The Enforcement of European Digital Regulation: Overlaps and Pathways

Giovanni De Gregorio[*] and Anna Vicinanza[•]

Abstract: The European Union has intensified its regulatory efforts in the digital domain, resulting in a complex and layered legal framework. Significant attention has focused on the lack of coherence across legislation and other regulatory instruments, while less consideration has been given to enforcement, particularly to the expansion of powers and overlaps of responsibilities distributed across multiple national and supranational authorities. This paper aims to address the primary challenges to the enforcement of the EU digital acquis and explore potential pathways for enhancing its effectiveness. The first part provides examples of how the growing number of EU legal instruments in the European digital policy, particularly targeting digital services, has not fully considered the intersections between different technologies and regulatory frameworks. The second part then underlines how these substantive overlaps translate into enforcement challenges. It addresses the quantitative dimension of the enforcement framework, detailing the multiplicity of bodies involved while analysing the overlapping competences that arise from this institutional complexity from the national and supranational perspectives. The final section explores possible solutions, evaluating opportunities and limitations of various pathways to improve the enforcement of European digital regulation.

Keywords. Public Enforcement – EU Law – Digital Technologies – Powers – Regulation

I. Introduction

European regulatory efforts around digital policy have accelerated over the last decade. The General Data Protection Regulation (GDPR),[1] the Digital Services Act (DSA),[2] the Digital Markets Act (DMA), and the Artificial Intelligence Act (AI Act)[3] are just four among the regulatory milestones aimed at addressing the constitutional challenges resulting from digitalisation. By introducing rules that strengthen procedural safeguards, rights and remedies,

[*] PLMJ Chair in Law and Technology, Católica Global School of Law.
[•] PhD Candidate in EU law, University of Bologna.
[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)
[2] Regulation (EU) 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
[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

and expand the powers of public authorities, the EU has broadly enlarged the digital *acquis communautaire*.[4]

This regulatory expansion has attracted significant attention,[5] but the resulting enforcement patchwork has received less scrutiny. Renewed concerns over what some have characterised as 'regulatory brutality'[6] have led to simplification efforts rather than enforcement restructuring and streamlining, most notably through the Digital Omnibus proposals,[7] which, despite minor coordination points, have largely overlooked the complexities in the enforcement architecture.[8] Moreover, enforcement challenges have been mostly examined at the level of the single regulation,[9] while the intertwinement of legal frameworks calls for a more integrated perspective and the exploration of possible systemic solutions to ensure not only regulatory coherence but also effectiveness across the EU digital acquis.[10]

The normative overlaps across legal instruments affecting the digital sector are numerous. A clear example can be found in the area of content curation. AI-driven systems for content curation and moderation operate at the junction of multiple legal frameworks, including content regulation and data protection,[11] while AI-powered political advertising can fall under electoral law, data protection, AI regulation, and digital services regulation simultaneously. Indeed, the DSA is just

[4] Scholars have increasingly started to refer to the growing body of legislation in the digital sector as the EU digital acquis. See: Giovanni De Gregorio and Simona Demkova, *Enforcing the EU Digital Acquis* (Digicon 2025); Artur Bogucki and others, 'The AI Act and Emerging EU Digital Acquis' (CEPS 2022) <https://www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/> accessed 13 January 2026; Irene Kamara and Marco Bassini, 'The Cybersecurity and AI Nexus in the EU Digital Acquis' [2025] MediaLaws <https://www.medialaws.eu/rivista/the-cybersecurity-and-ai-nexus-in-the-eu-digital-acquis/> accessed 13 January 2026.

[5] Regulatory overlap has recently seen the acknowledgment at the EU level, as noted, for example, by Commissioner Virkkunen (Toby Sterling, 'EU Commission Looks to Cut Overlap in Tech Directives - Virkkunen' *Reuters* (27 March 2025) <https://www.reuters.com/technology/eu-commission-looks-cut-overlap-tech-directives-virkkunen-2025-03-27/> accessed 11 April 2025.).

[6] Vagelis Papakonstantinou and Paul De Hert, 'The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of "Act-Ification", "GDPR Mimesis" and "EU Law Brutality"' (Social Science Research Network, 1 May 2022) <https://papers.ssrn.com/abstract=4123313> accessed 17 July 2025.

[7] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus).

[8] Giovanni De Gregorio and Simona Demkova, 'Reordering the Enforcement of European Digital Regulation in Times on Omnibus' *Enforcing the EU Digital Acquis* (Digicon 2025).

[9] Martin Husovec, 'Will the DSA Work? On Money and Effort' in Joris van Hoboken (ed), *Putting the Digitals Services Act Into Practice* (Verfassungbooks 2023); Filipe Brito Bastos and Przemysław Pałka, 'Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?' (2023) 19 European Constitutional Law Review 487 <https://www.cambridge.org/core/journals/european-constitutional-law-review/article/is-centralised-general-data-protection-regulation-enforcement-a-constitutional-necessity/65F232075D5ED87A1CE1E8F642E82206> accessed 13 February 2025; Hans-W Micklitz and Giovanni Sartor, 'Compliance and Enforcement in the AIA through AI' [2025] Yearbook of European Law yeae014 <https://doi.org/10.1093/yel/yeae014> accessed 17 July 2025; Ilaria Buri, 'A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023); Juian Jaursch, 'Platform Oversight' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks 2023); Catalina Goanta, 'Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice* (Verfassungbooks, 2023); Herwig CH Hofmann and Lisette Mustert, 'The Future of GDPR Enforcement' [2024] Verfassungsblog <https://verfassungsblog.de/the-future-of-gdpr-enforcement/> accessed 16 April 2025; Pietro Mattioli, 'Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action?' (2025) X(X) Utrecht Law Review 1.

[10] Simona Demková and Giovanni De Gregorio, 'The Looming Enforcement Crisis in European Digital Policy' [2025] Verfassungsblog <https://verfassungsblog.de/the-looming-enforcement-crisis-ai-dsa-eu/> accessed 13 February 2025; Peter Alexiadis and others, 'Coherence versus Fragmentation: Institutional Challenges to EU Digital Markets Regulation' (2023) 24 Business Law International 233 <https://heinonline.org/HOL/P?h=hein.journals/blawintnl24&i=253> accessed 20 January 2025; Miroslava Scholten, 'Mind the Trend! Enforcement of EU Law Has Been Moving to "Brussels"' (2017) 24 Journal of European Public Policy 1348 <https://doi.org/10.1080/13501763.2017.1314538> accessed 11 April 2025; Paul de Hert and Paweł 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 <https://techreg.org/article/view/19322> accessed 28 January 2025.

[11] Giovanni De Gregorio and Pietro Dunn, 'Artificial Intelligence and Freedom of Expression' in Alberto Quintavalla and Jeroen Temperman, *Artificial Intelligence and Human Rights* (Oxford University Press 2023) <https://papers.ssrn.com/abstract=4736744> accessed 23 July 2025.

one element of a broader regulatory system that overlaps with other regimes, not only with the GDPR, but also rules on audiovisual media services as defined by the Audiovisual Media Services (AVMS) Directive, or the AI Act.[12] The substantive intertwinement among these regimes also translates into concerns about the enforcement of such a broad regulatory framework. The expansion of substantive rules has not been accompanied by a coordination in the enforcement dimension. Indeed, rather than coordinating enforcement in cases of intersection across technological and regulatory overlaps, European digital regulation has introduced new powers and competences on top of that overlapping structure of uncoordinated rules and procedures at the EU and national level. This concern had been shared by the European Data Protection Board prior to the adoption of the Digital Services Package, particularly noting the emergence of overlaps in data protection across the DSA, DMA, and GDPR, resulting in parallel supervisory structures[13]. In fact, the fragmentation across legal regimes is accompanied by a patchwork of enforcement systems,[14] an approach that risks amplifying potential conflicts and inefficiencies.

This situation can be observed in both the number and diversity of authorities involved across distinct but overlapping legal regimes. The DSA, for instance, establishes Digital Services Coordinators (DSCs) at the national level, while the European Regulation on Political Advertising (PAR) and the AI Act require Member States to introduce further national authorities. In some cases, this institutional multiplication may lead to dozens of authorities involved in the same issue, thus increasing the risk of institutional conflicts and inconsistent enforcement, potentially undermining the constitutional goals of European digital regulation, and, broadly, the uniform application of EU law. While overlaps may be viewed positively in some respects, allowing for a plurality of perspectives and values to be considered, they also carry significant risks. The increased fragmentation of responsibilities can weaken enforcement efforts due to coordination costs for the administrations, stretch the principle of the rule of law, and create an unpredictable environment for economic operators.[12] Moreover, although not every instance of overlap results in conflict, such an outcome remains a possibility when authorities fail to coordinate or to reach an agreement, while regulatory gaps or inconsistent enforcement priorities may also arise.

This situation is even more concerning when considering that competent authorities are embedded in a web of complex horizontal and vertical relationships, at supranational and national levels. Overlapping mandates among authorities can arise either under the same regulatory framework (*intra-framework overlaps*), or under different ones (*extra-framework overlaps*), involving a

[12] Alexiadis and others (n 10) 244. See also below, par. II.
[13] European Data Protection Board, 'Statement on the Digital Services Package and Data Strategy' <https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-digital-services-package-and-data-strategy_en> accessed 20 January 2025.
[14] Hert and Hajduk (n 10). Similar questions concerning enforcement structures, their effectiveness, and the appropriate degree for harmonisation, and centralisation, also arise in other areas of EU law, such as financial and banking supervision, energy, and consumer protection.. For instance, in the area of financial supervision, see: Beatriz Garcìa Osma, Ana Gisbert and Begoña Navallas, 'What Are the Wider Supervisory Implications of the Wirecard Case?' (European Parliament | Economic Governance Support Unit (EGOV) | Directorate-General for Internal Policies 2020) PE 651.383 <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/651383/IPOL_STU%282020%29651383_EN.pdf?utm_source=chatgpt.com>; Miroslava Scholten and Annetje Ottow, 'Institutional Design of Enforcement in the EU: The Case of Financial Markets' (2014) 10 Utrecht Law Review 80 <https://papers.ssrn.com/abstract=2552571> accessed 15 January 2026; Matteo Gargantini, 'Regulatory Harmonization and Fragmentation in the Capital Markets Union' *Balancing Unity and Diversity in EU Legislation* (Edward Elgar Publishing 2024) <https://www.elgaronline.com/edcollchap/book/9781035302956/book-part-9781035302956-12.xml> accessed 15 January 2026. It may be worth exploring whether solutions developed in those sectors could be adapted to the digital field, following the model of comparative analyses such as, for instance: Filippo Annunziata and Mariateresa Maggiolino, 'The Single Supervisory Mechanism and the European Framework for the Enforcement of Competition Law: A Comparison between Two Models for Economic Governance in the EU' (2023) 24 Journal of Banking Regulation 264 <https://doi.org/10.1057/s41261-022-00197-1> accessed 15 January 2026.

single or different Member States. Intra-framework overlaps typically emerge when different authorities are designated to enforce the same regulation, while extra-framework overlaps stem from substantive overlaps between distinct regulatory instruments. Indeed, within Member States, multiple regulatory authorities may have overlapping mandates, leading to potential conflicts or inefficiencies. For example, national media regulators, data protection authorities, and competition regulators may each claim competence over different aspects of platform regulation, such as content moderation, data protection, and market dominance. Moreover, in transnational cases, authorities from different Member States may assert competence over the same practices, creating legal uncertainty and complicating compliance efforts. At the supranational level, intra-framework and extra-framework overlaps arise in the coordination between national regulatory authorities and supranational bodies, particularly the European Commission, as well as among different authorities at the EU level.

By examining landmark regulations on digital services,[15] this work primarily focuses on public enforcement, even though the new possibilities for private enforcement arising from the expansion of EU regulation in the digital domain introduce another layer of potential inconsistencies and conflicts.[16] Enforcement is thus understood here as the activity through which selected administrative authorities monitor compliance and impose sanctions, in accordance with individual regulatory frameworks.[17] The importance of enforcement within the regulatory process has long been acknowledged, as it is essential to ensure that legal obligations effectively translate into compliance.[18] While various approaches exist for determining the optimal level of enforcement,[19] there is a broad consensus effectiveness is central to foster both special and general deterrence.[20]

More in details, this work explores the different types of institutional overlaps and potential clashes of public enforcement powers in European digital policy, developing a taxonomy supported by concrete examples drawn from recent enforcement practice. This effort is essential to better understand where frictions arise and how enforcement structures could be reformed to

[15] While the digital regulatory landscape is broad, this paper concentrates on a core set of instruments: the Digital Services Act (DSA), the Digital Markets Act (DMA), the General Data Protection Regulation (GDPR), the Media Freedom Act, the Regulation on Political Advertising, including a glance at relevant provisions of competition law and consumer protection law. However, other regulatory frameworks – such as copyright law – which, although not addressed in detail here, may raise similar coordination and enforcement issues. For a more comprehensive list of EU regulations affecting the digital sector, see: J Scott Marcus, Kamil Sekut and Kai Zenner, 'A Dataset on EU Legislation for the Digital World' (*Bruegel | The Brussels-based economic think tank*, 4 June 2025) <https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world> accessed 5 June 2025.

[16] Giovanni De Gregorio and Simona Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' *European Yearbook of Constitutional Law 2024* (2024) <https://link.springer.com/chapter/10.1007/978-94-6265-647-5_10> accessed 20 May 2025; Daniel Holznagel, 'The Digital Services Act Wants You to "Sue" Facebook over Content Decisions in Private de Facto Courts' [2021] Verfassungsblog <https://verfassungsblog.de/dsa-art-21/> accessed 12 May 2025; Husovec (n 9); Paddy Leerssen and others, 'Report: Pathways to Private Enforcement of the Digital Services Act' (DSA Observatory 2025) <https://dsa-observatory.eu/2025/06/05/report-pathways-to-private-enforcement-of-the-digital-services-act-dsa/> accessed 15 January 2026.

[17] John AE Vervaele, *Compliance and Enforcement of European Community Law* (Wolters Kluwer 1999) VII; Miroslava Scholten and Leander Stähler, 'Introduction to Research Handbook on the Enforcement of EU Law' *Research Handbook on the Enforcement of EU Law* (Edward Elgar Publishing 2023) 3 <https://www.elgaronline.com/edcollchap/book/9781802208030/book-part-9781802208030-9.xml> accessed 25 July 2025.

[18] Scholten and Stähler (n 18) 2.

[19] Robert Baldwin, Martin Cave and Martin Lodge, 'Enforcing Regulation' in Robert Baldwin, Martin Cave and Martin Lodge (eds), *Understanding Regulation: Theory, Strategy, and Practice* (Oxford University Press 2011) 248 <https://doi.org/10.1093/acprof:osobl/9780199576081.003.0011> accessed 13 January 2026; Florentin Blanc and Michael G Faure, 'Smart Enforcement. Theory and Practice' (Social Science Research Network, 1 November 2018) <https://papers.ssrn.com/abstract=3372956> accessed 13 January 2026; S Shavell, 'The Optimal Structure of Law Enforcement' in Robert Baldwin, Colin Scott and Christopher Hood (eds), *A Reader on Regulation* (Oxford University Press 1998) <https://doi.org/10.1093/acprof:oso/9780198765295.003.0011> accessed 13 January 2026.

[20] Vervaele (n 18) VII.

ensure more coherent and effective oversight. Then, this work examines three possible approaches to address the situation, looking at their potential and limitations. A short-term option involves strengthening existing cooperation mechanisms between national and European authorities, including the possible establishment of a coordination forum. Another solution would be for the EU to adopt a more holistic positive framework by introducing an overarching regulation that aligns the enforcement mechanisms of different digital regulations, reducing redundancies, streamlining oversight, and creating binding conflict-resolution systems. Broadly, another alternative would consist of establishing a more centralised enforcement body at the EU level, which could oversee the implementation of particularly important or systemic cases in a more uniform manner.

The first part of this paper examines the issue of technological intersections and regulatory overlaps characterising the numerous legal instruments introduced by the EU in different areas of digital policy. The second part then underlines how these regulatory entanglements translate into enforcement challenges, thus analysing the horizontal and vertical overlaps that arise from the increasing number and powers of enforcement bodies. The third part examines the potential ways to address the complexity of enforcement by considering the opportunities and limitations of three proposals to enhance enforcement in European digital regulation.

II. Technological Intersections and Regulatory Overlaps

In the last ten years, the EU has intensified its regulatory efforts on digital policies. Particularly in response to the challenges posed by online platforms,[21] the Commission has moved towards a constitutional oriented approach, reflected in the adoption of regulations that represent a commitment to EU constitutional values. These include, the GDPR and the Digital Services Act which, in the words of President von der Leyen, express EU's stance: 'We embrace new technologies. But we stand by our values'.[22]

This expansion has produced regulatory overlaps, largely connected to technological intersections. Rules on content have entered the realm of data protection, considering how services generally operate in the digital environment.[23] Indeed, data collection lies at the core of digital business models, feeding the algorithms that determine, for instance, how content is disseminated. In this case, the DSA imposes restrictions on the use of personal data for personalised content recommendations,[24] especially regarding online advertising. In doing so, the regulation refers repeatedly to the GDPR. For instance, the DSA refers to the definition of 'special categories of data' given by the GDPR.[25] However, while the GDPR restricts the processing of particular categories of data to specific cases, the DSA goes further by completely prohibiting the profiling of users based on this data for online advertisement purposes.

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe COM(2016) 288 final.
[22] Ursula von der Leyen, 'President's speech at "Leading the Digital Decade"' (1 June 2021) <https://ec.europa.eu/commission/presscorner/detail/it/speech_21_2804> accessed 23 July 2025.
[23] Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) 131 <https://www.cambridge.org/core/books/digital-constitutionalism-in-europe/A3F61C6368D17D953457234B8A59C502> accessed 13 November 2024.
[24] See DSA, Article 26 and 28.
[25] Article 26 of the DSA refers to Article 9 of the GDPR.

Beyond the DSA, online advertising is shaped by a mix of AI, data and platform policies, as well as consumer protection laws and the PAR.[26] Particularly, when the advertisement is 'political',[27] the PAR introduces special obligations related to transparency and data use, complementing the requirements set by the DSA and other data protection regulations. Moreover, the regulation requires online platforms to obtain explicit user consent for processing personal data in the case of targeted political advertising, and to provide an option for users to access their services without giving such consent. Moreover, similarly to the DSA, it completely prohibits targeted political advertisement based on profiling using special categories of data, as defined by the GDPR.[28]

Additional restrictions on the use of data are introduced to foster competition by the Digital Markets Act,[29] which aims to curb abuses of market power by major platforms designated as 'gatekeepers'. More precisely, the DMA prohibits gatekeepers from combining users' data across different services without explicit consent,[30] a practice that may also be unlawful under the GDPR if lacking a legitimate basis.[31] Furthermore, such conduct could also be deemed anti-competitive under EU competition law, as demonstrated by the *Meta* case,[32] which originated from the German Federal Cartel Office's findings that the combination of user data from different sources was both a breach of the GDPR and an abuse of dominant position.

Further complexity arises from the intersection of the regulation on online platforms with media rules. The Audiovisual Media Services Directive, [33] which was not amended by the DSA, required Member States to impose stringent obligations on Video-Sharing Platforms (VSPs) to prevent the spread of certain harmful content, including illegal content, terrorism, and incitement to violence or hatred against groups or individuals.[34] A similar need to mitigate risks related to the spread of harmful content and the protection of minors is also imposed by the DSA on online platforms which qualify as Very Large Online Platforms or Very Large Online Search Engines (hereinafter jointly referred to as 'VLOPs').[35] The European Media Freedom Act (EMFA) also intersects with the DSA, complementing its safeguards on moderation decisions when the affected user is a media service provider.[36] More precisely, the EMFA mandates prior notification before any restriction is imposed and grants priority treatment for complaints related to content moderation when the affected party is a media service provider on a Very Large Online Platform.[37] The EMFA contains, however, some explicit coordination rules with the DSA, for instance, when establishing

[26] For instance, advertisement is regulated by the Unfair Commercial Practices Directive (Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council).
[27] As defined by PAR, Article 3(2).
[28] PAR, Article 18.
[29] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
[30] DMA, Article 5(2).
[31] GDPR, Article 6.
[32] CJUE, Meta platforms and others, C-252/21, 4.7.2023.
[33] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).
[34] AVMS Directive, Article 28b.
[35] DSA, Articles 34 and 35.
[36] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a Common Framework for Media Services in the Internal Market and amending Directive 2010/13/EU (European Media Freedom Act).
[37] EMFA, Article 18. Media services are defined by Article 2 of the EMFA.

that compliance with EMFA provisions concerning online platforms may be taken into consideration by the European Commission when enforcing the DSA.[38]

Likewise, the rules introduced by the AI Act relate to the GDPR, considering the strong relationship between the processing of data and AI technologies. The legal bases to process personal data are indeed a critical point for the development and deployment of AI technologies.[39] Nonetheless, the structure of the two legislations differs, particularly when looking at their risk-based approach.[40] Indeed, the accountability principle in the GDPR, based on a bottom-up approach, is not necessarily expressed in the AI Act, which instead introduces a definition of the risks from the top, as in the case of prohibited practices.[41] Likewise, risk assessment obligations in the GDPR, such as the Data Protection Impact Assessment,[42] are connected with risk assessment in the AI Act, particularly the Fundamental Rights Impact Assessment for certain categories of deployers.[43]

Moreover, the rules on AI are also relevant to online platforms, since some of the VLOPs have become AI powerhouses. For instance, providers of generative AI models with systemic risk bear specific risk-management obligations.[44] If a VLOPs also fall into this category, it could be required to conduct a systemic risk assessment and mitigation under both the AI Act and the DSA. This possibility is explicitly taken into consideration by the AI Act's preamble, which states that to the extent that AI systems or AI models are embedded within designated VLOPs, they are subject to the risk assessment framework of the DSA.[45] Consequently, the risk-management provisions of the AI Act should be considered 'automatically' fulfilled, unless distinct systemic risks specifically related to AI models emerge and are identified.[46] Another connection between the AI Act and the DSA arises in relation to the obligations placed on AI providers and deployers to enable the detection and disclosure of artificially generated or manipulated outputs,[47] which is explicitly recognised as relevant to addressing the risks to democratic processes, civic debates, and electoral integrity, as outlined in the DSA.[48] While these regulatory connections can be considered a positive step toward a more integrated framework, no corresponding coordination exists in the enforcement structure.

These examples reflect a complex and layered legal system characterised by substantive regulatory overlaps. As services and functionalities often operate interdependently, it is almost inevitable that a single technology falls under multiple legal regimes at once. For instance, due to technological intersections, a single service or entity may simultaneously be classified as a online platform, AI deployer, data processor, and video-sharing platform. This situation does not only

[38] Recital 55 EMFA states that, for enforcing the DSA, the Commission can consider the opinions submitted by the European Board of Media Services on the outcomes of the 'meaningful dialogue' VLOPs and media service providers can initiate in order to find an amicable solution for terminating unjustified restrictions (See: EMFA, Article 19). Furthermore, Recital 56 states that the outcomes of such dialogues may be taken into account by the Commission when supervising systemic risks assessment under Article 34 and 35 of the DSA.
[39] GDPR, Art. 6, 9.
[40] De Gregorio and Dunn (n 12).
[41] AI Act, Art. 5.
[42] GDPR, Art. 35.
[43] AI Act, Art. 27.
[44] AI Act, Article 55(1).
[45] As explicitly recognized by the AI Act itself at Recital 118.
[46] AI Act, Arts 51, 55.
[47] AI Act, Art. 50.
[48] AI Act, Recital 120 referring to DSA, Article 34.

affect substantive rules but also the enforcement of these legal instruments. Indeed, the enforcement structures of these regulations have not adequately considered their substantive regulatory overlaps resulting from technological convergence, with competencies and responsibilities that are spread across multiple national and supranational authorities, operating either under the same legal basis or across different regimes. The next section examines the complexity of enforcing European digital regulation, particularly looking at coexisting competences at the national level, both within single member states and in cross-border cases, before delving into the structure of supranational enforcement and horizontal or vertical overlaps that may arise.

III. Competences and Enforcement Overlaps

The expansion of the EU digital acquis has been accompanied by a proliferation of authorities with competence in the digital sector. The consequence is not merely bureaucratic expansion. While parallel competences can, in principle, foster beneficial synergies, for instance by encouraging specialisation and mutual oversight, their positive effects depend heavily on the presence of coordination mechanisms and systems of conflict resolution. In their absence, the dispersion of responsibilities across various actors undermines coherence and inflates operational costs for public administrations, broadly undermining legal certainty, or even leading to institutional conflicts. Although not every instance of institutional overlap leads to open conflict, the potential for such outcomes remains significant, particularly when coordination mechanisms are weak or non-existent. In such cases, courts remain the ultimate forum for resolving institutional conflicts, but relying on litigation is rather inefficient, especially in light of the numerous potential overlaps.

This situation results from a fragmented institutional architecture in which several bodies may become involved in addressing a single issue. The following table provides a sample of the bodies vested with enforcement powers for a selected set of regulations on digital services, using two Member States as examples.

Table 1. Overview of EU national and supranational authorities involved in the enforcement of selected regulations

		DSA	DMA	AI ACT	GDPR	PAR	EMFA	AVMS	COMP	CONS
EU	European Commission	✔	✔	✔					✔	
	European Board for Media Services						✔	✔		
	European Data Protection Board				✔					
	European Competition Network								✔	
	European AI Board			✔						
	Consumer Protection Cooperation Network									✔

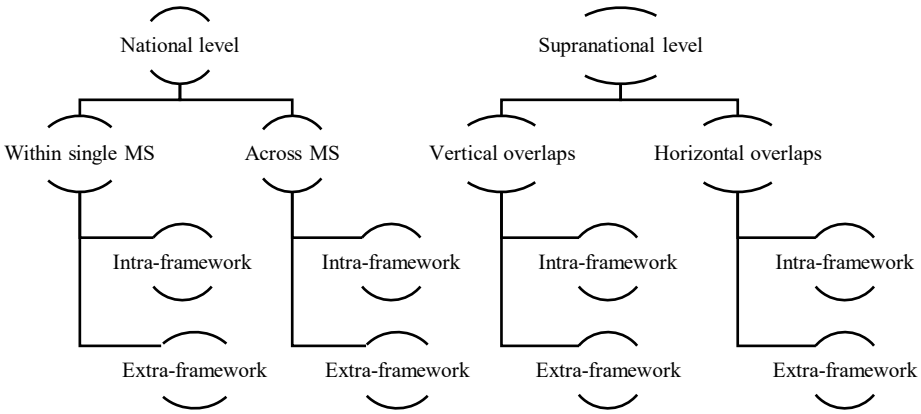
	European Board for Digital Services	✔							
IT	Media regulatory authority (AGCOM)	✔			✔	✔	✔		
	Data Protection Authority (Garante)			✔	✔				
	National competition authority (AGCM)							✔	✔
	National Cybersecurity Agency		◥						
	AgID		◥						
IE	Broadcasting Authority (BCI)						✔		
	Media Commission (Comisiún na Meán)	✔			✔	✔			
	Data Protection Authority			✔	✔				
	Competition and Consumer Protection Commission (CCPC)	✔						✔	✔
	AI Act supervisory authorities (still unclear)		✔						
+ 25 MS	[…]								

This institutional proliferation is not only relevant from a quantitative perspective but also qualitative. It indeed occurs at the national and supranational levels, creating both vertical and horizontal overlaps under the same regulatory framework (intra-framework) or across different ones (extra-framework). Enforcement at the national level presents several potential conflicts, as multiple authorities may become involved in the same case, either within a single Member State or across different Member States. In addition, many EU regulations establish a supranational layer of enforcement. The existence of EU authorities creates space for vertical overlaps between national and supranational bodies, as well as horizontal ones among different supranational institutions.

To facilitate the analysis of enforcement overlaps, this section is structured according to different criteria: the level at which the overlap arises (national or supranational), the geographic scope (within a single Member State or across Member States), the institutional relationship (vertical or horizontal),[49] and the relevant regulatory scope (distinguishing between intra-framework and extra-framework overlaps). This taxonomy is visually summarised in Figure 1.

[49] Conflicts at the national level are, by definition, horizontal, as they occur between authorities operating at the same institutional level within a Member State.

Figure 1. Types of overlaps between competent authorities



Therefore, this section examines the enforcement structure at the national and supranational levels. The first part analyses national overlaps, both within individual Member States, where multiple authorities may share juxtaposed mandates, and in transnational cases, where authorities from different Member States may claim competence on the same issue. It then turns to supranational conflicts, focusing on the coordination between national authorities and supranational bodies, particularly the European Commission.

A. Intra and Extra Framework Overlaps in a Single Member State

Within a single Member State, various authorities may be assigned enforcement responsibilities under the same regulatory framework, creating *intra-framework overlaps within a single Member State*. This multiplication results either from the rules directly established by the EU or from the discretion left to Member States regarding the enforcement structure.[50] For instance, the PAR assigns an oversight role to different authorities depending on the specific provisions at stake and the supervised entity. More precisely, supervision of rules on targeted online political advertisement falls under the competence of the national Data Protection Authority (DPA), while for other provisions, Member States are required to designate one or more competent authorities (*e.g.*, those responsible for consumer protection or audiovisual services).[51] Moreover, the Digital Services Coordinator is responsible for coordinating enforcement concerning online intermediaries,[52] including online platforms that fall into the category of VLOPs.[53] As a result,

[50] For instance, the DSA leaves Member States free to designate one or more competent authorities, even though coordination must be ensured through the appointment of a Digital Services Coordinator (Article 49(1)(2) states that the DSC is responsible for all matters relating to supervision and enforcement of the DSA at national level, unless the Member State concerned has assigned certain specific tasks or sectors to other competent authorities and that, in any case, the DSC ensures coordination). The same freedom can be found regarding the GDPR, Article 51(1). In this case, coherence should be ensured by paragraph 3 of the same provision, which requires MS to designate a single national authority for the European Data Protection Board (*infra*) and to provide for coordination measures.
[51] PAR, Article 22(1)(3)(4).
[52] Designated in line with Article 49(2) of the DSA.
[53] PAR, Article 22(1)(3)(4).

enforcing the PAR at the national level involves at least two different authorities, namely, the DPA and the DSC, but may also require the involvement of three or more entities, including the competition and the consumer authorities, depending on national institutional arrangements. However, coordination should be facilitated by the requirement for Member States to designate a single national contact point.[54]

Wider fragmentation emerges when examining overlaps across different regulatory frameworks and their respective national supervisory authorities, generating *extra-framework overlaps within a single Member State*. At the national level, the DSA is (primarily) enforced by the DSC, while the GDPR falls (primarily) under the competence of the DPA. Additionally, the enforcement of the PAR is divided among the DPA, the DSC, and another potential authority (e.g., those responsible for consumer protection or audio-visual services). Moreover, the AVMS Directive assigns responsibilities to an Authority for Audiovisual Services, the EMFA is supervised by the national media regulators but can be considered by the DSC when applying the DSA, and the AI Act requires the designation of additional national authorities. Finally, National Competition Authorities (NCAs) remain competent in cases related to digital markets and unfair competition, and there may be multiple authorities for consumer protection.

However, the level of actual enforcement fragmentation varies significantly across Member States. For example, in Spain, the Comisión Nacional de los Mercados y la Competencia (CNMC) is responsible for enforcing the DSA, the AVSM Directive, and competition law, creating a relatively centralised system. Conversely, some federal countries like Germany and Belgium have more fragmented enforcement systems, as AVSMD supervisory authorities are appointed at the level of federated states.

The result of this fragmentation is that conflicts among national authorities in enforcing different regulations may arise rather easily, particularly in the case of multiple regulatory frameworks applying simultaneously. One example of potential conflict is the above-mentioned *Meta Platforms* case, involving the competence of both the Data Protection Authority and the Competition Authority.[55] Additional examples of concurring competences among different national authorities can be found in Italy. In one case, the national consumer protection authority sanctioned Meta for unfair commercial practices, including its failure to provide an exhaustive explanation for service interruptions. However, the national DSC viewed this conduct as a violation of the DSA and asserted jurisdiction over the matter.[56] A comparable case involved TikTok, which was sanctioned by the national consumer protection authority for the algorithmic dissemination of harmful content among minors, creating addiction and impacting consumers' self-determination. The Italian DSC considered again this issue to fall within its jurisdiction under the DSA.[57] These two cases suggest that the overlapping authority (i.e., the DSC) could also initiate proceedings for the same conduct, potentially exposing the platform to double sanctions.[58]

[54] PAR, Article 22(9).
[55] See n 32.
[56] See: position taken by Italian DSC (AGCOM) on 30 April 2024 through Delibera 110/24/CONS: https://www.agcom.it/provvedimenti/delibera-110-24-cons-0
[57] See: position taken by the Italian DSC (AGCOM) on the 20 December 2023 through Delibera 325/23/CONS): https://www.agcom.it/provvedimenti/delibera-325-23-cons
[58] Such a scenario raises the question of whether this would infringe the *ne bis in idem* principle, as protected under Article 50 of the Charter of Fundamental Rights of the European Union. In this regard, it is worth recalling that, according to the Court of Justice, the duplication of sanctions or proceedings does not in itself amount to a violation of *ne bis in idem*. As clarified in *Bpost* (C-117/20), a

Table 2. Types of possible overlaps within a single Member State

	Within a single Member State
Intra-framework	Multiple authorities competent under the same legal regime in a single Member State
Example	DPA vs DSC designated for PAR enforcement
Extra-framework	Multiple authorities competent for different legal regimes in a single Member State
Example	DPA vs DSC of the same Member State

B. Intra and Extra Framework Overlaps Across Member States

Beyond overlaps within individual Member States, the fact that digital services typically operate in an international context introduces another layer of potential conflict, as multiple authorities from different Member States may claim a role over the same regulatory regime, creating *intra-framework overlaps across Member States*.

Most of the regulations examined establish clear criteria for determining the competent national authority in cross-border cases, often based on the country-of-origin principle. Under the DSA, the Member State in which the main establishment of the intermediary provider is located holds exclusive supervisory and enforcement competence, except for powers explicitly granted to the European Commission.[59] The country-of-origin rule also applies to oversight of Video-Sharing Platforms under the AVMSD,[60] and to the PAR.[61] Similarly, under the GDPR, when data processing occurs across multiple jurisdictions, the one-stop-shop mechanism ensures that the DPA of the country where the data processor's main establishment is located assumes a leading role in enforcement.[62] However, not all regulations affecting digital services follow the country-of-origin principle. For instance, under competition law and consumer protection regulations, the mere provision of services in a national market is sufficient to establish competence.

To facilitate enforcement in transnational cases, many of the examined regulations contain rules governing cooperation among national authorities and have established supranational networks to serve as *fora* for coordination. This is the case for the European Board for Digital Services established by the DSA (EBDS); the European Data Protection Board for GDPR (EDPB); the European Regulators Group for Audiovisual Media Services (ERGA) for AVSMD, now replaced by the European Board for Media Services (EBMS);[63] the Consumer Protection Cooperation Network (CPC), the European Competition Network (ECN), and the European Artificial

dual proceeding is permissible when the sanctions pursue complementary objectives, the overall burden on the individual is not disproportionate, and sufficient coordination and procedural safeguards are in place to prevent unjustified duplication.

[59] DSA, Article 56(1).

[60] AVSMD, Article 28a.

[61] PAR, Article 22.

[62] GDPR, Article 56.

[63] EMFA, Article 8.

Intelligence Board (EAIB). Regarding the PAR, a European network for national contact points is expected.[64]

While these explicit coordination mechanisms align enforcement in transnational cases under the same regulation, coordination across different legal regimes and Member States remains a significant challenge, due to *extra-framework overlaps across Member States*. Once again, this problem arises due to regulatory intersections, particularly when the same conduct falls under multiple regulations.

The situation becomes even more complicated when overlapping regulatory frameworks apply different criteria for determining jurisdiction in cross-border cases. Under the one-stop mechanism, the authority competent to enforce the GDPR in a given case may come from a different Member State than the authority competent under other frameworks, such as consumer protection, even when addressing the same underlying conduct. Likewise, in competition law, the competence of a national authority could clash with a data protection authority in another Member State. In the above-mentioned *Meta Platforms* case, both the German Competition Authority and the Irish Data Protection Authority could have claimed competence: the former based on the country where the service was provided, and the latter based on the country of establishment.

This situation has created institutional tensions, with national authorities asserting their jurisdiction and issuing independent fines, as in the cases of the Italian competition authority's investigation under the DMA into Google's consent practices,[65] the Dutch DPA sanctioning Clearview,[66] and the Italian DPA using emergency powers to ban ChatGPT.[67] These types of overlaps can lead to conflicts in the enforcement at the national level, as underlined in Table 3.

Table 3. Types of possible overlaps across Member States

	Across Member States
Intra-framework	Multiple authorities competent under the same legal regime across Member States
Example	A DPA in one Member State vs a DPA in another Member State
Extra-framework	Multiple authorities competent under different legal regimes across Member States

[64] Regulation on Political Advertisement, Recital 101.
[65] Italian Competition Authority, Investigation launched against Google for unfair commercial practices, PS12714 (18 July 2024) <https://en.agcm.it/en/media/press-releases/2024/7/PS12714>.
[66] Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition (3 September 2024) <https://autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition>
[67] Italian Data Protection Authority, Artificial intelligence: stop to ChatGPT by the Italian SA
Personal data is collected unlawfully, no age verification system is in place for children (31 March 2023) <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english>.

Example	A DPA in one Member State vs a NCA in another Member State

This situation at the national level does not exhaust the challenges in enforcing the EU digital acquis. Indeed, it is further compounded by inconsistencies at the supranational level, leading to vertical and horizontal overlaps.

C. Intra and Extra Framework Vertical Overlaps

The supranational enforcement structure not only mirrors many of the challenges seen at the national level but also increases the potential for conflicts. The existence of an EU layer of governance introduces the potential for both horizontal and vertical overlaps. Horizontal tensions concern coordination among different EU bodies, while vertical ones arise between national and supranational authorities. As with national enforcement, the intra-framework vertical enforcement structure is organised through regulation from the Union. In contrast, extra-framework enforcement reveals several inconsistencies, particularly because some regulations adopt a more centralised approach, while others primarily grant power to national authorities, thereby increasing the risk of vertical conflicts.

The expansion of the European regulatory approach has led to an increase in the supranational regulatory oversight of the European Commission, whose powers can potentially clash with the competencies of Member States' authorities, generating *vertical intra-framework overlaps*. Unlike the GDPR, the PAR and the AVMS Directive, which grant the Commission limited enforcement powers,[68] the adoption of the Digital Services Package, which includes both the DMA and the DSA, marked a shift toward a more centralised enforcement structure, which nonetheless applies only to major platforms.

While the DMA's enforcement, as it only applies to major platforms classified as 'gatekeepers', is completely centralised at the level of the European Commission, the DSA adopts a partially decentralised approach. The European Commission holds exclusive competence for designating VLOPs[69] and enforcing the special obligations applicable to them.[70] Nonetheless, enforcement of the broader requirements applicable to intermediary providers, hosting services, and platforms is shared between the European Commission and national DSCs, with the latter being competent also towards VLOPs when the Commission has not initiated proceedings for the same infringement.[71] Therefore, although both national authorities and the Commission may, in theory,

[68] Concerning GDPR enforcement, the powers conferred on the EC are very limited, mainly related to the ability to request opinions from the EDPB (see Articles 64(2), 68(5), and 70(1)). In the PAR, the EC has some coordination competences (e.g., Article 22(8)). Under the AVMSD, particularly regarding VSPs, the EC's competence is also primarily focused on coordination (see Articles 28a(6) and (7), 28b(9) and (10), and 29).

[69] As defined by DSA, Article 33.

[70] Article 56(2) of the DSA establishes the exclusive competence of the EC in the enforcement of the special obligations for VLOs and VLOSEs included in the Section 5 of the DSA, Article 33 to 45.

[71] DSA, Article 56(4). Recital 125 justifies the share competence considering that the EC is in a better position to address systemic violations of general DSA's provisions by major platforms, while national authorities could be better placed to address individual infringements that do not raise any systemic or cross-border issues. From a procedural point of view, Article 59 provides that DSCs may refer cases to the Commission when they believe that an alleged infringement has implications beyond the Member State of establishment or requires coherent enforcement at the EU level, while according to Article 66, if the Commission decides to initiate proceedings against VLOPs or VLOSEs, it must notify all DSCs and the EBDS through the information-sharing system established

initiate proceedings concerning the same case, the DSA establishes a clear criterion for the vertical allocation of enforcement powers.

Conversely, the intersection between centralised and decentralised regulatory frameworks can create significant enforcement challenges, creating *vertical extra-framework overlaps*. An example is represented by the interaction between the DSA and the GDPR. While the GDPR grants national data protection authorities the primary responsibility for enforcing data protection rules, the DSA introduces additional obligations related to online advertising transparency and data use, which, in the case of VLOPs, are enforced by the Commission.[72] This dual regulatory structure can trigger multiple competencies, where both the European and national authorities must coordinate their approaches to ensure consistent enforcement. Likewise, the intersection between the DSA and the AI Act could give rise to conflicts between the European Commission and national authorities, particularly in the area of risk assessment,[73] as the DSA and the AI Act establish different oversight mechanisms and enforcement responsibilities.[74]

The same tension exists in the relationship between centralised enforcement towards VLOPs under the DSA and the decentralised enforcement structure in the field of consumer protection.[75] This situation has become particularly evident regarding proceedings against the marketplace Temu, which has been subject to investigations initiated both by the European Commission and by national consumer protection authorities.[76] Temu was designated as a VLOPs on 31 May 2024, thereby allowing the European Commission to act under the DSA, particularly concerning obligations related to systemic risks, transparency of recommender systems, and data access for researchers. In parallel, consumer protection authorities operate under the consumer protection acquis,[77] pursuing concerns such as misleading advertising and the sale of unsafe products. In this context, both a coordinated action led by the CPC Network and individual actions launched by single national authorities have been reported.[78] The European Commission clarified that the CPC Network's coordinated action against Temu is without prejudice to ongoing proceedings initiated by other national authorities. Moreover, all proceedings under consumer law are without prejudice to any action that the European Commission may initiate under the DSA. While the Commission is coordinating with the CPC Network, national authorities appear to be excluded from this dialogue, potentially leading to duplication of sanctions and conflicting decisions.

The Temu case also illustrates a broader point. Supranational enforcement is not limited to the European Commission but also includes European regulatory networks, increasing the potential

under Article 85 of the DSA. From that moment on, the Commission holds exclusive responsibility for the investigation, and the relevant national authorities are relieved of their supervisory and enforcement powers in relation to that specific matter.

[72] A similar comparison can be drawn between the fully centralised DMA and the decentralised structure of the GDPR (see below on the "pay-or-consent" model and the EDPB Opinion). By contrast, the case of competition law is peculiar: Articles 101 and 102 of the TFEU are enforced through a parallel structure, allowing both the European Commission and National Competition Authorities to act. However, Regulation 1/2003, Article 11, establishes a coordination mechanism, requiring NCAs to inform the Commission about ongoing cases, while granting the Commission the power to assume competence when deemed necessary. This means that in the absence of an intervention by the Commission, NCAs remain fully competent.

[73] Reference is made to the relationship between the AI Act, Article 55, and the DSA, Article 35.

[74] This is especially relevant given that VLOs under the DSA and general-purpose AI models with systemic risks (AI Act, Article 88) are both supervised by the European Commission, yet these categories do not fully align.

75 This is true for instance for the Unfair Commercial Practices Directive (2005/29).

[76] European Commission, 'Commission and national authorities urge Temu to respect EU consumer protection laws' (*European Commission*, 8 November 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5707> accessed 16 April 2025.

[77] Including the Unfair Commercial Practices Directive, the Consumer Rights Directive, the Price Indication Directive, the e-Commerce Directive and the Unfair Contract Terms Directive.

[78] European Commission, 'Commission and national authorities urge Temu to respect EU consumer protection laws' (n 77).

for both vertical and horizontal overlaps to arise. As already mentioned in the previous sub-section, most of the regulations that have been examined establish supranational networks and bodies, whose powers and role, however, may vary significantly. Some of these bodies primarily serve advisory and coordination functions, ensuring consistency across enforcement actions but without binding authority. This includes the European Board for Digital Services under the DSA,[79] and the network of national contact points introduced by the PAR.[80] Others, however, hold stronger powers, including the ability to adopt binding opinions and resolve conflicts between national authorities. This is the case for the European Data Protection Board and, to some extent, the European Board for Media Services, which substituted the ERGA.[81]

A notable example of vertical tension involving supranational networks arose in the context of GDPR enforcement. In a case regarding online targeted advertising, the adoption of a binding opinion by the EDPB based on the request of the Irish Data Protection Commission has led to a conflict.[82] Indeed, although the Irish authority followed the binding opinion of the EDPB in its decision, it later brought the matter to the European General Court, claiming that the EDPB had exceeded its powers and thereby undermined the discretion of the Irish authority. However, the General Court dismissed the case, underlining how the power of the EDPB to adopt binding opinions directly results from the GDPR,[83] which has the role to ensure the consistent application of the GDPR.

The types of overlaps at the supranational level presented in this section can lead to various vertical conflicts in the enforcement of the EU digital acquis, as summarised in Table 4.

Table 4. Types of possible vertical overlaps at the supranational level

	Vertical
Intra-framework	EU and national authorities competent under the same legal regime
Example	EU Commission vs DSC *or* EDPB vs DPA
Extra-framework	EU and national authorities competent under different legal regimes
Example	EU Commission vs Consumer Protection Authority

D. *Intra and Extra Framework Horizontal Overlaps*

[79] A list of the functions of the Board can be found in Article 63 of the DSA.
[80] Its role is presented in Article 22(8) of the Regulation on Political Advertisement.
[81] A list of the functions of the EBMS can be found in Article 13 of the EMFA. The main functions of the EDPB are listed in Articles 70, 64 and 65 of the GDPR.
[82] Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited.
[83] Joined Cases T-70/23, T-84/23 and T-111/23, Data Protection Commission v European Data Protection Board (2025).

Overlaps also exist among different supranational networks and between the Commission and sectoral networks. These types of overlaps are referred to as 'horizontal', as they involve only EU-level bodies, and reflect challenges in coordinating enforcement actions within the EU institutional framework.

Within a single regulatory framework, *horizontal intra-framework overlaps* are generally more structured. Even when a regulation assigns roles to both the Commission and a sectoral body, their respective responsibilities are often clearly defined. For instance, under the DSA, the European Board for Digital Services plays a primarily consultative role. It coordinates national enforcement actions in cases with a transnational dimension and provides support and advice to the European Commission, without exercising direct enforcement powers. However, this formal clarity does not entirely eliminate the potential for internal tension. Forms of institutional friction may still arise, for instance, over differing interpretations of legal provisions or varying priorities. These tensions may not manifest as open conflict across different authorities but can shape internal dynamics, such as disagreements over the pace or direction of enforcement efforts.

Conversely, the absence of an overarching framework ensuring comprehensive coordination among sector-specific coordination bodies increases the risk *horizontal extra-framework overlaps*. The European Commission, by its presence across many of them, may serve as a *de facto* coordinating entity, but institutionalised system of cooperation are weak. Nonetheless, some regulations mention the possibility of cooperating with other EU authorities. This is the case, for instance, for the European Artificial Intelligence Board, which includes the participation of the European Data Protection Supervisor, as well as any other body or authority whose expertise may be relevant on a case-by-case basis.[84] The possibility of cooperating with other authorities is also addressed by the PAR, which explicitly mentions the European Board for Media Services,[85] while the DSA foresees cooperation between the European Board for Digital Services and the European Data Protection Board.[86]

An example of extra-framework horizontal overlapping competence at the supranational level concerns data protection. Since certain data combination practices are now forbidden under the DMA, a potential clash could result not only from the vertical intra-framework overlaps between the powers of the European Commission and national DPAs but also between the European Commission and the EDPB which may intervene on the same conduct. This is precisely the reason why the 'pay-or-consent' model adopted by Meta,[87] which has been sanctioned by the European Commission for infringing the DMA,[88] had first been the subject of a binding opinion issued by

[84] AI Act, Article 65(2) and 66(h).
[85] PAR, Article 22(8).
[86] DSA, Article 62 and Recital 134.
[87] To comply with the DMA, and particularly its Article 5(2), and Meta introduced a binary 'pay or consent' model on its platforms since November 2023, Under this system, EU users of Facebook and Instagram received a notification to choose between: (i) paying a monthly subscription for an ads-free experience, or (ii) the traditional free-of-charge access to platforms with personalised ads. As a result, users gained a new option to access Meta's services without consenting to the data processing covered by the DMA, but only by paying a fee of approximately €250 per year (See: Noyb, '28 NGOs Urge EU DPAs to Reject "Pay or Okay" on Meta' (*noyb*, 16 February 2024) <https://noyb.eu/en/28-ngos-urge-eu-dpas-reject-pay-or-okay-meta> accessed 18 February 2025.).
[88] EC, 'Commission closes investigation into Apple's user choice obligations and issues preliminary findings' (*European Commission*, 23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1086> accessed 29 April 2025; EC, 'Commission finds Apple and Meta in breach of the Digital Markets Act' (*European Commission*, 23 April 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085> accessed 29 April 2025.

the EDPB assessing its compatibility with the GDPR.[89] Although the Commission can take this opinion into account when assessing the same practice under the DMA, it is under no obligation to do so. This case thus illustrates the potential for parallel, and possibly diverging, legal assessments of the same practice, raising questions about consistency of positions taken by EU bodies.

The types of overlaps at the supranational level presented in this section can lead to various horizontal conflicts in the enforcement of the EU digital acquis, as summarised in Table 5.

Table 5. Types of possible horizontal overlaps at the supranational level

	Horizontal
Intra-framework	EU authorities competent under the same legal regime
Example	EU Commission vs European Board for Digital Services
Extra-framework	EU authorities competent under different legal regimes
Example	EU Commission vs EDPB

This section has illustrated the patchwork of an enforcement structure that involves multiple authorities, often with overlapping mandates. Given these complexities, ensuring effective enforcement requires acknowledging the substantial overlaps in regulations affecting EU digital regulations and designing mechanisms to mitigate conflicts and enhance coordination among authorities at different levels. Therefore, the following section explores three potential paths to address these challenges.

IV. Pathways for Enforcement

This fragmented enforcement landscape presents significant challenges from different perspectives, such as consistency of decision-making, efficiency of public administrations, legal certainty, and the protection of fundamental rights. The absence of a consistent enforcement of EU law leads to varying interpretations and unequal treatment, undermining legal certainty, while duplicated efforts across jurisdictions create inefficiencies and higher administrative costs. This situation also makes it more difficult for authorities, businesses, and citizens to understand their obligations and exercise their rights, raising constitutional questions for EU law.

[89] European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en> accessed 18 February 2025.

Enforcement fragmentation undermines the effective enforcement of EU law.[90] The potential duplication of proceedings, where multiple authorities initiate parallel investigations or enforcement measures based on the same or different legal regimes, exacerbates inefficiencies and drives up administrative and compliance costs for both regulators and regulated entities.[91] Moreover, an excessive diffusion of responsibility, in which no single authority assumes clear and comprehensive accountability for addressing a specific regulatory violation, could lead to underenforcement. In such cases, enforcement gaps can emerge, with violations either falling through the cracks or being addressed ineffectively, also weakening the overall coherence and credibility of the regulatory system.

At the same time, overlapping competences can undermine legal certainty and, broadly, the rule of law, thereby challenging one of the fundamental principles of EU law.[92] When multiple authorities assert overlapping or conflicting mandates, individuals and companies may struggle to identify which rules apply, how they will be interpreted, and which body has ultimate jurisdiction. This unpredictability risks arbitrary or inconsistent application of the law, eroding trust in regulatory frameworks from citizens and other public administrations while weakening the safeguards of transparency and foreseeability. Likewise, this situation can have a significant impact on EU competitiveness, as legal uncertainty may deter investment and hinder the development of the internal market.

In addition, this situation poses serious risks for the access and effectiveness of remedies.[93] While recent regulations have expanded the range of redress mechanisms available, the proliferation of these remedies across multiple authorities and legal frameworks can itself become a barrier.[94] Users and affected parties seeking to trigger regulatory scrutiny may encounter substantial complexity and opacity in enforcement structures, which can reduce their ability to have their rights respected, also in the case of judicial protection, which, however, lies beyond the scope of this paper. In this context, the right to an effective remedy becomes instead closely intertwined with the right to good administration,[95] which requires high-quality decision-making processes.[96]

To address these issues, different possible pathways can be explored, ranging from more flexible coordination mechanisms to stronger centralisation, each with its own advantages and limitations. At least, as analysed in the following sub-sections, three main solutions can be considered to address the questionable framework of public enforcement in European digital regulation. A first and less disruptive solution would be to enhance coordination mechanisms rather than altering the enforcement structure itself. A second approach would be to adopt a meta-regulation to coordinate enforcement and resolve conflicts between existing frameworks. A third and more trenchant solution would be to centralise the enforcement of digital regulation at the EU level in specific areas, such as in the case of VLOPs, following the model of the DSA. While any reform of enforcement structures must respect the principle of conferral, as well as the broadly recognised

[90] This problem has also been raised with regards to the GDPR enforcement by Bastos and Pałka (n 9) 494.
[91] Alexiadis and others (n 10) 278.
[92] TEU, Art. 2.
[93] Article 47 CFR.
[94] This argument has indeed already been raised regarding the private enforcement of the EU Digital Acquis [De Gregorio and Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' (n 17).].
[95] Article 41 CFR.
[96] De Gregorio and Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' (n 17) 8.

principle of procedural and institutional autonomy of Member States, there is already a discernible trend toward the 'Europeanisation' of enforcement.[97] The proposals outlined here build on this existing trajectory, drawing from mechanisms already in place rather than introducing entirely novel approaches. These three models should not be seen as mutually exclusive alternatives, but rather as steps along a possible gradual path toward greater harmonisation of enforcement from a short-term to a long-term perspective. Their implementation may evolve incrementally over time, also depending on practical experimentation and political feasibility.

A. Soft Coordination Mechanisms

A first and less disruptive solution would be to enhance coordination mechanisms rather than altering the enforcement structure or establishing rigid hierarchies between supranational and national authorities. This approach would focus on improving communication and informal coordination processes among national and EU authorities, facilitating conflict resolution on a case-by-case basis.

This model follows the approach adopted by the CJEU while examining a case of abuse of a dominant position. In *Meta Platforms*, the Court observed that national competition authorities may be in the position of examining compliance with rules outside competition law, such as the rules on the protection of personal data laid down by the GDPR.[98] In this context, the CJUE stated that the national competition authority should either adhere to previous decisions by the competent data protection authority or seek its opinion, in line with the principle of sincere cooperation.[99] The Court focused on institutional cooperation, rather than strict fungibility between authorities, also underlining the relevance of the proposed European regulation that aims to provide a new framework for enforcing the GDPR.[100]

This approach has been primarily driven by the goal of ensuring substantive enforcement and the effective protection of data subjects, in line with the principle of sincere cooperation within the Union. Indeed, the CJEU stated that, when applying the GDPR, all national authorities involved are bound by the duty of sincere cooperation enshrined in Article 4(3) TEU. In accordance with settled case law, in areas covered by EU law, this duty requires Member States, including their administrative authorities, to assist each other in full mutual respect, to ensure the fulfilment of the obligations arising from EU law, and to refrain from jeopardising its objectives.[101] Therefore, the application of the principle of sincere cooperation in enforcement may require reciprocal consultation among authorities, even in the absence of a dedicated legal framework.

While informal practices between enforcement authorities remain possible, aligned with the principle of sincere cooperation, the complexity of the enforcement landscape, including the number of potentially involved authorities, may call for a strengthening of coordination

[97] Scholten and Stähler (n 18) 6; Scholten (n 10).
[98] Meta Platforms (n 32), para 62.
[99] Ibid, para 56-59; para 63.
[100] Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM (2023) 348.
[101] Ibid, para 53.

mechanisms.[102] In this perspective, an institutional solution could take the form of digital clearinghouses, as inspired by the model recently proposed by the European Data Protection Supervisor (EDPS).[103] Acknowledging the proliferation of regulatory requirements under the EU Digital Rulebook, the potential for conflicts and inconsistencies arising from simultaneous actions by various regulators, and the need for enhanced cooperation to ensure a predictable and effective legal environment that puts fundamental rights at its core, the EDPS has advocated for the establishment of a Digital Clearinghouse 2.0.[104] This initiative would provide authorities and bodies responsible for enforcing EU digital legislation with a forum to exchange information, coordinate enforcement strategies, and align on legal interpretations and policy approaches. In this context, participating authorities could share information on ongoing enforcement actions, facilitating engagement and collaboration on specific, cross-cutting cases. While the EDPS believes that legislative action is ultimately needed, informal meetings among authorities could remain possible even without any legal changes.

This mechanism could be operating at both national and supranational levels. At the national level, a forum composed of representatives from all competent authorities could issue non-binding opinions on enforcement conflicts, acting as an intermediary across different regulatory frameworks.[105] At the European level, a similar structure could be established to handle transnational cases and vertical conflicts, ensuring a more coherent approach across Member States. Such a mechanism would institutionalise a forum for coordination, facilitating sincere cooperation among various enforcement authorities, each of which is competent under a different regulatory framework.

Pursuing the enhancement of 'soft' coordination mechanisms would be the more realistic solution in the short-term, as it does not require major changes to existing legal frameworks and current divisions of competences. Moreover, it would allow for a flexible approach, capable of adapting to the specificities of single cases, where the interplay between different regulatory frameworks may reflect varying proportions of relevance. At the same time, it would preserve a complementary perspective, enabling different regulatory approaches and values to coexist. Finally, such a mechanism would also be well-suited to accommodate future changes in the regulatory landscape, particularly in light of the new simplification agenda announced by the European Commission.[106]

However, this solution presents drawbacks. Relying on case-by-case coordination may perpetuate legal uncertainty. Indeed, the absence of binding mechanisms could weaken the rule of law, as enforcement outcomes would depend on negotiation rather than clear, pre-established rules and informal practices which would escape accountability and judicial review.[107] Moreover, this

[102] The need to strengthen cooperation through institutional and/or regulatory mechanisms is also expressed by Alexiadis and others (n 10) 280. and with regards to the enforcement of the DSA, Pietro Mattioli, 'Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action?' (2025) Utrecht Law Review 1, 15..

[103] European Data Protection Supervisor, 'Towards a Digital Clearinghouse 2.0' (2025) <https://www.edps.europa.eu/data-protection/our-work/publications/other-documents/2025-01-15-towards-digital-clearinghouse-20> accessed 28 January 2025.

[104] In 2016, the EDPS had already proposed the establishment of a Digital Clearinghouse to bring together competent authorities from the areas of competition, consumer and data protection.

[105] Some precedents already exist at the national level, such as the UK Digital Regulation Cooperation Forum and the Dutch Digital Regulation Cooperation Forum. Hert and Hajduk (n 10) 306.

[106] Sterling (n 5).

[107] Rule-of-law concerns related to informal cooperation in multilevel administrative systems are also mentioned in: Filipe Brito Bastos, *Judging Composite Decision-Making. The Transformation of European Administrative Law* (Bloomsbury Publishing 2024) 66 <https://www.bloomsbury.com/uk/judging-composite-decisionmaking-9781509980444/> accessed 5 June 2025.

approach would not entirely prevent conflicts, particularly when negotiations fail to reach an agreement, also considering that, on the ground, institutional culture, resources, and desire to collaborate may vary significantly.[108] Therefore, regulatory inconsistencies or competing enforcement claims could persist, potentially increasing conflicts whose resolution would also be caught outside traditional accountability and transparency mechanisms.

Several of these limitations could be addressed through the introduction of different binding coordination mechanisms. Such mechanisms might include formalised procedures for information sharing, joint decision-making frameworks, and mandatory dispute resolution processes between competent authorities. However, even these solutions come with their own challenges, as will be discussed in the following paragraphs.

B. A Meta-regulation on Enforcement

A second approach would be based on the introduction of a meta-regulation to coordinate enforcement and resolve conflicts between existing legal regimes. This overarching framework would establish predefined rules determining which authority takes precedence in cases of overlap and would establish binding mechanisms for consultation to ensure consistent decision-making. Such a regulation could introduce a dedicated procedure applicable to a selected group of regulatory frameworks, to be triggered when one or more competent authorities consider that a regulatory overlap may arise. This mechanism should encompass both national-level and EU-level enforcement, ensuring coordination across all layers of regulatory governance. Theoretically, this approach could align with the current simplification effort. The recently proposed Digital Omnibus Regulation represents an example of a horizontal instrument that amends multiple regulations in the digital sector to improve consistency. However, as mentioned above, it does not significantly tackle the enforcement architecture, representing, in this sense, a missed opportunity.

Another possible model to implement this solution can be found in the ongoing discussions on improving GDPR enforcement,[109] which presents an opportunity to enhance regulatory coherence not only from an intra-framework perspective but also across different regulatory regimes, thus including extra-framework enforcement. Indeed, the Commission's proposal aims to strengthen GDPR enforcement in cross-border cases. While the GDPR already provides for a dispute resolution procedure in such contexts,[110] the proposal seeks to improve coordination in the earlier stages of the procedure. The rationale is that dispute resolution should remain a last resort, used only where sincere cooperation among DPAs failed to produce consensus. To facilitate consensus-building, the proposal harmonises some procedural rules at the national level and adds formal coordination tools between authorities, for instance, by establishing common duties to exchange information and setting deadlines for the submission of opinions.[111] A similar logic has been adopted in the field of consumer protection, where mechanisms for coordinating cross-border enforcement have also been introduced in 2017.[112]

[108] Moreover, the adoption of technical tools to facilitate coordination could be necessary, such as a repository for ongoing cases.
[109] See n 100.
[110] GDPR, Article 65.
[111] See for instance Article 8, 9 and 10 of the Proposal.
[112] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004. Other than

Even if these solutions do not address all the potential clashes identified in this work while also adding procedural complexity and granting an overly prominent role to the lead supervisory authority,[113] they nevertheless provide some examples of meta-regulation which could be used to streamline enforcement. From the perspective of this work, a meta-regulation addressing extra-framework coordination could establish clear consultation and coordination procedures. For instance, the DSC could be required to consult the DPA and share information for any case involving data protection aspects. To strengthen this mechanism, the DPA could be granted the power to issue binding opinions on the interpretation and application of the GDPR, ensuring that enforcement decisions remain consistent with data protection principles.[114]

Another possibility is to establish an arbiter to solve disputes across different regulatory authorities. This role could be assigned to the CJEU as an independent actor counterbalancing executive powers. Nonetheless, the degree of technicality and expertise required in these cases could expand the workload of the court, thus making a supranational independent body competent for dispute resolution a potential solution.[115] This mechanism could build upon the system of national and supranational digital clearinghouses discussed in the previous paragraph, but with the added capacity to issue binding decisions. Such an overarching framework would help to positively coordinate enforcement across different regimes, ensuring greater legal certainty. It would also provide a first solution to institutional conflicts, helping to prevent an increased burden on the CJEU, which would however play a role in reviewing these decisions.

However, establishing binding coordination mechanisms presents its own challenges. Establishing ex-ante coordination procedures would require the prior identification of potential conflicts, implying a significant effort in mapping regulatory intersections. In addition, such a mechanism would need to determine which areas of regulation it should cover, potentially leading to hierarchies between different areas of digital policy, which would also require a political agreement. A rigid framework may also struggle to adapt to new regulatory developments, limiting its effectiveness in addressing unforeseen conflicts. In addition, introducing yet another layer of regulation may give rise to further interpretative uncertainties.

Moreover, the proposal to create a dispute-resolution authority raises further concerns. Beyond the complexity of introducing a new layer of governance, potentially involving 27 national authorities and a supranational body, there is also the question of its legal basis and broader consistency with primary law. A legal basis could arguably be found in Article 114 TFEU,[116] as

introducing certain common procedural rules and consultation procedures, this meta-regulation also introduced specific coordination provisions for widespread infringements with a Union dimension (Article 15-25).

[113] Hofmann and Mustert (n 9); 'EU Pledged to Improve GDPR Cooperation - and Made It Worse' (*noyb*, 17 April 2024) <https://noyb.eu/en/eu-pledged-improve-gdpr-cooperation-and-made-it-worse> accessed 17 April 2025; Hendrik Alexander Mildebrath, 'An Analysis of the Newly Proposed Rules to Strengthen GDPR Enforcement in Cross-Border Cases' <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)757613> accessed 16 April 2025.

[114] This solution is also envisaged in Hert and Hajduk (n 10) 306.

[115] However, the monopoly held by the Court over the interpretation of EU law under Article 267 TFEU (see: CJUE, *Achmea*, C-284/16) could pose an obstacle to the establishment of a collective administrative body tasked with resolving competence disputes. To ensure compatibility with the EU legal order, the possibility to challenge such decisions before the CJEU should nonetheless be guaranteed.

[116] Article 114 of the TFUE is also the legal basis used for most regulation on digital services (Annegret Engel, 'Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market' in Annegret Engel, Xavier Groussot and Gunnar Thor Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer Nature Switzerland 2025) <https://doi.org/10.1007/978-3-031-65381-0_2> accessed 11 April 2025.)

the fragmentation of enforcement across Member States risks creating regulatory inconsistencies that may undermine the functioning of the internal market. Moreover, the issuance of binding opinions by an EU body, in the absence of any amendment to primary law, risks contravening the *Meroni* doctrine,[117] which restricts the delegation of discretionary regulatory powers to EU agencies.[118]

Another option, presenting however many of the same obstacles as a meta-regulation, would be the centralisation of enforcement at the EU level in certain areas of digital regulation. This solution could be adopted either alongside or in place of enhanced coordination mechanisms and would help ensure greater consistency and efficiency, particularly in cases involving significant cross-border impacts or where national enforcement has been fragmented or ineffective. Centralising enforcement may also streamline procedures and strengthen the EU's capacity to address systemic issues, limiting different interpretations across Member States. However, it raises important constitutional questions about subsidiarity and democratic accountability as examined in the following sub-section.

C. Enforcement at the EU Level in Specific Areas

A third solution would be to enhance enforcement powers at the EU level in specific areas. One illustrative model of this approach is the enforcement structure applied to VLOPs under the DSA. These service providers are defined by reference to user thresholds, which lead to the centralisation of enforcement, particularly of risk assessment provisions, in the hands of the European Commission.[119] For other obligations under the DSA, enforcement on these major platforms is shared between the Commission and the competent national authority, with the latter being competent only if the Commission has not initiated proceedings for the same infringement.[120]

Regarding this division of competences, the preamble of the DSA explicitly acknowledges that the Commission is better placed to address systemic infringements committed by VLOPs, such as those affecting multiple Member States or serious repeated infringements. However, on the other hand, it also states that national authorities could be better placed to address individual infringements committed by those providers that do not raise any systemic or cross-border issues. Moreover, in the interest of efficiency and to avoid duplication, particularly to ensure the principle of the *ne bis in idem*, the Commission can assess whether it deems it appropriate to exercise those shared competences in a given case.[121] Such a structure provides a clear coordination mechanism for vertical enforcement, ensuring that the Commission can take over cases of broader concern, while maintaining the competencies of national authorities in all other instances. Similar

[117] CJEU, Meroni v High Authority of the European Coal and Steel Community, C-9/56, §149-150.
[118] Mattioli (n 9) 15; Alexiadis and others (n 10) 285. On this point see also: Miroslava Scholten and Marloes van Rijsbergen, 'The *ESMA-Short Selling* Case: Erecting a New Delegation Doctrine in the EU upon the *Meroni-Romano* Remnants' (2014) 41 Legal Issues of Economic Integration <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\LEIE\LEIE2014022.pdf> accessed 11 April 2025. However, following Bastos and Pałka [(n 81) 515.] the creation of an autonomous EU agency with a competence in data protection could be consistent with the EU Treaties and the Meroni doctrine, as the establishment of an independent authority in this field is directly required by primary law.
[119] See n 70.
[120] See n 71.
[121] Recitals 125 of the DSA.

arrangements can be found in other areas, such as AI regulation, particularly regarding general-purpose AI models with systemic risks.[122]

Theoretically, this logic of partial centralisation could be extended to other regulatory frameworks, although such a solution would face multiple constitutional and institutional obstacles. Nevertheless, centralisation could be desirable in cases of 'common European concern' in the digital sector,[123] which would need to be appropriately defined. To this end, for online platforms, the existing notion of VLOPs could serve as a common reference point. This would imply that regulations such as the GDPR, the PAR, the AI Act, the AVMS Directive, and EU consumer protection rules could be enforced centrally when concerning VLOPs. The same approach could be adopted for generative AI models presenting with systemic risks. For other relevant regulations, no major adjustment may be necessary, as they already provide for centralised enforcement by the Commission. In particular, this is the case for the DMA, which already follows this logic by targeting only gatekeepers[124] and, broadly, EU competition law.[125]

Unlike the mechanism described in the previous paragraph, this solution would not merely involve a supranational authority coordinating enforcement through binding decisions, but it would entrust it with direct enforcement powers. Centralising enforcement would represent a further step in an already emerging trend towards greater EU-level enforcement powers,[126] reducing conflicts and enhancing efficiency. Indeed, it would avoid duplication of efforts and prevent situations where different authorities launch separate but overlapping investigations into the same conduct, potentially leading to conflicting decisions.

First, it would help resolve enforcement conflicts by providing a chain of authority. As already underlined, many of the current regulatory challenges stem from overlapping competencies and unclear boundaries between national and supranational bodies. A centralised model would improve the management of conflicts across Member States and between national and supranational enforcement bodies. A central enforcer would have the capacity to address cases and ensure coherence across different regulatory frameworks. At the same time, individuals would still be able to lodge complaints at the national level, thereby safeguarding proximity to redress mechanisms, maintaining a degree of local accessibility to enforcement, and preserving the benefits of decentralisation where appropriate.

Secondly, centralisation would contribute to the effectiveness of European digital policy, as Member States can prove weak against major technological players.[127] Indeed, a significant concern in the current decentralised system is the unequal distribution of resources among national regulators. Reports from the European Union Agency for Fundamental Rights indicate that some Member States' DPAs lack the financial and human resources needed to effectively

[122] As already mentioned, the AI Act centralises enforcement for general-purpose AI models with systemic risk (AI Act, Article 88).
[123] Bastos and Pałka (n 9).
[124] However, the possibility of designating certain AI systems – or the companies developing them – as gatekeepers under the DMA remains under discussion and is not yet final (see, for instance: Alba Ribera Martínez, 'Generative AI in Check: Gatekeeper Power and Policy Under the DMA' (Social Science Research Network, 13 November 2024) <https://papers.ssrn.com/abstract=5025742> accessed 9 July 2025.).
[125] See n 72.
[126] Miroslava Scholten, 'Mind the Trend! Enforcement of EU Law Has Been Moving to "Brussels"' (2017) 24 Journal of European Public Policy 1348.
[127] Hert and Hajduk (n 10) 297.

enforce the GDPR.[128] This disparity is also noticeable in other sectors, such as competition, communication, and consumer protection, where countries like Italy, France, and the Netherlands have been proactive, while others have struggled to monitor compliance or have faced infringement procedures from the European Commission for not implementing EU law, including its enforcement system. The variance in local institutional dynamics is also influenced by national priorities in certain regulatory areas over others, which is underlined by the differing approaches of Member States. For instance, Italy's proactive stance, as demonstrated by its Competition Authority's investigation into Google's consent practices under the DMA,[129] contrasts with the Irish Data Protection Commission's inconsistent engagement in targeted advertising investigations as per its own rulings from December 2022. These discrepancies reflect not only domestic political concerns but also entrenched regulatory cultures that may resist alignment with the EU's broader objectives of harmonisation and market integration.

Thirdly, centralisation would limit forum shopping by establishing a single, centralised enforcement authority with greater independence from national priorities.[130] In this perspective, centralisation ensures that enforcement is carried out by a body with the necessary expertise, capacity, and technical resources to monitor compliance and act effectively, thereby addressing some of the shortcomings currently existing in the enforcement of non-centralised regulations, such as the GDPR,[131] broadly characterised by uneven enforcement across Member States.[132]

However, centralising enforcement faces some significant legal and institutional challenges. Beyond the risk of additional complexity, such a solution would need to carefully align with the division of competencies between the EU and Member States, as established by the Treaties. Since most relevant regulations in the digital sector are based on Article 114 TFEU,[133] which defines the internal market as a shared competence, any shift toward centralised enforcement should consider the Treaties, and particularly the principles of subsidiarity and proportionality. However, given that this regulatory change would apply only to particularly relevant cases, for instance only to major platforms operating transnationally, centralisation could be justified, also considering the significant effort and resources required across Member States.

An additional challenge for a centralised approach relates to institutional independence. If the European Commission were to be designated as the central enforcer, it must be acknowledged that it is a political body rather than an independent regulator, making it susceptible to political pressures.[134] This could lead to situations where the Commission must balance conflicting policy

[128] European Union Agency for Fundamental Rights, 'GDPR in Practice – Experiences of Data Protection Authorities' <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities> accessed 11 April 2025.
[129] Autorità Garante della Concorrenza e delMercato, 'AGCM - Avviata istruttoria nei confronti di Google per pratiche commerciali scorrette' <https://www.agcm.it/media/comunicati-stampa/2024/7/PS12714> accessed 15 April 2025.
[130] Bastos and Pałka (n 9) 493.
[131] Bastos and Pałka (n 9) 489.
[132] Demková and De Gregorio (n 10) 3.
[133] Annegret Engel, 'Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market' in Annegret Engel, Xavier Groussot and Gunnar Thor Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer Nature Switzerland 2025). The stretching of EU competences through the use of Article 114 TFEU as a legal basis is particularly visible in the context of the EMFA. The adoption of this Regulaton marked the first time the Union has taken legislative action on media freedom, an area traditionally regarded as falling primarily within the competencies of Member States. See, Christina Etteldorf, 'Why the Words "But" and "However" Determine the EMFA's Legal Basis' (2023) Verfassungsblog <https://verfassungsblog.de/why-the-words-but-and-however-determine-the-emfas-legal-basis/> accessed 11 April 2025.
[134] Hert and Hajduk (n 10) 297.

objectives,[135] including those unrelated to platform regulation but still influencing enforcement decisions. For example, broader economic, trade, or geopolitical considerations could indirectly shape regulatory priorities. For these reasons, granting the Commission additional enforcement powers would require careful safeguards to ensure impartiality.

This problem is particularly pressing in the field of data protection, where the requirement for an independent supervisory authority is explicitly affirmed by EU primary law.[136] A comparable issue has already manifested since the origin in the field of EU competition law, where the Commission has always acted as both regulator and enforcer. In this context, the lack of impartiality has been mitigated through internal safeguards designed to ensure procedural autonomy. While this model could serve as a precedent, it remains unclear whether it provides a sufficient degree of institutional independence, especially in areas where impartiality is constitutionally mandated. These considerations suggest an alternative solution consisting in the centralisation of enforcement within a newly created independent body structured along the lines of the EDPB,[137] which could combine expertise with institutional distance from political interests.

Moreover, national authorities and Member States may exhibit reluctance in relinquishing areas of competencies and powers. This resistance can stem from a desire to maintain national sovereignty over certain regulatory domains, fearing loss of control over domestic issues or a reduction in the ability to cater to local needs and political climates. Thus, the call for EU-wide uniformity in regulations can be perceived as a threat to national autonomy, leading to a cautious approach in adopting comprehensive EU mandates towards centralisation and a preference for retaining their established practices and powers.[138]

Partial centralisation offers a pragmatic compromise between full supranational enforcement and fragmented national oversight. By selectively entrusting EU bodies with direct powers in clearly defined areas, while preserving the role of national authorities, this model would balance the need for coherence and efficiency with the principles of subsidiarity and independence. Such an approach reflects an evolving enforcement landscape within the EU that increasingly requires robust and coordinated responses to cross-border digital challenges. However, its legal and political feasibility still appears highly problematic, positioning this solution more as a long-term objective than an immediately viable reform option.

V. Conclusions

The European effort to expand the digital acquis reflects an ambitious political commitment to shaping the digital space in accordance with European constitutional values. Yet, the growing density of regulatory instruments, from the GDPR to the AI Act, has given rise to a fragmented and overlapping landscape that challenges effective and coherent enforcement of European digital regulation. While substantive overlaps are now in the spotlight of the simplification agenda, the institutional architecture responsible for the enforcement remains complex and leave European

[135] Ilaria Buri, 'A Regulator Caught Between Conflicting Policy Objectives. Reflections on the European Commission's Role as DSA Enforcer' in Joris van Hoboken (ed), *Putting the Digital Services Act into Practice*, Verfassungbooks 2023, 80.
[136] See Article 16 TFEU and Article 8 of the Charter.
[137] However, this solution would – again – have to take into account the *Meroni* doctrine (see n 117).
[138] The functional and political considerations lying behind the allocation of competences among national and supranational level are further described in: Bastos (n 108) 53.

and national authorities in a situation of uncertainty characterised by vertical or horizontal, intra-framework or extra-framework overlaps.

The increasing number of competent authorities, even within a single Member State, compounded by overlaps in cross-border cases and the partial centralisation of enforcement under certain regulations risks undermining the effectiveness of the EU digital agenda, particularly when dealing with major actors, such as VLOPs and gatekeepers. Additional concerns include the stretch of the rule of law in the activities of public authorities and reduced legal certainty as an adverse effect not only on the internal market but also on fundamental rights and democratic values.

To address this situation, the EU should focus more on enforcement and consider moving toward more integrated enforcement structures. This paper has outlined three possible approaches, ranging from the more achievable, enhancing existing coordination tools and establishing dedicated forums, to the more ambitious, such as binding conflict-resolution mechanisms and the further centralisation of enforcement powers. While more far-reaching reforms may offer greater systemic effectiveness, they face significant obstacles, both in terms of building political consensus and ensuring compliance with the limits set by EU primary law.

In this perspective, advancing the more achievable solutions would already mark meaningful progress. Choosing inaction, on the other hand, carries the real risk of replicating, or even exacerbating, the enforcement shortcomings observed under previous frameworks, most notably the GDPR. Although enforcement design has not traditionally been central to EU regulatory efforts, largely due to the principle of procedural autonomy, the scale and ambition of today's digital legislation require enforcement mechanisms capable of matching their scope.