Common Market Law Review **63**: 153–166, 2026.

STANDING UP FOR THE EUROPEAN DIGITAL CONSTITUTION

ANASTASIA ILIOPOULOU-PENOT*

Abstract

This contribution takes a stand against the growing narrative that the EU's digital rulebook, currently under both external and internal pressure, acts as a hindrance to the EU's innovation capacity and geopolitical relevance. It argues that, on the contrary, this regulatory framework is a vital asset, closely tied to the EU's broader goals and missions, and to its distinctive mix of values. If properly implemented and enforced, the EU's digital rules can enable the EU to defend its liberal democratic order in the algorithmic age, by safeguarding its essential institutions: free markets; the integrity of public discourse; and individual and collective agency. As such, the digital rulebook carries a distinctly constitutional dimension that must be upheld and promoted.

1. The EU's digital rulebook in times of pressure

In recent years, the EU has adopted a number of flagship legislative instruments to regulate the digital realm. Heavily lobbied, bearing evocative names and known well beyond legal circles, the General Data Protection Regulation (GDPR),[1] the Digital Services Act (DSA),[2] the Digital Markets Act (DMA)[3] and the Artificial Intelligence Act (AIA)[4] form the centre of the European

* Professor of European Law, Centre for European Law, University Paris Panthéon-Assas.

1. 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 L 119, 1–88.

2. 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 L 277, 1–102.

3. Regulation 2022/1925 of the European Parliament and the 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 L 265, 1–66.

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 L 2024/1689, 1–144.

regulatory universe. Other sector-specific laws, such as the European Media Freedom Act[5] and the Regulation on the transparency and targeting of political advertising,[6] gravitate around these key horizontal frameworks, complementing and expanding their scope. The surge in law-making has given rise to a multi-layered and ever-evolving system of governance that recognizes that digital and AI technologies and the companies behind them pose a wide array of challenges that cannot be tackled solely through traditional competition law and consumer protection measures.

While celebrated as Europe's contribution to tech governance and a source of inspiration for global standards, the EU's digital regulation has quickly come under fire both externally and internally. The US has led the charge, casting the first and most forceful stone. While criticisms of the EU's so-called digital protectionism, discriminating against American tech giants, had already been voiced under the Obama and Biden administrations, the second Trump era has crossed a line in both tone and substance. EU regulations are increasingly portrayed in the discourse of federal authorities and high-ranking US officials, including President Trump himself, as protectionist tariffs in disguise or forms of economic extortion targeting American innovation, as well as tools of censorship threatening global free speech. These criticisms have been accompanied by threats of trade retaliation and even suggestions of withdrawing America's security umbrella at a time when Russia's military aggression has reignited war to the European continent. They have also been echoed in the statements and attitudes of tech executives, who increasingly behave like oligarchs and seek to undermine the application of European laws to their companies.

Alongside external attacks, EU digital regulation is facing growing pressure from within Europe, with industry stakeholders leading the push-back, notably against the implementation of the AIA. Internal critique has gained momentum in the wake of Mario Draghi's call for enhanced European competitiveness, with his high-profile report noting, particularly with reference to the GDPR and the AIA, that 'the EU's regulatory stance towards tech companies hampers innovation'.[7] The Commission swiftly responded with the announcement of a Competitiveness Compass[8] and

5. 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) [2024] OJ L 2024/1083, 1–37.

6. Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, 1–44.

7. Mario Draghi, 'The Future of European Competitiveness', September 2024, 30 <commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059> (all websites last visited 13 November 2025).

8. European Commission, Communication on a Competitiveness Compass for the EU, COM (2025) 30 final, <eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0030>.

omnibus packages aimed at reducing regulatory hurdles for companies. Since then, calls for a legislative pause and for the simplification of the existing digital *acquis* have multiplied. Beneath these demands, however, lies the siren song of deregulation tempting EU actors.

The dangers posed by both inside and outside pressures are already becoming apparent. These dangers stem from the fact that the Commission, central to the implementation and enforcement of the EU's digital rules, is also a key *political* actor within the EU's architecture. As such, its decisions in the digital domain may be influenced by its explicitly assumed geopolitical character and by the need to navigate competing priorities and tensions across other policy areas (especially trade and security). This dynamic can lead to existing enforcement actions against major US companies losing vigour or being delayed, and to new ones not seeing the light of day. It can also entail the deliberate slowing of implementation of certain rules, notably of the AIA, disturbing legal certainty and compliance efforts by firms. Meanwhile, ongoing and forthcoming efforts to review the legislative framework (especially the GDPR and the AIA), though potentially beneficial in some respects, risk unravelling hard-won achievements and diluting the EU's regulatory ambition.

At this watershed moment, it is of vital importance to return to first principles and reflect on what is truly at stake. This brief contribution takes a stand against the growing narrative that the digital rulebook is a hindrance to the EU's innovation capacity and geopolitical standing. It argues that this rulebook is, in fact, an essential resource deeply connected to the EU's broader goals and missions. Its legal and jurisprudential moorings lie in the heritage of internal market and competition law, as well as in the protection of fundamental rights, all of which have been central to the success of European integration. If properly implemented and enforced, this regulatory framework can offer the EU long-term advantages in the global race to shape digital and AI environments. In short, the contribution argues that the set of digital rules is a strategic asset enabling the EU to defend its liberal democratic order in the algorithmic age. As such, it carries a distinctly constitutional dimension that must be upheld and promoted.

2. Understanding the European Digital Constitution: Key traits

Beneath its lengthy, complex and technical façade, the EU's digital regulatory framework reveals the foundations of what can be described as a European Digital Constitution,[9] which seeks to place limits on the

9. See Anastasia Iliopoulou-Penot, 'La Constitution numérique européenne' (2023) Revue Française de Droit Administratif 945.

unprecedented forms of power stemming from the development and use of digital and AI technologies and to safeguard fundamental rights in the face of such multi-faceted power.[10] First, the EU's digital ruleset establishes *mechanisms* designed to serve as checks and balances on the activities of tech corporations that act as gatekeepers of markets, public communications and fundamental rights. These mechanisms seek to prevent and mitigate the economic and societal harms their business models cause while building knowledge on them. Risk management tools and compliance techniques, alongside the creation of new rights for users, are deployed to reduce power and information asymmetries and to reinforce the resilience of society. Second, the core digital laws give tangible expression to structural *principles* such as transparency, accountability, competition, fairness and due process. These principles, which have proven effective in democratic public governance, can also serve as key building blocks for responsible tech governance and for the ordering of online spaces. Third, the EU's digital legislation articulates laudable *objectives*, widely shared by Europeans, such as fostering a 'safe, predictable and trusted online environment',[11] ensuring 'contestable and fair markets in the digital sector'[12] and promoting 'the uptake of human-centric and trustworthy artificial intelligence'.[13] Its goals further include supporting innovation,[14] which is to be assessed in terms of its impact on consumers and society at large, and the diversity of which must be preserved. In other words, innovation is not understood as any technological development imposed by oligopolies, to which society has to automatically adapt, but as advancement that is ethical, safe, responsible and rights-protecting. Finally, the core digital laws aim to contribute to the proper functioning of the internal market, which serves as a pillar of European sovereignty and a source of leverage against American and Chinese tech giants.

These core *mechanisms*, organizing *principles* and overarching *objectives* embody a balance of rights and interests reflecting a distinctly European vision of societal life, rooted in the *acquis* of the European Convention on Human Rights, as it has evolved within the EU framework. They give concrete expression to a unique equilibrium of *values* that lies at the heart of European identity and that the EU seeks to embed in the digital sphere. The

10. Giovanni De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society* (CUP 2021); Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?* (Hart Publishing 2021).
11. Art 1 DSA.
12. Art 1 DMA.
13. Art 1 AIA.
14. Art 1 DSA, Art 1 AIA and Recital 107 DMA.

GDPR, for instance, puts flesh on the bones of the fundamental right to personal data protection and reflects a particular conception of privacy, also strongly defended in the case law of the Court of Justice,[15] starting with the consecration of the right to be forgotten, which empowers individuals in relation to operators of online search engines.[16] A similar concern for respect for privacy and also for human dignity, grounded in European tradition, is reflected in the AIA. As for the DSA, its content moderation and risk management frameworks seek to prevent platform censorship and to preserve a diverse information environment; in doing so, the DSA enables and promotes free expression as Europeans conceive it.[17] More broadly, the entire digital legal framework is geared toward ensuring a high level of protection for the fundamental rights enshrined in the Charter, itself a prominent embodiment of European values. Interestingly, while digital technologies disrupt territoriality, EU legislation regulating them actively contributes to shaping a *territory of the EU*, understood 'as a legal place underpinned by common values; and as a place where the EU legal order is engaged to protect Union citizens'.[18] This conception of EU territory also underpins the seminal judgments in *Schrems*[19] on transatlantic data transfers, which establish red lines for cooperation with third countries whose approaches to privacy diverge substantially from European standards.

The emerging digital constitutional order is expressive and aspirational. It embodies the European belief in the necessity of public intervention to shape and steer technological development towards human flourishing. It makes statements regarding the proper uses of technology and the boundaries that must not be crossed. It signals an enduring faith in the law's ability to instil discipline in (digital) markets, ensuring they remain truly competitive, and to uphold the conditions for a vigorous (online) public sphere. It carries significant messages about the kind of economic and communicational spaces Europeans aspire to and about the conduct of the actors within them (both users and service providers). In particular, there is a clear expectation that large-scale companies will reduce the market and societal

15. Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25 ELJ 140, doi: 10.1111/eulj.12316.

16. Case C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, EU:C:2014:317.

17. See the contribution of Douglas-Scott in this issue.

18. Niamh Nic Shuibhne, 'The "Territory of the Union" in EU Citizenship Law: Charting a Route from Parallel to Integrated Narratives' (2019) 38 YEL 267 at 270, doi: 10.1093/yel/yez006.

19. Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, EU:C:2015:650 (*Schrems I*); Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, EU:C:2020:559 (*Schrems II*). A light-touch review of the equivalence of protection is provided in Case T-553/23, *Latombe v Commission*, EU:T:2025:831.

externalities of their business models and align their actions, so far driven by profit maximization and ideological agendas, with basic principles of public interest. These companies are also expected to disclose meaningful information about their rules and processes enabling regulators, researchers and society at large to build knowledge and foster resilience.

The so-called 'European way',[20] translated in the digital Constitution and proposing a publicly regulated, value-laden and rights-based digital order, offers a valid and credible alternative to both the Chinese model of State control and the American *laissez faire* approach towards the corporations that command technological progress and market dynamics.[21] Digital platforms and AI systems have become critical socio-technical infrastructures. Like telecommunications, transport and energy utilities, banks and defence industries, their development should operate under both corporate governance and a public regulatory framework. Indeed, the regulatory faith placed by the US in the major tech corporations has shown its limits, especially as their voluntary commitments grow fewer and less credible. This proves that respect for fundamental rights, democracy and the rule of law cannot be sufficiently ensured by soft-law instruments alone but requires hard-law obligations. In this context, the absence of US federal legislation on issues that enjoy bipartisan and public support, such as online child safety or platform transparency, stands in stark contrast to the European *acquis*, which reflects the growing 'techlash' in public opinion. The very existence of a *binding* framework that constrains Big Tech, despite its shortcomings, represents a significant achievement in itself. Ultimately, its purpose is to preserve liberal democracy in Europe and the collective autonomy that sustains it by protecting its foundational institutions: free and competitive markets; the integrity of public sphere and democratic discourse; agency as an individual and collective good.

First, in line with the EU's ordoliberal tradition, which emphasizes the nexus between competition and democracy, the digital Constitution seeks to liberate markets from the hegemony of a few large corporations, whose influence produces far-reaching effects that extend beyond purely economic concerns. A telling illustration of these effects can be found in *Google (Alphabet)*,[22] where the General Court, dealing with Google's self-preferencing

20. European Commission, 'Communication on the 2030 Digital Compass: The European way for the Digital Decade', COM(2021) 118 final; 'European Declaration on Digital Rights and Principles for the Digital Decade, adopted on 15 December 2022 by the European Parliament, the Commission and the Council' <digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>.

21. Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP 2023).

22. Case T-604/18, *Google (Alphabet)*, EU:T:2022:541.

practices as a form of abuse under Article 102 TFEU, lucidly underlines the non-economic, democracy-related interests which are at stake:

> 'Google's abusive practices had the effect, inter alia, of depriving competitors of the possibility of offering, without hindrance, alternatives to the general search service Google Search to those users wishing to use them. Thus, in general terms, those practices were detrimental to the *interest of consumers in having more than one source for obtaining information on the internet.* Accordingly, in more concrete terms, those practices also restricted the development of search services directed at those segments of consumers that attached *particular value to, inter alia, the protection of privacy or specific linguistic features within the EEA.* Such interests were not only consistent with competition on the merits, in that they encouraged innovation for the benefit of consumers, but were also necessary in order to *ensure plurality in a democratic society*'.[23]

While being contrary to anti-trust law, self-preferencing is now also prohibited by the DMA, along with several other practices repeatedly deemed anticompetitive by gatekeeper companies in digital markets. In doing so, the DMA targets core elements of their business models. It is complemented, in this respect, by the DSA's requirements for advertising transparency, recommender systems and platform design. The impact of the DMA and DSA adds to that of competition law, enriched by its interaction with the GDPR, an element which has been highlighted in the ground-breaking judgment in *Meta platforms.*[24] The Court pragmatically affirms that access to and processing of personal data have become 'a significant parameter of competition between undertakings in the digital economy' and that disregarding the reality of this development 'would be liable to undermine the effectiveness of competition law'.[25] The breach of the GDPR can therefore serve as a 'vital clue' in assessing whether a company's conduct has the effect of hindering the maintenance or the growth of competition in a market.[26] It becomes clear then that both competition law, reinforced by the GDPR, and the DMA, complemented by the DSA, aim to tackle the key sources of market power in the digital economy. Together, they seek to curb the dominance of digital oligopolies and dismantle the structures of dependency they create, helping to open up the digital ecosystem to all players. Ensuring

23. ibid, para 1028 (emphasis added).
24. Case C-252/21, *Meta platforms*, EU:C:2023:537.
25. ibid, para 47.
26. ibid, para 40.

a fair chance for all participants is essential for a well-functioning market and for a healthy democracy.

Second, the European Digital Constitution seeks to safeguard the integrity of the public sphere. Democracy requires that citizens form their political preferences through rational, truth-oriented and pluralistic processes that foster informed debate and a willingness to engage in reasonable compromise. These processes are increasingly undermined by social media platforms that have become *de facto* public spaces. These platforms control the flow of information in the attention-based economy, operating under a business model described as surveillance or informational capitalism. To maximize user engagement, they prioritize sensationalist and emotionally charged content, often with little regard for objectivity, rationality or scientific credibility. At the same time, insufficient or irresponsible content moderation practices contribute to the proliferation of hate speech and fake news, polluting the European digital town square. Hate speech distorts and brutalizes public discourse, while silencing historically disempowered and marginalized groups. Disinformation, in turn, undermines sound decision-making and erodes the social trust on which democracy is based. Moreover, social media platforms tend to provide information that aligns with users' interests, views and preferences, while filtering out content deemed irrelevant or contrary to the user's beliefs and affinities. This algorithmic shaping of citizens' convictions and decisions contributes to polarization (and at times radicalization), making compromise extremely hard, while fostering a broader sense that objective truth is elusive or even non-existent. This sense is further reinforced by the proliferation of AI-generated content and the growing reliance on large language models (LLMs) as sources of information. While these developments affect the prerequisites for free and fair elections, more direct forms of interference and manipulation in electoral campaigns have also become increasingly common. The DSA seeks to address these challenges through its risk management framework, while also aiming to curb the spread of hate speech and disinformation by improving the quality of content moderation practices. Its impact can be reinforced through the parallel application of relevant provisions of the AIA, as recommender systems, content moderation tools and online search engines are increasingly powered by AI technologies.

Third, the European Digital Constitution seeks to defend agency, understood as the capacity for free and purposive action. Agency is both intrinsic to human dignity and self-development and foundational to democracy, which relies on the idea that citizens are capable of self-rule. Digital and AI technologies can diminish the sense of agency in several ways, thereby

negatively affecting the quality of social interaction and political participation. Pervasive data collection, profiling, data and AI-driven surveillance create environments where individuals may feel constantly watched. These environments can lead to self-censorship and withdrawal from communication, association and protest, key forms of personal agency. The Court of Justice has recognized this threat. In its case law on (the prohibition of) generalized metadata retention,[27] it highlights how such retention may affect the private life of a large part of the European population, evoke a feeling of constant surveillance and exert chilling effects on the exercise of other freedoms, especially freedom of expression and assembly. The language of the Court has been repeated in Recital 18 of the AIA in order to justify the prohibition of certain uses of biometric identification systems, which was one of the most hotly debated issues in the legislative negotiations. The AIA, alongside the GDPR, addresses another crucial risk to agency: the increasing reliance on algorithmic decision-making and the disempowerment of individuals it entails. Indeed, complex and opaque systems, which operate as black boxes, make it difficult for people to understand how decisions are made or to challenge outcomes that affect their rights and opportunities (for example in credit scoring or recruitment).[28] To counter this, the AIA mandates human oversight of the operation of high-risk AI systems (in several key sectors), while empowering individuals to lodge complaints and to request an explanation of the role AI plays in decisions affecting them. In this way, the AIA pursues the path opened by the GDPR which ensures that individuals affected by automated decisions are able to understand and contest them. Furthermore, the AIA seeks to safeguard agency as the ability to construct one's identity through genuine feedback from the social environment. It then prohibits certain forms of manipulation and requires transparency safeguards for the use of deepfakes. Finally, as previously noted, its provisions are meant to work in tandem with those of the DSA and GDPR, to address risks associated with personalization and micro-targeting techniques, which shape our perception of reality.

3. Navigating troubled waters: Enforcing, streamlining and projecting the Digital Constitution

Societies with strong individual and collective agency, alongside free markets and robust public discourse, are better equipped to respond to crises,

27. See especially Joined Cases C-511, 512 & 520/18, *La Quadrature du Net v Premier ministre and Others*, EU:C:2020:791.

28. Case C-634/21, *SCHUFA Holding*, EU:C:2023:957; Case C-203/22, *CK*, EU:C:2025:117.

resist authoritarianism, and adapt to change. Retreating in any way from the European digital Constitution is therefore not an option, as it would mean forfeiting our democratic future and the very framework within which we live our lives. Instead of watering down digital rules, weakening or delaying their enforcement, the EU's response must be clear: enforce the digital framework effectively and promptly, encouraging interaction between its components; streamline it, where necessary; and promote the 'European way' through digital diplomacy.

The need for strong and timely enforcement is clearly articulated in the order of the Vice-President of the Court of Justice, which rejects Amazon's request to suspend the obligation to make an advertisement repository publicly available (as required by Article 39 of the DSA);[29] the reasoning developed in relation to the DSA can be transposed to the DMA and the AIA. The order emphasizes that the DSA 'is a central element of the policy developed by the EU legislature in the digital sector. In the context of that policy, that regulation pursues objectives of great importance'.[30] It then notes that 'not applying certain obligations laid down by that regulation will lead to a delay, potentially for several years, in the full achievement of those objectives. *Not applying those obligations will therefore give rise to a risk of potentially allowing an online environment which threatens the fundamental rights provided for in the Charter to persist and develop.*'[31] The order signals the Court's intention to interpret digital laws in light of their objectives and the Charter of Fundamental Rights,[32] as it has already done with the GDPR. It also suggests a continued willingness to give precedence to users' fundamental rights over the financial and commercial interests of platforms, in line with the Court's approach in *Meta platforms*[33] concerning GDPR compliance. Furthermore, the order draws attention to the peril of allowing rights-undermining spaces and technologies to grow unchecked. This danger is both present and evident at a time where several Big Tech have openly defied the European digital framework (and the

29. Order of the Vice-President of the Court of Justice, 27 March 2024, *European Commission supported by the European Parliament and Council v Amazon*, Case C-639/23 P(R), EU:C:2024:277.

30. ibid, para 155.

31. ibid, para 157 (emphasis added).

32. The first requests for a preliminary ruling on the AIA (C-806/24, C-159/25) also seek clarification of certain provisions of the Act read in conjunction with the fundamental rights enshrined in the Charter. National judges are thus inviting the Court to continue along the path of a rights-oriented reading of the new digital legislation.

33. Case C-252/21, *Meta platforms.*

philosophy underpinning it) and are engaging in legal battles to challenge various aspects of it.[34]

In this context, the Commission, bearing sole responsibility for enforcing the DMA and, in the case of very large online platforms and search engines, the DSA, while also assuming supervisory tasks under Article 75 of the AIA concerning general-purpose AI models, has emerged as a key player in confronting Big Tech.[35] However, its role as a counter-power to the 'East India Companies' of the digital era has drawn criticism, particularly due to its political nature and potentially conflicting goals outlined above. This criticism echoes earlier concerns raised after the judgment in *Schrems I*, when the Commission appeared to downplay the privacy and due process standards set by the Court of Justice in the negotiation of the new transatlantic data transfer agreement. Such concerns have intensified following the announcement of the so-called Turnberry Framework on Trade, signalling the Commission's capitulation to US demands. In light of these developments, the call for the establishment of a dedicated, independent EU agency tasked with enforcing the EU's digital rulebook[36] is gaining momentum and merits careful consideration.

In the meantime, it is crucial for the Commission to remain fully committed to its task. A new chapter of 'forbearance politics',[37] this time in the enforcement of digital rules, would deal a serious blow to the EU's credibility as a global regulatory power. The Commission must therefore stand firm in its role as guardian of the Treaties and intensify its enforcement efforts. While coercive measures are not the only route to ensuring compliance, which can also be achieved through constructive dialogue, the

34. Challenges are increasingly being brought before the General Court. While Amazon has contested its designation as a very large online platform under the DSA (Case T-367/23) in order to request the suspension of several related obligations, Meta (Case T-55/24, EU:T:2025:842), TikTok (Case T-58/24, EU:T:2025:843) and Google (Case T-92/25) have challenged the Commission's methodology for calculating supervisory fees under the same regulation. Apple (Case T-1080/23), Meta (Case T-1078/23) and Bytedance (Case T-1077/23, EU:T:2024:478; C-627/24) have challenged the Commission's designation decisions under the DMA while Apple is also disputing the Commission's decision finding a violation of the interoperability obligations under the DMA, as well as the validity these obligations themselves (Case T-354/25, T-359/25, T-438/25).

35. Paul-John Loewenthal, Cristina Sjödin and Folkert Wilman, 'Europe's Digital Revolution: The DSA, the DMA, and Complementary Regimes' (Institutional FIDE Report 2025) 40.

36. See Martin Husovec, FIDE General Report on the Digital Services Act and the Digital Markets Act. EU Digital Economy: General Framework (DSA/DMA) and Specialized Regimes (2025) 27; Eurostack, 'The 'European Way. A Blueprint for Reclaiming our Digital Future' (2025) 28 <papers.ssrn.com/sol3/papers.cfm?abstract_id=5251254>.

37. Roger Daniel Kelemen and Tommaso Pavone, 'Where Have the Guardians Gone? Law Enforcement and the Politics of Supranational Forbearance in the European Union' (2023) 75 *World Politics* 779, doi: 10.1353/wp.2023.a908775.

Commission should not shy away from a hard-line approach when discussions reach an impasse. It possesses the authority and expertise; now, it must demonstrate the will, by fully and appropriately wielding its investigative and sanctioning powers. Whereas the (relatively) modest fines imposed on Meta and Apple in the first decisions under the DMA[38] and on X under the DSA[39] can be understood as cautious warning signals, in the future the Commission must not falter when sanctioning major companies that appear to respond only to the language of power. Indeed, the experience of the GDPR has shown that, in order to be truly deterrent, fines must exceed the profits gained through non-compliance and that the threat to be banned from the EU's market can *in fine* be more effective than any financial penalty.

Moreover, the Commission must clearly articulate its priorities since its enforcement resources, while significant, are not unlimited. It must be more transparent about its agenda and processes than it has been so far, if it wants to convince stakeholders both within and outside Europe of the rationality and legitimacy of its actions. Transparency is also essential for building and sustaining trust in public interventions related to Internet governance and, more broadly, digital and AI technologies. Furthermore, enforcement strategies in this field must be informed by science. They should draw on insights and guidance derived from scientific knowledge produced by researchers, including those benefiting from access to data under Article 40 of the DSA. These researchers can be valuable allies to the Commission, alongside national regulators whose findings help ensure that the 'central enforcer' remains attentive to local challenges and contexts. As public enforcement progresses, we can also continue to rely on the creativity and determination of legal practitioners, users and civil society organizations to open new channels for private enforcement.[40] After all, EU law and integration have a long-standing tradition of individuals and groups asserting rights through strategic litigation. The EU rights-based culture is deeply rooted in the doctrine of direct effect and effective remedies, and the Court of Justice has already strongly encouraged private enforcement, including collective redress, in the context of the GDPR.

The EU must also resist the deregulatory trend. This does not mean it should avoid efforts to streamline or, when necessary, recalibrate its rules. Simplifying overly complex provisions, alleviating cumbersome processes, clarifying legal requirements and fixing duplications and inconsistencies are

38. Commission implementing decisions of 23.4.2025, Case DMA.100055-Meta, C (2025) 2091 final and Case DMA.100109-Apple, C(2025) 2090 final.

39. European Commission, 'Commission fines X €120 million under the Digital Services Act' (Press release, 5 December 2025) <ec.europa.eu/commission/presscorner/detail/en/ip_25_2934>.

40. See the proceedings initiated by the association *Bits of Freedom* against Meta regarding recommender systems and the widely publicized order issued on 2 October 2025 by the Amsterdam district court, NL:RBAMS:2025:7253.

all welcome exercises of sound regulatory practice. Such improvements can benefit both companies and enforcement authorities. However, simplification must not serve as a pretext for dismantling core protections and oversight, as has already been observed in the rollback of key elements of the Green Deal achieved under the first von der Leyen Commission, especially the retreat from corporate sustainability commitments. Care must be taken to ensure that the reviewed digital rulebook is not weakened or hollowed out. To this end, any reconsideration of digital laws must be accompanied by strong procedural safeguards, including broad public consultation (extending beyond selected stakeholders) and comprehensive impact assessments, to ensure that it is grounded in a robust body of evidence. These requirements are insufficiently met by the Digital Omnibus presented by the Commission.[41] Finally, instead of insisting on the downsides of having a plurality of laws, it is more constructive to consider the benefits of interaction between diverse legal instruments and focus on improving coordination and cooperation among competent enforcement authorities at both national and European levels. Indeed, several issues warrant being addressed from multiple legal standpoints. The examples of Meta's 'pay or consent' model, captured by the GDPR[42] and the DMA[43] (and also consumer law), and of deepfakes, which fall within the scope of the AIA, the DSA and the AIA, are illustrative.

Furthermore, it is crucial to counter the misconception that the EU is alone in its quest to regulate the impact of digital and AI technologies on markets and society. While the 'Brussels effect' of the GDPR has been documented,[44] Australia's Online Safety Act, the UK's Online Safety Act and Digital Markets, Competition and Consumers Act, South Korea's law on AI (and the proposed Platform Competition Promotion Act), Japan's Act on Improving Transparency and Fairness of Digital Platforms, and Canada's proposed AI legislation (awaiting reactivation) all show that the EU is not acting in isolation. This view is further supported by the strong interest that the DSA and the DMA have sparked in Latin American countries (especially Brazil) and in India. The

41. 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.

42. EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 17 April 2024. Meta has challenged it in vain before the General Court (Case T-319/24, EU:T:2025:435) and an appeal is pending before the Court of Justice (Case C-454/25 P).

43. Commission implementing decision of 23.4.2025, Case DMA.100055-Meta, C(2025) 2091 final.

44. Anu Bradford, *The Brussels Effect: How the EU Rules the World* (OUP 2020) ch 5 'Digital Economy' 131.

EU can therefore engage in a process of mutual learning in digital governance by deepening ties with like-minded democracies, willing to promote technological development (and the economic growth it brings) without becoming subordinate to dominant digital powers like the US or China. These countries share several European concerns, such as ensuring child safety on Internet, protecting consumers in online marketplaces, holding Big Tech accountable for their actions and promoting ethical AI. In this context, the EU has the opportunity both to develop bilateral partnerships, similar to its relationship with the US via the EU-US Trade and Technology Council, and to engage in coordinated action through international organizations, such as the Council of Europe, the United Nations or the OECD, global policy fora and standard-setting bodies. The EU's participation in the drafting of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, and the launch of the EU's international digital diplomacy initiative[45] point to a promising path forward.

Finally, energy and political capital should be directed not toward debates on 'overregulation' or the simplistic dichotomy of 'regulation versus innovation', but toward addressing Europe's persistent investment shortfall in the advanced technology sector. The EU's digital rulebook is just one component of a broader ecosystem that requires the definition and implementation of a long-term vision, informed by sustainable objectives, concrete reforms and targeted policy action. Key measures have been clearly outlined in both the Draghi and Letta Reports, as well as in a more recent initiative by Eurostack.[46] They include: completing the internal market, by eliminating the remaining barriers that hinder European companies from scaling across borders; advancing the Capital Markets Union and Banking Union, to facilitate and enhance cross-border investment; introducing an optional 28th regime for companies; reforming public procurement rules to support European technologies. By adopting these measures, the EU can reduce its dependencies and vulnerabilities while maintaining the faith in the capacity of our continent – historically a frontrunner in progress – to remain in the race to shape the technological future. This calls for political leadership rooted in the values and philosophy underpinning our digital laws, which ultimately seek to preserve Europe's capacity for self-determination. Despite their imperfections, these laws can be a powerful tool when applied with conviction. Upholding them is both our responsibility and our challenge.

45. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint communication to the European Parliament and the Council: An International Digital Strategy for the European Union, JOIN(2025) 140 final.

46. Eurostack (n 36).