

ARTICLE

Enforcement Design in EU Digital Regulation: Lessons for the Digital Fairness Act

Laura Zoboli¹  and Joanna Mazur²

¹IE University, Spain and ²University of Warsaw, Poland

Corresponding author: Laura Zoboli; Email: laura.zoboli@ie.edu

Abstract

While the legislative text of the Digital Fairness Act (DFA) has not yet been published, it is already clear that its effectiveness will depend as much on its enforcement design as on the content of its substantive provisions. Experience with recent instruments – including the Digital Services Act, the Digital Markets Act, the Artificial Intelligence Act and the Data Act – reveals persistent difficulties in ensuring consistent and timely enforcement across Member States. Building on the findings of the Commission’s *Fitness Check of EU Consumer Law on Digital Fairness*, this article examines how the enforcement design developed in these legal acts can inform the institutional and procedural design of the DFA. It argues that the challenges identified by the *Digital Fitness Check* reflect deeper patterns of procedural, institutional and epistemic fragmentation in EU enforcement. By analysing how different enforcement designs address these tensions through mechanisms of centralisation, coordination and capacity-building, the article identifies key design choices that may shape the emerging enforcement framework of the DFA.

Keywords: Digital Fairness Act; Digital regulation; Enforcement design

I. Introduction

The European Union’s (EU) digital rulebook appears to have reached a moment when consolidation has become inevitable. After a decade of rapid regulatory expansion – from data protection and platform governance to artificial intelligence (AI) and algorithmic accountability – the system has grown increasingly dense and fragmented. The recent Digital Omnibus proposal,¹ part of the European Commission’s (Commission) forthcoming Digital Package on Simplification,² indicates that simplification has become a guiding theme of the next phase of EU digital policy. At the same time, the recently released 2030 consumer agenda confirms that the EU is committed to robust consumer protection in rapidly changing markets.³

¹ See Commission, “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)” COM (2025) 837 final.

² The Digital Package on Simplification is expected to include a comprehensive Digital Fitness Check – a horizontal review aimed at assessing the coherence and cumulative impact of the EU’s digital *acquis*, and at identifying areas where regulatory simplification or alignment may be warranted.

³ See Commission, “2030 Consumer Agenda and Action Plan for Consumers in the Single Market: A New Impulse for Consumer Protection, Competitiveness and Sustainable Growth” COM (2025) 848 final.

Within this evolving landscape, the forthcoming Digital Fairness Act⁴ (DFA) is expected to play a central role, serving as the connective tissue between consumer protection and the EU's broader digital governance framework. It represents the next step in the EU's ambition to ensure that the principles of fairness and transparency, long familiar in consumer law, extend to the infrastructures of the digital market itself. Yet experience with recent legislative initiatives – most notably the Digital Services Act (DSA),⁵ the Digital Markets Act (DMA),⁶ the Data Act,⁷ and the Artificial Intelligence Act (AI Act)⁸ alongside the more established General Data Protection Regulation (GDPR)⁹ – suggests that the effectiveness of these frameworks depends not only on the sophistication of their substantive rules, but equally on the design and operation of their enforcement.¹⁰

Despite the importance of the DFA in current policy discourse,¹¹ attention has so far concentrated mainly on its substantive aspirations – even though the legislative text has not yet been published. Much less consideration has been given to its prospective *enforcement design*, even though the record of existing EU digital regulation reveals how decisive it can be. The *Fitness Check of EU Consumer Law on Digital Fairness* (Digital Fairness Fitness Check)¹² – the Commission's most comprehensive recent evaluation of enforcement under EU consumer law – diagnosed a persistent enforcement deficit. It pointed to structural weaknesses in how EU and national authorities coordinate, resource and implement consumer-law obligations in online markets. These weaknesses, which have become increasingly visible as digitalisation accelerates, are not merely operational shortcomings but symptoms of deeper tensions within the EU's multi-level enforcement architecture. They reveal what may be described as procedural, institutional and epistemic fragmentation – three interlocking dimensions of a system struggling to translate substantive fairness norms into effective regulatory action.

⁴ The EU Commission acknowledged the need for a Digital Fairness Act in their [Digital Fairness Fitness Check Report](#). The European Parliament called for the need for additional consumer protections regarding addictive design on digital platforms in their [Resolution on Addictive Design](#). The last step in the process toward a draft of the DFA consists in the public consultation on the forthcoming Digital Fairness Act, conducted between July and October 2025 and available at <https://digitalfairnessact.com/public-consultation> (last accessed 2 February 2026). The DFA Proposal is expected for the third quarter of 2026.

⁵ See 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) [2022] OJ L277/1.

⁶ See 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) [2022] OJ L265/1.

⁷ See Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L2023/2854.

⁸ See 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) [2024] OJ L2024/1689.

⁹ See 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 (General Data Protection Regulation) [2016] OJ L119/1.

¹⁰ Out of these legal acts, the enforcement of the GDPR has been the most thoroughly scrutinised, see, for the meta-analysis of the studies assessing the effectiveness of the GDPR's enforcement, see W Li, Z Li, W Li, Y Zhang, and A Li, "Mapping the Empirical Literature of the GDPR's (In-) Effectiveness: A Systematic Review" (2025) 57 *Computer Law & Security Review* article number: 106129. For literature criticising its legal design, see below.

¹¹ See the public consultation on the DFA and the academic debate, e.g., C Busch, "Enabling Innovation and Protecting Consumers in the Agentic Economy: Why the Digital Fairness Act Should Regulate Agentic AI" (2025) <https://doi.org/10.2139/ssrn.5369055> (last accessed 15 January 2026).

¹² See Commission, "Commission Staff Working Document Fitness Check of EU consumer law on digital fairness" SWD (2024) 230 final.

The purpose of this article is to examine the enforcement design of the DFA – that is, the institutional, procedural and epistemic mechanisms through which digital-market rules are implemented and supervised – in order to identify the core choices that shape the protection of consumers’ rights in the digital domain. While the DFA will build on the institutional foundations of EU consumer law¹³ – particularly its decentralised enforcement model and the Consumer Protection Cooperation (CPC) framework¹⁴ – our analysis considers its prospective evolution within the wider architecture of EU digital regulation. Although the instruments examined in this article do not all pursue consumer protection as their primary objective, their enforcement systems have a direct bearing on the position of individuals in digital markets. The increasing fragmentation of the EU’s digital rulebook – across data protection, platform governance, competition-inspired regulation and data-sharing frameworks – means that consumer-facing practices are shaped by institutional and procedural arrangements dispersed over multiple legal acts. Understanding these acts is therefore essential to identifying the enforcement choices available to the DFA.

This article focuses on the form of fragmentation most relevant to enforcement: the diversity of institutional and procedural architectures through which existing EU instruments operate in practice. To that end, the discussion draws on the enforcement models developed in instruments such as the GDPR, the Data Act, the DSA, the DMA and the AI Act, which together form key pillars of the EU’s digital *acquis* and confront challenges closely related to those identified in the Digital Fairness Fitness Check. The analysis does not aim to provide a comprehensive account of enforcement practice under each regime; rather, it isolates specific mechanisms that illustrate how different regulatory models have addressed comparable problems in enforcement design, and what insights they may offer for the emerging DFA framework.

Methodologically, the article proceeds in three steps. The diagnostic section (Section II) outlines the enforcement challenges highlighted in the Digital Fairness Fitness Check and groups them into a triad of procedural, institutional and epistemic fragmentation.

The comparative section (Section III) situates these challenges within the broader literature on regulatory governance – drawing on theories of responsive, experimentalist and polycentric approaches to regulation – and examines how recent EU instruments operationalise these approaches through different enforcement designs. The selection of legal acts analysed in Section III follows two criteria. First, the acts were chosen because they regulate consumer-facing dynamics in digital markets¹⁵ and therefore confront enforcement problems closely related to those identified in the Digital Fairness Fitness Check. Instruments primarily concerned with adjacent objectives – such as cybersecurity or technical infrastructure – are not included, as they raise distinct enforcement logics and would dilute the comparative focus. Secondly, the selection aims to capture variation in

¹³ This article does not revisit the enforcement framework of EU consumer law, which is already well documented in the literature and in the Commission’s own assessments – for an overview, see, e.g., C Riefa and M Grochowski, “Chapter 22: The enforcement of EU consumer law” in M Scholten (ed), *Research Handbook on the Enforcement of EU Law* (Cheltenham, UK: Edward Elgar Publishing, 2023), pp 350–364. Its focus is instead on the enforcement architectures developed in adjacent digital regimes, which offer insights particularly relevant to the design of the DFA.

¹⁴ See 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 [2017] OJ L345/1, consolidated version of 12 September 2025.

¹⁵ This article does not revisit the enforcement framework of EU consumer law, which is already well documented in the literature and in the Commission’s own assessments – for an overview, see, e.g., C Riefa and M Grochowski, “Chapter 22: The Enforcement of EU Consumer Law” in M Scholten (ed), *Research Handbook on the Enforcement of EU Law* (Cheltenham, UK: Edward Elgar Publishing 2023), pp 350–64. Its focus is instead on the enforcement architectures developed in adjacent digital regimes, which offer insights particularly relevant to the design of the DFA.

enforcement architecture within the EU digital *acquis*, ranging from centralised (DMA) to decentralised (GDPR, Data Act) and hybrid models (DSA, AI Act). The comparison focuses on three features of enforcement design that recur across these regimes and that correspond to the triad developed in the diagnostic section: the institutional dimension (allocation of enforcement competences and the identity/level of the enforcers), the procedural dimension (how enforcement is organised, including cooperation structures and the balance between *ex ante* and *ex post* mechanisms), and the epistemic dimension (how access to information, technical capacity and resources is addressed). The analysis is doctrinal in method – grounded in the text, structure and preparatory rationales of the relevant instruments – but governance-oriented in purpose: it treats these regimes as alternative enforcement designs from which lessons can be drawn for the DFA.

Thus, the prescriptive section (Section IV) distils the lessons that follow from this comparison and formulates design principles for the DFA's enforcement framework, including selective centralisation for systemic actors, stronger EU-level coordination, procedural time-limits, fairness-by-design obligations, and the creation of shared digital-analysis tools for enforcement authorities. Section V concludes. Analytically, the article reconceptualises digital fairness not merely as a matter of substantive prohibitions but as an issue of *institutional capacity*, *procedural coherence* and *epistemic adequacy* within the EU's evolving architecture of digital enforcement.

II. Digital Fairness Fitness Check: what are the challenges for enforcement in the digital sphere?

The Digital Fairness Fitness Check, published by the European Commission in October 2024, provides the most comprehensive recent assessment of the adequacy of the EU's consumer-law enforcement framework in the digital economy. Its findings suggest that the principal difficulties arise not only from gaps in substantive law, but also from persistent structural weaknesses in the operation of enforcement and cooperation mechanisms. The report depicts a landscape characterised by slow and cumbersome procedures, uneven institutional capacities, limited use of digital-specific investigative and monitoring tools, fragmented sanctioning and coordination practices, and significant obstacles in addressing traders operating across or beyond the EU. Together, these weaknesses undermine both the uniform application of EU law and the attainment of the high level of consumer protection envisaged by Article 169 of the Treaty on the Functioning of the EU (TFEU).¹⁶

I. The structural enforcement gap

At the heart of the Commission's diagnosis lies a *structural enforcement gap*. The primary horizontal consumer-law directives – the Unfair Commercial Practices Directive (UCPD),¹⁷ the Consumer Rights Directive (CRD),¹⁸ and the Unfair Contract Terms

¹⁶ Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47. As Craig has observed, enforcement is not merely a technical function but a foundational condition of the vitality of the EU legal order, whose multi-level structure renders it particularly vulnerable to fragmentation, see P Craig, "Foreword" in M Scholten and L Stähler (eds), *Research Handbook on the Enforcement of EU Law* (Edward Elgar 2024), pp xii–xiii.

¹⁷ See 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 ("Unfair Commercial Practices Directive") [2005] OJ L149/22, consolidated version of 28 May 2022.

¹⁸ See Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the

Directive (UCTD)¹⁹ – are built on open-textured, principle-based norms. While this flexibility once served regulation well, it now hinders effective oversight of complex digital business models. According to the Digital Fairness Fitness Check, the rules are not specific enough to allow them to be applied effectively to commercial practices and system architectures in the digital environment, nor do they facilitate the use of automated enforcement tools.²⁰ Traders thus struggle to translate broad obligations of fairness and transparency into concrete interface or algorithm design choices, while regulators often lack clear benchmarks and tools suitable for large-scale digital enforcement – what regulatory-capacity theory would describe as a “technology-law gap.”²¹ This mismatch between evolving market realities and enforcement capacity exemplifies epistemic fragmentation, and is compounded by uneven access to technical and analytical resources across Member States.

2. Lengthy and cumbersome procedures

The Digital Fairness Fitness Check identifies the length and complexity of procedures as a significant factor undermining the effectiveness of the CPC network in digital markets.²² While the network has markedly improved cross-border coordination, the 2024 *Application Report on the CPC Regulation*²³ shows that limited resources, procedural complexity and the absence of digital-specific investigative tools continue to impede timely enforcement. In practice, coordinated actions and subsequent litigation frequently outlast the commercial lifecycle of the products or services concerned, enabling firms to adjust interfaces or business models before a decision is reached. This temporal misalignment between the pace of digital markets and the rhythm of enforcement exemplifies procedural fragmentation. Within the EU’s multilevel system, subsidiarity constrains any move towards full centralisation; acceleration must therefore rely on more effective coordination, clearer prioritisation and more harmonised procedural frameworks across authorities.

3. Expertise and capacity asymmetries

A further set of challenges identified in the Digital Fairness Fitness Check concerns the uneven distribution of expertise and resources across Member States. The report notes that recent technologies and business models require enforcement authorities to develop specialised expertise at national level, while differences in the capacity of national authorities to deal with enforcement cases due to limited resources, differences in investigation and enforcement powers, etc., continue to hinder consistent outcomes. The 2024 *Application Report on the CPC Regulation* confirms this divergence: some authorities, such as the Netherlands Authority for Consumers and Markets or Germany’s

Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (“Consumer Rights Directive”) [2011] OJ L304/64, consolidated version of 28 May 2022.

¹⁹ See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (“Unfair Contract Terms Directive”) [1993] OJ L95/29, consolidated version of 28 May 2022.

²⁰ See Commission (n 12) 87. The supporting *Final Report Part 1* develops this diagnosis conceptually under the rubric of digital asymmetry: information, technical expertise, and market power have shifted decisively towards digital traders, creating enforcement environments that traditional, principle-based norms cannot easily penetrate.

²¹ G E Marchant, “The Growing Gap between Emerging Technologies and the Law” in G Marchant, B Allenby and J Herkert (eds) *The Growing Gap between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Dordrecht: Springer 2011), pp 19–33.

²² See Commission (n 12) 87.

²³ See Commission, “Report from the Commission to the European Parliament and the Council on the application of Regulation (EU) 2017/2394 of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws” COM (2024) 311 final.

Bundesnetzagentur, have invested in data-science and behavioural-analysis teams, whereas others remain reliant almost exclusively on legal staff. This asymmetry results in uneven enforcement intensity and invites forum shopping by traders.²⁴

From a regulatory-governance perspective, such disparities exemplify the principal-agent problem that characterises EU enforcement more broadly: harmonised norms rely on national agents whose capacities and priorities the EU cannot directly command. The resulting imbalance constitutes a form of institutional fragmentation – a gap between the level at which rules are formulated and the level at which they are applied. Enhancing horizontal cooperation, investing in capacity-building, and developing shared analytical infrastructure therefore emerge as essential to strengthening enforcement in the digital sphere.

4. Absence of digital-specific enforcement tools

The Digital Fairness Fitness Check repeatedly stresses the lack of technologically adapted investigative tools. Traditional mechanisms – consumer complaints, ad hoc sweeps, manual monitoring – cannot detect algorithmic manipulation or behavioural targeting operating at scale. The report highlights the absence of tools to detect infringements in online markets and calls for coordinated investment in AI-assisted detection, web-crawling and automated data-analysis infrastructure. The Commission’s experimental e-Lab initiative offers only limited crawling capabilities, while regulators outside the EU such as the UK Competition and Markets Authority’s Digital Markets Unit or the Australian Competition and Consumer Commission’s Digital Platforms Branch already integrate data-science functions within their enforcement teams. The resulting disparity in technological capacity constrains the ability of national authorities to engage in proactive oversight and contributes to uneven enforcement outcomes across the Union. Addressing this gap – through shared analytical infrastructure and the development of common digital-investigation tools – emerges as a central challenge for any future enforcement framework of the DFA.

5. Coordination of sanctions and deterrence

The Digital Fairness Fitness Check highlights persistent difficulties in coordinating the imposition of sanctions within the CPC network. According to the report, due to difficulties experienced by CPC authorities to effectively coordinate the imposition of fines in the context of coordinated actions, the deterrent effect of the CPC Regulation remains limited. Although the Modernisation (*Omnibus*) Directive²⁵ introduced turnover-based penalties of up to 4 per cent for widespread cross-border infringements, the 2023 *Application Report on the CPC Regulation* shows that national practice continues to diverge widely. Penalties imposed for comparable infringements may range from a few thousand euros to several million, reflecting variations in legal frameworks, procedural rules, and institutional capacity.

Such disparities weaken the predictability of enforcement outcomes and dilute deterrence at Union level. By contrast, other EU regimes – notably in competition law – achieve a higher degree of coherence through centralised enforcement and harmonised

²⁴ The Commission acknowledges that even participation in EU-wide “sweeps” and coordinated actions remains uneven across the Member State authorities – see Commission (n 12) 88.

²⁵ See Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC, and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

fining methodologies.²⁶ In light of these challenges, the Digital Fairness Fitness Check notes that the Commission is reflecting on the possible need to reform the CPC Regulation in order to strengthen it. Ensuring a more consistent approach to sanctioning thus emerges as a necessary component of any future effort to improve the enforcement effectiveness of EU consumer law in the digital sphere.

6. Enforcement against non-EU traders

The Digital Fairness Fitness Check observes that enforcement against traders without establishment or assets in the EU or European Economic Area who target consumers residing in the EU has proven to be difficult. The difficulty reflects the territorial limits of EU enforcement mechanisms in an increasingly global digital marketplace. Supporting studies confirm that a substantial share of online traders serving EU consumers are domiciled outside the Union, complicating both the service of orders and the execution of fines. In the absence of effective mutual-assistance arrangements, authorities may issue decisions that remain unenforceable abroad.

Recent regulatory initiatives have begun to mitigate this gap. The DSA requires intermediary platforms to ensure trader traceability and obliges non-EU providers to appoint an EU representative, thereby improving authorities' ability to identify and contact traders established outside the Union.²⁷ The Digital Fairness Fitness Check nonetheless indicates that these measures remain partial and that additional forms of platform-assisted enforcement – such as requiring marketplaces to act upon verified orders against traders established in third countries – could strengthen cross-border compliance. Any reform of the CPC framework or future DFA will therefore need to confront this enduring constraint: the effectiveness of enforcement remains territorially bounded, whereas the digital economy is not.

7. Regulatory fragmentation and institutional overlap

The EU's digital rulebook – spanning the DSA, DMA, AI Act, Data Act and other sectoral regimes²⁸ – creates an increasingly polycentric enforcement landscape. The Digital Fairness Fitness Check notes that extremely limited provisions dealing with cooperation between the enforcement authorities designated under the relevant enforcement system and authorities outside that enforcement system exist. In practice, parallel investigations may arise: a consumer-law authority might assess a manipulative interface under the UCPD while a Digital Services Coordinator examines the same design under Article 25 DSA. Such overlaps risk inconsistent outcomes and procedural inefficiency, particularly where authorities proceed independently on the basis of different mandates and evidentiary thresholds. The challenge is therefore not only one of coordination, but also of ensuring that the various digital regimes interact in a manner that enables coherent and predictable enforcement across the EU.

8. Evidentiary burdens and legal uncertainty

A further obstacle lies in the epistemic asymmetry between traders and enforcers. The Digital Fairness Fitness Check records excessive difficulties with meeting the burden of

²⁶ M Bernatt and L Zoboli, "Chapter 25: Competition law" in *Research Handbook on the Enforcement of EU Law* (Cheltenham, UK: Edward Elgar Publishing 2023).

²⁷ See DSA (n 6) Art 13.

²⁸ For a table collecting the legal acts constituting EU digital regulations, see Bruegel Dataset (2023) "A dataset on EU legislation for the digital world", version of 6 June 2024, <<https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world>> (last accessed 21 November 2025).

proof in technologically complex cases. Algorithms operate as black boxes, leaving regulators unable to prove causation between interface design and consumer harm. Empirical findings from the stakeholder survey show an almost even split: 46% of respondents favoured shifting the burden of proof to traders in cases of major digital asymmetry, while 48 per cent opposed.²⁹ The absence of consensus freezes reform but exposes a structural problem: current evidentiary rules assume transparency of conduct, whereas algorithmic systems conceal it. A doctrinal analogy lies in the GDPR's accountability principle, which reverses evidential duties by requiring controllers to demonstrate compliance. Extending such logic to consumer law – through rebuttable presumptions of unfairness for opaque personalisation or manipulative design – would align enforcement with informational reality.

9. Under-enforcement of unfair terms and collective redress

Enforcement has traditionally concentrated on unfair practices rather than unfair contract terms. The Commission notes that comparatively fewer resources were placed on the monitoring of unfair contract terms. The supporting study's *Case Study on Unfair Terms* confirms this imbalance: national authorities described contract-term supervision as resource-intensive with limited visible impact. Consequently, unlawful terms – especially those in “free” data-for-service contracts – persist unchallenged. Landmark actions, such as the one started by *Union Fédérale des Consommateurs – Que Choisir* against Facebook and Twitter yielded fines of only €30,000 and €50,000, respectively, sums not deterrent compared to the companies' revenues. Collective redress under the Representative Actions Directive³⁰ faces further obstacles: conflicts of applicable law and divergent transpositions of the UCTD mean that various national laws may be applicable depending on the consumers concerned. This patchwork weakens the preventive and restorative aims of EU consumer law.

10. Data and monitoring deficiencies

Effective enforcement presupposes reliable information. Yet many authorities are not able to provide estimates of resources devoted to digital enforcement, and data on CPC activities are fragmented and inconsistent. The *Final Report Part 1* confirms that fewer than half of national authorities maintain separate statistics for online cases. Without empirical feedback, policymaking becomes impressionistic. The Commission therefore advocates the deployment of automated market-sweep tools and the establishment of an EU-wide Digital Fairness Observatory – building on the e-Lab model – to aggregate enforcement metrics. This shift from reactive to reflexive governance would allow continuous calibration of policy and resource allocation. For the DFA, embedding such reporting duties will be vital to measure progress towards a uniform level of protection.

11. Synthesis: the triple fragmentation of enforcement

The cumulative picture emerging from the Digital Fairness Fitness Check and its supporting studies is one of triple fragmentation – procedural, institutional and epistemic.

²⁹ See also European Law Institute (2023) “Response of the European Law Institute – European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law”, European Law Institute 2023, 37, <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_to_the_European_Commission_s_Public_Consultation_on_Digital_Fairness_.pdf> (last accessed 2 February 2026).

³⁰ See Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L409/1, consolidated version of 12 September 2025.

Procedurally, enforcement remains slow and nationally bounded; institutionally, multiple specialised regimes coexist without coherent coordination; epistemically, regulators lack access to the data and expertise required to decipher complex digital systems. Each dimension reinforces the others: procedural delays deter cooperation, institutional silos prevent knowledge sharing, and informational deficits perpetuate uncertainty. The overall consequence is an erosion of both the effectiveness and the legitimacy of EU consumer-law enforcement.

As summarised in Table 1, the enforcement challenges identified in the Digital Fairness Fitness Check are reorganised and systematised through the analytical framework developed in this article. The first two columns reflect the challenges and underlying causes as described by the Commission, while the third column sets out indicative enforcement-design responses derived from our comparative analysis of existing EU digital regulation. The table therefore offers an analytical synthesis that bridges the diagnostic findings of the Fitness Check with the comparative and prescriptive discussion developed in Sections III and IV. The table provides a bridge between the descriptive analysis developed here and the comparative examination of enforcement design in Section III, illustrating how lessons from current instruments may inform a more coherent and technologically responsive enforcement architecture for digital fairness in the EU presented in Section IV.

The forthcoming DFA is explicitly framed, in the Commission's Call for Evidence,³¹ as a response to several of these deficiencies. Its objectives are described as ensuring a level playing field, reducing market fragmentation and legal uncertainty, and making enforcement easier. In light of the diagnostic picture set out in this section, the central question becomes how far existing enforcement designs in the GDPR, the DSA, the DMA, the Data Act and the AI Act already offer elements of a solution. The next section therefore turns to a comparative analysis of those regimes, using the triad of procedural, institutional and epistemic fragmentation as a lens through which to assess their enforcement architectures and their relevance for the emerging DFA.

III. Grounding comparative approach in the state-of-art

The diagnostic exercise in Section II revealed that the enforcement deficit identified in the Digital Fairness Fitness Check is multi-dimensional, combining procedural, institutional and epistemic elements. To translate this diagnosis into design guidance, the comparative analysis that follows rests on two complementary foundations. First, it draws on established frameworks in regulatory governance – particularly responsive, experimentalist and polycentric governance – which conceptualise enforcement as a problem of institutional design, procedural timing and informational capacity under conditions of complexity. Second, it examines the legislative rationales that accompanied recent EU digital acts – including the DMA, DSA, AI Act, Data Act and the GDPR³² procedural proposal – in order to understand the considerations that shaped their enforcement architectures.

This dual grounding allows for a comparative analysis that is both theoretically informed and empirically anchored. It highlights the principal design variables – centralisation versus coordination, *ex ante* versus *ex post* control, and the distribution of expertise and analytical capacity – that condition enforcement performance across regimes. Section III.1 elaborates the theoretical foundations of this approach,

³¹ See Commission, Directorate-General for Justice and Consumers, “Call for Evidence for an Impact Assessment” Ares (2025) 5829481.

³² See also Commission, “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 final.

Table 1. Enforcement challenges and implications for the DFA.

Enforcement challenge (Digital Fairness Fitness Check)	Underlying cause(s)	Relevant EU frameworks/instruments (as referenced in the Digital Fairness Fitness Check)	Indicative implications for DFA enforcement design
Cross-border practices and fragmented action	CPC cooperation improves coordination, but procedures remain lengthy; national resources uneven; parallel national files when CPC is not activated.	CPC Regulation model (enhanced); DMA High-Level Group for cross- network coordination (consumer/ DSA/DMA/DPAs).	Establish <i>lead-authority</i> or <i>single-venue</i> pathways for widespread infringements; introduce EU-level coordination triggers and joint investigation teams.
Lengthy and cumbersome proceedings	Complex, multi-jurisdictional actions; slow litigation; heavy evidentiary burdens.	CPC joint actions; Representative Actions Directive (RAD) mechanisms for collective commitments.	Introduce <i>fast-track</i> procedures with deadlines and interim orders; enable negotiated settlements and commitments; adopt presumptions to streamline evidence.
Insufficient expertise and administrative capacity	Wide divergence in national capabilities; lack of digital, data-science and behavioural expertise.	Commission-supported training projects; CPC mutual-assistance framework.	Create EU-funded <i>Tech & Data Units</i> ; establish shared forensic labs and algorithmic audit teams; introduce mandatory staff exchanges and capacity-building schemes.
Absence or uneven uptake of digital enforcement tools	Principle-based directives not easily operationalised in automated monitoring; lack of technical infrastructure.	Commission e-Lab initiative; Fitness Check recommendations on AI-based detection.	Provide statutory basis for <i>EnfTech</i> (AI-driven crawlers, mystery-shopping bots, API access, data-access orders).
Uncoordinated and insufficient sanctions	Turnover-based fines harmonised only for cross- border CPC cases; domestic sanctions vary widely; low deterrence.	Modernisation (Omnibus) Directive; CPC penalty coordination proposals.	Introduce EU-wide minimum and graduated penalty levels; coordinate sanction decisions across Member States; apply recidivism multipliers.
Traders established outside the EU	Difficulties enforcing orders and fines against non- EU traders; lack of jurisdictional tools.	DSA trader-traceability rules; CPC mutual-assistance framework.	Impose <i>representative-in-EU</i> duties with joint liability; use <i>platform-assisted enforcement</i> for traders on marketplaces; adopt geo-targeting jurisdiction rules.
Regulatory fragmentation across regimes (DSA/ DMA/GDPR vs consumer law)	Parallel enforcement systems with limited cooperation; risk of divergent decisions on identical facts.	DMA High-Level Group; emerging DPA–CPC coordination networks.	Include <i>inter-regime coordination clauses</i> (mandatory information-sharing, conflict rules, joint case teams); create a cross-regime <i>consistency mechanism</i> .

(Continued)

Table 1. (Continued)

Enforcement challenge (Digital Fairness Fitness Check)	Underlying cause(s)	Relevant EU frameworks/instruments (as referenced in the Digital Fairness Fitness Check)	Indicative implications for DFA enforcement design
Data asymmetries and evidentiary burdens	Algorithmic opacity and lack of access to internal data; few national or CJEU precedents.	Fitness Check survey on burden of proof; GDPR accountability principle; RAD evidence provisions.	Introduce <i>burden-shifting</i> or rebuttable presumptions for hidden practices; enable disclosure orders and algorithmic audits; issue binding interpretative guidelines.
Under-enforcement of unfair terms and collective-redress frictions	Enforcement focused on practices; national divergences in UCTD transposition hinder cross-border cases.	Representative Actions Directive; Omnibus Directive penalty regime.	Update UCTD black and grey lists for digital contracts; harmonise conflict-of-law rules in collective actions; require standardised key-term summaries.
Evidence and monitoring gaps	Fragmented administrative data; no common indicators for enforcement performance.	Fitness Check proposal for systematic monitoring and data collection.	Establish <i>EU Digital Fairness Observatory</i> ; introduce standardised reporting taxonomy and periodic sweeps; publish enforcement dashboards.

while Section III.2 examines the institutional rationales reflected in recent legislative acts, and Section III.3 sets out the typology of enforcement designs used for comparison in Section IV.

Two forms of fragmentation can be distinguished in the EU's digital regulation. The first concerns the proliferation of legal acts governing consumer-facing digital practices, which distribute relevant norms across regimes that use different terminologies and regulatory techniques. The second concerns the diversity of institutional and procedural arrangements through which these regimes organise enforcement. It is this latter, enforcement-related form of fragmentation that is of primary relevance for the DFA and that serves as the focus of the comparative analysis in this section.

1. Theoretical frameworks for analysing enforcement design

A comparative analysis of enforcement design in EU digital regulation requires grounding in theories that explain how regulation operates under conditions of complexity, technological acceleration and multi-level governance. Three strands of scholarship – responsive regulation, experimentalist governance and polycentric governance – provide particularly useful analytical lenses.

Responsive regulation, as developed by Ayres and Braithwaite,³³ conceptualises enforcement as an adaptive process rather than a fixed hierarchy of sanctions. Regulators escalate interventions when voluntary compliance fails, and de-escalate when cooperation is restored. This “regulatory pyramid” supports the EU's increasing reliance on mixed enforcement toolkits, combining *ex ante* obligations (such as risk assessments and audits) with *ex post* corrective powers. The DMA's obligations on gatekeepers and the DSA's systemic risk assessments both reflect this logic of calibrated responsiveness.

Experimentalist governance, associated with Sabel and Zeitlin,³⁴ interprets EU regulation as iterative and participatory. Framework goals are defined centrally, implementation is delegated to national authorities and results are reviewed through mechanisms of mutual monitoring and revision. This model resonates with the enforcement architectures of the DSA and AI Act, where day-to-day supervision is largely decentralised, but coordinated through EU-level bodies such as the Digital Services Board and the European Artificial Intelligence Office. Joint investigations, harmonised guidelines, and delegated acts are thus not ancillary, but integral to enforcement effectiveness.

Polycentric governance, drawing on Ostrom,³⁵ addresses the challenge of coherence in multi-actor, multi-level systems. Decentralised arrangements can enhance resilience and innovation, but risk fragmentation if coordination and information-sharing are weak. The Digital Fairness Fitness Check's findings on procedural delays, capacity asymmetries and informational gaps are symptomatic of insufficiently structured polycentricity. Recent regulatory initiatives – selective centralisation under the DMA, strengthened cooperation under the DSA and the creation of a technical hub under the AI Act – may be understood as corrective attempts to anchor a dispersed enforcement ecosystem.

Taken together, these approaches highlight three dimensions of enforcement design: institutional (who enforces and at what level), procedural (how and when enforcement occurs) and epistemic (what data, tools and expertise enforcers can rely upon). These dimensions frame the comparative discussion that follows.

³³ See I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992).

³⁴ See C F. Sabel and J Zeitlin, (eds.), *Experimentalist Governance in the European Union: Towards a New Architecture* (Oxford University Press 2010).

³⁵ See E Ostrom, “Beyond Markets and States: Polycentric Governance of Complex Economic Systems” (2010) 100(3) *American Economic Review* 641.

2. Legislative rationales underlying enforcement design choices in digital regulation

Another vital source of information on the choices concerning enforcement design are explanations preceding the proposal of legal acts. For the purposes of this analysis, we scrutinised the proposals for the DMA,³⁶ the DSA,³⁷ the AI Act,³⁸ the Data Act,³⁹ and the reform of the GDPR's enforcement design⁴⁰ in order to identify how the Commission refers to the choices concerning enforcement with regard to its institutional and procedural elements.

The search reveals that the threat of regulatory fragmentation, the size and reach of the companies, and their number are mentioned as key factors for selecting a centralised enforcement design under the DMA:

Given the pan-European reach of the targeted companies, a decentralised enforcement model does not seem to be a conceivable alternative, including in light of the risk of regulatory fragmentation that the initiative is meant to address, nor would it be proportionate given the limited number of gatekeepers that would be in scope of the proposed framework.⁴¹

In the case of the DSA, the reasons for the proposed enforcement taking place mostly at the level of the Member States is to ensure “the swiftest and most effective enforcement of rules and protects all EU citizens.”⁴² However, the systemic risks are mentioned as a factor which should trigger a more centralised form of enforcement, taking place at the level of the EU. While the AI Act proposal is the most laconic with regard to the structure of the enforcement design, the final shape of AI Act's enforcement design entails both centralised and decentralised elements, differentiating the responsibility for the enforcement on the basis of the type of the AI system in question.

This illustrates that there are various ways of addressing the tension between the enforcement being “close” to the citizens, while also being consistent across the Member States and adequate for the size and scope of activities of the companies under regulation.⁴³ However, it is clear that either centralisation (DMA, to a certain extent: DSA and the AI Act) or coordination (to a certain extent the DSA and the AI Act, as well as the GDPR⁴⁴) is necessary for the cases concerning companies whose activities span across the number of Member States. It is also worth to underscore that certain forms of the

³⁶ See Commission, “Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)” COM/2020/842 final.

³⁷ See Commission, “Proposal for a Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC” COM/2020/825 final

³⁸ See Commission, “Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts” COM/2021/206 final.

³⁹ See Commission, “Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)” COM/2022/68 final – while we subjected the proposal to our study, it does not include any vital remarks on the enforcement design except for its decentralised character.

⁴⁰ See Commission (n 32).

⁴¹ Commission (n 35).

⁴² Commission (n 36).

⁴³ It is this dilemma that was supposed to be addressed by the GDPR's enforcement design: “The ‘one-stop-shop’ decentralised enforcement system aims to ensure consistent interpretation and application of the GDPR while preserving the principle of proximity, where individuals have the possibility to contact their local DPA and receive an answer.” – Commission (n 31).

⁴⁴ “Experience in the enforcement of the GDPR in cross-border cases shows that there is insufficient cooperation between DPAs prior to the submission of a draft decision by the lead DPA. Lack of sufficient cooperation and consensus-building on key issues in the investigation at this early stage has resulted in the submission of numerous cases to dispute resolution.” – *ibid.*

integration of the national expertise in the enforcement design are also an element of a centralised approach to enforcement.⁴⁵

Another choice concerning the enforcement design discussed in the proposals concerns *ex ante* or *ex post* character of the implemented obligations or prohibitions and, as a result, the character of the enforcers' intervention. While the DMA belongs rather to the former category,⁴⁶ for the AI Act the suggested solution constituted a combination of these approaches⁴⁷ and stresses the role of self-assessment in the enforcement design. Other elements concerning procedural aspects of the enforcement mentioned as important factors to consider when structuring the enforcement design with regard to its pace – similarly as the *ex ante* versus *ex post* approach – include the deadlines, which importance is especially crucial for the proposed changes to the GDPR's enforcement.⁴⁸

Last but not least, the proposals also refer to the resources available to the enforcers. The proposal of the DSA highlights that it “creates important efficiency gains in the cooperation across Member States and mutualising some resources for technical assistance at EU level.”⁴⁹ Hence, the aspects concerning the impact of the resources available to the enforcers should also be considered as crucial factors for proposing the adequate solutions.

3. Typologies of enforcement designs in EU digital regulation

Against this background, to compare enforcement architectures across legal acts, this article adopts a typology structured around the three identified dimensions: institutional, procedural and epistemic.

Institutionally, enforcement may be centralised, with primary responsibility vested in an EU authority; decentralised, relying on national authorities coordinated through cooperation mechanisms; or hybrid, dividing responsibilities based on the nature or size of the regulated entity. The example of centralised enforcement is the DMA, which “sole enforcer”⁵⁰ is the Commission. While it includes provisions foreseeing a certain role for the national authorities,⁵¹ the Commission exercises control over the enforcement activities undertaken on the basis of the DMA's provisions. Next, the enforcement may be decentralised, meaning that it is assigned to the authorities operating at the level of the Member States. Such a solution has been adopted under the GDPR and in the Data Act. While under the GDPR there are mechanisms facilitating and necessitating cooperation and consistency between the national authorities,⁵² they are supplementary to the enforcement being placed on the level of the Member States and their main role is to

⁴⁵ See “However, to integrate the national expertise in the platform economy, the initiative envisages that the Commission consults before taking certain decisions (e.g., on non-compliance; fines) a committee composed of representatives of Member States.” – Commission (n 35).

⁴⁶ “The current proposal minimises the detrimental structural effects of unfair practices *ex ante*, without limiting the ability to intervene *ex post* under EU and national competition rules.” – *ibid*.

⁴⁷ “Among those who formulated their opinion on the enforcement models, more than 50%, especially from the business associations, were in favour of a combination of an *ex-ante* risk self-assessment and an *ex-post* enforcement for high-risk AI systems.” – Commission, “Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts” COM/2021/206 final.

⁴⁸ See Commission (n 31).

⁴⁹ See Commission (n 36).

⁵⁰ See DMA (n 6) Art 38(7).

⁵¹ See, e.g., DMA (n 6) Art 38. For the analysis of the DMA's enforcement design, especially the balance between the role of the Commission and the role of national authorities, see A Ribera Martínez, “The Decentralisation of the DMA's Enforcement System” (2024) 73(12) GRUR International 1111 and I Maher, “Regulatory Design in the EU Digital Markets Act: No Solo Run for the European Commission” (2024) 12(2) Journal of Antitrust Enforcement 273.

⁵² See, e.g., GDPR (n 9) Chapter VII – on cooperation and consistency.

indicate the authority responsible for handling the given case. Additionally, there is a hybrid model, where the enforcement is assigned either to the EU or to the Member State level, depending, e.g., on the types of the companies. This is the case of the DSA, where the Commission is responsible for the enforcement against Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs),⁵³ while the national authorities for the enforcement concerning other companies.⁵⁴

Procedurally, enforcement models vary according to who may initiate proceedings (public, private or hybrid systems) and whether obligations operate *ex ante* (compliance-oriented, preventive monitoring) or *ex post* (reactive intervention after infringement). With regard to the criterion of who is empowered to initiate enforcement action, in the public enforcement, it is the authority that may initiate the enforcement activity, while in the private enforcement, it is the individuals. A hybrid system described the situation in which an individual appeals the decision concerning, e.g., the initiation of the proceeding issued by the public enforcer.⁵⁵ Most of the scrutinised enforcement architectures include – in the EU regulatory frameworks governing them – the elements concerning both of these systems, however often one of them is dominant. For example, under the DMA the public enforcement is dominant, while under the GDPR the area in which both public and hybrid enforcement is present. With respect to the *ex ante* and *ex post* nature of the enforcement, most digital acts combine elements of both: the DMA and DSA impose significant *ex ante* duties but retain *ex post* corrective mechanisms; the GDPR is predominantly *ex post* with selective *ex ante* tools such as data protection impact assessments.⁵⁶

Epistemically, all acts formally require that authorities possess adequate technical, financial and human resources, yet few establish clear benchmarks for measuring adequacy or mechanisms for mutualising technical capacity. Consequently, formal obligations do not always translate into uniform enforcement practice. Hence, in the following section, we also provide certain insights concerning the practice of the enforcement.

Table 2 summarises the enforcement design features of the selected regimes. This bird's-eye perspective is complemented, in Section IV, by a closer examination of specific mechanisms that may inspire the design of the DFA's enforcement architecture.

IV. Lessons for the DFA's enforcement design

Having identified in the previous sections the structural and operational weaknesses that hinder effective enforcement in the digital sphere, the analysis now turns to the institutional and procedural responses already developed within EU law. Section II, together with the synthesis presented in Table 1, showed that the enforcement deficit identified in the Digital Fairness Fitness Check reflects systemic features of the Union's multi-level governance rather than isolated gaps in substantive law. Addressing these weaknesses requires examining the enforcement architectures through which existing EU instruments allocate competences, coordinate authorities, structure investigative powers, organise sanctioning mechanisms and deploy digital-monitoring capacities.

⁵³ See DSA (n 5) Chapter IV, Section IV.

⁵⁴ See DSA (n 5) Chapter IV, Section V.

⁵⁵ Hybrid enforcement describes the situation of the proceeding where an individual takes court action against the administrative decision of the given authority – see J-U Franck, “Private Enforcement versus Public Enforcement” in F Hofmann and F Kurz (eds), *Law of Remedies: A European Perspective* (Cambridge 2019), pp 107–32 at 108.

⁵⁶ See GDPR (n 9) Art 36.

Table 2. Comparison of the enforcement design of the EU legal acts which have impact on the protection of consumer rights in digital sphere.

Aspects of enforcement design	Institutional	Procedural		Epistemic
Observed approaches	Centralised/hybrid/decentralised	Public/hybrid/private	Ex ante/ex post	Access to resources
<i>Regulation</i>				
<i>Data Act</i>	Mostly Member State level (decentralised)	Both public and private	ex post	“sufficient human and technical resources and relevant expertise to effectively carry out their tasks” (Art. 37(9))
<i>GDPR</i>	Mostly Member State level (decentralised), cooperation via European Data Protection Board and procedural measures	Depending on the Member State, both public and hybrid (private claims against public enforcement)	Mostly ex post, with certain ex ante elements (e.g., DPIA)	“human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers” (Art. 52(4))
<i>DSA</i>	Both EU and Member State level (hybrid), with EU level for VLOSEs and VLOPs (decentralised), coordination via European Board for Digital Services and procedural measures	Mostly public, with elaborate elements on private	Both ex ante and ex post (emphasis on compliance)	“All necessary resources to carry out their tasks, including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence” (Art. 50(1))
<i>DMA</i>	Mostly EU level (centralised)	Mostly public, with scarce provisions on private	Mostly ex ante (emphasis on compliance), with strong presence of ex post measures	“adequate human, financial and technical resources should be allocated to the Commission” (Rec 106)
<i>AI Act</i>	Mostly Member State level (decentralised), with EU level for general purpose AI systems (centralised)	Mostly public, with limited elements of private	Mostly ex ante (emphasis on compliance), with strong presence of ex post measures	“national competent authorities are provided with adequate technical, financial and human resources, and with infrastructure to fulfil their tasks effectively under this Regulation” (Art. 70(3))

Table 3. Categorisation of challenges to enforcement of DFA with respective potential solutions.

Specific challenges indicated in Digital Fairness Fitness Check	Categories of challenges	Potential solutions
Cross-border practices and fragmented action Regulatory fragmentation across regimes (DSA/DMA/GDPR vs consumer law) Uncoordinated and insufficient sanctions Under-enforcement of unfair terms and collective-redress frictions	Institutional fragmentation	Supporting more centralised enforcement Strengthening cooperation and coordination at the level of EU bodies Strengthening civil society within both public and private enforcement
Lengthy and cumbersome proceedings Data asymmetries and evidentiary burdens Evidence and monitoring gaps	Procedural fragmentation	Cooperation procedures, including concerning evidence sharing among enforcers <i>Ex ante</i> obligations Deadlines
Insufficient expertise and administrative capacity Absence or uneven uptake of digital enforcement tools	Epistemic fragmentation	Supporting more centralised enforcement <i>Ex ante</i> obligations Sharing new tools among enforcers
Traders established outside the EU	Substantive rules versus enforcement	To a certain extent: supporting more centralised enforcement

A comparative assessment of the GDPR, the DSA, the DMA, the Data Act and the AI Act allows us to identify which design elements mitigate – and which reproduce – the challenges diagnosed earlier. Rather than analysing these regimes in isolation, the discussion groups the Digital Fairness Fitness Check's findings into three categories corresponding to the triad developed in this article: institutional fragmentation, procedural shortcomings, and epistemic asymmetries. The solutions proposed below draw on the experience accumulated under these instruments and on the structural choices reflected in their enforcement systems.

In line with the diagnosis set out above, we do not treat enforcement against non-EU traders as a separate category. Its resolution depends primarily on substantive scope rules rather than enforcement architecture. Nevertheless, some of the solutions identified below – particularly those relating to centralisation and to the development of shared technical tools – also contribute to addressing this challenge.

Table 3 summarises the categorisation of enforcement challenges derived from the Digital Fairness Fitness Check and links them to the design approaches discussed in this section.

1. Addressing institutional fragmentation

The three solutions discussed in this subsection are to a large extent in line with the notion of polycentric enforcement: they suggest adoption of the measures which would support coordination of the enforcement of the DFA between the EU and the national level by learning from the experience gained in the context of the adoption and the enforcement of other legal acts. The experimentalists governance perspective, on the other hand, inspired the suggestion of the inclusion of the expert bodies and civil society as a form of participatory enforcement.

a. Shifting the balance towards selective centralisation

Institutional fragmentation often arises where enforcement is dispersed across numerous national authorities with divergent capacities, priorities and procedural frameworks.

Experience under the GDPR illustrates these difficulties particularly clearly: decentralisation has contributed to inconsistent outcomes, protracted proceedings and uneven levels of regulatory scrutiny.⁵⁷ In this respect, the enforcement designs of the DMA and the DSA provide valuable guidance. Both instruments employ quantitative and structural criteria – such as the size, reach and systemic relevance of regulated entities – to determine whether responsibility lies with the Commission or with national authorities.

Adopting a similar logic for the DFA would allow enforcement to be allocated more coherently across levels of governance. Centralising responsibility for categories of traders whose activities pose cross-border or systemic risks could enhance consistency, reduce inter-authority coordination burdens, and limit the institutional fragmentation identified in the Digital Fairness Fitness Check. At the same time, a selective centralisation model preserves decentralised enforcement for less complex or purely domestic cases, thereby maintaining proximity while ensuring that the most resource-intensive and far-reaching cases are handled at the EU level. Such an approach would also facilitate more coherent sanctioning practice and strengthen the coordination of enforcement actions across digital-market regimes.⁵⁸

b. Enhancing coordination mechanisms at the EU level

A second avenue for addressing institutional fragmentation is to strengthen the coordination mechanisms operating at EU level. The DFA's enforcement design should therefore include structures that facilitate the organisation and supervision of Member State enforcement efforts, ensuring more consistent approaches across jurisdictions. Endowing EU bodies with clearer coordinating competences would also help mitigate gaps in oversight and reduce the risks that arise when complex digital-market cases are managed in isolation by individual national authorities.⁵⁹

At the same time, recent regulatory developments illustrate the challenge posed by the proliferation of EU bodies involved in digital governance. The creation of multiple advisory or oversight structures risks generating further fragmentation rather than resolving it. For this reason, it would be advisable for the DFA to build on existing networks rather than introduce new institutional layers. Established bodies – such as the AI Board and the Panel of Independent Experts under the AI Act, or the European Data Innovation Board created under the Data Governance Act and included also in the Data Act's enforcement design⁶⁰ – already provide forums in which regulators, civil-society actors, industry representatives and scientific experts engage in ongoing coordination. Leveraging these bodies, rather than duplicating them, would enable the DFA to improve coherence while avoiding unnecessary institutional complexity.

c. Expanding the role of civil society in enforcement

A further dimension of institutional fragmentation concerns the limited role currently played by civil-society actors in the enforcement of digital-market rules. The difficulties

⁵⁷ Especially with regard to the cross-border practices – for the crucial work on this topic, see G Gentile and O Lynskey, “Deficient by Design? The Transnational Enforcement of the GDPR” (2022) 71(4) *International and Comparative Law Quarterly* 799 and for the arguments for the necessity of centralisation, see F Brito Bastos, and P Palka, “Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?” (2023) 19(3) *European Constitutional Law Review* 487.

⁵⁸ For work analysing the trend of the enforcement moving to Brussels, see M Scholten, “Mind the Trend! Enforcement of EU Law Has Been Moving to ‘Brussels’” (2017) 24(9) *Journal of European Public Policy* 1348.

⁵⁹ See Bruegel Dataset (n 27).

⁶⁰ See Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.

highlighted in the Digital Fairness Fitness Check regarding unfair contract terms and collective-redress mechanisms illustrate how reliance on public enforcement alone may leave certain systemic infringements insufficiently addressed. Extending the scope of the Representative Actions Directive to the DFA would therefore be a natural first step. Yet the experience of data protection law⁶¹ shows that civil-society organisations have also proved essential in identifying harmful practices, mobilising dispersed consumer interests and initiating high-impact litigation.

Strengthening the role of such organisations – both within formal representative actions and through complementary enforcement channels – could compensate for capacity constraints among public authorities and contribute to a more balanced enforcement ecosystem. Their participation should, however, complement rather than substitute public enforcement. Embedding civil-society involvement within the DFA's enforcement design, including through advisory and consultative mechanisms similar to those developed for example under the AI Act, would enhance transparency, broaden the informational base available to enforcers, and support consistent oversight of digital markets across the EU.

2. Addressing procedural fragmentation

Procedural shortcomings – manifested in lengthy proceedings, fragmented cooperation among authorities, and evidentiary asymmetries – emerged in the Digital Fairness Fitness Check as one of the most significant obstacles to timely and effective enforcement in the digital sphere. The enforcement practice under the GDPR, the DSA, and the DMA suggests that the DFA should not rely exclusively on *ex post* intervention after harm has occurred, but should instead embed strong *ex ante* compliance mechanisms, which is also in line with the responsive regulation approach, and clear procedural coordination rules, inspired by polycentric governance perspective. Procedural innovation is essential to ensure predictable and efficient outcomes across the EU.

a. Embedding strong *ex ante* obligations

The evolution of EU digital regulation over the decade reflects a progressive shift from *ex post* enforcement toward continuous compliance monitoring. Instruments such as the DMA and the DSA are explicitly premised on proactive obligations – risk assessments, transparency reports, algorithmic documentation – that enable enforcers to intervene before consumer harm materialises.⁶² Likewise, the GDPR's concept of “data protection by design and by default” anchors a preventive logic that has shaped compliance cultures in significant ways.⁶³ The AI Act reinforces this trajectory through mandatory conformity assessments and extensive technical documentation requirements.

Building on these models, the DFA could embed a “fairness by design” principle, requiring traders to document how their interfaces, ranking systems or personalisation mechanisms comply with consumer-law standards.⁶⁴ Such *ex ante* duties would mitigate information asymmetries, facilitate early detection of problematic design features and reduce the investigative burden placed on authorities during *ex post*

⁶¹ See V Golunova and M Eliantonio, “Civil Society Actors as Enforcers of the GDPR: What Role for the CJEU?” (2024) 15(2) JIPITEC 180.

⁶² See P Larouche and A de Streel, “The European Digital Markets Act: A Revolution Grounded on Traditions” (2021) 12 JECL & P 542; OECD, “Ex Ante Regulation and Competition in Digital Markets” (2021) OECD Roundtables on Competition Policy Papers No. 272, <<https://doi.org/10.1787/c83e178d-en>> (last accessed 2 February 2026).

⁶³ See L A Bygrave, “Data Protection by Design and by Default” in S Garben and L Gormley (eds), *The Oxford Encyclopedia of EU Law* (Oxford University Press 2023).

⁶⁴ See K Yeung, “Algorithmic Regulation: A Critical Interrogation” (2018) 12(4) Regulation & Governance 505.

enforcement.⁶⁵ By integrating preventive obligations into traders' internal compliance systems, the DFA would help rebalance enforcement away from reactive interventions and towards anticipatory oversight – thereby addressing one of the principal sources of procedural delay identified in the Digital Fairness Fitness Check.

b. Establishing clear and swift cooperation procedures

The experience of the CPC Network, discussed in Digital Fairness Fitness Check, and, more recently, of the GDPR's cooperation and consistency mechanism shows that the absence of clear procedural rules leads to divergent timelines and inconsistent results, as demonstrated by well-known delays in cross-border GDPR cases. Where such rules are absent or insufficiently developed, cross-border cases tend to suffer from duplication of effort, gaps in information flows and prolonged deliberation among authorities.

For the DFA, cooperation mechanisms should therefore include structured procedural templates for coordinated investigations; secure digital platforms for real-time information exchange; mandatory time limits for contributions among authorities; joint investigative teams for complex or systemic infringements; shared technical evidence infrastructures, such as EU-level repositories or "evidence pools." Evidence sharing is particularly crucial in cases involving algorithmic systems, where no single authority possesses all the relevant data or expertise.⁶⁶ Coordinated access to technical information would accelerate enforcement, reduce duplicative requests and support more consistent decision-making across the Union.

c. Introducing procedural deadlines

The experience with the GDPR's decentralised enforcement – largely left to the discretion of the Member States – demonstrates that, particularly in cross-border cases involving numerous data subjects, more specific procedural rules are necessary. One of such essential procedural elements concerns the introduction of defined timeframes, whose absence has proved to be a major systemic weakness in the enforcement of the GDPR. The significance of this issue is highlighted in the *Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules for the enforcement of Regulation (EU) 2016/679*. The proposal acknowledges that, given the varying complexity of investigations and the discretion of data protection authorities (DPAs) to pursue infringements, it is neither feasible nor desirable to prescribe deadlines for every procedural stage. Nonetheless, it emphasises that imposing deadlines where appropriate would help prevent undue delays in the completion of cases.⁶⁷

The DFA should follow the same logic by establishing, at least, indicative timeframes for key procedural stages such as the initiation of investigations, coordination exchanges among competent authorities, and the adoption of final measures. It should also empower the Commission to adopt implementing acts setting procedural templates to ensure uniform application. Predictable timelines would enhance legal certainty for both traders and enforcement bodies. They would also function as an institutional safeguard against procedural drift in complex cross-border cases.

⁶⁵ See L Edwards and M Veale, "Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For" (2017) 16 Duke Law & Technology Review 18.

⁶⁶ See Yeung (n 63).

⁶⁷ See Commission (n 31) that reads: "In light of the varying complexity of investigations and the discretion of DPAs to investigate infringements of the GDPR, it is not desirable to prescribe deadlines for every stage of the procedure. However, the imposition of deadlines where appropriate will help prevent undue delay in the completion of cases."

3. Addressing epistemic fragmentation

Epistemic asymmetries – manifested in uneven expertise, limited technological capacity, and restricted access to data – constitute the third pillar of the enforcement deficit identified in the Digital Fairness Fitness Check. Enforcement in digital markets requires not only legal authority but also the ability to understand, audit and interrogate complex socio-technical systems. The DFA will therefore achieve its objectives only if enforcement bodies are equipped with the analytical capabilities necessary to supervise digital actors effectively. Existing EU instruments offer several approaches to addressing these epistemic constraints and suggest introduction of innovative solutions, including some inspired by experimentalist governance perspective (e.g., shared technical tools to be used by the enforcers).

a. Leveraging *ex ante* obligations to rebalance epistemic capacity

Beyond their procedural dimension, *ex ante* duties can also function as resource-equalising mechanisms. By imposing disclosure, documentation, and auditing requirements on traders, the DFA can shift part of the investigative burden from public authorities to the regulated entities themselves. This approach mirrors the accountability principle under the GDPR and the AI Act's requirement for providers to compile and maintain technical documentation, conduct conformity assessments and conduct post-market monitoring.

Adapting this logic to consumer-facing digital fairness, the DFA could require traders to perform periodic assessments of interface design, personalisation systems, and ranking architectures, and to maintain and submit technical documentation evidencing compliance. Such obligations would mitigate informational asymmetries, alleviate pressure on public investigators, and enable earlier detection of potential infringements. To ensure proportionality, these duties could be calibrated according to company size or systemic relevance. Ultimately, *ex ante* transparency obligations serve a dual function: they embed fairness considerations into product design and enhance the epistemic position of enforcement authorities.

b. Leveraging selective centralisation to pool expertise

Where epistemic asymmetries stem from significant disparities in national enforcement capacity, selective centralisation can serve as an important corrective. Experience under the GDPR illustrates the magnitude of these discrepancies: according to a 2023 European Data Protection Board publication, only a minority of data-protection authorities reported sufficient technical resources, and even fewer considered their human, financial and technical capacities to be adequate across all categories.⁶⁸ This unevenness weakens enforcement and exacerbates the informational imbalance between regulators and sophisticated digital operators.

While centralisation cannot entirely eliminate resource disparities, concentrating responsibility for systemically significant or cross-border cases at EU level can mitigate them by pooling expertise, enabling economies of scale, and promoting more balanced enforcement outcomes across the Union. Drawing on the DMA and DSA models, the DFA could allocate the most complex or high-impact digital fairness cases to an EU-level enforcer, while leaving routine or purely domestic matters with national authorities. Such selective centralisation would enhance analytical capacity where it is most needed, without undermining the benefits of decentralised supervision for localised or lower-risk cases.

⁶⁸ See EDPB, "Contribution of the EDPB to the report on the application of the GDPR under Article 97. Adopted on 12 December 2023" 33, <https://www.edpb.europa.eu/system/files/2023-12/edpb_contributiongdprevaluation_20231212_en.pdf> (last accessed 2 February 2026).

c. Leveraging shared technical tools to enhance enforcement capacity

A complementary means of addressing epistemic asymmetries is the shared development and dissemination of technical tools among enforcement authorities. Under the GDPR, national data-protection authorities increasingly rely on technologies developed by their counterparts, ranging from forensic utilities to automated audit scripts.⁶⁹ Similar practices have emerged in competition and consumer law, where digital-market analysis tools, crawling technologies and screening algorithms are deployed across agencies.

The DFA could build on these experiences by promoting the creation of common enforcement-technology infrastructures (EnfTech), such as automated crawlers, interface-analysis tools, algorithmic inspection systems, and shared data-access repositories. Making such tools available across Member States would enhance investigative capacity, facilitate consistent supervision, and reduce dependence on ad hoc national solutions. Coordinated investment in shared technical infrastructure would thus complement the institutional and procedural reforms discussed above and strengthen the overall epistemic foundation of DFA enforcement.

4. Addressing the substantive–enforcement interface

A final set of challenges concerns the enforcement of obligations directed at traders established outside the EU. As noted in the Digital Fairness Fitness Check, the difficulty in securing compliance or collecting fines from non-EU traders stems primarily from substantive scope rules – jurisdictional reach, representative requirements, and the legal architecture governing access to EU markets – rather than from shortcomings in enforcement design alone. For this reason, the issue is not treated here as a distinct category of fragmentation.

Nevertheless, certain enforcement-design measures can complement substantive solutions and strengthen oversight in this area. The DSA provides a notable example: its trader-traceability obligations and requirement that non-EU providers appoint an EU representative enhance authorities' ability to identify, contact, and supervise providers operating from outside the Union. Similarly, improvements in investigative capacity – such as enhanced monitoring tools, algorithmic detection techniques and stronger cooperation mechanisms with platforms hosting third-country traders – can support enforcement by increasing the visibility of non-compliant actors.

Ultimately, however, the most effective responses to this challenge lie in defining the material and territorial scope of the DFA itself. Enforcement design can assist at the margins – particularly through selective centralisation and shared technical infrastructures – but cannot by itself overcome the jurisdictional limits highlighted in the Digital Fairness Fitness Check. For this reason, the principal lessons developed in this section focus on institutional, procedural, and epistemic reforms, while recognising that substantive scope choices will determine the outer boundaries of the DFA's enforcement reach.

Taken together, the institutional, procedural and epistemic reforms outlined in this section suggest that the DFA must transform digital fairness from a declaratory aspiration into a practical enforcement paradigm. Drawing on the experience of the GDPR, the DSA, the DMA, the Data Act and the AI Act, an effective enforcement framework will require a structured allocation of competences, robust cooperation mechanisms, minimum investigative and sanctioning standards, and a data-driven oversight model capable of supporting continuous monitoring. Although each of these instruments faces challenges of

⁶⁹ For example, the Latvian DPA has on its website a link to the Spanish DPAs' data protection impact assessment tool, see Datu valsts inspekcija, "Rīks datu apstrādes reģistra un risku analīzei," <<https://www.dvi.gov.lv/lv/riks-datu-apstrades-registra-un-risku-analizei>> (last accessed 2 February 2026).

its own, they nevertheless offer valuable guidance for addressing the institutional fragmentation, procedural shortcomings and epistemic asymmetries identified in the Digital Fairness Fitness Check. These insights provide the foundation for the enforcement-design principles summarised in the conclusion.

V. Conclusions

The analysis undertaken in this article has proceeded through three stages: diagnostic, comparative and prescriptive. The diagnostic inquiry, developed in Section II, reconstructed the enforcement challenges identified by the European Commission in the Digital Fairness Fitness Check and showed that they crystallise around a triad of institutional, procedural and epistemic fragmentation. These three dimensions reinforce one another, weakening both the coherence and effectiveness of consumer-law enforcement in the digital environment.

Using this triad as an analytical frame, Section III examined a selection of existing EU digital instruments – the GDPR, the DSA, the DMA, the Data Act, and the AI Act – in order to identify the considerations that informed their enforcement design and the structural choices they embody. This comparative exercise revealed recurring questions that any enforcement architecture must confront: the degree of centralisation appropriate for systemic or cross-border cases; the relationship between public and private enforcement; the balance between *ex ante* and *ex post* approaches; and the definition and provision of the resources and technical capacities required for effective supervision.

Building on these insights, Section IV developed a series of prescriptive suggestions for the DFA. The analysis argued that the forthcoming framework would benefit from a more structured allocation of competences, enhanced coordination among EU and national bodies, and a meaningful role for civil society in identifying and pursuing systemic infringements. Procedurally, it emphasised the value of embedding *ex ante* obligations, clarifying cooperation procedures and introducing indicative deadlines to avoid the procedural drift observed under existing instruments. Epistemically, it stressed the need to rebalance informational and technical capacities, whether through selective centralisation, transparency and documentation duties imposed on traders, or the sharing of common enforcement technologies among authorities.

Taken together, these proposals point towards an enforcement architecture that is more resilient, coherent and technologically responsive.⁷⁰ The experience of other EU digital regimes suggests that such reforms can significantly reduce institutional fragmentation, accelerate decision-making and mitigate epistemic asymmetries. If designed with these considerations in mind, the DFA has the potential to deliver effective digital fairness in practice and to strengthen the EU's broader digital governance framework.

Funding statement. This research is supported by the research grant of the National Science Centre, Poland (grant number 2024/53/B/HS5/00169).

⁷⁰ For a theoretical framework framing the meaning of “responsive” in this context, see J Black and R Baldwin, “Really Responsive Regulation” (2008) 71(1) *Modern Law Review* 59.