice of Disinformation.[29] A crucial feature of this definition is the element of "intention," which distinguishes disinformation from misinformation. As such, false information that is spread with an intention to deceive is classed as disinformation; and this notion is the focus of this Mapping Report.[30] Of note, in later phases of the DEM-Debate project, when critically analysing the European legal framework on election disinformation as applied to community-governed platforms, there will be space to unpack and critique the Commission's definition of disinformation.

[26] See, Commission opens formal proceedings against TikTok on election risks under the Digital Services Act, 17 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487.

[27] See, European Commission, "Commission opens formal proceedings against TikTok on election risks under the Digital Services Act", 17 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487.

[28] European Commission, Communication on the European democracy action plan, COM(2020) 790 final. See also, European Commission, Tackling online disinformation: a European Approach, COM/2018/236 final, ("verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm").

[29] Strengthened Code of Practice on Disinformation 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[30] Notably, while there has been critique of this definition in particular, there is also critique of the notion of disinformation as a policy concept generally. See, for example, R. Ó Fathaigh, N. Helberger, & N. Appelman, "The perils of legally defining disinformation" (2021) 10(4) *Internet Policy Review* 1.

The third point relates to the European regulatory frameworks mapped in this Report. In this regard, European Union law and policy is first set out that is applicable to election disinformation. In addition, the Council of Europe (a separate European inter-governmental organisation) legal framework is also set out, which includes the European Convention on Human Rights (ECHR) and the case law of the European Court of Human Rights.[31] This is essential, as EU law is interpreted and applied consistent with the human rights guaranteed under the ECHR, and indeed the EU Charter of Fundamental Rights specifically mentions the ECHR. The Court of Justice of the EU has also confirmed that rights under the EU Charter, such as freedom of expression, should be given the "same meaning and the same scope" as freedom of expression under the ECHR, "as interpreted by the case-law of the European Court of Human Rights."[32]

And the final preliminary point relates to the concept of community-governed platforms. As mentioned above, building on work by scholars such as Grimmelmann,[33] Rozenshtein,[34] and Seering,[35] this Report uses the term community-governed platforms to broadly encompass those online platforms where content moderation is generally not undertaken centrally in a "top-down" approach, but rather, adopt a "user-led moderation" model, where content moderation is generally undertaken by a community of users of the platform in a decentralised manner.[36] Crucially, however, community-governed platforms may not be fully decentralised, in the sense that some content moderation decisions may ultimately be undertaken by a central host or provider of the platform, and as such, content moderation is "generally" community-led.

An example of a community-governed platform would be Reddit, which has been labelled by some as a "content moderation success story" (and contested by others).[37] Here, individual communities, known as "subreddits", have community-specific rules which are "created and

[31] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, 213 U.N.T.S. 221, Article 10.

[32] See Case C-345/17, Sergejs Buivids v. Datu valsts inspekcija, ECLI:EU:C:2019:122, para. 65 (2019).

[33] J. Grimmelmann, "The Virtues of Moderation" (2015) 17 *Yale Journal of Law and Technology* 42.

[34] A. Rozenshtein, "Moderating the Fediverse: Content Moderation on Distributed Social Media" (2023) *Journal of Free Speech Law* 217.

[35] J. Seering, "Reconsidering Self-Moderation: the Role of Research in Supporting Community-Based Models for Online Content Moderation", (2020) *Proceedings of the ACM on Human-Computer Interaction*, Vol. 4, 1. See also, J. Seering & S. Kairam, "Who Moderates on Twitch and What Do They Do?: Quantifying Practices in Community Moderation on Twitch", Proceedings of the ACM on Human-Computer Interaction, Vol. 7, 1.

[36] A. Rozenshtein, "Moderating the Fediverse: Content Moderation on Distributed Social Media" (2023) Journal of Free Speech Law 217.

[37] K. Roose, "Reddit's I.P.O. Is a Content Moderation Success Story", *The New York Times*, 21 March 2024, https://www.nytimes.com/2024/03/21/technology/reddit-ipo-public-content-moderation.html. However, see also, Huang et al., "Politically biased moderation drives echo chamber formation: An analysis of user-driven content removals on Reddit" (2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4990476.

enforced" by "community moderators" based on their community's "unique and often highly specific topics", and these moderators, according to Reddit, "perform the majority of community moderation actions across the platform.[38] However, in certain instances, Reddit may enforce its own central rules, such as Reddit's platform-wide rules, which includes provisions on CSAM (Child Sexual Abuse Material).[39] Similarly, on Wikipedia, which is another example of a community-governed platform, [40] the Wikimedia Foundation, which hosts Wikipedia, may engage in content moderation in certain instances.[41]

Notably, the term community-governed platform is not contained in EU law, and is used in this Mapping Report as a helpful concept (and not a strict definition) to distinguish a certain type of community-led moderation model, from those with a centralised form of content moderation. In this Mapping Report, the guiding lens is upon one particular community-governed platform – Wikipedia – where content moderation is mainly conducted by a community of volunteer editors. In the second phase of the DEM-Debate project, the organisational structure and content moderation practices of Wikipedia (and the Wikimedia Foundation) will be unpacked; but for the present purpose of this Mapping Report, the Wikipedia model of user-led moderation is used as a guiding lens.

3. EU regulatory framework on election disinformation

In this section, the EU regulatory framework that applies to election disinformation will be set out, examining the EU's Digital Services Act and other crucial regulatory measures, including the 2024 European Commission's Guidelines for VLOPs on the mitigation of systemic risks for electoral processes, and the Strengthened Code of Practice on Disinformation; while rules under

[38] Reddit, "Content Moderation, Enforcement, and Appeals", https://support.reddithelp.com/hc/en-us/articles/23511059871252-Content-Moderation-Enforcement-and-Appeals. See G. Corsi, E. Seger, S. Ó hÉigeartaigh, "Crowdsourcing the Mitigation of disinformation and misinformation: The case of spontaneous community-based moderation on Reddit" (2024) 43 Online Social Networks and Media, https://doi.org/10.1016/j.osnem.2024.100291 (examining Reddit's community-based content moderation and how it is a "potential tool in combatting disinformation").

[39] Reddit, Reddit Rules, https://redditinc.com/policies/reddit-rules.

[40] Wikipedia Foundation, "EU Digital Services Act information", https://wikimediafoundation.org/about/transparency/2023-2/eu-digital-services-act-information/.

[41] Wikimedia Foundation, "Wikimedia Foundation Digital Millennium Copyright Act ("DMCA") Policy", https://foundation.wikimedia.org/wiki/Policy:Wikimedia_Foundation_Digital_Millennium_Copyright_Act_(%22DMCA%22)_Policy; and Wikimedia Foundation, "EU Digital Services Act information", https://wikimediafoundation.org/about/transparency/2023-2/eu-digital-services-act-information/.

the EU's Regulation on Political Advertising 2024, and the European Media Freedom Act 2024, are also set out.

3.1 The Digital Services Act

Currently, the main EU legal instrument designed to protect individuals from the risks of election disinformation in the EU is the DSA. As mentioned in Recital 9 DSA, the goal of this Regulation is to ensure "a safe, predictable and trusted environment," to address the "dissemination of illegal content online", and crucially, to address the "societal risks that the dissemination of disinformation" may generate.[42] To pursue these general goals, the DSA sets out various obligations and liability exemptions for so-called "intermediary services".[43] What the scope is of these services, how these apply to community-governed platforms, which important obligations there are for these platforms, and how they are applicable to election disinformation on these platforms, will be discussed in the following sections.

3.1.1 Definitions under the DSA and community-governed platforms

First, it is important to set out some of the most important definitions under the DSA. Beginning with the scope of the DSA, as mentioned above, this Regulation applies to intermediary services. There are different kinds of intermediary services, with various obligations and liability exemptions depending on the role and category a service provider falls into. To make it more concrete, this means that the level of compliance is contingent upon how an intermediary service operates. Therefore, it is important to know to what category community-governed platforms may belong to determine which obligations under the DSA they are subject to.

There are three kinds of intermediary services that the DSA distinguishes, namely a "mere conduit" service,[44] a "caching" service,[45] and a "hosting" service.[46] In the context of this Report, and the concept of community-governed platforms, the last type of service is the most relevant.

---

[42] DSA, Recital 9.

[43] See DSA, Article 3(g), where an intermediary service "means one of the following information society services": a "mere conduit" service; a "caching" service; or a "hosting" service.

[44] See DSA, Article 3(g)(i) ("a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network").

[45] See DSA, Article 3(g)(ii) ("
a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request")..

[46] See, DSA, Article 3(g)(iii).

A hosting service is a service "consisting of the storage of information provided by, and at the request of, a recipient of the service".[47]

Within this definition of a hosting service, the DSA distinguishes "online platforms", which must meet certain additional obligations. Under Article 3(i) DSA, an online platform is "a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".[48] To clarify, while hosting services in general simply provide a technical function of storage of third-party information, this definition of an online platform makes it clear that services that exercises this activity for instance as a minor and purely ancillary feature of another service, cannot be defined as an online platform. Storing and distributing to the public needs to be a core feature to be defined as an online platform.

Notably, certain community-governed platforms would come within this definition of an online platform. For example, the European Commission has issued a 2024 Decision that states Wikipedia is an online platform, as it is a "hosting service within the meaning of [Article 3 (g)(iii) DSA] that stores and disseminates information to the public at the request of recipients of its service", and it is "therefore an online platform within the meaning" of the DSA.[49]

A further distinction within the category of online platforms are "Very Large Online Platforms" (VLOPs).[50] These VLOPs are online platforms which have "a number of average monthly active recipients of the service in the [EU] equal to or higher than 45 million".[51] Therefore, this designation is not based on how inherently risky the platforms are, but rather on the size of their user base. The distinction between online platforms and VLOPs is important, since VLOP designation places certain platforms under greater regulatory scrutiny, which makes these platforms subject to the most extensive risk management responsibilities. Wikipedia, for example, is one of the 25 designated VLOPs under the DSA.[52] It is also important to note that it

[47] See DSA, Article 3(g)(iii).

[48] See DSA, Article 3(i).

[49] European Commission, Commission Decision designating Wikipedia as a very large online platform in accordance with Article 33(4) of Regulation (EU) 2022/2065 of the European Parliament and of the Council, 24 March 2023, C(2023) 2742 final, para. (1).

[50] See DSA, Article 33 (Very large online platforms and very large online search engines).

[51] See DSA, Article 33(1) DSA.

[52] See European Commission, "Supervision of the designated very large online platforms and search engines under DSA", https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.

does not matter whether one of these intermediary services is established in the European Union or not: the rules in the DSA apply to all intermediary services "located in the Union, irrespective of where the providers of those intermediary services have their place of establishment".[53]

3.1.2 Micro- and small enterprise exception

As discussed, intermediary services are subject to a range of general rules under the DSA, including relating to liability, orders to act against illegal content, orders to provide information, designate a point of contact for certain public authorities, designate a point of contact for recipients of the service. Hosting services are subject to additional obligations, including establishing a notice and action mechanism; while online platforms are subject to even more obligations, such as establishing internal complaint-handling systems. As follows from Article 15 DSA, all intermediary services, unless they qualify as micro- or small firms, are required to make publicly available annual reports on content moderation that they are engaged in, the so-called "transparency reporting".[54] However, there are a number of exceptions for what are called micro- and small enterprises.[55,]

In order to define micro and small enterprises, the DSA relies upon the definition of micro and small enterprises previously defined by the European Commission under a 2003 Recommendation.[56] As such, small enterprises are defined as enterprises which "employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed 10 million EUR".[57] While a micro enterprise is defined as an enterprise which "employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed 2 million EUR".[58] When a small- or micro-enterprise qualifies as an online platform, then, according to Article 19 DSA, certain provisions applicable to online platforms do not apply to them. However, if a micro- and small enterprise qualifies as a VLOP, it remains under the obligations mentioned in the VLOP sections of the DSA. Further, it should be noted that an enterprise is defined as "any entity engaged in an economic activity, irrespective of its legal form".[59]

---

[53] See DSA, Article 2(1).

[54] See DSA, Article 15.

[55] Also see the exception of micro- and small enterprises in Article 19 DSA for exclusion of these platforms for the obligations that apply to online platforms; Article 29 DSA.

[56] European Commission, Commission Recommendation concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC, 6 May 2003, https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng.

[57] European Commission, Commission Recommendation concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC, 6 May 2023, Article 2.

[58] See the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Article 2.

[59] European Commission, Commission Recommendation concerning the definition of micro, small and medium-sized enterprises, 2003/361/EC, 6 May 2003, Article 1.

As such, where a community-governed platform would come with the definition of a micro or small enterprise, it would not be subject to the whole host of rules under the DSA which other online platforms are subject too. However, in order to qualify as a micro or small enterprise, a community-governed platform would need to (a) employ fewer than 10 people and have annual turnover of less than 2 million EUR, or (b) employ fewer than 50 people and have annual turnover of less than 10 million EUR.

3.1.3 Community-governed platforms and the DSA

As mentioned above, community-governed platforms encompass those online platforms where content moderation is generally undertaken by users of the platform in a decentralised manner. For instance, according to the Audit Report of Wikipedia under the DSA, it is within a "unique, decentralised nature of Wikipedia and the volunteer community governance model, where most content moderation decisions are taken at the community level".[60] Thus, the concept of community-governed platforms is not limited by the services these platforms offer, but by the way content moderation is exercised within these platforms. In other words, we can define more specifically what a community-governed platform is based on the definition and different kinds of content moderation.

Crucially, the DSA includes a definition of content moderation, and is defined as "activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account."[61] Within this definition, content moderation could be either automated or manual.

Notably, the definition of content moderation mentions that it is undertaken by "by providers of intermediary services". As such, it remains an open question whether this definition would capture content moderation undertaken by platform-users in a community-governed platform; but it would seem clear that it would capture the content moderation undertaken by the online platform itself, or its host.

---

[60] See, Wikimedia Foundation, "Wikipedia DSA Audit Report 2023-24 Public", under article 12, entry 2, https://upload.wikimedia.org/wikipedia/foundation/6/6c/Wikipedia_DSA_Audit_Report_2023-24_Public.pdf.

[61] See, DSA, Article 3(t).

3.1.4 Provisions under DSA applicable to election disinformation

The first point that must be made about the DSA and disinformation, is how the DSA is being presented as the most important EU tool against disinformation. Following its adoption, the European Commission described the DSA as setting out an "unprecedented new standard" for the accountability of online platforms regarding "disinformation."[62] Indeed, the Commission's President has framed the DSA as the main EU legal instrument to "protect European citizens from targeted disinformation."[63]

However, what also needs to be pointed out, and what is very important to emphasise, is that when reading the DSA, it is apparent that disinformation is nowhere mentioned in any of its actual provisions. Crucially, disinformation is also nowhere defined anywhere in the DSA. It is only mentioned in some recitals. Crucially, Recital 9 DSA states that one of the purposes of the DSA is to address the "dissemination of illegal content online" and the "societal risks" that the "dissemination of disinformation" may generate.[64] And while disinformation is not mentioned in the provisions of the DSA, as will be explained below, many of the articles in the DSA are directly applicable to disinformation.

Indeed, in the run-up to the DSA proposal being published, it was considered EU policy that disinformation was a category of expression that is not illegal, but is harmful (and yet, lawful); which had crucial consequences for how the DSA sought to regulate disinformation. For example, the Commission's High-Level Expert Group (HLEG) on fake news and online disinformation emphasised that disinformation is "not necessarily illegal", but it can "nonetheless be harmful for citizens and society at large", and falls "outside already illegal forms of speech", such as hate speech, and incitement to violence.[65] While the Commission itself also describes disinformation as "harmful content", which is "not, per se, illegal".[66] However, in the intervening period, there

[62] European Commission, "The Commission sends request for information to X under the Digital Services Act", 12 October 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953.

[63] European Commission, "Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act", 20 April 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373.

[64] DSA, Recital 9.

[65] A multi-dimensional approach to disinformation, Report of the independent High level Group on fake news and online disinformation (European Commission, 2018), p. 5, https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[66] European Commission, Digital Services Act: deepening the Internal Market and clarifying responsibilities for digital services, Document Ares(2020)2877686, 2 June 2020, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=pi_com:Ares(2020)2877686. See also, European Commission, Tackling COVID-19 disinformation

has been research on disinformation laws in the EU, and a growing realisation, that the notion of disinformation is in fact illegal in many EU member states.[67] Research points to national legislation in 11 EU member states which is applicable to the notion of disinformation. And notably, it is criminalised in some member states. For example, in Malta, Article 82 of the Criminal Code criminalises the spreading of "false news", and makes it an offence to "maliciously spread false news which is likely to alarm public opinion or disturb public good order or the public peace or to create a commotion among the public or among certain classes of the public". Similarly, the Criminal Code of Cyprus makes it an offence to disseminate "false news" or "news that can potentially harm civil order or the public's trust towards the State or its authorities or cause fear or worry among the public or harm in any way the civil peace and order", and the offence carries a possible two-year prison sentence.[68]

And what this means is that all of the DSA's provisions in relation to illegal content on online platforms are actually applicable to disinformation that has been made illegal in some EU member states. In this regard, there are three main provisions to mention, namely Article 9 DSA on orders against illegal content; Article 16 on notice and action mechanisms; and Article 22 on trusted flaggers, which will be discussed below.

3.1.4.1 Orders against illegal content

The first provision of the DSA to mention is Article 9, which allows national judicial and administrative authorities to order providers of intermediary services, including online platforms, to "act against" user content that is deemed "illegal content".[69] When a provider receives an order from an authority asking it to "act against "specific '(illegal) content', Article 9 DSA obliges the provider to notify it "without undue delay, specifying if and when effect was given to the order". Recital 33 clarifies that specific time limits can be created under specific national (or Union) laws. Very importantly, it is not only courts that can order content to be taken down, but this idea of "national administrative authorities" can also include "law enforcement authorities".[70] Crucially, illegal content is given a very broad definition under the DSA defined as "any information which, in itself or in relation to an activity, including the sale of products or the provision of services, is

- Getting the facts right, JOIN(2020) 8 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008.

[67] See, European Regulators Group for Audiovisual Media Services, *Notions of Disinformation and Related Concepts* (ERGA, 2021) https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf and R. Ó Fathaigh, N. Helberger, & N. Appelman, The perils of legally defining disinformation (2021) *Internet Policy Review*, 10(4), 1.

[68] Cyprus Criminal Code, Article 50.

[69] See, DSA, Article 9(1).

[70] See, DSA, Recital 31.

not in compliance with Union law [or national law], irrespective of the precise subject matter or nature of that law".[71] As follows from Recital 34, the goal of Article 9 is to cover all possible criminal, administrative, or civil orders that one might find in national law. As such, this definition of illegal content captures all of the national legislation applicable to disinformation, and means that Article 9 can be utilised to allow national administrative authorities and national courts to order platforms to remove content under national provisions applicable disinformation.

It is important to note that this rule does not contain an independent legal basis for issuing these orders. As such, the legal basis must be provided elsewhere, either in European or national law.[72] These rules lay down certain minimum conditions applicable to such orders. Here, the minimum conditions that should be met for each order are explained in Article 9 (2) DSA. This is only a baseline rule: national law can go beyond these conditions when giving rise to the obligation to inform the authorities about the effectiveness given to orders.[73]

3.1.4.2 Notice and action mechanisms

The next article to mention is Article 16 DSA on notice and action mechanisms. According to Article 16 DSA, providers of hosting services, including online platforms, have the obligation of putting in place "mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content".[74] The platforms should process any notices and take their decisions in a "timely, diligent, non-arbitrary and objective manner", depending on the type of illegal content being notified and the urgency of taking action.[75] Again, because of the very broad definition of illegal content, this notice-and-action mechanism will also be applicable to all national legislation on disinformation. As such, Article 16 obliges platforms to put in place notice-and-action mechanisms to allow notices to be submitted of (allegedly) illegal content considered disinformation, with platforms required to make a decision on this content without undue delay.

Further, Article 16(3) DSA provides that properly-submitted notices of (alleged) illegal content "shall be considered to give rise to actual knowledge or awareness" for the purposes of Article 6 DSA, which protects platforms from liability.[76] In this regard, Article 6 DSA provides that platforms "shall not be liable" for any user content, even if it illegal, provided the platform (a) does not

[71] See, DSA, Article 3 (h).
[72] Wilman 2022, p. 7-8.
[73] Husovec 2024, p. 153.
[74] See, DSA, Article 16(1).
[75] See, DSA, Recital 52.
[76] See, DSA, Article 16(3)).

have "actual knowledge" of the illegal content, or (b) upon obtaining such knowledge or awareness, "acts expeditiously" to remove or to disable access to the illegal content.[77] What Article 16 DSA now means is that properly-submitted notices of illegal content "shall be considered to give rise to actual knowledge" on the part of platforms for the purposes of Article 6 DSA.

3.1.4.3 Trusted flaggers

Lastly, while the DSA focuses mainly on providers, their action can sometimes be only as good as the environment to which they are responding to.[78] Therefore, the DSA provides rules for other "content moderation relevant" actors, the so-called "trusted flaggers." These trusted flaggers, as follows from Article 22 DSA, are originations with a particular expertise which can, next to users, also notify platforms on illegal content, while working independently from platforms. Entities are awarded such a status, upon an application by any EU-based entity, by the Digital Services Coordinator (DSC) of the Member State in which the applicant is established.[79] When awarded this status, the trusted flagger should be recognised by all providers of online platforms within the scope of the DSA, by which notices by trusted flaggers shall be "given priority" and "processed and decided upon without undue delay" by all online platforms.[80]

Organisations flagging disinformation could obtain an official trusted flagger status under the DSA in member states where legislation exists applicable to disinformation. At the time of writing, one[81] of the current trusted flaggers focuses on combating disinformation.[82] However, before the DSA, trusted flaggers already existed, and there are also possibilities for organisations to obtain an "informal" trusted flagger status. This is for instance the case with the Dutch Ministry of Interior and Kingdom Relations, which has had a trusted flagger status at X, Meta, and Google, TikTok and Snapchat for disinformation around elections. This

[77] See, DSA, Article 6(1)).

[78] Husovec 2024, p. 206.

[79] See, DSA, Article 22(2).

[80] See, DSA, Article 22 (1) and (2).

[81] See, European Commission, "Trusted flaggers under the Digital Services Act (DSA)", https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa#:~:text=Trusted%20flaggers%20are%20special%20entities,it%20to%20the%20online%20platforms. The Greek organisation FactReview aims, "to systematically address disinformation as well as inform the reading public on how to identify and avoid the spread of false information online".

[82] See, European Commission, "Trusted flaggers under the Digital Services Act (DSA)", https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa#:~:text=Trusted%20flaggers%20are%20special%20entities,it%20to%20the%20online%20platforms.

means that there are more flaggers than the one 'formal flagger' who tackle disinformation. In addition, there are also police task forces with flagging roles, which are called “referrals” since they “do not issue legally binding orders; rather, they “refer” content on the ground that it may potentially violate the platforms’ Terms of Service.[OBJ]With the DSA, organisations that were not able to obtain the informal trusted flagger status on a voluntary basis with platforms themselves, could now theoretically become a trusted flagger under the DSA.[83]

Recital 61 DSA gives examples of such trusted flaggers, which can be “public” bodies, and “internet referral units” of national law enforcement authorities or the European Union Agency for Law Enforcement Cooperation” (Europol). Again, because of the broad definition of illegal content under the DSA, Article 22 will be applicable to national legislation concerning disinformation, and can facilitate internet referral units of national law enforcement authorities submitting notices of alleged disinformation, where such notices must be decided upon with priority and without delay.

3.1.5 Very Large Online Platforms and disinformation

The rules discussed in the previous section generally apply to online platforms and can thus apply to community-governed platforms that come within the definition of online platform under Article 3 DSA. As earlier mentioned, VLOPs must comply with stricter due diligence provisions than the other types of online platforms (or even services). This distinction comes from the risk-based approach within the DSA. These specific rules contain several regulations regarding risk-mitigation. Within this section, these articles will be discussed within the context of disinformation.

Since VLOPs can cause “societal and economic harm”, given their reach and impact, they should assess any systemic risks stemming from their services.[84] And under Article 34 DSA, VLOPs must carry “risk assessments” to identify and assess “any systemic risks” stemming from the design or functioning of their service and systems, including algorithmic systems.”[85] This is where disinformation becomes crucial, as one of the explicit purposes of the DSA is to address the “societal risks that the dissemination of disinformation” may generate.[86]

[83] Goldberger 2024.
[84] See, DSA, Recital 79
[85] See, DSA, Article 34(1).
[86] See, DSA, Recital 9.

Article 34 lists a number of systemic risks that must be included in the risk assessment by VLOPs: (a) dissemination of illegal content through their services; (b) any actual or foreseeable negative effects for the "exercise of fundamental rights" enshrined in the EU Charter, including freedom of expression; (c) any actual or foreseeable negative effects on "civic discourse and electoral processes", and "public security"; and (d) any actual or foreseeable negative effects in relation to "gender-based violence", the protection of public health and minors and "serious negative consequences to the person's physical and mental well-being".

Crucially, disinformation is not explicitly mentioned as one of the four potential systemic risks. And the question is how does disinformation fit within this provision. In this regard, it is important to look to the recitals of the DSA concerning systematic risks. Notably, Recital 83 states that risks of actual or foreseeable negative effect on the protection of "public health" can stem from "coordinated disinformation campaigns related to public health". Thus, it seems disinformation is most readily identified with risk (d) under Article 34, namely negative effects on the protection of "public health". Further, Recital 84 states that when assessing the systemic risks, VLOPs should focus on information "which is not illegal", and pay "particular attention" on how their services are used to disseminate or amplify "misleading or deceptive content", including "disinformation", and how amplification of such information "contributes" to the systemic risks. As such, from Recital 84, it seems that disinformation can contribute to all the systemic risks. Notably, the recitals concerning Article 34 and Article 35 do not state that disinformation, in and of itself, is a systemic risk; only that disinformation can contribute to systemic risks, or that systemic risks can stem from disinformation. Thus, on a strict reading of Article 34, the dissemination of disinformation is not a systemic risk, in and of itself. However, as will be seen below, the systemic risk most associated with disinformation is risk (c) concerning negative effects on "civic discourse and electoral processes", and this is where most regulatory action is currently occurring.

Once VLOPs have conducted their risk assessments and identified the risks, the next step is mitigating these risks. Crucially, if VLOPs identify these risks, under Article 35 DSA, VLOPs must put in place reasonable, proportionate and effective "mitigation measures", tailored to the specific systemic risks identified pursuant to Article 34". Article 35 sets out over 11 measures which platforms can take. These are (a) adapting the design, features or functioning of their services, including their online interfaces; (b) adapting their terms and conditions and their enforcement; and (c) adapting content moderation processes, as well as adapting any relevant decision-making processes and dedicated resources for content moderation; (d) adapting algorithmic systems, including recommender system; (e) adapting advertising systems; (f) reinforcing internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk; (g) initiating or adjusting cooperation with trusted flaggers; (h) initiating or adjusting cooperation with other providers of online

platforms through the codes of conduct and crisis protocols; (i) taking awareness-raising measures in order to give users more information; (j) taking targeted measures to protect the rights of the child, and (k) ensuring that items of information that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces.

Lastly, the Commission may take steps related to enforcement of these obligations for VLOPs, and impose a penalty of up to 6% of their annual worldwide turnover against a VLOP that failed to comply with the DSA.[87] These consequences of non-compliance with the above are therefore important to take into account for community-governed platforms designated as VLOPs.

3.1.6 European Commission's regulatory activity targeting election disinformation

Scholars have commented on the somewhat vague nature of the DSA's Article 34 and 35 systemic risk provisions,[88] and the lack of specifics in terms of how disinformation, for example, should be tackled. And coupled with this vagueness, the DSA is a relatively new piece of legislation, with little guidance yet on how Article 34 and 45 will be applied; while the first set of risks assessment under Article 34 was just published at the end of 2024.[89] However, there has been considerable regulatory activity pursuant to Article 34 and 35 by the European Commission, which can be informative on how Article 34 and 35 will be applied in practice, and especially around election disinformation.

And how the DSA will be operationalised to tackle election disinformation was very much to the fore at the tail end of 2024. In this regard, during the 2024 presidential and parliamentary elections in Romania, the European Commission issued a landmark order under the Digital Services Act against TikTok, ordering the platform to "freeze and preserve data" related to "systemic risks its service could pose on electoral processes and civic discourse in the EU" from 24 November 2024 to 31 March 2025.[90] The Commission noted that it had received information "pointing to foreign interference from Russia" in the Romanian presidential elections, and the European Digital Media Observatory had "identified several disinformation narratives and tactics such as violation of electoral law, unmarked political content (including through influencers) and

[87] DSA, Article 73 and 74.

[88] See, for example, Sullivan, D. & Pielemeier, J. (2023). Unpacking "Systemic Risk" Under the EU's Digital Service Act. *Tech Policy*. https://www.techpolicy.press/unpacking-systemic-risk-under-the-eus-digital-service-act/.

[89] The DEM-Debate project will examine the Wikipedia risk assessment and audit report in the next phase of the research.

[90] See, European Commission, "Commission, online platforms and civil society increase monitoring during Romanian elections", 5 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243.

suspicion of coordinated inauthentic behavior".[91] Indeed, on 17 December 2024, the European Commission opened formal proceedings against TikTok for a "suspected breach" of the DSA, for failing to "properly assess and mitigate systemic risks linked to election integrity, notably in the context of the recent Romanian presidential elections on 24 November".[92] These proceedings will focus on management of risks to elections or civic discourse, linked to (i) TikTok's recommender systems, notably the risks linked to the coordinated inauthentic manipulation or automated exploitation of the service, and (ii) TikTok's policies on political advertisements and paid-for political content. The Commission already initiated the same proceedings for X in 2023.[93]

The European Commission President stated that proceedings were opened "following serious indications that foreign actors interfered in the Romanian presidential elections by using TikTok".[94] How this investigation by the European Commission proceeds will be an important consideration during the later parts of the DEM-Debate research, especially the implications of any regulatory decision under the DSA for the regulation of elections disinformation generally. Further, in January 2025, in the context of upcoming elections in Germany, the European Commission and Germany's Digital Services Coordinator, organised a roundtable with VLOPs, to "highlight" the responsibilities of VLOPs under the DSA related to systemic risks and elections.[95] While the European Commission also held a "stress test" with VLOPs to "test to see whether they are doing enough to counter disinformation in the run-up" to the German elections.[96] Separately, the Commission also issued a "retention order" against X in January 2025, which requires X to "preserve internal documents and information regarding future changes to the design and functioning of its recommender algorithms, for the period between 17 January 2025 and 31 December 2025,"[97] which would apply during the German elections, for instance.

---

[91] See, European Commission, "Commission, online platforms and civil society increase monitoring during Romanian elections", 5 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243.

[92] See, Commission opens formal proceedings against TikTok on election risks under the Digital Services Act, 17 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487.

[93] See the press release statement, 18 December 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709.

[94] See, European Commission, "Commission opens formal proceedings against TikTok on election risks under the Digital Services Act", 17 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487.

[95] European Commission, "Digital Services Coordinator for Germany hosts roundtable with online platforms", 24 January 2025, https://digital-strategy.ec.europa.eu/en/news/digital-services-coordinator-germany-hosts-roundtable-online-platforms.

[96] See, "EU to test Facebook, X and others on disinformation ahead of German election", Reuters, 24 January 2025, https://www.reuters.com/technology/meta-tiktok-x-join-eu-stress-test-german-election-2025-01-24/.

[97] European Commission, "Commission addresses additional investigatory measures to X in the ongoing proceedings under the Digital Services Act", 17 January 2025, https://digital-strategy.ec.europa.eu/en/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services.

The power of the Commission to initiate these kinds of proceedings derives from Article 66 DSA. However, as follows from Article 66(1) DSA, the Commission may only initiate proceedings when it suspects an infringement of the DSA.[98] In addition, Article 67 DSA empowers the Commission to send information requests to providers of VLOPs relating to a suspected infringement.

3.2 Regulatory guidance and co-regulatory measures under the DSA

In addition to the DSA itself, there are important co-regulatory measures that are applicable to election disinformation that are relevant for the application of Article 34 and 35 of the DSA to community-governed platforms, namely the European Commission's Guidelines for providers of VLOPs on the mitigation of systemic risks for electoral processes;[99] and the Strengthened Code of Practice of Disinformation.[100] Both regulatory instruments are intimately related to the DSA, and are examined next.

3.2.1 Guidelines for VLOPs on the mitigation of systemic risks for electoral processes

Under Article 35(3) DSA, the European Commission may issue guidelines on the application of risk-mitigation measures in relation to specific risks, including to present best practices and recommend possible measures. Crucially, just before the European Parliament elections in June 2024, the Commission adopted guidelines under Article 35(3) on the mitigation of systemic risks for electoral processes. These guidelines are applicable to VLOPs, including community-governed VLOPs, such as Wikipedia.

The Guidelines were designed, as the Commission's Executive Vice-President stated, to provide concrete guidelines to VLOPs on their obligation to protect users from "risks related to electoral processes", including "disinformation".[101] Notably, the Guidelines contain specific measures for VLOPs to implement targeting disinformation, including the following. First, in order to "prevent the spread of disinformation" during the electoral process, VLOPs should facilitate access to "official information concerning the electoral process", based on official information from the

[98] Also see F. Wilman, S. Lukas Kaleda & P.J. Loewenthal, *The EU Digital Services Act*, Oxford University Press: Oxford 2024, p. 436.

[99] 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, C/2024/3014, 26 April 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277.

[100] The Strengthened Code of Practice on Disinformation 2022, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[101] European Commission, "Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections", 26 March 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707.

electoral authorities.[102] Second, VLOPs should apply "inoculation measures" that "preemptively build resilience" against "disinformation narratives," by informing and preparing users, for example through the use of games, videos and other content on the generation of disinformation, which "encourages a critical reflection on the tactics" used for disinformation.[103] Third, VLOPs should use fact-checking labels on identified disinformation provided by independent fact checkers, and fact-checking teams of independent media organisations.[104]

The foregoing measures are very much in the vein of providing the user with more information to address disinformation. However, there are particular measures which go much further, and are framed in the sense of reducing the spread of disinformation. In this regard, these include that VLOPs should "reduce the prominence" of disinformation in the context elections, including deceptive content that has been fact-checked as "false", or from accounts that have been "repeatedly found to spread disinformation".[105] Further, VLOPs should put systems in place to prevent the misuse of advertising systems to disseminate disinformation; engage in the "demonetisation" of disinformation content;[106] ensure the "enforcement" of terms and conditions to "significantly decrease" the reach of generative AI content that depicts disinformation on the electoral process; and reduce the "virality" of content that "threatens the integrity of electoral processes".[107] Thus, these measures are a mix of providing users with more information to counter disinformation; and also measures to reduce the reach and monetisation of disinformation. Importantly, VLOPs should also put in place an internal incident response mechanism, involving senior leadership, during elections; and should set up contact points with national and European authorities, to be able to implement "rapid" measures in urgent situations.[108] It should be noted that the Commission organised what are called "Stress Tests", to safeguard the integrity of the 2024 European Parliament elections in April 2024.[109]

---

[102] 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) 2022/206., Section 3.2.1

[103] 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, p.7.

[104] 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, p .7.

[105] 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, p. 8.

[106] 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, p. 9.

[107] 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, p. 9.

[108] 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) 2022/206., p. 16.

[109] European Commission, "Commission stress tests platforms' election readiness under the Digital Services Act", 24 April 2024, https://digital-strategy.ec.europa.eu/en/news/commission-stress-tests-platforms-election-readiness-under-digital-services-act.

Notably, the Commission was quite forthright in terms of VLOPs being required to implement these measures. The Commission explicitly stated that VLOPs which "do not follow" these guidelines "must prove" to the Commission that the measures undertaken are "equally effective in mitigating the risks"; and "should the Commission receive information casting doubt on the suitability of such measures, it can start formal proceedings under the Digital Services Act."[110] This was very much a warning to VLOPs to follow these guidelines. Finally, and crucially, the Guidelines also explicitly state that the mitigation measures "should draw" on the EU Code of Practice on Disinformation, and it is to this Code we now turn.[111]

3.2.2 Strengthened Code of Practice on Disinformation

When examining the DSA's regulation of election disinformation, it is crucial to examine the EU's Strengthened Code of Practice on Disinformation 2022; which is inextricably linked to the DSA, and explicitly states that it "aims to become" a recognised code of conduct under the DSA.[112] Further, the DSA's recitals explicitly mention the Code of Practice on Disinformation;[113] and that adherence to and compliance with a given code of conduct by a VLOP may be considered as an "appropriate risk mitigating measure" in relation to systemic risks.[114] While the "refusal without proper explanations" by a VLOP to participate in the application of a code of conduct could be "taken into account" when determining whether a platform "has infringed the obligations" laid down by the DSA.[115] And Article 35(1)(h) explicitly mentions cooperation through codes of conduct as a risk-mitigation measure.[116]

As such, given how closely the Code of Practice and the DSA are linked, it is important for community-governed platforms to be aware of how the Code is operating. The Code was first put together in 2018 by the European Commission and a number of commercial online platforms, and was updated in 2022, with specific measures designed to target disinformation. At the time of writing, the platforms signed up to the Code were mainly centralised-governed online platforms, and community-governed platforms, such as Wikipedia, were no signatories.

---

[110] European Commission, "Commission publishes guidelines under the DSA for the mitigation of systemic risks online for elections", 26 March 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707.

[111] 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) 2022/206., p. 1.

[112] The Strengthened Code of Practice on Disinformation 2022, p. 2.

[113] DSA, Recital 10.

[114] DSA, Recital 104.

[115] DSA, Recital 104.

[116] DSA, Article 35(1)(h) ("initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct and the crisis protocols referred to in Articles 45 and 48 respectively").

Notably, the Code's measures include that platforms should (a) put in place a functionality to allows users to flag "false or misleading information"; and should lead to "appropriate, proportionate and consistent" follow-up actions;[117] (b) provide functionalities to allow users assess the "authenticity or accuracy" of content;[118] (c) provides users with factual accuracy of sources through fact-checks from fact-checking organisations that have flagged potential disinformation, and "warning labels" from "authoritative sources";[119] and (d) commit to "defund" the dissemination of disinformation.[120] Now a very important aspect of the Code is Measure 18.2, where platforms commit to "enforce" policies to limit the spread of false information, which can include "prohibiting" false or misleading information".[121]

Crucially, reporting from platforms under the Code reveals a large amount of content considered disinformation is being taken down pursuant to Measure 18.2. For example, reporting by TikTok in its report covering the period of the European Parliament elections, TikTok removed over a quarter of million videos in the EU in the run-up to the elections.[122] Similarly, YouTube reported removing over 19,000 videos in the run-up to the EU elections based on its disinformation policy.[123] While LinkedIn reported removing over 20,000 pieces of content under its disinformation policy in its March 2024 report.[124] This is a considerable amount of content that is being removed under the Code, and only during a six-month period. Scholars such as Galantino have explicitly mentioned how the Code seems to fail to "tightly control the scope of content removals and account sanctions".[125] Indeed, the European Commission has previously explicitly highlighted examples from the reports, including that "140,635 videos accounting for more than 1 billion views were removed" by TikTok for violations of its disinformation policy during a six-month period in 2023.[126]

---

[117] The Strengthened Code of Practice on Disinformation 2022, Measure 23.1.

[118] The Strengthened Code of Practice on Disinformation 2022, Measure 20.1.

[119] The Strengthened Code of Practice on Disinformation 2022, Measure 21.

[120] The Strengthened Code of Practice on Disinformation 2022, Commitment 1.

[121] The Strengthened Code of Practice on Disinformation 2022, Measure 18.2.

[122] TikTok, "Code of Practice on Disinformation – Report of TikTok for the period 1 January 2024 - 30 June 2024", https://disinfocode.eu/reports-archive/?years=2024.

[123] Google, "Code of Practice on Disinformation – Report of Google for the period of 1 January 2024 to 30 June 2024", https://disinfocode.eu/reports-archive/?years=2024.

[124] Microsoft, Code of Practice on Disinformation – Report of Microsoft for the period 1 July – 31 December 2023, https://disinfocode.eu/reports-archive/?years=2024.

[125] S. Galantino, "How Will the EU Digital Services Act Affect the Regulation of Disinformation?" (2024) SCRIPTed, 20(1), 89, at p. 126.

[126] European Commission, "Code of Practice on Disinformation: new reports available in the Transparency Centre", 26 September 2023, https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-reports-available-transparency-centre.

As such, while the DSA does not explicitly prohibit disinformation, the Code of Practice on Disinformation is where disinformation is being prohibited, and where a large amount of removal is occurring. This is a crucial issue to highlight, as the Code is now seen as a co-regulatory measure under the DSA. This has important consequences for community-governed platforms that may be incentivised to join the Code, especially as a way of demonstrating risk-mitigation under the DSA.

3.3 European Media Freedom Act

A further piece of EU legislation that is relevant for community-governed platforms and election disinformation is the European Media Freedom Act (EMFA) 2024.[127] While the EMFA basically sets down rules applicable to media services in the EU, it does contain important provisions which may impact upon community-governed platforms that are designated as Very Large Online Platforms (VLOPs) under the DSA. Indeed, the EMFA recognises that certain media services may be "controlled by certain third countries" and "systematically engage in disinformation or information manipulation and interference".[128] But the EMFA also recognises that "quality media services are also an antidote against disinformation and foreign information manipulation and interference".[129] Crucially, the EMFA is the first piece of EU legislation to lay down a legal qualification for disinformation, where it provides in Article 19 that disinformation is a form of "harmful content".[130]

The first relevant provision is Article 18 EMFA, which applies to VLOPs under the DSA. Article 18 EMFA basically provides that VLOPs must give prior notice to a media organization before a VLOP seeks to restrict the visibility of a specific piece of media content or suspend a media organization's account. In particular, Article 18(1) EMFA provides that VLOPs must provide a functionality allowing media organisations to "declare that they are media service providers".[131] Once a VLOP accepts a media service's declaration, the VLOP must then comply with Article 18(4) which provides that where a VLOP "intends to take a decision to suspend the provision" of its services in relation to content provided by a media service provider or a decision to "restrict the visibility of such content, on the grounds that such content is incompatible with its terms and conditions", prior to such a decision to suspend or restrict visibility taking effect, it must (a) communicate to the media service provider concerned a statement of reason; and (b) give the

[127] Regulation (EU) 2024/1083 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act).

[128] EMFA, Recital 4.

[129] EMFA, Recital 14.

[130] EFMA, Article 19(c).

[131] EMFA, Article 18(1).

media service provider the opportunity to reply to the statement of reasons within 24 hours of receiving it.[132] Basically, VLOPs must give certain media organisations prior notice before removing their content or suspending their accounts.

Notably, under Article 18(8), VLOPs are not required to give media organisations prior notice of a content removal or suspension where it is done "in compliance with their obligations" under Article 34 and 35 DSA.[133] This means that where VLOPs seek to remove media content in order to mitigate risks of "any actual or foreseeable negative effects on civic discourse and electoral processes",[134] which may include election disinformation, then Article 18(8) EMFA provides an exemption to VLOPs to restrict such content or suspend an account engaging in dissemination of such content.

As such, where a community-governed platform is designated as a VLOP under the DSA, such community-governed platform must provide a functionality to allow users that are media organisations to declare themselves as a media service provider the EMFA. However, the EMFA allows such VLOPs to restrict content and suspend accounts of media service providers, where it is done "in compliance with their obligations" under Article 34 and 35 DSA, including to protect against risks of negative effects on "electoral processes".[135]

A final provision to mention is Article 19 EMFA on what are called "structured dialogues" around VLOPs, media content and disinformation. Article 19 EMFA provides that the European Board for Media Services, composed of representatives of national media authorities, is required to regularly organise a "structured dialogue" between VLOPs, representatives of media service providers, and representatives of civil society, in order to discuss (a) best practices on the functioning of VLOPS and their processes for moderating media content; (b) "foster access to diverse offerings" of "independent media" on VLOPs; and (c) monitor adherence to self-regulatory initiatives which aim to protect users from "harmful content", including "disinformation" and "foreign information manipulation and interference".[136] The Board must report on the dialogues to the Commission, and these reports should be public. This Article 19 EMFA provision is significant in terms of providing an official legislative mechanism for community-governed platforms that are designated as VLOPs to contribute to how initiatives to protect users from disinformation are adhered to, and contribute to how VLOPs should deal with media content that is labelled as disinformation.

[132] EMFA, Article 18(4).
[133] EMFA, Article 18(8).
[134] See, DSA, Article 34(1).
[135] EMFA, Article 18(8).
[136] EMFA, Article 19(1)(a)-(c).

3.4 Regulation on political advertising

The final piece of EU legislation which is relevant for community-governed platforms and election disinformation is the EU's recently enacted 2024 Regulation on the transparency and targeting of political advertising.[137] Notably, this regulation was first published by the European Commission in 2021, and had been planned to enter into force by April 2023, a year before the 2024 European Parliament elections, to be held on 6-9 June 2024.[138] However, the legislative procedure moved slower than planned, with the Regulation only officially entering in force in March 2024, and will generally only apply from October 2025. Similar to the DSA, this piece of legislation is quite significant for the regulation of online platforms generally, and is the first time the EU adopted legislation regulating political advertising in particular.

The basic purpose of the RPA is to lay down harmonised rules for the provision of political advertising. Crucially, the RPA ties political advertising to disinformation, emphasising that political advertising can be a "vector" of disinformation, particularly where the advertising "does not disclose its political nature", comes from sponsors "outside" of the EU, or is subject to "targeting techniques or ad-delivery techniques."[139]

And the first point to note is that the RPA applies to all intermediary services under the DSA, including online platforms and VLOPs.[140] Crucially, political advertising is generally defined as the "dissemination, by any means, of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign" by, for or on behalf of a "political actor", or "which is liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level".[141] This a very broad definition, and covers both elected-related ads, and so-called issue ads, where ads seek to "influence" a "legislative or regulatory" process, and would capture ads by NGOs and advocacy groups.[142] However, the most crucial aspect of the definition is that it only

[137] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, 2024/900, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R0900.

[138] See R. Ó Fathaigh, "European Parliament adopts Proposed Regulation on the transparency and targeting of political advertising" (2024) IRIS 2024-3, 6.

[139] RPA, Recital 4.

[140] RPA, Article 1.

[141] RPA, Article 3(2)(b).

[142] RPA, Article 3(2)(b).

seeks to apply to political advertising which is "normally provided for remuneration,"[143] which means there needs to be a paid-for element or a "benefit in kind".[144]

As such, community-governed platforms that allow paid political advertising on their platforms would be required to comply with the RPA. Of course, some community-governed platforms, such as Wikipedia, do not allow advertising; while other community-governed platforms, such as Reddit, do allow advertising; and the application of the RPA would depend on the specific community-governed platform. It should also be noted that some commercial VLOPs, such as Google, have indicated that they will no longer offer political advertising services in the EU due to the RPA's enactment.[145] Further, in relation to user-uploaded content without payment to a platform, the RPA does state that the rules "should not apply" to content "uploaded by a user of an online intermediary service, such as an online platform, and disseminated by the online intermediary service without consideration" for the "placement, publication, delivery or the dissemination of the specific message", unless the user "has been remunerated by a third party" for the political advertisement.[146] As such, the rules under the RPA would apply where a user, such as an online influencer, uploads content that could be considered political advertising, where the user has been paid by a third party.

Importantly, there are a number of provisions under the RPA which are relevant for community-governed platforms that allow advertising. First, under Article 5 RPA, in the last three months preceding an election or referendum organised at EU level or Member State level, political advertising services pertaining to that election or referendum "shall only be provided" to a sponsor who declares itself to be a legal person "established" in the EU which is "not ultimately owned or controlled by a third-country national" or by a "legal person established in a third country".[147] The basic purpose of this provision is to prevent political advertising from outside of the EU (i.e. third countries), and is designed to counter disinformation, information manipulation and interference from third countries.[148] And thus, community-governed platforms must generally not allow political advertising from sponsors outside of the EU during the three months before an election in the EU.

[143] RPA, Article 3(1).

[144] RPA, Recital 16.

[145] Google, "An update on political advertising in the European Union", 14 November 2024, https://blog.google/around-the-globe/google-europe/political-advertising-in-eu/.

[146] RPA, Recital 47.

[147] RPA, Article 5.

[148] RPA, Recital 4.

Second, Article 11 RPA contains labelling and transparency requirements for political advertisements. In this regard, political advertising publishers, which can include online platforms, must ensure all political advertisements contain certain information, including that a statement that it is a political advertisement, the identity of the sponsor, and the election to which the political advertisement is linked. Notably, the information must "remain in place in the event that the political advertisement is further disseminated".[149]

Third, under Article 12 RPA, political advertisements must also include a specific "transparency notice" (or a link to such a notice), which includes additional information, including the (a) period during which the political advertisement is intended to be published", (b) the "aggregated amounts and the aggregated value of other benefits received by the providers of political advertising service", and (c) the "reach of the political advertisement in terms of the number of views and of engagements with the political advertisement".[150]

Fourth, under Article 15, political advertising publishers must also put in place mechanisms to enable individuals to notify them if a particular political advertisement that they have published does not comply with the RPA. Notably, political advertising publishers must "without undue delay" make "best efforts to examine and address the notifications" and inform, at least upon request, the individual which made the notification "of the follow-up given to it".[151] Notably, VLOPs must "without undue delay" examine and address the notifications and inform the individual who made the notification "of the follow-up given to it".[152]

Final relevant provisions to mention are Article 18 and 19 RPA which contain specific rules regulating the use of micro-targeting in political advertising.[153] In this regard, Article 18 RPA provides that targeting techniques, or ad-delivery techniques,[154] that involve the processing of personal data in the context of online political advertising shall be permitted "only" when certain conditions are fulfilled, including that the data subject has provided "explicit consent" to the processing of personal data "separately for the purpose of political advertising,"[155] and when those techniques do not involve using special categories of personal data (e.g, ethnicity, religion,

[149] RPA, Article 11(3).

[150] RPA, Article 12(1).

[151] RPA, Article 15(5)(b).

[152] RPA, Article 15(5).

[153] See, RPA, Article 3(11) ("'targeting techniques' means techniques that are used to address a political advertisement only to a specific person or group of persons, or to exclude them, on the basis of the processing of personal data").

[154] See, RPA, Article 3(12) ("'ad-delivery techniques' means optimisation techniques that are used to increase the circulation, reach or visibility of a political advertisement on the basis of the automated processing of personal data and that can serve to deliver the political advertisement to a specific person or group of persons only").

[155] RPA, Article 18(1).

sexual orientation). Importantly, under Article 19 RPA, when using targeting techniques or ad-delivery techniques in the context of online political advertising involving the processing of personal data, controllers must provide "additional information" with the political advertisement, including (a) the specific groups of recipients targeted; (b) the categories of personal data used; (c) the targeting goals, mechanisms and logic; and (d) meaningful information on the use of artificial intelligence systems.[156]

Notably, the RPA does *not* have specific rules on the *content* of political advertisements, such as that political advertisements must be accurate or not contain false information or disinformation. As such, the RPA is very much concerned with only transparency around political advertising, and in this way seeks to protect elections from political advertising that can be used as "vector" of disinformation, such as where the advertising does not disclose its political nature, comes from sponsors outside of the EU or is subject to targeting techniques or ad-delivery technique.[157] And as mentioned, where a community-governed platform comes within the definition of an online platform, and allows advertising on its platforms, then the RPA would apply.

4. Council of Europe

While the EU and national regulatory frameworks applicable to election disinformation are particularly relevant for community-governed platforms, it is also essential to set out the Council of Europe's regulatory framework on election disinformation. This is crucial, as any regulation, whether EU or national, targeting election disinformation or community-governed platforms must be consistent with the fundamental right to freedom of expression, guaranteed under Article 10 of the European Convention on Human Rights (ECHR).[158] This is because all EU member states are signatories to the European Convention on Human Rights, and subject to the jurisdiction of the European Court of Human Rights, which interprets and applies the ECHR. And under the EU Charter of Fundamental Rights, the meaning and scope of fundamental rights "shall be the same" as those laid down under the ECHR.[159] For example, the European Commission has confirmed that any measures taken under legislation such as the DSA must be in line with "jurisprudence by the European Court of Human Rights".[160]

[156] RPA, Article 19.

[157] RPA, Recital 4.

[158] Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, 213 U.N.T.S. 221, Article 10.

[159] Charter of Fundamental Rights of the European Union, 2000/C 364/01, Article 51.

[160] See, for example, Access Now, "Civil society gets its confirmation from EU Commissioner: no internet shutdowns under DSA", 2 August 2023, https://www.accessnow.org/press-release/commissioner-breton-responds-dsa/.

4.1 European Court of Human Rights

Importantly, the European Court of Human Rights has considered a number of false information laws that have applied during elections. In this regard, the ECtHR has unanimously held that a prosecution for "dissemination of false information", under election legislation in Ukraine, violated the right to freedom of expression under Article 10 ECHR.[161] The Court laid down a crucial principle that Article 10 ECHR "does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful".[162] The was premised on the "requirements of free expression and free discussion of information" enshrined in Article 10 ECHR.[163]

In a similar vein, scholars have discussed how the European Court has also delivered three unanimous judgments concerning a provision under election legislation in Poland, where election candidates can apply to a court for an order prohibiting publication of campaign material or statements containing "untrue data or information", and where the court is required to examine the application "within 24 hours".[164] Notably, the European Court found in all these judgments that proceedings under this law violated Article 10 ECHR. Crucially, in its 2019 judgment *Brzeziński v. Poland*, the Court unanimously found a violation of Article 10 as the national courts had "immediately classified as lies" statements made by a local politician during an election, and "[b]y following such an approach the domestic courts effectively deprived [the politician] of the protection afforded by Article 10".[165] Similarly, in *Kwiecień v. Poland*, the Court found serious deficiencies under proceedings for "untrue information" during an election, and even held that the "fairness of the proceedings may be called into question" .[166] While in *Kita v. Poland*, the Court also unanimously held there had been a violation of Article 10 over the "untrue information" proceedings, finding the national courts "unreservedly qualified all of [the statements] as statements which lacked any factual basis," and the "standards applied" by the national courts were "not compatible with the principles embodied in Article 10".[167]

Crucially, these principles from the ECtHR must be taken into account when measures are adopted under any EU or national legislation applicable to election disinformation, and in a

[161] Salov v. Ukraine, Application no. 65518/01, 6 September 2005, https://hudoc.echr.coe.int/?i=001-70096.
[162] Salov v. Ukraine, Application no. 65518/01, 6 September 2005, para. 113, https://hudoc.echr.coe.int/?i=001-70096.
[163] Salov v. Ukraine, Application no. 65518/01, 6 September 2005, para. 114, https://hudoc.echr.coe.int/?i=001-70096.
[164] Brzeziński v. Poland, Application no. 47542/07, 26 July 2019, para. 28, https://hudoc.echr.coe.int/?i=001-194958.
[165] Brzeziński v. Poland, Application no. 47542/07, 26 July 2019, para. 58, https://hudoc.echr.coe.int/?i=001-194958.
[166] Kwiecień v. Poland, Application no. 51744/99, 9 January 2007, para. 55, https://hudoc.echr.coe.int/?i=001-78876.
[167] Kita v. Poland, Application no. 57659/00, 8 July 2008, para. 51, https://hudoc.echr.coe.int/?i=001-87424.

certain sense, provide protection to community-governed platforms in terms of ensuring any regulation is not a disproportionate interference with freedom of expression.

4.2 Standard-setting on election disinformation

Not only is the European Court of Human Rights case law relevant for the regulation of election disinformation, the standard-setting instruments adopted by other Council of Europe bodies are also important to note. In this regard, adopted instruments by the Council of Europe's Committee of Ministers are routinely relied upon by the European Court of Human Rights when it interprets the ECHR, including its case law relating to freedom of expression.[168] Indeed, the EU Court of Justice also cites recommendations of the Committee of Ministers in its case law.[169]

Notably, the Council of Europe's Committee of Ministers and the Steering Committee for Media and Information Society have adopted important and specific instruments relating to election disinformation. In this regard, the Guidance on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, adopted by the Steering Committee for Media and Information Society, is especially relevant.[170] First, ensuring a "favourable and enabling environment" for freedom of expression is essential to tackling disinformation,[171] and under human rights standards, "fostering an enabling environment for free expression, with a diverse communications environment, including media diversity", is a "key means of addressing disinformation".[172] Second, when platforms apply measures to restrict disinformation, such measures must respect the rights of users, and be implemented using the "least restrictive means", done in a "transparent and non-discriminatory manner", and should be limited in scope and duration to what is strictly necessary to avoid the "collateral unjustified restriction or removal of legal content".[173] Further, the Committee of Ministers has explicitly stated that "State authorities should obtain an order by a judicial authority

[168] See, for example, Delfi AS v. Estonia [GC], Application no. 64569/09, 16 June, 2015, para. 113.

[169] For recent examples, see, Court of Justice of the European Union, Joined Cases C-924/19 PPU and C-925/19 PPU, Judgment of the Court (Grand Chamber) of 14 May 2020, FMS and Others v Országos Idegenrendészeti Főigazgatóság Dél-alföldi Regionális Igazgatóság, para. 218; and Case C-622/17, Opinion of Advocate General Saugmandsgaard Øe, 28 February, 2019, Baltic Media Alliance Ltd v. Lietuvos radijo ir televizijos komisija, para. 44.

[170] Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, Adopted by the Steering Committee for Media and Information Society (Council of Europe, 2023), https://rm.coe.int/cdmsi-2023-015-msi-inf-guidance-note/1680add25e.

[171] Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, p. 36.

[172] Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, p 37.

[173] Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, appendix, para. 2.3.1 - 2.3.2.

or other independent administrative authority, whose decisions are subject to judicial review, when demanding intermediaries to restrict access to content".[174]

These principles also apply to community-governed platforms and must also be taken into account in any measures regarding election disinformation. Crucially, these principles are premised on the notion that any measures applied be the least restrictive, and fully consistent with freedom of expression.

5. National regulation

In addition to the discussed EU regulatory frameworks, it is also important to have regard to national legislation that may be applicable to election disinformation, and may also be relevant for community-governed platforms. And the first point in this regard is that EU policy on election disinformation had been mainly based on the notion that disinformation is a category of expression that is not illegal, but is harmful (and yet, lawful). For example, the European Commission's High Level Expert Group (HLEG) on fake news and online disinformation has emphasized that disinformation is "not necessarily illegal", but it can "nonetheless be harmful for citizens and society at large", and falls "outside already illegal forms of speech", such as hate speech, and incitement to violence.[175] While the European Commission itself also describes disinformation as "harmful content", which is "not, per se, illegal".[176]

However, there has now been considerable research on this point of national legislation applicable to election disinformation, and a number of EU member states do in fact have legislation applicable to the notion of disinformation. For example, in France, under the Law on the fight against the manipulation of information, in the three-month period before an election, a judge may order measures to prohibit the dissemination of "any allegation or charge of an inaccurate or misleading fact likely to alter the sincerity of the forthcoming vote, which is deliberately, artificially or in an automated and massive manner, disseminated through an online

[174] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, CM/Rec(2018)2, Section 1.3.2. See also Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on on the impacts of digital technologies on freedom of expression, Section 1.1.

[175] High Level Expert Group on fake news and online disinformation, A multi-dimensional approach to disinformation (European Commission, 2018), p. 4, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1.

[176] European Commission, Digital Services Act: deepening the Internal Market and clarifying responsibilities for digital services, Document Ares(2020)2877686, 2 June 2020, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=pi_com:Ares(2020)2877686. See also, European Commission, Tackling COVID-19 disinformation - Getting the facts right, JOIN(2020) 8 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008.

public communication service".[177] There is also an obligation on the court to deliver a judgment within 48-hours. In addition, under France's Freedom of the Press law, it is prohibited to disseminate "false news" when done in "bad faith", and it disturbs, or is likely to disturb, public peace;[178] while Article 97 of the Electoral Code makes it a criminal offence to spread "false news" with the effect of distorting the outcome of an election.[179]

Similar laws exist in numerous other EU member states.[180] Indeed, research points to national legislation in 11 EU member states which is applicable to the notion of disinformation. And notably it is criminalised in many member states. For example, in Malta, Article 82 of the Criminal Code criminalises the spreading of "false news," and makes it an offence to "maliciously spread false news which is likely to alarm public opinion or disturb public good order or the public peace or to create a commotion among the public or among certain classes of the public".[181] Similarly, the Criminal Code of Cyprus makes it an offence to disseminate "false news" or "news that can potentially harm civil order or the public's trust towards the State or its authorities or cause fear or worry among the public or harm in any way the civil peace and order", and the offence carries a possible two-year prison sentence.[182] And while these national laws do not in a strict sense target community-governed platforms, these laws on false news and false information are quite relevant for information published on community-governed platforms. Community-governed platforms could be ordered to remove such information under national court procedures and, as mentioned above, could be operationalised under the DSA's provisions applicable to illegal content.

6. Concluding remarks

In light of the forgoing, there are a number of concluding points to consider from this mapping of European regulatory frameworks on election disinformation. First, it is important to note that for community-governed platforms the EU legislation, including the DSA, does not set out a legal definition of disinformation, and no legal definition of election disinformation is contained in EU

[177] Law on the fight against the manipulation of information [LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information], Article 1.

[178] Law of July 29, 1881 on freedom of the press, Article 27.

[179] Code électoral [Electoral Code] Article L97.

[180] See, European Regulators Group for Audiovisual Media Services, *Notions of Disinformation and Related Concepts* (ERGA, 2021) https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf; and R. Ó Fathaigh, N. Helberger, & N. Appelman, The perils of legally defining disinformation (2021) *Internet Policy Review*, 10(4), 1.

[181] Malta Criminal Code, Article 82.

[182] Cyprus Criminal Code, Article 50.

law. While there are certain policy definitions which are used by the European Commission, and in the Strengthened Code of Practice on Disinformation,[183] for the purposes of legal obligations applicable to community-governed platforms, there is no legal definition that community-governed platforms are required to adopt. Indeed, for the first time in EU legislation, the EMFA states that disinformation is "harmful content",[184] not illegal content. As such, community-governed platforms do seem to have some discretion, as do centralised-governed platforms, to define election disinformation in their own terms.

Second, and a further basic point about the European regulatory framework on election disinformation, is that most obligations placed on centralised-governed platforms under the DSA are also applicable to community-governed platforms. This is because the definition of online platforms is quite broad,[185] meaning that community-governed platforms are captured by the definition, and no distinction is made based on how moderation is undertaken. As such, in principle, most obligations under the DSA which are applicable to centralised-governed online platforms are also applicable to community-governed platforms (unless a platform qualifies as a micro enterprise). Notably, the DSA did not adopt an approach similar to the Digital Single Market Directive, where there is an explicit exemption for "not-for-profit online encyclopedias" from the definition of "online content-sharing service provider".[186] Similarly, the definition of an "online content-sharing service provider" under the Digital Single Market Directive includes a for-profit element, so it only includes those providers with "profit-making purposes".[187] And a consequence of the foregoing point is that community-governed platforms are not generally exempt from DSA obligations because they operate a community-based content moderation framework.

Third, in relation to the DSA, it should be emphasised that there is no provision requiring online platforms, including community-governed platforms, to remove election disinformation. However, where election disinformation qualifies as illegal content under EU member state legislation, the DSA does contain provisions (e.g., Article 9), where platforms may be ordered to remove certain illegal content. Further, in relation to VLOPs, there is also no provision in the DSA requiring VLOPs to remove election disinformation. However, there are sophisticated mechanisms under the DSA's systemic risk provisions (Article 34 and 35), which require VLOPs to assess any systemic risks stemming from their services, including relating to negative effects on

[183] The Strengthened Code of Practice on Disinformation 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[184] EMFA, Article 19.

[185] See, DSA, Article 3(1)(i).

[186] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Article 2(6).

[187] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Article 2(6).

"electoral processes", which may stem from the dissemination of disinformation; and for VLOPs to put in place "mitigation measures" to address these systemic risks.

Fourth, the current regulatory activity by the European Commission targeting election disinformation in member states, such as Romania, is also quite relevant for community-governed platforms that qualify as VLOPs. This is because the nature of the orders being issued by the Commission, such as retention orders, which require a platform to "freeze and preserve data related to actual or foreseeable systemic risks its service could pose on electoral processes and civic discourse in the EU",[188] over an extended period of time, is quite an unprecedented power. It demonstrates the path of the Commission's enforcement of the DSA targeting election disinformation, and the outcome of these enforcement proceedings will be highly relevant from community-governed platforms that qualify as VLOPs.

Fifth, while the DSA is not overly specific on how election disinformation can be tackled, two pieces of co-regulatory measures are crucial to take into account for specific action to be taken by community-governed platforms in relation to election disinformation. In the first instance, the Strengthened Code of Practice on Disinformation contains detailed provisions in relation to how disinformation during elections can be tackled. Notably, while the DSA does not mandate explicitly that disinformation should be removed, the Code of Practice does contain a provision that signatories should enforce policies to "limit the spread of harmful false or misleading information", such as "prohibiting" harmful false or misleading information.[189] Indeed, a considerable amount of content is being removed under this provision, as documented in platform reports under the Code of Practice on Disinformation. Further, the 2024 Commission Guidelines on the mitigation of systemic risks for electoral processes are also quite detailed on how community-governed platforms that qualify as VLOPs can tackle election disinformation.

Fifth, the regulatory measures under the European legal framework which apply to community-governed platforms are quite diverse in the sense of the nature of the measures (i.e., targeting demonetisation of disinformation (monetisation focus), or mechanisms for users to flag disinformation (user empowerment)). The Commission's Guidelines on elections have a focus on advertising, algorithmic amplification, and demonetisation; and similar to the Guidelines, the Code of Practice also focuses on measures such as demonetisation, political advertising, and advertising. However, other measures, such as the edit history of content, are also envisaged. Thus, given the diversity of community-governed platforms in terms of business model (non-commercial, and advertising-based), the regulatory framework can take account of these different

[188] See, European Commission, "Commission, online platforms and civil society increase monitoring during Romanian elections", 5 December 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6243.

[189] The Strengthened Code of Practice on Disinformation 2022, Measure 18.2, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

models. It is an open question whether community-governed platforms should join the Code of Practice. One notable feature of the Code is that platforms have discretion to choose which measures to adopt, and can opt out of certain measures not applicable to a community-governed platform's system. Becoming a signatory could also bring transparency in terms of what a community-governed platform is doing in terms of implementing the measures.

Sixth, it is helpful to distinguish between a number of types of regulatory measures under European legal frameworks, such as organisational measures, process-based measures, and content-based measures (but this is not a strict dichotomy). An example of the organisational- and process-based measures would be where community-governed platforms are required to put in place organisational structures to deal with election disinformation, such as establishing a dedicated team during elections to coordinate responses to disinformation campaigns. While an example of a content-based measure would be including in a platform's terms and conditions that false information during an election is prohibited.

Seventh, in addition to the DSA, the 2024 Regulation on Political Advertising is also quite important to take account of for those community-governed platforms that operate an advertising business model.[190] It contains important provisions designed to apply to foreign-government political advertising that may serve as a vector for disinformation during elections. The European Media Freedom Act also contains important provisions applicable to community-governed platforms that qualify as VLOPs which seek to remove media content that may qualify as disinformation.[191]

Eighth, the EU regulatory frameworks are somewhat general on specifics in terms of how measures targeting election disinformation should be consistent with freedom of expression. In this regard, the Council of Europe regulatory frameworks are helpful for community-governed platforms in terms of how to ensure that any measures taken against election disinformation are consistent with freedom of expression (e.g., least-restrictive measure; special protection for election-related expression).

Finally, the above points will be taken into account as the DEM-Debate project proceeds to the analysis of a specific community-governed platform, and when critically analysing the application of the above frameworks to community-governed platforms.

[190] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, Article 5.

[191] Regulation (EU) 2024/1083 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), Article 17.

January 2025