European Journal of Risk Regulation (2025), 1–26
doi:10.1017/err.2025.10034

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The DSA's Tower of Babel: On Digital Services Coordinators and Freedom of Expression

Jacob van de Kerkhof

School of Law, Utrecht University, Netherlands
Email: j.j.w.vandekerkhof@uu.nl

Abstract

The Digital Services Act (Regulation 2022/2065, "DSA") creates a new national administrative authority to enforce the DSA across member states: the Digital Services Coordinator ("DSC"). DSCs perform a linchpin role in the DSA enforcement. DSCs have a number of tasks that interact with the content moderation process, such as certifying trusted flaggers or participating in drafting codes of conduct. They also have significant investigatory- and sanctioning powers to enforce the DSA vis-à-vis platforms, shaping content moderation processes and protecting users' rights against platform misconduct. These interactions with content moderation affect users' freedom of expression. This contribution scrutinises the role of the DSC in light of that freedom, describing how DSCs shape freedom of expression online through their powers in the DSA, and identifying instances where exercise of DSA powers can lead to different levels of protection for freedom of expression across Member States in the decentralised enforcement network. Finally, it proposes avenues in the DSA to anchor protection of freedom of expression in the application of the DSA by DSCs, through pursuing centralisation in cases with significant fundamental rights impact, and encouraging better usage of guideline competencies.

Keywords: content moderation; digital services coordinator; DSA; freedom of expression

I. Introduction

In an effort to combat harmful content online and shift the power imbalance in speech governance, the European Union adopted Regulation 2022/2065, the Digital Services Act ("DSA").[1] The DSA marks a watershed moment in platform governance, adding a significant accountability and transparency framework onto the existing liability framework of the e-Commerce Directive.[2] The DSA promises to ensure a safe, predictable and trusted online environment in which fundamental rights enshrined in the Charter of Fundamental Rights in the European Union ("CFR") are better protected.[3] The DSA creates

[1] 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), *OJ L 277 27.10.2022*, pp 1–102.

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *OJ L 178, 17.7.2000*, pp 1–16. See on the DSA in general: M Husovec, *Principles of the Digital Services Act* (Oxford University Press 2024); F Wilman, "The Digital Services Act (DSA): An Overview", accessible via https://dx.doi.org/10.2139/ssrn.4304586; G De Gregorio and P Dunn, "The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age" (2022) 59 Common Market Law Review 473, 483–8.

[3] Charter of Fundamental Rights of the European Union, *OJ C 326, 26.10.2012*, pp 391–407.

a layered approach to platform obligations, increasing duties as the size of the platform increases. Platforms with the most reach, and therefore the most potential for harms, have the most obligations under the DSA.[4] Very Large Online platforms and Very Large Online Search Engines ("VLOPSEs," platforms with a number of monthly active users exceeding 45 million)[5] need to abide by a range of risk-mitigating and transparency-building measures,[6] whereas micro- and small enterprises are excluded from the scope of a number of DSA provisions.[7]

In addition to creating a multi-layered regime for platform obligations, the DSA introduces a new administrative authority at the national level, tasked with overseeing DSA compliance: the Digital Services Coordinator ("DSC").[8] The DSC has a two-dimensional relationship with the right to freedom of expression of European internet users in enforcing the DSA. The first dimension is that DSCs can shape the freedom of expression of internet users through drafting norms for content moderation practices and empowering civil society actors to influence the content moderation process along the lines of national laws and speech traditions; although there is a common core of freedom of expression in Europe, there are regional differences. The second dimension is that DSCs protect the right to freedom of expression of internet users by acting as a complaint platform for internet users, and by sanctioning platforms for non-compliance. Their role is therefore also to rebalance the power in the online sphere between internet users, providers of intermediary services, and state actors.[9] If enforcement protects the freedom of expression of users, differences in enforcement can lead to different levels of protection of that freedom for internet users in the EU.

This article explores the role of the DSC in the DSA in light of its two-dimensional impact on the freedom of expression of internet users in the EU. It asserts that, while freedom of expression of internet users is anchored to an extent in DSA enforcement, there is a seeming disconnect between the impact DSCs can have on freedom of expression and the safeguards around their position. To this end, it is structured as follows: the first section describes the position of the DSC in the DSA and how its powers interact with the freedom of expression of internet users. The second section argues that the decentralised enforcement structure of the DSA affects the protection of freedom of expression of internet users. The third section makes suggestions as to how freedom of expression can be better safeguarded in the DSCs role in enforcing the DSA.

II. The digital services coordinator

This section dissects the role of the DSC in the DSA, and outlines how its powers interact with the freedom of expression of internet users. Subsection 1 describes the role, competence, and institutional embedding of DSCs, Subsection 2 provides a brief introduction into the legal framework for freedom of expression, Subsection 3 explores how the DSCs' powers interact with freedom of expression, and finally Subsection 4 provides an interim conclusion.

[4] Regulation 2022/2065, rec. 76.
[5] Regulation 2022/2065, art. 33(1).
[6] Regulation 2022/2065, Section 5, arts. 33–43.
[7] As defined in Recommendation 2003/361/EC; Regulation 2022/2065, Art 15(2); Art 19(1), Art 29(1).
[8] Regulation 2022/2065, Art 49(1)&(2).
[9] On the balancing of power, see generally: G De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (1st edn, Cambridge University Press 2022); G Gentile, "Between Online and Offline Due Process: The Digital Services Act" in A Engel and X Groussot (eds), *New Directives in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer 2023), pp 219–38.

1. DSCs as an institution and their competence

DSCs are national administrative authorities tasked with enforcing the DSA in a Member State.[10] Member States may choose to create a new enforcement authority to fulfil the role of DSC, but can also appoint an existing authority, or even divide the enforcement tasks over multiple existing authorities under one "coordinating" DSC.[11] DSCs – as decentral[12] enforcers of EU law – are embedded in the procedures of the DSA, but also in national administrative law, which lays down the procedural framework around its supervisory tasks and powers. This contribution touches upon that framework, but predominantly from the perspective of the DSA.[13] Currently, Member States have appointed existing consumer-, media-, and telecom-protection authorities as DSC. DSCs must perform their DSA tasks in an impartial and timely manner.[14] Member States shall provide them with sufficient technical, financial, and human resources to fulfil their oversight- and enforcement tasks.[15] DSCs must fulfil their tasks with complete independence, without prejudice to judicial review or budgetary control.[16] The principle of independence in this regard is contentious. Independence of DSCs could be necessary since they concern themselves with freedom of expression on the internet[17]; independence limits the procedural autonomy of Member States, however, and in the case of the DSA is not derived from primary law.[18] Independence in the DSA is therefore "rather thin."[19] The possibility of appointing different, existing, actors, the oversight role of the Commission (which is inherently not an independent authority[20]), and the various mandatory cooperation mechanisms all limit the supposed required of the DSC. An independent EU agency for oversight was proposed, but eventually rejected because "it stood in the way of expediency

[10] Regulation 2022/2065, Art 49(1)&(2).

[11] Regulation 2022/2065, Art 49(2), rec. 110.

[12] Generally, on centralised and decentralised enforcement: R Schütze, "From Rome to Lisbon: 'Executive Federalism' in the (New) European Union" (2010) 47 Common Market Law Review 1385.

[13] Assessing each DSC in the context of its own jurisdiction would be beyond the scope of this article. In addition to that, not all member states have fully adopted the national implementation laws attributing powers to the DSC, such as Spain and Bulgaria, or have even formally appointed a DSC, such as Belgium and Poland, see on this: <https://digital-strategy.ec.eruopea.eu/en/policies/ds-dscs>.

[14] Regulation 2022/2065, Art 50(1).

[15] Ibid.

[16] Regulation 2022/2065, Art 50(2). See also P Van Cleynenbreugel, "Independent Administrative Authorities and the Sectoral 'Europeanisation' of National Administrative Law: A European Union Law Perspective" (2023) available at <https://orbi.uliege.be/bitstream/2268/313933/1/EUDAIMONIA_WP20241.pdf> (last accessed 17 October 2024). The standard that needs to be applied in this case is unclear. On defining "independence," there is a high standard in the context of data protection Regulation 2016/679, art. 52; Court of Justice of the European Union, judgment of 16 October 2012, *European Commission v Republic of Austria,* C-614/10; Court of Justice of the European Union, judgment of 9 March 2010, *European Commission v Federal Republic of Germany,* C-518/07. In the context of competition law, there is a different standard, see for example Court of Justice of the European Union, judgment of 13 June 2018, *Commission v Poland,* C-530/16. It appears that the Commission had intended for DSCs to not necessarily be independent from other authorities, see Regulation 2022/2065, rec. 110, also G Spindler, "Der Referentenentwurf für ein Digitales Dienste Gesetz (DDG-RefE) – good bye TMG und NetzDG: Erster Überblick über die wesentlichen Weichenstellungen" (2023) 39 Computer und Recht 602, para 35, referring to M Cornlis, L Auler and S Kirsch, *Vollzug des Digital Services Act in Deutschland – Implementierung einer verbraucherorientierten Aufsichtsbehördenstruktur* (Mainzer Medieninstitut 2022) p 41.

[17] Timo Rademacher in F Hofmann and B Raue (eds), *Digital Services Act: Article-by-Article Commentary* (1st edn, Nomos 2025) pp 852–7.

[18] As is the case for data protection for example, see Art 16(2) Treaty on the Functioning of the European Union.

[19] Rademacher in Hofmann and Raue (n 17) 853.

[20] The Greens had rejected the proposal to put the Commission in charge of VLOP supervision as it is a political organ. See Husovec (n 2) 425 fn 39.

of the legislative process;"[21] i.e., harmonisation on aspects of enforcement was not desired at this stage.

DSCs are responsible for the oversight of providers of intermediary services with their main establishment in that Member State.[22] DSCs have competence when an intermediary service provider located in their jurisdiction violates the DSA, when an inhabitant of that member state complains about non-compliance of providers of intermediary services under the DSA, and when it receives complaints from another jurisdiction about an intermediary service provider located in its jurisdiction. DSCs rely on cooperation with other DSCs when enforcing against providers of intermediary services outside of their jurisdiction.[23] Competence as regulated in the DSA is without prejudice to Union law and national rules on private international law, which can aid in determining which DSC is relevant in a particular case.[24] However, the cross-border nature of the internet and the issues addressed in the DSA require an EU-wide approach.[25] The European Board of Digital Services is formed to streamline that cooperation.[26] The Board consists of high-level officials from each Member State DSC, and is chaired by the European Commission.[27] It contributes to a consistent application of the DSA across the European Union – a feature discussed more extensively in Section III.

Decentralised enforcement is a deliberate choice: it ensures that procedures take place at close proximity to citizens of Member States, and avoids unnecessary extension of the Commission's competence. That said, the EU regulator codified an exception to this: VLOPSEs. VLOPSEs are challenging to oversee due to their size and limited enforcement power at a national level.[28] Further, the EU regulator may have feared regulatory capture if VLOPSE enforcement was located in a single Member State, potentially endangering the required harmonisation and cooperation necessary to ensure a safe online environment.[29] After a VLOPSE is designated as such, DSCs share competence with the Commission.[30] The Commission mitigates potential large-scale harms within the EU arising from VLOPSEs by (partly) enforcing the DSA for intermediary service providers with more than 45 million monthly active users.[31] The Commission has exclusive competence over obligations laid down in Chapter III Section 5, containing predominantly transparency-and risk-mitigation obligations.[32] The Commission may also enforce other obligations under the DSA against VLOPs and VLOSEs when it deems appropriate[33]; this could be in the case of systemic infringement of the DSA that seriously affects recipients in a Member State.[34] Once the

[21] Ibid.

[22] Regulation 2022/2065, Art 56(1). 'Main establishment' is defined in the DSA as "where the provider has its head office or registered office within which the principal financial functions and operational control are exercised" (rec. 123.) It mirrors the definition of "place of central administration" *ex* Art 4(16)(a) of Regulation 2016/679. See also Opinion 04/2024 on the notion of main establishment of a controller in the European Union under Art 4(16)(a) GDPR, 13 February 2024.

[23] See, for example, Regulation 2022/2065, Arts 57, 58.

[24] Regulation 2022/2065, rec. 126.

[25] Regulation 2022/2065, rec. 130–31.

[26] Regulation 2022/2065, Art 61(2)(a).

[27] Regulation 2022/2065, Art 62(1)(2); the Commission does not have voting rights (61(3)).

[28] Regulation 2022/2065, rec. 124–125; the enforcement power of the Commission is inflated in this regard due to its supervisory body being paid for by designated VLOPSEs through Art 43; national supervisory bodies remain state-funded.

[29] Regulation 2022/2065, rec. 155.

[30] Regulation 2022/2065, Art 56(3).

[31] Rademacher in Hofmann and Raue (n 17) 991.

[32] Regulation 2022/2065, Art 56(2).

[33] Regulation 2022/2065, Art 56(4), rec. 125.

[34] Regulation 2022/2065, Art 65(2).

Commission has initiated proceedings under article 65(1), Member States can no longer start proceedings on the same infringement, to avoid *ne bis in idem*.[35]

At first glance, this reduces the impact of DSCs on freedom of expression; after all, most content is disseminated through VLOPSEs, for which competence is partially vertically centralised with the Commission. However, the DSC Database maintained by European Digital Rights shows that nearly all DSCs have received complaints under Article 53 DSA for enforcement against online platforms, and the Irish DSC has requested information from twelve intermediary service providers.[36] In cases of complaints, Article 53 does not provide the possibility submitting a complaint with the Commission,[37] only to the DSC of establishment; therefore, for all cases outside of Chapter III Section V, DSCs are the enforcing actor toward VLOPSEs for individual user complaints.[38] The fact that for all obligations outside of Chapter III Section V the Commission's enforcement role is limited procedurally, due to the required appropriateness for its involvement, as well as substantively, being that provider oversight in many cases requires significant knowledge of the impact of services on society and significant "political-cultural know-how,"[39] supports the role of the DSC as a key actor in DSA enforcement. Recent cases, such as the Belgian investigation into Telegram,[40] a messaging service noteworthy for its spreading of illegal content that does not yet qualify as a VLOP, or Twitch, a streaming service located in Luxembourg associated with livestreaming public shootings, show that enforcement on the national level by DSCs is highly relevant for platforms just below the VLOPSE threshold.[41] Conversely, inquiries fuelled by the Romanian DSC into the role of TikTok in Romanian elections illustrate the relevance of DSCs as a signalling entity, even when it comes to enforcement against VLOPSEs: the Romanian elections were annulled because of alleged interference through TikTok.[42] This resulted in the Romanian DSC requesting the blocking of TikTok in Romania,[43] and the European Commission launching an official investigation.[44] Individual cases and the Commission's significant, but limited competence, underscore the need for freedom of expression safeguards around the role of DSCs as national enforcers of the DSA.

[35] Regulation 2022/2065, Art 56(4), rec. 125.

[36] "The Digital Services Coordinators Database" (*DSC Database*) available at <https://dscdb.edri.org/> (last accessed 5 May 2025).

[37] Regulation 2022/2065, Art 53: "[. . .] the Digital Services Coordinator shall assess the complaint and, where appropriate, transmit it to the *Digital Services Coordinator* of establishment [. . .]" [emphasis added]. *Compare* for obligations under Chapter III Section V: Art 65(2).

[38] Rademacher in Hofmann and Raue (n 17) 944.

[39] Ibid, 991.

[40] "Telegram Still Doesn't Meet Large Platform Requirements under DSA" available at <https://sg.news.yahoo.com/telegram-still-doesnt-meet-large-095311777.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGA_0t6lA009T3PlmMHDv1K228kVtDkXBlkuappqM2CuEPAlK-YLwk0wp5XpT96_vaubJGnEV1UPgbwFNEBQsyAQ7o2LyJE8V8Y5na55OlvFvRvSUQEKMWwxHUZzHcvzrMzAVkyJforkxdgsxHWdAI6LoHmo7upC6Icn_8fnfQMi> (last accessed 1 November 2024).

[41] "Twitch Says Livestream of Buffalo Mass Shooting Was Removed in Less than 2 Minutes" | *CNN Business* available at <https://edition.cnn.com/2022/05/15/business/twitch-livestream-buffalo-massacre/> (last accessed 29 April 2025).

[42] "Romanian Authorities Ask EU Commission to Investigate TikTok Role in Election" | *Euronews*" available at <https://www.euronews.com/next/2024/11/27/romanian-authorities-ask-eu-commission-to-investigate-tiktok-role-in-election> (last accessed 3 December 2024).

[43] J Henley, "Romania Regulator Calls for TikTok Suspension amid Vote Interference Fears" *The Guardian* (27 November 2024) available at <https://www.theguardian.com/world/2024/nov/27/romanian-regulator-tiktok-suspended-cyber-interference-election-georgescu> (last accessed 14 January 2025).

[44] "Commission Opens Formal Proceedings Against TikTok under DSA" (*European Commission – European Commission*) available at <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487> (last accessed 18 December 2024).

2. Freedom of expression

EU citizens enjoy a similar right to freedom of expression under Article 11 CFR[45] on the internet as they do in the "offline world," with the notable distinction that, because of the nature of the internet, harms can be exacerbated by increased reach and longer availability.[46] Correspondingly, the right to freedom of expression requires speakers to take into account the wide audience they reach by communicating online: freedom of expression on the internet is a complex balancing act between the rights of the speaker on the internet and the societal interests concerned with being exposed to that speech on the internet.[47] Aside from an active right to freedom of expression, Article 11 CFR also encompasses a "passive" right to receive information.[48] This also encompasses right to access the internet.[49] As such, interferences with access to (parts of) the internet must be balanced with the freedom to access information.[50]

The scope of freedom of expression on the internet is determined predominantly through content moderation. Content moderation is the process by which providers of intermediary services determine what can be expressed and seen on the internet through removing content, amplification and de-amplification, and design of affordances.[51] The process involves a network of stakeholders affecting content moderation, such as civil society, users and government officials.[52] This process is primarily governed by the intermediary service provider, creating a complicated landscape in which private actors determine the scope of public values such as freedom of expression.[53] This creates a tension: fundamental rights norms, such as Article 11 CFR, are primarily addressed at the state or supranational organisations such as the EU; providers of intermediary services, as private parties, are not directly bound by Article 11 CFR.[54] Providers of intermediary services may be subjected to a horizontal effect of freedom of expression, depending on the national jurisdiction,[55] and can be affected by fundamental rights norms in the

[45] The right to freedom of expression in this contribution is interpreted in light of both Art 11 of the Charter of Fundamental Rights of the European Union, which is used as a reference point in Regulation 2022/2065, and in light of the European Convention of Human Rights; case law by the European Court of Human Rights can be used as a tool for interpretation following Art 52(3) Charter of Fundamental Rights of the European Union.

[46] European Court of Human Rights, 18 May 2021, *OOO Informatsionnoye Agentstvo Tambov-Inform v Russia,* 43351/12, para 84; European Court of Human Rights, 25 November 2021, *Biancardi v Italy,* 77419/15, para 62.

[47] European Court of Human Rights, 15 May 2023, *Sanchez v France,* 45581/15, paras 161–162; European Court of Human Rights, 16 June 2015, *Delfi v Estonia,* 64569/09.

[48] European Court of Human Rights, 13 February 2003, *Cetin et al v Turkey,* 40153/98 & 40160/98, para 64.

[49] European Court of Human Rights, 9 April 2019, *Navalnyy v Russia (no 2),* 43734/14, para 80.

[50] Court of Justice of the European Union, 27 March 2014, *UPC Telekabel Wien v Constantin Film Verleih & Wega Filmproduktionsgesellschaft,* C-314/12, para 55–6.

[51] K Gill, "Regulating Platform's Invisible Hand: Content Moderation Policies and Processes" (2021) 21 Wake Forest Journal of Business and Intellectual Property Law 171, 175–82; E Goldman, "Content Moderation Remedies" (2021) 28 Michigan Technology Law Review 1. See on amplification and de-amplification: P Leerssen, "An End to Shadow Banning? Transparency Rights in the Digital Services Act between Content Moderation and Curation" (2023) 48 Computer Law & Security Review 105790; T Gillespie, "Do Not Recommend? Reduction as a Form of Content Moderation" (2022) 8 Social Media + Society 20563051221117552; D Keller, "Amplification and Its Discontents: Why Regulating the Reach of Online Content Is Hard" (2021) 1 Journal of Free Speech Law 227.

[52] See, e.g., R Caplan, "Networked Platform Governance: The Construction of the Democratic Platform" (2023) 17 International Journal of Communication 3451.

[53] On how platforms govern freedom of expression on the internet, see, e.g., K Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech" (2018) 131 Harvard Law Review 1598; T Gillespie, *Custodians of the Internet* (1st edn, Yale University Press 2018).

[54] De Gregorio (n 9) 196–200; CE Haupt, "The Horizontal Effect of Fundamental Rights" in G De Gregorio, O Pollicino and P Valcke (eds), *Oxford Handbook on Digital Constitutionalism* (Oxford University Press 2024) p 10.

[55] J Gerards, "The Right to Freedom of Expression and of Information" in J Gerards (ed), *Fundamental Rights: the European and International Dimension* (Cambridge University Press 2023) 105, arguing that following Court of Justice of the European Union, 13 May 2014, *Google Spain v Mario Gonzalez,* C-131/32, it could be argued that freedom of

interpretation of private law, but such approaches are not clear-cut and differ per member state.[56] Similarly, the DSA, despite being inherently a market harmonisation instrument,[57] creates some fundamental rights obligations to providers of intermediary services.[58] Some scholars argue that the nature of individual fundamental rights is less compatible with the scale of content moderation,[59] and that application of fundamental rights to the digital realm in its current form requires rethinking.[60] Until such time, the realisation of fundamental rights in the digital sphere is dependent on platforms moderating content, and how regulators require platforms to include fundamental rights considerations in the content moderation process. DSCs affect freedom of expression against this background[61]: they enforce a regulation that directly affects the content moderation process, which invariably has effects on the freedom of expression of internet users. In their enforcement, they are required to take freedom of expression into account, both by application of the Charter and indirectly by the DSA.[62]

3. DSCs interacting with freedom of expression

DSCs, in their role as enforcer of the DSA, have a number of tasks that affect the freedom of expression of internet users. As iterated above, DSC tasks are predominantly aimed at content moderation on a systemic level, focusing on procedural safeguards and risk mitigation, not on individual pieces of content.[63] Their competence can be divided in two themes: powers that directly affect content moderation (I.3.a & I.3.b), and powers that

information has some horizontal effects in EU law: "the obligation to take action to ensure the freedom of information or balance it against other rights is, after all, directly imposed on the search engine operator." De Gregorio (n 13) also underlines that the Court of Justice of the European Union may be open to such an interpretation based on Court of Justice of the European Union, 27 March 2014, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, C-314/12; Court of Justice of the European Union, 15 September 2016, *Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH*, C-484/14. Also, e.g., Amélie Heldt, *Intensivere Drittwirkung* (Mohr Siebeck 2023).

[56] See, e.g., Bundesverfassungsgericht, 22 May 2019, *Der III. Weg*, 1 BvQ 42/19. More generally A Kuczerawy and J Quintais, "'Must-Carry', Special Treatment and Freedom of Expression on Online Platforms: A European Story" (forthcoming, on file with author).

[57] Regulation 2022/2065, preamble; Treaty on the Functioning of the European Union, Art 114; A Engel, X Groussot and GT Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*, vol 13 (Springer Nature Switzerland 2025) available at <https://link.springer.com/10.1007/978-3-031-65381-0> (last accessed 17 April 2025).

[58] See, e.g., Regulation 2022/2065, Art 14(4):

> Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expressions, freedom of pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.

See also JP Quintais, N Appelman and R Ó Fathaigh, "Using Terms and Conditions to Apply Fundamental Rights to Content Moderation" (2023) 24(5) German Law Journal 1.c

[59] E Douek, "The Limits of International Law in Content Moderation" (2020) 6 U.C. Irvine Journal of International, Transnational and Comparative Law 37; B Sander, "Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation" (2020) 43 Fordham International Law Journal 939.

[60] G Teubner, "Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution" (2017) 3 The Italian Law Journal 193.

[61] Paradoxically despite the DSA not directly requiring them to engage with the legality of individual pieces of content, see Regulation 2022/2065, rec. 109: "[. . .] This Regulation does not require Member States to confer on Competent Authorities the task to adjudicate on the lawfulness of specific items of content."

[62] E.g., Regulation 2022/2065, Art 49(6); rec. 115.

[63] Wilman (n 2) 18. Regulation 2022/2065, rec. 109; compare Rademacher in Hofmann and Raue (n 17) 870–2.

affect content moderation indirectly through investigating or sanctioning intermediary service providers (I.3.c & I.3.d).

a. Powers that affect the content moderation process

DSC may affect content moderation through Article 9 DSA, allowing "relevant national judicial or administrative authorities" to order the provider of intermediary services to act against illegal content.[64] DSCs explicitly fulfil a role as go-between for judicial or administrative authorities issuing orders to remove content or issuing orders to provide information; they must be informed by- and inform other DSCs of the content of such orders.[65] The institutional set-up explained in Section II.1 creates a peculiarity in this framework. The DSC itself qualifies as a relevant national authority, if appointed to this extent under national administrative law.[66] Aside from the DSC, it is possible that the authority hosting the DSC, e.g., the consumer authority of a member state, qualifies as a relevant national administrative authority. In the first instance, the interface with freedom of expression by the DSC is clear: if the DSC issues an order to act against illegal content and the provider of intermediary services follows up on that order by limiting access to the litigious content, the right to freedom of expression of the internet user is affected. In the second instance, if the hosting authority orders to act against illegal content, the DSC may still be involved, and therefore interacting with the right to freedom of expression of internet users. DSCs are currently part of oversight authorities that have tasks under national or EU law, which can qualify them as relevant national administrative authorities, allowing them to submit orders to act against illegal content or request information. This can cloud the oversight roles at one organisation. Ideally, oversight authorities separate their tasks: the requirement of independence for DSCs as laid down in Article 50(2) DSA requires that "competent authorities [. . .] act in *complete independence* from private *and public* bodies, without the obligation or possibility to seek or receive instructions [. . .]."[67] However, there is no guidance on what safeguards around the dual functioning of DSCs should look like in practice, meaning that, as said above, independence is "rather thin."[68] A consumer authority might issue an order to act against illegal content, but it would be unclear whether this is order originated from the DSC hosted at the consumer authority or the consumer authority itself. In any case, if the provider of intermediary services follows up on that order, the freedom of expression of the internet user is interfered with on behalf of the DSC or its hosting authority.

A second possible interference with freedom of expression is found in the explicit role for DSCs in formulating codes of conduct. Under Article 45, DSCs should encourage and facilitate the creation of codes of conduct, together with the Commission.[69] In encouraging or facilitating, DSCs can take varying roles which may affect the content of codes of conduct, for example by encouraging moderation of a specific type of content.[70] Although Codes of Conduct are a voluntary effort, there is significant informal pressure exuding

[64] Regulation 2022/2065, Art 9.

[65] Regulation 2022/2065, Art 9(3)(4) and 10(3)(4). Providing information to other DSCs reflects the wish to prevent *ne bis in idem* and contributes to the principle of mutual assistance *ex* art. 57(1).

[66] Compare Regulation 2022/2065, rec. 109.

[67] Regulation 2022/2065, rec. 112. See also more detailed fn. 16.

[68] Spindler (n 16) para 36.

[69] Regulation 2022/2065, Art 45.

[70] C Angelopoulos and Others, "Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation" (Institute for Information Law 2016). Notable examples are The EU Code of Conduct on Countering Illegal Hate Speech Online available at <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en#relatedlinks>; The 2022 Strengthened Code of Practice on Disinformation available at <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.

from encouragement or facilitation for providers of intermediary services to partake, which may lead to cynicism on the presentation of state-led regulatory efforts as "voluntary."[71] The "voluntary" nature of such codes, which is reinforced by non-participation in Codes of Conduct being interpreted as a contra-indicator for DSA compliance,[72] can also be interpreted as an interference with freedom of expression of internet users that lacks a legal basis if platforms remove content on the basis of Codes of Conduct that are not codified in law.[73]

This reasoning also applies to the enforcement of Article 14 on terms and conditions and Article 16 on notice and action mechanisms. Article 14 poses a number of requirements for intermediary service providers regarding their terms and conditions, such as providing information on policies, procedures and tools used for content moderation, and stipulates that providers of intermediary services must act diligently, objectively and enforce their terms of services in a proportionate manner, with due regard for the freedom of expression and the pluralism of the media.[74] Terms and conditions are commonly used by platforms to form guidelines that shape speech on their platforms.[75] This is one of the first regulatory interventions in the drafting and enforcement of terms and conditions, and provides significant power for DSCs to intervene in private norm-setting, for example on moderating certain types of content under terms and conditions.[76] Quintais et al underline this operational concern and raise questions on the enforcement of Article 14(4) in light of how well fundamental rights align with large-scale content moderation, as touched upon in I.2.[77] The enforcement of the article can therefore have far-reaching consequences, since moderation on the basis of terms and conditions forms the overwhelming majority of all content moderation decisions.[78]

How DSCs enforce or sanction compliance with article 16 forms a similar intervention in the content moderation process. Article 16 requires intermediary service providers to facilitate the submission of notices on illegal content. The mechanisms by which notices are shaped can affect the degree to which users report illegal content.[79] More pertinent for DSCs effect on freedom of expression of users is the enforcement of article 16(6).[80]

[71] R Griffin, "Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns" (2024) 2024 Technology and Regulation 167, 185.

[72] Regulation 2022/2065, rec. 104:

> The refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission's invitation to participate in the application of such a code of conduct could be taken into account, where relevant, whether the online platform or the online search engine has infringed the obligations laid down by this Regulation [. . .].

[73] J van de Kerkhof, "Jawboning Content Moderation from a European Perspective" in C van Oirsouw and Others (eds), *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era* (TMC Asser Press 2024) available at <https://doi.org/10.1007/978-94-6265-647-5_4> (last accessed 13 December 2024).

[74] Regulation 2022/2065, Art 14(1); Art 14(4).

[75] N Elkin-Koren, G De Gregorio and M Perer, "Social Media as Contractual Networks: A Bottom Up Check on Content Moderation" (2022) 107 Iowa Law Review 987; JP Quintais, G De Gregorio and JC Magalhães, "How Platforms Govern Users' Copyright-Protected Content: Exploring the Power of Private Ordering and Its Implications" (2023) 48 Computer Law & Security Review 105792.

[76] Quintais, Appelman and Ó Fathaigh (n 58) 29. See also Rademacher in Hofmann and Raue (n 17) 859.

[77] Quintais, Appelman and Ó Fathaigh (n 58).

[78] R Kaushal and Others, "Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database", *The 2024 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2024) available at <https://dl.acm.org/doi/10.1145/3630106.3658960> (last accessed 9 September 2024).

[79] See in the context of NetzDG: B Wagner and Others, "Regulating Transparency?: Facebook, Twitter and the German Network Enforcement Act" in *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (ACM 2020) available at <https://dl.acm.org/doi/10.1145/3351095.3372856> (last accessed 18 October 2023); A Heldt, "Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports" (2019) 8 Internet Policy Review 1–18.

[80] Regulation 2022/2065, Art 16(6).

Article 16(6) requires that intermediary service providers process notices in a timely, diligent, non-arbitrary, and objective manner.[81] The standards by which intermediary service providers moderate on the basis of notices determines the scope of freedom of expression of users whose content notices are submitted on. Enforcement aimed at the processing of such notices therefore shapes the right to freedom of expression online.

In a further intervention in the content moderation process, DSCs are tasked with certifying stakeholders in the content moderation process such as out-of-court dispute settlement bodies and trusted flaggers. If a user disagrees with the decision of an internal complaint-handling system on a complaint regarding a content moderation decision,[82] they have the right under the DSA to select any certified out-of-court dispute settlement body to appeal that decision.[83] Out-of-court dispute settlement bodies are independent entities certified by the DSC that decide on such matters in a fair, swift and cost-effective manner.[84] A well-known current example of such an entity is the Meta Oversight Board, which, although it has been criticised as a form of "governance-washing," has a significant norm-setting power in issuing decisions, affecting Meta's content moderation practices.[85]

Out-of-court dispute settlement bodies under Article 21 may have a less profound impact due to the fact that their decisions are non-binding.[86] Their impact is also limited by the fact that internet users are free to choose the out-of-court dispute settlement body of their preference; users are free to avoid out-of-court dispute settlement bodies that do not align with their values.[87] However, the normative power that non-binding decisions exude over content moderation practices can shift existing policy in favour of avoiding future adverse decisions, in line with the reasoning of the "chilling effect" platform liability can have on freedom of expression.[88] Authors so far have different visions on the impact out-of-court dispute settlement bodies will have on content moderation and freedom of expression in general: Wimmers argues that certifying more entities to decide on content moderation leads to further fragmentation, which goes against the spirit of the DSA.[89] He further argues that "free speech disputes do not lend themselves to settlement

[81] See D Holznagel, "How to Apply the Notice and Action Requirements under Art 16(6) Sentence 1 DSA — Which Action Actually?" (2024) 25 Computer Law Review International 172; Objectivity can be contentious: currently X is under investigation by the Commission *inter alia* for not handling notices objectively. See <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709>; see further M Fabbri, "The Role of Requests for Information in Governing Digital Platforms Under the Digital Services Act: The Case of X" (2025) 6 Journalism and Media 41.

[82] Regulation 2022/2065, Art 20.

[83] Regulation 2022/2065, Art 21(1).

[84] Regulation 2022/2065, Art 21(3)(e).

[85] LH Muniz Da Conceicao, "A Constitutional Reflector? Assessing Societal and Digital Constitutionalism in Meta's Oversight Board" (2024) 13 Global Constitutionalism 557–90; K Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression" (2020) 129 Yale Law Journal 2418; D Wong and L Floridi, "Meta's Oversight Board: A Review and Critical Assessment" (2023) 33 Minds and Machines 261.

[86] Regulation 2022/2065, Art 21(2). See also R Harrison, J Shipp and A Curtis, "Settling DSA-Related Disputes Outside the Courtroom: The Opportunities and Challenges Presented by Article 21 of the Digital Services Act" (2024).

[87] Regulation 2022/2065, Art 21(1). Currently, the number of out-of-court dispute settlement bodies that are onboarded with online platforms is still somewhat limited, however.

[88] Court of Justice of the European Union, 6 October 2020, *La Quadrature du Net*, C-511/18, C-512/18 & C-520/18, para 113; Court of Justice of the European Union, 8 April 2014, *Digital Rights Ireland*, C-293/12 & C-594/12, para 25; E.g. A Kuczerawy, "Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative" (2015) 31 Computer Law & Security Review 46; G Frosio and C Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime" (2023) 29 European Law Journal 31; Gerards (n 55) 103.

[89] J Wimmers, "The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act" (2021) 12 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 381.

by private bodies."[90] Ortolani proposes a more nuanced "wait-and-see" approach with regards to out-of-court dispute settlement bodies.[91] Assuming that out-of-court dispute settlement bodies have a significant impact on content moderation because of the normative weight of their decisions recalibrating content moderation practices, a question rises about the DSC certifying such bodies: they have the power to accredit entities that affect content moderation, an impact that is felt Union-wide, making the selection and accreditation of these entities an important interface with user's freedom of expression. The role of individual DSCs in this is crucial: if an out-of-court dispute settlement body fails to meet the requirements laid down in Article 21(3), only the certifying DSC can revoke that bodies' status, limiting the safeguards for EU citizens outside that Member State that may be affected by the normative power exuding from an out-of-court dispute settlement bodies' decisions.

The selection and certification of trusted flaggers presents a similar interface with freedom of expression. Trusted flaggers are state- and non-state entities that have priority access to the content moderation process, meaning that notices, "flags,"[92] they submit with the provider of intermediary services are treated expediently and with priority.[93] DSCs appoint trusted flaggers based on expertise, independence, diligence, accuracy and objectivity; priority of those flags is granted based on the experience such entities hold on a specific topic, usually leading to higher quality notices aiding online platforms in their content moderation process.[94] The status of trusted flagger can, especially when state entities act as trusted flaggers, exude pressure on providers of intermediary services to comply with removal requests.[95] This has a direct impact on the visibility of user-generated content. Trusted flaggers can report content on the basis of national or EU law following article 3(h), creating a risk for extraterritorial application of national law.[96] The fact that users do not have the freedom to select the trusted flaggers involved in their content moderation process exacerbates these concerns as opposed to the freedom they have in choosing out-of-court dispute settlement bodies. Selecting what entity takes part in the content moderation process requires DSCs to take into account the freedom of expression of internet users, or at least to consider the capacity of the trusted flagger to do so. However, similar to Article 21(3), the DSA does not provide clear guidance in this regard on Article 22(2), and the Commission is yet to exercise its power in issuing guidelines on the certification of trusted flaggers under Article 22(8).[97]

[90] Ibid, 383. This critique applies to freedom of expression in content moderation in general; see Douek (n 59); Sander (n 59); JM Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 University of California, Davis Law Review 1149.

[91] P Ortolani, "If You Build It, They Will Come" (2022) *Verfassungsblog* available at <https://verfassungsblog.de/dsa-build-it/> (last accessed 30 September 2024).

[92] K Crawford and T Gillespie, "What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint" (2016) 18 New Media & Society 410.

[93] Regulation 2022/2065, Art 22; see also N Appelman and P Leerssen, "On Trusted Flaggers" (2022) 24 Yale Journal of Law and Technology 452; SF Schwemer, "Trusted Notifiers and the Privatization of Online Enforcement" (2019) 35 Computer Law and Security Review 105339.

[94] Regulation 2022/2065, Art 22(2). See also B Raue, "Artikel 22 Vertrauenswürdige Hinweigeber" in F Hofmann and Others (eds), *Digital Services Act: Gesetz über digitale Dienste* (1. Auflage, Nomos 2023) pp 385–408.

[95] J van de Kerkhof, "Constitutional Aspects of Trusted Flaggers in The Netherlands" in J van Dijck and Others (eds), *Governing the Digital Society: Platforms, Artificial Intelligence, and Public Values* (Amsterdam University Press 2025) pp 83–99.

[96] Regulation 2022/2065, Art 16(1) and Art 3(h).

[97] One could argue that fundamental rights expertise is captured in "particular expertise and competence for the purpose of detecting, identifying and notifying illegal content" in Art 22(2), but this is not explicitly mentioned.

b. The European board of digital services

DSCs cooperate across the EU in the European Board of Digital Services. The Board is tasked with harmonising DSA enforcement across the EU. On a general level, DSCs contribute in the Board to drafting guidelines on matters covered by the DSA.[98] Although the Commission has explicit competences to issue guidelines, its role in the Board is limited because it has no voting powers. DSCs, in their norm-setting role in the Board, influence how the DSA is enforced throughout the European Union. In this role, they need to cooperate with twenty-six other DSCs, but larger DSCs, hosting more online platforms, may have more influence in the setting of guidelines, since they oversee more and larger providers of intermediary services and have more resources to engage in norm-development.[99] They have, as such, a more prominent position in shaping freedom of expression online than other DSCs, a "Dublin-Effect."[100]

Aside from general guidelines on DSA enforcement that may affect content moderation, there is an explicit role for the Board in crisis situations. The Board makes recommendations to the Commission on triggering the crisis response mechanism laid down in Article 36(1). In such cases, VLOPSEs must enact crisis response mechanisms that include the assessment of whether the functioning of their services contributes to a serious threat to public security or public health.[101] VLOPSEs must then apply specific, effective, and proportionate measures to mitigate threats and report back on these measures with the Commission.[102] These measures can have a significant impact on content moderation in the European Union: case law of the European Court of Human Rights such as *Cengiz et al v Turkey* and *Yilderim v Turkey* underline that crises can interfere with freedom of expression on the internet.[103] Similarly, the COVID-19-crisis showed that internet services are key sources of information on public health, sparking a rich debate on content moderation, freedom of expression, and disinformation.[104] The power to issue recommendations on enacting crisis protocols therefore has a significant impact on the freedom of expression of internet users. The influence of a single DSC in the grander scheme of Article 36 may be limited: a recommendation is issued by the Board, not by a single DSC, and the Commission has the final say in declaring states of crisis.[105] However, if a single DSC were particularly influential due to their size and the number of providers of intermediary services they host (the "Dublin-effect"), they may inspire the Commission to declare a state of crisis. It may be difficult for smaller, less influential DSCs to acquire a similar status. In the recent case of the alleged interference of the Romanian elections via

[98] Regulation 2022/2065, Art 61(2)(a)&(b).

[99] See also J Orlando-Salling, "The Digital Services Act in the European Periphery: Critical Perspectives on EU Digital Regulation" (2025) 3 European Law Open 1. taking a European core – periphery perspective on this matter.

[100] A play on Bradford's seminal "Brussels effect," see A Bradford, "The Brussels Effect" (2012) 107 Northwestern University Law Review 1. See also in commenting on the Draft DSA: D Holznagel, "Ireland Cannot Do It Alone" (*Verfassungsblog*, 27 April 2021) available at <https://verfassungsblog.de/dsa-ireland/> (last accessed 23 April 2025).

[101] Regulation 2022/2065, Art 36(1).

[102] Regulation 2022/2065, Art 36(3)(a).

[103] European Court of Human Rights, decision of 1 March 2016, *Cengiz et al v Turkey*, 48226/10 & 14027/11; European Court of Human Rights, decision of 18 March 2013, *Ahmet Yilderim v Turkey*, 3111/10.

[104] E.g., M Karanicolas, "Even in a Pandemic, Sunlight Is the Best Disinfectant: COVID-19 and Global Freedom of Expression" (2021) 22 Oregon Review of International Law 1; BBE van der Donk, "Should Critique on Governmental Policy Regarding Covid-19 Be Tolerated on Online Platforms? An Analysis of Recent Case-Law in the Netherlands" (2021) 13 Journal of Human Rights Practice 426.

[105] Regulation 2022/2065, Art 36(1): "Where a crisis occurs, the Commission, acting upon a recommendation of the Board, may adopt a decision" [. . .]; compare Art 56(2).

TikTok therein, it was difficult for the Romanian DSC to trigger a similar crisis situation for TikTok.[106]

c. Powers related to investigating service providers

To enforce the DSA, DSCs are attributed a range of investigatory and sanctioning powers to relating to providers of intermediary services for non-compliance with the DSA. Part of these powers is aimed at creating knowledge about platform practices. Regulators suffer from a significant knowledge deficit, and the DSA provides a toolbox for overcoming that.[107] DSCs can request updated transparency reports from intermediary service providers,[108] and request access with the Commission to risk assessments of VLOPSEs established in its jurisdiction.[109] DSCs can also request access to data with VLOPSEs under Article 40(1) for the purpose of monitoring and assessing compliance with the DSA with a reasoned request.[110] DSCs vet researchers, meaning they issue data access requests on behalf of researchers seeking to study systemic risks (Article 34(1)) under Article 40(8).[111] In granting applications, DSCs have a role in shaping the interpretation of systemic risk, even though that falls under the Commissions competence.[112] The information gathered through these research and data access requests shapes the understanding and therefore the enforcement of the systemic risk assessment, mitigation and auditing framework.[113]

Aside from requesting data access, it can request information from providers of intermediary services, as well as auditing organisations, including all members of staff.[114] It can further inspect the premises of providers of intermediary services and confiscate information relating to suspected infringement.[115] These are so-called "dawn-raids," which are already prevalent in other fields of law, such as consumer protection and competition law. In those fields they are considered impactful measures from a procedural- and human rights perspective, underlining the DSCs significant investigatory powers in the DSA.[116]

[106] Of course, this is difficult since the alleged misinformation campaign was largely only discovered after the fact, being that the election had already transpired. The Commission has since released an "election toolkit," see: available at <https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-best-practice-election-toolkit-digital-services-act> (last accessed 17 June 2025).

[107] E.g., Regulation 2022/2065, rec. 96.

[108] Regulation 2022/2065, Art 24(3) and (4).

[109] Regulation 2022/2065, Art 34(3).

[110] Regulation 2022/2065, Art 40(1).

[111] Regulation 2022/2065, Art 40(8), see also Draft Commission Delegated Regulation supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data pursuant to Art 40 of Regulation (EU) 2022/2065; see further A Liesenfeld, "The Legal Significance of Independent Research Based on Art 40 DSA for the Management of Systemic Risks in the Digital Services Act" (2024) 16 European Journal of Risk Regulation 184–96.

[112] Regulation 2022/2065, Art 56(2); on the cooperation with the Commission in issuing guidelines to mitigate systemic risks, see Art 35(3).

[113] MC de Carvalho, "It Will Be What We Want It to Be: Sociotechnical and Contested Systemic Risk at the Core of the EU's Regulation of Platforms' AI Systems" (2025) 16 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 35.

[114] Regulation 2022/2065, Art 51(1)(a).

[115] Regulation 2022/2065, Art 51(1)(b).

[116] H Andersson, *Dawn Raids Under Challenge: Due Process Aspects on the European Commission's Dawn Raid Practices* (Bloomsbury Publishing 2024). See also Court of Justice of the European Union, judgment of 20 June 2018, *Cesky Drahy v Commission,* T-325/16; European Court of Human Rights, judgment of 21 March 2017, *Janssen Cilag S.A.S. v France,* 33931/12. In a GDPR context, the power to "dawn-raid" is also provided in Art 58(1)(f) Regulation 2016/679, but it has not received similar criticism.

d. Powers related to sanctioning intermediary service providers

If investigatory powers indicate a violation of the DSA, the DSC can use its sanctioning powers to combat infringement. It can agree on binding commitments with providers aimed at ceasing the infringement,[117] or order cessation of the infringement under a periodic penalty.[118] It can also fine providers of intermediary services[119] or adopt interim measures that avoid the risk of serious harm arising from the infringement.[120] Penalties imposed on providers of intermediary services must be effective, proportionate and dissuasive; if sanctions do not lead to cessation of the infringement and the infringement causes serious harm that cannot be avoided, the DSC has the power to require the management body of the provider of intermediary services to examine the situation and adopt an action plan that must be carried out and reported upon.[121] If the infringement continues and entails a criminal offence and continues to involve a threat to the life or safety of people, the DSC can request a competent judicial authority in its Member State to temporarily restrict access to the service infringing on the DSA, or, if such is technically unfeasible, to the online interface of the provider of intermediary services.[122] The power to block access to platforms has been linked to freedom of expression infringements by the European Court of Human Rights, and underlines the enforcement power that DSCs hold.[123]

e. Safeguards around DSA enforcement

The DSA must be enforced in light of the principle of proportionality: any action taken must be proportional to the nature, gravity, duration, recurrence of the infringement, without unduly restricting access to the service; measures must also take into account the technical- and operational capacity of the provider of the intermediary service concerned.[124] Furthermore, Member States need to lay down rules and procedures to ensure that the exercise of sanctioning powers is compliant with applicable national law, the Charter, and general principles of EU law.[125] Affected parties of DSA enforcement enjoy the right to an effective judicial remedy through a range of private- and public

[117] Regulation 2022/2065, Art 51(2)(a).
[118] Regulation 2022/2065, Art 51(2)(d).
[119] Regulation 2022/2065, Art 51(2)(c).
[120] Regulation 2022/2065, Art 51(3).
[121] Regulation 2022/2065, Art 51(3)(a).
[122] Ibid.
[123] E.g., European Court of Human Rights, decision of 18 March 2013, *Ahmet Yilderim v Turkey,* 3111/10.
[124] Treaty on the European Union, Art 5(4); Regulation 2022/2065, Art 51(5). In this regard, the investigatory powers outlined in the previous subsection have a key role: in platform regulation, and intermediary service providers often claim that interventions requested by administrative or judicial authorities are technically unfeasible and therefore disproportionate. Examples of such arguments are found in: Court of Justice of the European Union, judgment of 13 May 2014, *Google Spain v AEPD & Mario Gonzalez,* C-131/12; Court of Justice of the European Union, judgment of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Ltd,* C-18/18; Court of Justice of the European Union, judgment of 22 June 2021, *Peterson v Google and Elsevier v Cyando,* C-682/18 and C-683/18; Court of Justice of the European Union, judgment of 26 April 2022, *Republic of Poland v European Parliament & Council of the European Union,* C-401/19. When it comes to the technical feasibility of content moderation orders, there is an awkward tension between the fact that Member States may not order providers of intermediary services to adopt general monitoring instruments under Article 8 DSA, but still request that *de facto* they employ general monitoring instruments in order to adhere to the highest industry standards (for example Article 19(4)(b) Directive 2019/790, to avoid liability for copyright infringement). Such is also established in European Court of Human Rights, 5 September 2023, *Zoechling v Austria,* 4222/18, para 13; European Court of Human Rights, 15 May 2023, *Sanchez v France,* 45581/15, para 190. See further on this M Senftleben and C Angelopoulos, "The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the e-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market" (2020) Amsterdam/Cambridge, accessible at =https://ssrn.com/abstract=3717022.
[125] Regulation 2022/2065, Art 51(6), see also Charter of Fundamental Rights of the European Union, Art 52(1).

enforcement mechanisms.[126] Public enforcement mechanisms involve filing complaints with Digital Services Coordinators under Article 53 or access to national courts.[127]

In terms of substantive fundamental rights, Article 51(6) emphasises the right to respect for private life and the rights of defence, including the right to be heard and access to the file.[128] Recital 153 further emphasises that the right to freedom of expression must also be taken into account in DSA enforcement.[129] Exactly how the right to freedom of expression is taken into account in the enforcement of the DSA is not clarified. DSCs likely have fundamental rights anchored in their national system as well, but scope of those fundamental rights may differ, as illustrated in Section III.2. This raises the question whether freedom of expression is sufficiently anchored in DSA enforcement.

4. Interim conclusion

Section II has outlined the various interfaces that the DSC's role under the DSA has with the freedom of expression of internet users. DSCs hold significant power that intervene with the content moderation process, and as such the DSC has the potential to influence freedom of expression on the internet: a responsibility that requires considerable safeguards. These safeguards, outlined in I.3.e, are relatively limited. Under the DSA, the DSC also has the responsibility to protect the freedom of expression of internet users. In that protecting role, the decentralised network of enforcement of the DSA presents a challenge. This is explored in the next section.

III. Decentralised enforcement leading to different applications of the DSA

This section builds on the previous section by explaining how the decentralised enforcement framework in the DSA can fragment its application, which can diminish the protection of freedom of expression. Decentralised enforcement has benefits: enforcement takes place in close proximity to where the effects are felt, builds on "political and cultural know-how," and Member States maintain administrative and procedural autonomy.[130] However, this article proposes that the decentralised structure of the DSA can lead to different levels of protection of freedom of expression, which is not sufficiently mitigated in DSA enforcement network. This is explained following an introduction of the DSA's decentralised enforcement structure.

1. The DSA's decentralised enforcement structure

The DSA's enforcement is dictated by national administrative authorities and the European Commission, relying on the competence structure described in Section II.1.[131] Rademacher and Marsch describe the DSA enforcement network as both horizontally and vertically

[126] Charter of Fundamental Rights of the European Union, Art 47.

[127] Regulation 2022/2065, Art 53; rec. 39; see also G De Gregorio and S Demková, "The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe" in C Van Oirsouw and Others (eds), *European Yearbook of Constitutional Law 2023*, vol 5 (TMC Asser Press 2024) available at <https://link.springer.com/10.1007/978-94-6265-647-5_10> (last accessed 23 December 2024).

[128] Charter of Fundamental Rights of the European Union, Art 8 and 48.

[129] Regulation 2022/2065, rec. 153.

[130] Court of Justice of the European Union, 16 December 1976, *Rewe v Landwirtschaftskammer für das Saarland*, C-33/76; Schütze (n 12).

[131] Ibid; K Jancewicz, P van Cleynenbreugel and J Bois, "Inconsistent Administrative Enforcement of EU Law at Member State Level: The Lisbon Treaty's Hidden Constitutional Challenge" (2024) available at <https://orbi.uliege.be/bitstream/2268/314238/1/EUDAIMONIA_WP20242.pdf> (last accessed 17 October 2024).

centralised.[132] DSA enforcement is centralised horizontally by a country-of-origin principle,[133] somewhat resembling the one-stop-shop found in the General Data Protection Regulation ("GDPR").[134] That framework can be used as a frame of reference for decentralised enforcement; other fields of EU law, such as consumer or competition law, have a different competence structure.[135] DSCs have competence over the providers of intermediary services located in their jurisdiction, but if intermediary service providers fall outside of their competence, they must rely on other DSCs to investigate and enforce.

The DSA creates a legally binding cooperation mechanism that is distinct from the framework in the GDPR. Under Article 58(1), a DSC of destination (i.e., in which the intermediary service is delivered) can request the DSC of establishment to take investigatory and enforcement measures to ensure compliance with the DSA.[136] These requests require the DSC of establishment to provide an assessment of the suspected infringement and an explanation of any investigatory or enforcement measures taken within two months following the request.[137] If deemed insufficient, the Commission acts as a dispute resolution mechanism, issuing non-binding conclusions to the DSC of establishment indicating whether the investigatory or enforcement measures are sufficient.[138] Similarly, the DSC of establishment can request, or be recommended to, launch a joint investigation, enabling more enforcement capacity over complicated matters.[139] These avenues help overcome potentially inactive administrative authorities; without such cooperation mechanisms, activation would have to be realised through infringement procedures under Article 258 TFEU.

Decentralised enforcement structures are no novelty in EU law. However, DSA enforcement is also vertically centralised, which is markedly different from other fields of law. For example, in data protection law the Commission is a relatively subordinate actor due to the strict independence of national data protection authorities,[140] and in consumer protection law, the Commission does not have significant enforcement powers, but is tasked with streamlining enforcement by independent national authorities.[141] As discussed in Section II.1, the Commission has exclusive competence over VLOPSE-specific obligations under Section 5 of Chapter 3, and can initiate proceedings against VLOPSEs for other obligations if appropriate. The Commission's position raises concerns about the independence requirement for enforcement of the DSA, since the Commission is an inherently political institution.[142] Adding to this, the Commission takes significant powers

[132] Rademacher and Marsch in Hofmann and Raue (n 17) 973–4.

[133] Regulation 2022/2065, Art 56(1).

[134] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016,* pp 1–88, Art 55 and 56.

[135] For example, consumer law requires the coordinated enforcement with a network of consumer protection authorities under Regulation 2017/2394, see also C Goanta and J Spanakis, "Discussing the Legitimacy of Digital Market Surveillance" (2022) 2 Stanford Journal of Computational Antitrust 44. Competition law is marked by the fact that the European Commission is the only enforcer in cases of merger control (Regulation 2004/139) or the DMA (Regulation 2022/1925), and it enforces concurrently with national competition authorities in cases concerning art. 101 TFEU and 102 TFEU.

[136] Regulation 2022/2065, Art 58(1).

[137] Regulation 2022/2065, Art 58(5).

[138] Regulation 2022/2065, Art 59(3).

[139] Regulation 2022/2065, Art 60(1).

[140] Regulation 2016/679, Art 51(1), rec. 117. Treaty on the Functioning of the European Union, Art 16(2); Charter of Fundamental Rights of the European Union, Art 8. See also L Mustert, "Cross-Border Enforcement of the GDPR by Independent Administrative Authorities" (University of Luxembourg 2023) 54–63 available at <https://orbilu.uni.lu/handle/10993/55782>.

[141] Regulation 2017/2394, see also Goanta and Spanakis (n 135).

[142] Rademacher in Hofmann and Raue (n 17) 851.

regarding fundamental rights of EU citizens, despite the DSA being entirely based on a legal basis of market harmonisation under Article 114 TFEU, creating the concern for competence creep.[143] From a practical perspective however, the Commission's involvement alleviates the enforcement burden on national coordinators for dealing with the largest intermediary service providers, and prevents regulatory capture of a single national authority as it occurred in data protection.[144] The vertical centralisation of enforcement in the DSA also mitigates concerns arising from a one-stop-shop model; however three factors troubling freedom of expression in the DSA's enforcement remain: (i) different scope of freedom of expression being facilitated in the DSA (ii) differences in the procedural frameworks in member states, leading to different levels of protection, and (iii) differences at an institutional level – the DSA is enforced by different types of institutions with varying levels of enforcement experience and resources, which can affect the nature of enforcement and its effectiveness.

2. *Different scope of freedom of expression facilitated by the DSA*

Fragmentation in the application of the DSA may be caused by substantively different interpretations of its contents by Digital Services Coordinators.[145] The primary concern is the wide definition of "illegal content" in Article 3(h), a core concept throughout the DSA. In its current phrasing, Article 3(h) is a content-agnostic enigma[146]: "any information that [. . .] is not in compliance with Union law, or the law of any Member State which is in compliance with Union law."[147] The definition is central in the DSA and weighs upon aspects that the DSC needs to enforce. In theory, its scope of application is near-limitless; Mauritz explains that because article 3(h) obfuscates the question what law is applicable, because it lacks a clear connecting factor connecting circumstances of the case to applicable national law.[148] Holznagel underlines this with an example[149]: holocaust denial

[143] Engel, Groussot and Petursson (n 57) 24.

[144] Rademacher in Hofmann and Raue (n 17) 991.

[145] It could be argued that different interpretations of procedural norms in the DSA can have an effect on the freedom of expression of internet users, for example affecting their right to an effective remedy. This is beyond the scope of this article.

[146] It is the intention of Art 3(h) to provide a wide definition. Regulation 2022/2065, rec 12: "[. . .] the concept of "illegal content" should broadly reflect the existing rules in the offline environment. In particular, the concept of "illegal content" should be defined broadly to cover information relating to illegal content, products, services and activities. [. . .] The question is whether this definition can lead to competency creep: a situation in which the Digital Services Coordinator, building on a broad definition of its subject matter (see, by comparison with data protection law, Purtova's commentary on how the broad concept of personal data in the GDPR leads to an overly wide scope of application: N Purtova, "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 Law, Innovation and Technology 40.) can assume competence over cases that could also fall under other enforcement authorities, particularly in light of the overlap between GDPR (Regulation 2016/679), DSA (Regulation 2022/2065), and AI Act (Regulation 2024/1689, with the exception of systemic risk assessments following rec. 118). See on this P de Hert and P Hajduk, "EU Cross-Regime Enforcement, Redundancy and Interdependence. Addressing Overlap of Enforcement Structures in the Digital Sphere after Meta" (2024) 2024 Technology and Regulation 291, commenting on Court of Justice, 4 July 2023, *Meta Platforms Inc v Bundeskartellamt*, C-252/21, presenting a similar struggle between competition- and data protection authorities. See also S Demková and G De Gregorio, "The Looming Enforcement Crisis in European Digital Policy" (*Verfassungsblog*, 10 February 2025) available at <https://verfassungsblog.de/the-looming-enforcement-crisis-ai-dsa-eu/> (last accessed 25 April 2025).

[147] Regulation 2022/2065, Art 3(h).

[148] FK Mauritz, "To Define Is Just to Define" (*Verfassungsblog*, 8 April 2024) available at <https://verfassungsblog.de/to-define-is-just-to-define/> (last accessed 20 August 2024).

[149] D Holznagel, "Safeguarding Adequate Rights Enforcement through the Digital Services Act (DSA)" available at <https://hateaid.org/wp-content/uploads/2022/05/2021-09-08-DSA-How-to-improve-enforcement-through-the-DSA.docx.pdf> (last accessed 26 August 2024).

is explicitly criminalised in some countries in the EU, such as Germany and France, but not in other countries, where it may be covered under more general hate speech provisions.[150] Another example: currently Hungary's anti-LGBT laws outlaw companies advertising in solidarity with the LGBT-community.[151] This begs the question whether, for example, the Irish DSC must sanction intermediary service providers that fail to suspend accounts spreading content related to these examples under article 23(1).[152]

The only back-stop delimiting "illegal content" in the DSA is found in the phrasing: "in compliance with Union law," meaning that the Charter can render any law incompatible with EU law inapplicable. This operationalises the principle of mutual trust[153] and confirms a basic understanding about what defines illegal content. This appears to be a sufficient safeguard, but in practice it creates a number of tensions. Firstly, it forces entities seeking a definition for "illegal content," such as providers of intermediary services, trusted flaggers, out-of-court dispute settlement bodies, but also Digital Services Coordinators, to evaluate whether the law they seek to apply is compliant with the Charter. This is a complicated endeavour that, aside from raising a range of legitimacy- and rule of law concerns related to this quasi-constitutional review of the litigious set of laws, could exceed the expertise of such entities, therefore proving an ineffective backstop. Secondly, it is unlikely that the interpretation of this backstop is uniform, potentially endangering the coherence of Union law. Article 61(2) attributes a harmonising role in this matter to the Board of DSCs.[154] However, this does not provide a clear avenue for DSCs seeking a guiding interpretation of the DSA with the Board, and even less so for out-of-court dispute settlement bodies and trusted flaggers, who ultimately interpret Article 3(h) by themselves. This may result in content being removed on the basis of Charter-incompatible or inapplicable law, contravening the legality requirement of interference with the right to freedom of expression laid down in Article 52(1) CFR.[155]

3. Different procedures on a national level

Differences in the implementing law of the DSA can also affect its application. This occurs when, under the discretion that Member States have to appoint supervisory authorities for each of the DSA's oversight tasks, different entities across member states can have the same supervisory tasks under the DSA.[156] The degree to which these enforcement structures can affect enforcement can be illustrated using the Netherlands and Austria as

[150] See on this: P Lobba, "Holocaust Denial before the European Court of Human Rights: Evolution of an Exceptional Regime" (2015) 26 European Journal of International Law 237: "the utterance alone does not warrant criminal punishment." See also, for example: Council Framework Decision 2008/913/JHA of 28 November 2008 on certain forms and expressions of racism and xenophobia by means of criminal law. Generally, holocaust denial is not covered by the right to freedom of expression as laid down in article 10 ECHR: European Court of Human Rights, 23 September 1998, *Lehideux & Isorni v France,* 55/1997/839/1045; also Oversight Board, 2023, *Holocaust Denial*, 2023-022-IG-UA.

[151] Act LXXIX of 2021 on taking more severe action against paedophile offenders and amending certain acts for the protection of children; See for commentary on its threat to the EU legal order: KL Scheppele, "The Treaties Without a Guardian: The European Commission and the Rule of Law" (2023) 29 Columbia Journal of European Law 93; BB Arcila and R Griffin, "Social Media Platforms and Challenges for Democracy, Rule of Law and Fundamental Rights" (European Parliament 2023) PE 743.400.

[152] Regulation 2022/2065, Art 23(1).

[153] Court of Justice of the European Union, 18 December 2014, Opinion 2/13, para 168; Treaty on the European Union, Art 2.

[154] Regulation 2022/2065, Art 61(2)(b).

[155] See also European Court of Human Rights, 26 April 1979, *Sunday Times v the United Kingdom,* 6538/74, para 49.

[156] Regulation 2022/2065, Art 49(2), rec. 109.

an example. An internet user in Austria complains[157] with the Austrian DSC (*KommAustria*) on being presented with advertisements based on profiling as defined in Article 4(4) GDPR,[158] by the provider of an online platform with its main establishment in the Netherlands, which infringes on Article 26(3) DSA.[159] The Austrian DSC must refer this matter to the Dutch DSC (*Autoriteit Consument en Markt)*.[160] The Dutch DSC will under the Dutch implementation law forward the case to the Dutch Data Protection Authority ('DPA'), who is attributed the task to oversee Article 26(3).[161] The Dutch DPA can then fine the intermediary service provider or make binding commitments, also under Dutch administrative law.[162] In the reverse scenario, if the user were a Dutch citizen complaining about an online platform established in Austria, the Dutch DSC would forward the case to the Dutch DPA.[163] The Dutch DPA would forward the case to the Austrian DPA, who then forwards the case to *KommAustria,* because *KommAustria* is the competent authority to enforce the DSA, including Article 26(3) under the Austrian implementation.[164] Final result is that, depending on the national implementation of the DSA, the same complaint is addressed by two different institutions.

The enforcement structure illustrated above is complex, raising concerns that are only somewhat mitigated in the DSA. The reality is that this enforcement structure can be further complicated if composite procedures are added because the Member State has a federal structure, meaning that competences may be attributed to regional rather than national authorities. In other fields of law, complex enforcement structures have been shown to ultimately lead to reduced accountability and protection of individual rights.[165] In DSA enforcement, each coordinating DSC is responsible for the uninterrupted functioning of their national composite procedures.[166] However, information deficits due to insufficient sharing of information[167]; supervision of administrative action; and, in the case of one-stop-shop mechanisms, administrative paralysis due to the overload that can arise from many platforms being located in a single member state[168] may interrupt composite procedures. Similarly, complaints under Article 53 suffer reduced potential for judicial review if they involve a cross-border aspect, since in principle only courts of the same legal order are able to review decisions of administrative authorities. This implies that complainants in a different jurisdiction may not be able to challenge a decision taken by a foreign DSC if it is adopted by their own DSC in their own jurisdiction, or that such a challenge requires the national court of one jurisdiction to review the assessment of that

[157] Regulation 2022/2065, Art 53; *Bundesgesetz über den Koordinator für digitale Dienste nach der Verordnung(EU) 2022/2065 über einen Binnenmarkt für digitale Dienste,* StF: BGBI. I Nr. 182/2023 (NR: GP XXVII RV 2309 AB 2344 S. 247 S. 247 BR: 11366 AB 11400 S. 961, para 2(3)11.

[158] Regulation 2016/679, Art 4(4).

[159] Regulation 2022/2065, Art 26(3).

[160] Regulation 2022/2065, Art 57(2) and 58(1).

[161] *Uitvoeringswet digitaledienstenverordening,* Art 3.2 para 1.

[162] *Algemene wet bestuursrecht*, Art 5:20.

[163] Uitvoeringswet Digitaledienstenverordening, Art 3.2(1).

[164] *Bundesgesetz K-DDG*, para 2(1). The Austrian DSC must interact with other competent authorities, and must have regular exchanges of views on issues that are concerned with the regulation of providers of intermediary services, and thus take the Austrian DPA's view into account.

[165] G Gentile and O Lynskey, "Deficient by Design? The Transnational Enforcement of the GDPR" (2022) 71 International and Comparative Law Quarterly 799.

[166] Rademacher in Hofmann and Raue (n 17) 850.

[167] HCH Hofmann, "Composite Decision Making Procedures in EU Administrative Law" in HCH Hofmann and AH Türk (eds), *Legal Challenges in EU Administrative Law* (Edward Elgar Publishing 2009) pp 3–4 available at <https://china.elgaronline.com/view/edcoll/9781847207883/9781847207883.00013.xml> (last accessed 28 April 2025).

[168] "Europe's Enforcement Paralysis" (*Irish Council for Civil Liberties* 2021) available at <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf> (last accessed 24 October 2024).

of another court in a different jurisdiction. Seeing as the national law applied in these cases is crucial (see II.2), this may leave complainants with limited potential for judicial review.[169]

Administrative law can also disperse levels of protection under the DSA. DSCs are ultimately rooted in their respective national legal orders, creating an interaction between national and EU law. Rules for such interactions are missing, according to van Cleynenbreugel.[170] National authorities could afford more protection under national administrative law than required under principles of EU administrative law,[171] resulting in different levels of protection, which may subsequently affect the right to freedom of expression. National administrative law, then, determines the level of protection that citizens have, potentially creating tensions in cross-border setting.[172] For example: appealability may differ under national administrative law. That affects decisions such as appointing trusted flaggers, out-of-court dispute settlement bodies, bilateral commitments with providers of intermediary services; all of which are decisions that shape the freedom of expression on the internet. If one member state has strict time limits regarding administrative procedures, but an internet user is waiting for an enforcement decision against a provider of intermediary services in the jurisdiction in which the intermediary service provider is located, it may lead to a situation in which enforcement decisions are not appealable because delays are caused across jurisdictions. This diminishes the protection and right to judicial review of EU internet users.

4. *Different enforcement strategies leading to different applications of the DSA*

Member States can select existing authorities, found new authorities, or select multiple authorities as DSC; currently, they overwhelmingly opt for appointing existing authorities.[173] The nature of the institution hosting the DSC affects the application of the DSA in three ways: (i) differences based on available resources, (ii) differences based on enforcement strategies and priorities; (iii) differences based on enforcement traditions of the national authority selected as DSC. Different enforcement strategies indirectly shape the freedom of expression of internet users: they determine the degree to which intermediary service providers can self-regulate, how strictly the DSA is enforced, but also how internet users are protected through effective remedies for potential infringements.[174]

[169] Rademacher and Marsch in Hofmann and Raue (n 17) 986–8. Rademacher and Marsch propose a horizontal preliminary ruling procedure under EU secondary law to overcome possible boundaries arising from the foreign review of national law.

[170] Van Cleynenbreugel (n 16).

[171] Ibid, 9–10; HCH Hofmann, "Multi-Jurisdictional Composite Procedures – The Backbone to the EU's Single Regulatory Space" (2019) available at <https://www.ssrn.com/abstract=3399042> (last accessed 24 October 2024).

[172] See in a data protection context: GG Fuster and Others, "The Right to Lodge a Data Protection Complaint: OK, but Then What?" (*AccessNow* 2022).

[173] P Van Cleynenbreugel and P Mattioli, "Digital Services Coordinators and Other Competent Authorities in the Digital Services Act: Streamlined Enforcement Coordination Lost?" (*European Law Blog*, 2023) available at <https://europeanlawblog.pubpub.org/pub/digital-services-coordinators-and-other-competent-authorities-in-the-digital-services-act-streamlined-enforcement-coordination-lost> (last accessed 19 August 2024). Van Cleynenbreugel and Mattioli suggest that rec. 109s phrasing that Member States "should be able to entrust more than one competent authority, with specific supervisory or enforcement tasks and competences concerning the application of this Regulation" should be interpreted as favouring conferring powers to existing authorities competent in related fields.

[174] Charter of Fundamental Rights of the European Union, Art 47; Court of Justice of the European Union, 22 December, *DEB v Germany*, C-279/09, para 33. See also De Gregorio and Demková (n 127).

The first instance that causes different levels of enforcement is related to resources and available expertise. Article 50(1) requires that DSCs have the necessary technical, financial, and human resources to supervise all providers of intermediary services in their competence,[175] solidifying sincere cooperation in DSA enforcement between Member States.[176] Some DSCs will therefore have to be larger than others, due to the number of providers of intermediary services established in their territory. However, differing levels of resources, particularly under-resourcing, can impact DSA enforcement. Orlando-Salling proposes that the financial resources of DSCs in "peripheral"[177] Member States, against a background of fiscal and debt crises, could strain the enforcement of the DSA in those member states.[178] Orlando-Salling rightly notes that this creates a disbalance in the degree to which the DSA is shaped by "core" Member States, where citizens of "peripheral" Member States could be less protected.[179] As a result DSCs with limited resources may not have the full expertise required to deal with complicated matters at scale. Differences in resources in other sectors with a decentralised enforcement structure, such as competition law and data protection, are found to lead to fragmented enforcement.[180] Being under-resourced can cause (a) case-overload and (b) failure to investigate potentially new infringements, ultimately endangering the protection of fundamental rights – such as the right to freedom of expression in the case of the DSA. For example, in a data protection setting, the EU Agency for Fundamental Rights notes that insufficient resources[181] has caused DPAs to prioritise certain enforcement tasks causing an inability to take action against potential harms to data subjects.[182] Strowel and Somaini theorise that the Irish DSC will be strained for resources due to the large number of providers of intermediary services established in that Member State.[183] Similarly, underfunding and understaffing is also identified as a barrier in consumer law enforcement.[184] Differences in resources could ultimately affect DSA

[175] Regulation 2016/679, Art 52(4).

[176] Treaty on the European Union, Art 4(3). It ensures the smooth operating of cooperative mechanisms such as Article 57 and 58, but also crucial processes such as the sharing of information through the system developed by the Commission under Article 85.

[177] referring to J Reynolds, "The Political Economy of States of Emergency Symposium: Third World Approaches to International Law (TWAIL) Conference: Capitalism and the Common Good" (2012) 14 Oregon Review of International Law 85.

[178] Orlando-Salling (n 100) 9–10.

[179] Orlando-Salling (n 100); building on D Kukovec, "Law and the Periphery" (2015) 21 European Law Journal 406.

[180] J Steenbergen, "Challenges to Enforcers" in C Rusu and Others (eds), *New Directions in Competition Law Enforcement*, vol 4 (Wolf Legal Publishers 2020) 1–19; "Overview on Resources Made Available by Member States to Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities" (*European Data Protection Board*) available at <https://www.edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf> (last accessed 31 October 2024).

[181] As required in Regulation 2016/679, Art 52(4).

[182] "GDPR in Practice: Experiences of Data Protection Authorities" (*European Union Agency for Fundamental Rights* 2024).

[183] A Strowel and L Somaini, "Towards a Robust Framework for Algorithmic Transparency to Tackle the Dissemination of Illegal and Harmful Content on Online Platforms" (2021) available at <https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf> (last accessed 17 October 2024); see also 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 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 66. Strowel and Somaini's critique is predominantly based on "What the DPC-Meta Decision Tells Us about the EU GDPR Dispute Resolution Mechanism" available at <https://iapp.org/news/a/what-the-dpc-meta-decision-tells-us-about-the-gdprs-dispute-resolution-mechanism> (last accessed 17 October 2024).

[184] G Straetmans and J Vereecken, "Towards a New Balance Between Private and Public Enforcement in EU Consumer Law" (2024) 4 European Review of Private Law 41, 63.

enforcement as well, and thus how freedom of expression of EU internet users is protected by DSCs.

The second instance that can affect DSA enforcement is varying enforcement strategies. Decentralised authorities can serve national interests in enforcing EU law.[185] Gentile and Lynskey describe how different enforcement strategies led to a fragmented application of the GDPR.[186] Enforcement tasks are interpreted differently across competent authorities: some authorities are more aggressive in enforcement, others are more idle.[187] National interests can play a role in this regard: being a lenient authority can be a way to attract such companies, A-G Bobek observes in *Facebook Belgium.*[188] This may also apply in a DSA context: DSCs may choose to be more lenient in investigating and sanctioning intermediary service providers to maintain their establishment in that jurisdiction. Lenient enforcement can affect internet user's rights, *de facto* sacrificing protection of freedom of expression online for economic gain. These practices can inspire forum-shopping, meaning that intermediary service providers determine their establishment based on that stance the DSC in that jurisdiction takes toward enforcement.[189]

A final factor contributing to different enforcement strategies are the enforcement traditions on which appointed DSCs build. While some DSCs, building on an institution concerned with media law, can rely on expertise on matters concerning freedom of expression, other DSCs building on consumer law or traffic authorities, have less experience in this regard. At the very least, these authorities may have different priorities based on the field of law in which they are rooted.[190] Conversely, entities rooted in a media law background may not have enforcement experience to fully exhaust the investigative and sanctioning powers outlined in I.3.c and I.3.d, since their respective field traditionally does not involve dawn raids and hefty fines as competition law or consumer law do.[191] This, again, requires expertise-building on the level of the DSC, which may lead to different enforcements of the DSA.

5. Interim conclusion

Sections II and III have described the role of the DSC in relation to the internet user's freedom of expression. On the one hand, the DSC shapes the freedom of expression through powers that affect the content moderation process; on the other hand, it protects the freedom of expression of internet users through sanctioning intermediary service providers and enforcing the DSA. In that regard, it is likely that the DSA is enforced differently across member states, because of different national landscapes, interests and administrative procedures. While this is not problematic in itself, the protection of freedom of expression under the DSA can be a concern when its enforcement leads to extraterritorial enforcement of inapplicable laws, or when enforcement strategies and

[185] See on this, for example, Court of Justice of the European Union, 9 March 2010, *Commission v Germany,* C-518/07, para 35.

[186] Gentile and Lynskey (n 165) 820–1.

[187] González Fuster and Others (n 172).

[188] Court of Justice of the European Union, Opinion of AG Bobek of 13 January 2021, *Facebook v Gegevensbeschermingsautoriteit,* C-645/19, para 124.

[189] Strowel and De Meyere (n 183) 79; T Mast, "Platform Law as EU Law" (2024) 73 GRUR International 607, 612; Frosio and Geiger (n 89) 44–6. Of course, providers of intermediary services rely heavily on infrastructure, sectoral regulation and tax benefits of member states, and therefore DSA enforcement will not always be a determining factor in determining the main place of establishment. See Gentile and Lynskey (n 165) 822.

[190] Orlando-Salling (n 100) 14.

[191] K Irion, *The Independence of Media Regulatory Authorities in Europe* (European Audiovisual Observatory 2019) 120. Although most media authorities have a power of inspection, that power can be objected to by the subjected party. Similarly, although media authorities have the capacity to fine, those fines are incomparable to the potential 6 per cent of annual worldwide turnover under Art 52(3) DSA.

practices harm the protection of freedom of expression of internet users. This supports the assertion in the introduction: there is a seeming disconnect between the profound impact that DSCs can have on freedom of expression of internet users and the safeguards surrounding their role. This is addressed in the next section.

IV. Suggestions for better safeguarding freedom of expression in DSA enforcement

This Section describes some avenues for better safeguarding freedom of expression through the application of the DSA. These are by no means exhaustive, and some of the risks identified above are inherent to the chosen enforcement structure in the DSA, and cannot be altered without significant DSA amendments. However, two avenues fitting the existing framework of DSA enforcement may mitigate the risks to freedom of expression outlined above: centralisation in cases of common concern – more so than currently foreseen in Article 56 DSA – to ensure better protection of freedom of expression in such cases; and guidance by the Board in standardising DSA enforcement, on the interpretation of illegal content, and better streamlining exchanges on national law, for more coherent DSA enforcement with regards to freedom of expression.

1. Further centralise DSA enforcement

Firstly, in complex cases with significant fundamental rights impact beyond VLOPSEs, the Commission and/or the Board should be involved in enforcement. DSA enforcement is vertically centralised for VLOPSEs, but some platforms with less than 45 million active monthly users cause similar concerns despite not meeting the "simple" threshold of monthly active users.[192] For example, Section II.1 mentioned the relevance of non-VLOPSE platforms such as Telegram or Twitch. Instances in which non-VLOPSEs can affect European elections, involve widespread censorship allegations, or cause significant harm to European citizens across borders, could warrant enforcement beyond the competence of the DSC of establishment. In the context of data protection, which lacks vertical centralisation compared to the DSA, Bastos and Palka suggest that enforcement must be centralised with the Commission or the EDPB in "cases of common European concern"[193] to overcome enforcement deficits and protect constitutional rights to data protection.[194] Despite VLOPSEs already accounting for centralisation – to a degree – in cases of common European concern,[195] further centralisation in sensitive cases avoids complications arising from enforcement at the national level described in Section III. Centralising enforcement in sensitive non-VLOPSE cases can ensure that freedom of expression is not harmed by inactive or politically motivated DSCs, or that the application of national law in such cases would create interferences with freedom of expression across the EU. This can be achieved in two ways: vertical centralisation with the Commission, and with the Board.[196]

[192] Regulation 2022/2065, art. 33(1). The number of monthly active users has been further specified in the Commission's Guidance on the requirement to publish user numbers: <https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers>; Under Article 33(2) and (3) the EU legislator expresses the desire for the threshold for VLOPSEs to correspond to roughly 10 per cent of the EU population.

[193] In cases of common European Concern they refer to cases that involve multiple jurisdictions and have a significant potential impact on fundamental rights across the EU.

[194] FB Bastos and P Pałka, "Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?" (2023) 19 European Constitutional Law Review 487.

[195] Regulation 2022/2065, rec. 76.

[196] Of course, the proposed independent European Digital Services Coordinator (see n 20) would be a third avenue, but this suggestion departs even further from the existing framework, and is therefore beyond the scope of this contribution.

Attributing enforcement competence beyond VLOPSEs to the Commission in cases of common European concern requires amendment to the DSA. Centralisation is enabled to some extent by the procedure laid down in article 59 on referral to the Commission, but that article only foresees the Commission reviewing enforcement actions taken by national authorities, not actually deciding on enforcement itself. This means that the risk of regulatory capture or administrative paralysis in sensitive cases is still located at the national level. The Board could make a recommendation of whether online platforms have a particular sensitivity toward fundamental rights in the EU that invokes the competence of the Commission, much akin the framework of Article 58(2). Complaints by service recipients across the EU are incorporated in assuming this competence, and maintains proximity of the complainant to the procedure that will ultimately affect their freedom of expression, while simultaneously aligning with the wish of the Parliament for more involvement of the Commission in the DSA's enforcement.[197] This ensures that the DSA's application is not nationalised, and "difficult" platforms do not necessarily need to be supervised by a single DSC; essentially, it sacrifices a degree of member state competence for more efficient enforcement. Of course, there are downsides to this approach: the Commission is not officially attributed competence in these manners, and its competence would require member states ceding additional enforcement powers. This approach may also contravene the principle of mutual trust, because it implies ineffectiveness of national enforcement in particularly sensitive cases.[198] Additionally, the critique of Section II on the independence of the Commission as an enforcement actor in the DSA framework still stands; this suggestion would therefore require a DSA amendment or member states to explicitly cede additional enforcement competence to the Commission. Enforcement in such instances could also be advised by the Board under article 63(1)(d), further solidifying Europe-wide support for the Commission's enforcement action.

Centralising enforcement with the Board could be achieved by allowing the Board to issue binding recommendations on initiating joint investigations. Currently, the Board may recommend joint investigations to the Member State of establishment[199]; if the Member State of establishment disagrees with the requested enforcement action, they communicate so in their preliminary position.[200] If that is deemed insufficient, the Board may refer the matter to the Commission for dispute resolution under Article 59, which would ultimately require the DSC of establishment to report back to the Commission, having taken "the utmost account" of the Commission's view.[201] Allowing the Board to make binding requests for joint investigations, altering Article 60, ensures enforcement in cases of common European concern, even if the DSC of establishment is unwilling to enforce the DSA, without the complexity of an infringement procedure *ex* Article 258 TFEU. This would of course affect the procedural autonomy of member states; to somewhat justify that, the DSA would need to be amended, and requests should be justified by a majority or qualified majority of DSCs.

[197] European Parliament Resolution of 20 October 2020 on the Digital Services Act and fundamental rights issued posed (2020/2022), *OJ C 404*, 6.10.2021, p. 53–62, para 18, 30, 40. See also Rademacher and Marsch Hofmann and Raue (n 17) 985.

[198] Court of Justice of the European Union, 18 December 2014, Opinion 2/13, para 168; Treaty on the European Union, Art 2.

[199] Regulation 2022/2065, Art 60(1)(b).

[200] Regulation 2022/2065, Art 60(2). This is also subject to a requirement of good faith cooperation under Art 60(4).

[201] Regulation 2022/2065, Art 60(3)(b); Art 59(3).

2. Further guide DSA enforcement

A second avenue that should be pursued is better use of guidelines by the Commission and the Board to guide DSA enforcement in alignment with freedom of expression. This is already explicitly established throughout the DSA, for example in the context of the selection of trusted flaggers,[202] and for the Board on the development of European guidelines.[203] Some aspects in the DSA require further guidance by the Commission and the Board. Practical guidelines on ensuring the independence of DSCs from their hosting authority are currently missing; as illustrated in Section II.3.a, the "thin" independence requirement can blur competences and create questions on the nature of DSA enforcement. Similarly, the Board must coordinate harmonious application of the DSA – the Commission may, through its seat on the Board, nudge the Board in that direction. Guidelines should be issued on interpreting illegal content in Article 3(h); these guidelines should address (a) the connecting factor of a set of laws to a particular case[204]; and (b) how the safeguard of compliance with EU law for national law can best be interpreted by actors relying on the definition of Article 3(h).

Further, the interpretation of national laws may, in cross-border cases, be dependent on foreign DSCs. In cases of unclarity of the substance of those laws, there are options for sharing information and mutual assistance between DSCs. The *lex ferenda* proposed by Rademacher and Marsch for "the introduction of an explicit horizontal preliminary ruling procedure under EU secondary law" streamlines this even further.[205] If a national court of the competent DSC, or the competent DSC itself, has issues interpreting aspects of a foreign law, they may refer those issues back to a court or the DSC in the requesting member state. This may prevent issues of extraterritorially or wrongly applying national laws identified *inter alia* under II.2, and it has the added benefit of allowing the complainant to be in closer proximity, and perhaps even appeal, decisions taken by the court of DSC in their member state in that preliminary reference procedure. The downside of this proposed solution is that the risks of composite procedures, such as delay and administrative paralysis, compound when the composite procedure requires authorities to refer issues back to member states that had originally forwarded the complaint; as such, the expedience of the procedure is an important factor to take into account before relying on Rademacher and Marsch's proposed horizontal procedure.

V. Conclusion

This article has analysed the role of the Digital Services Coordinator under the DSA in light of the freedom of expression of internet users. It highlights how DSCs, on the one hand, shape content moderation practices, and on the other hand how the DSC's role in the decentralised enforcement structure of the DSA affects the protection of freedom of expression of users from platform's content moderation practices. Both of these dimensions ultimately affect the right to freedom of expression of internet users. Safeguards around the protection of that right are sparse in the DSA: as an instrument, it mostly emphasises the responsibility that intermediary service providers have with regards to respecting freedom of expression, but does not acknowledge the risks that enforcement of the DSA at the national level can pose to the freedom of expression of internet users, either by varying speech traditions, or by its decentralised enforcement framework. DSCs only have responsibility toward freedom of expression in generally phrased safeguards, without a sufficient risk mitigation mechanism in place to address

[202] Regulation 2022/2065, Art 22(8).
[203] Regulation 2022/2065, Art 61(3)(e).
[204] Mauritz (n 148).
[205] Rademacher and Marsch in Hofmann and Raue (n 17) 988.

manifesting harms. This contribution proposes that these risks can be mitigated by a more uniform understanding of "illegal content" facilitated by horizontal preliminary proceedings, a possible enforcement competence for the Commission or the Board beyond VLOPSEs, and exhaustive use of guidance by the Board, especially on the requirement of independence for DSCs.

DSCs have a set of instruments to affect content moderation, and to regulate platforms that ultimately determine user's freedom of expression online. How these instruments are used is therefore key in creating a digital space in which freedom of expression is protected. The DSA talks the talk when it comes to protection of freedom of expression. If the DSA is to really protect freedom of expression online, its enforcement should walk the walk.

Acknowledgments. The author is grateful to Catalina Goanta, Peter Blok, Janneke Gerards, Viktorija Morozovaite, Lisette Mustert, and Nadya Purtova, and participants of the RESHUFFLE Young Scholars Workshop for comments on earlier drafts and insightful conversations on this topic. All mistakes are my own.

Cite this article: J van de Kerkhof, "The DSA's Tower of Babel: On Digital Services Coordinators and Freedom of Expression". *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.10034