Jean Monnet Network on EU Law Enforcement
Working Paper Series

Conference:

'The many faces and facets of the enforcement of European Union law: adapting in the ever-evolving landscape and empowering change for successful policies'.

11-12 December 2025, Utrecht University

The failure of the EU's 'meta-regulation' of the digital sector – Too much paperwork, too few sanctions

Jan Blockx[*]

Abstract

There is ample empirical evidence that compliance with the EU digital laws is poor. This paper argues that one of the reasons for this may be that the EU digital laws are increasingly framed as 'meta-regulation', i.e. a framework that provides for legal subjects to self-regulate. As a regulatory technique meta-regulation only works if there is sufficient alignment with the incentives of regulatees, and if there is a credible threat of enforcement in the case of failure to comply. Both of these assumptions are not applicable in the case of the EU digital laws. The paper concludes that regulators should not be drowned by paperwork and that public enforcement should be stepped up.

Keywords: digital; meta-regulation; enforcement; simplification

[*] Assistant Professor at the Faculty of Law of the University of Antwerp, visiting lecturer at Kyushu University, and member of the College (decision making body) of the Belgian Competition Authority. jan.blockx@uantwerpen.be. I am grateful to Miroslava Scholten and Matteo Nebbiai for comments on an earlier version of this paper. All opinions expressed in the paper and any remaining errors are my own.

I. Introduction

Digital technologies have provided humans with new tools that can improve productivity, facilitate communication, and provide easier access to arts and entertainment. As a consequence, a significant part of our life now takes place online: office workers collaborate with colleagues on documents that are stored in the cloud, in the evening we watch movies online, and inbetween we connect with friends and colleagues over social networks and messaging services.

But digital technologies also carry many risks. The online services that we access collect vast amounts of personal information about us. This data can in turn be used to nudge us into behaviour that we consciously object to, including addiction and extremism. Digital technologies further induce strong network effects, which means that users tend to become dependent on a small number of providers.

The EU has therefore adopted legislation to addresses some of the risks posed by digital technologies, but compliance with these digital rules is poor. This paper argues that one reason for this may be that the approach that was followed in this legislation was not appropriate to deal with these risks.

The remainder of the paper is structured as follows. Section II describes the growth of EU digital legislation since the start of the 21st century. Section III describes the 'meta-regulation' approach and how it has been used by the EU, including in its digital legislation. Section IV discusses the empirical evidence that points to a lack of compliance with the EU digital legislation. Section V describes how the premises of meta-regulation (alignment of incentives with regulatees and a credible threat of enforcement) are not present for digital laws. Section VI argues that stronger public enforcement is necessary. Section VII concludes.

II. The growth of EU digital legislation

In the past 10-15 years, the EU has adopted a growing number of regulations and directives specifically aimed at the digital sector.[1] This growth is largely in line with the growing importance of the digital sector in today's economy and society.

Some of the new legislation aims to adapt existing EU economic policy areas to the changes brought about by digitisation. An obvious example is consumer protection law. The EU has had consumer protection rules since the 1980s, in order to tackle key problems such as misleading advertising[2] and unfair terms in consumer contracts.[3] Some of these rules were easily transferable to digital markets, such as the rules protecting consumers in distance contracts.[4] But digital markets still pose specific risks for consumers, which informed the adoption of a modernisation directive in 2019.[5] A similar adjustment to digital realities can be observed for instance in the field of copyright.[6]

---

1 I focus here on economic regulation. In addition, the EU has adopted rules that tackle specific technological challenges, such as cybersecurity rules.

2 Council Directive 84/450/EEC of 10 September 1984 concerning misleading and comparative advertising (1984) OJ L 250/17. This directive has now been replaced by Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (2006) OJ L 376/21.

3 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (1993) OJ L 95/29.

4 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (1997) OJ L 144/19. These rules have now been included in 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 Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (2011) OJ L 304/64.

5 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 L 328/7.

6 See, in particular, Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L

Other legislation was specifically designed to regulate the digital economy. An obvious example is the E-commerce Directive of 2000, which aimed to encourage the uptake of so-called 'information society services' and to overcome national barriers for such services.[7] More recent examples include several pieces of legislation that aim to specifically regulate digital platforms which bring together consumers and businesses (in particular the Platform-to-Business (P2B) Regulation,[8] the Digital Markets Act (DMA)[9] and the Digital Services Act (DSA))[10] and the Artificial Intelligence (AI) Act.[11]

Digitisation also gave rise to major concerns in areas of policy that were of little interest before. The obvious example of such a field is privacy and particularly data protection. While privacy legislation has long existed at the member state level, the ability of digital technologies to capture and process vast amounts of personal data led the EU to adopt harmonising legislation in this field in 1995.[12] The popularisation of the internet provoked the adoption of the ePrivacy Directive a few years later,[13] and the exponential growth of data harvesting and profiling resulted in the General Data Protection Regulation (GDPR) in 2016.[14]

The growth of EU legislation for the digital economy has created a web of interlinking and sometimes overlapping legislation. This has provoked calls for simplification, mainly from business lobbies whose members are subject to the obligations contained in the various pieces of legislation, and who therefore also plead for deregulation. The von der Leyen II Commission seems to be willing to heed to these calls, in line with its ambition to strengthen the EU's 'competitiveness'. Among the 'Omnibus' simplification packages that it has so far proposed, the package announced on 21 May 2025 provides for a broader exception of the obligation for personal data controllers to keep a record of processing activities.[15] A more extensive digital simplification package was announced on 19 November 2025: it proposes quite significant modifications to the GDPR and the AI Act, the abolition of most of the P2B Regulation, and various changes to data regulation adopted in recent years, amongst other topics.[16]

130/92.

7 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000) OJ L 178/1.

8 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (2019) OJ L 186/57).

9 Regulation (EU) 2022/1925 2065 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 L 265/1.

10 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.

11 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 L 2024/1689.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L 281/31.

13 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002) OJ L 201/37.

14 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 (2016) OJ L 119/1.

15 European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures (COM (2025) 501 final).

16 European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of

III. The role of 'meta-regulation'

The digital legislation that has been developed in recent years is a child of the 'responsive regulation' and 'smart regulation' movement in policy studies. This movement, pioneered by mainly Australian scholars in the 1990s, aims to replace the traditional 'command-and-control' approach to governance by a more cooperative approach, whereby governments rely on others (including the regulated subjects themselves) for compliance and enforcement.[17] As Neil Gunningham and Darren Sinclair explain: 'smart regulation argues that enforcement is possible not just by the state (as traditional theories of regulation assume) but also by second and third parties who act as surrogate regulators.'[18] The idea is that, by relying more on private enforcement and compliance tools, responsive/smart regulation leads to more effective compliance and that it does so at a lower cost for the public.

One aspect of this, is that third parties (such as business partners or non-governmental organisations (NGOs)) are specifically empowered to monitor compliance by regulated subjects. This idea was not entirely new in EU law. On the contrary, in its milestone *Van Gend & Loos* judgment, the CJEU relied on exactly the same idea. By introducing the principle of direct effect, the CJEU empowered all EU citizens to defend the rights that they derive from the treaties. The Court also acknowledged that the private enforcement that results from this constitutes an important additional tool to ensure compliance: 'The vigilance of individuals concerned to protect their rights amounts to an effective supervision in addition to the supervision entrusted … to the diligence of the Commission and of the Member States.'[19]

But another important aspect of responsive/smart regulation is that regulators rely more on compliance efforts by the regulated subjects themselves. Rather then trying to regulate every nook and cranny of business operations, the idea is that governments impose responsibilities on businesses themselves to find ways to achieve the objectives of regulation. This approach is often denoted as 'meta-regulation': instead of directly regulating what firms should do, governments mainly regulate how firms should regulate themselves.[20] In their book on *Responsive Regulation*, Ayres and Braithwaite called it 'enforced self-regulation'.[21] Coglianese and Mendelson similarly define meta-regulation as 'ways that outside regulators deliberately … seek to induce targets to develop their own internal, self-regulatory responses to public problems'.[22]

This meta-regulation approach is also not entirely new in EU law. In particular, the 'new approach' to EU harmonisation which was proposed by the European Commission in its White Paper 'Completing the Internal Market' of 1985, relied to a large extent on the elaboration of common European standards by businesses themselves.[23] Self-regulation was thus already viewed as an important complement to top-down EU legislation to strengthen the internal market.

---

harmonised rules on artificial intelligence (Digital Omnibus on AI) (COM (2025) 836 final) and European 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).

17 Foundational works are Ian Ayres & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) and Neil Gunningham, Peter Grabosky & Darren Sinclair, *Smart Regulation: Designing Environmental Policy* (OUP 1998).

18 Neil Gunningham and Darren Sinclair, 'Smart regulation' in Peter Drahos, *Regulatory theory: foundations and applications* (2017 ANU Press) (133) 135.

19 CJEU, case 24/62 *Van Gend & Loos* ECLI:EU:C:1963:1.

20 Neil Gunningham, 'Enforcement and Compliance Strategies' in Robert Baldwin, Martin Cave, and Martin Lodge (ed), *The Oxford Handbook of Regulation* (OUP 2010) 120.

21 Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 101ff.

22 Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave, and Martin Lodge (ed), *The Oxford Handbook of Regulation* (OUP 2010) 146.

23 European Commission, 'Completing the internal market' (COM (85) 310 final).

Today meta-regulation often entails a very process-oriented form of regulation, whereby the focus is on the procedures that firms should follow to set up their compliance systems and on how they should monitor and report on their compliance efforts. This is evident in the digital legislation mentioned above, which contains several specific obligations as regards the internal organisation of legal subjects. An obvious example is provided in the GDPR, with its Articles 37-39 requiring public authorities and certain firms to appoint a Data Protection Officer (DPO) who is meant to monitor and foster compliance with the regulation. The P2B Regulation does not introduce specific staffing obligations, but it nevertheless requires providers of online intermediation services to set up an internal complaint handling system for business users (Article 11) and it requires the contracting of external mediation services (Article 12). These obligations were extended in the Articles 20 and 21 of the Digital Services Act, which introduced additional organisation obligations for very large online platforms, who need to create a crisis response mechanism to deal with serious threats to public security or public health (Article 36) and who need to have a yearly independent audit conducted (Article 37). Finally, Article 28 of the Digital Markets Act requires gatekeepers to introduce a compliance function to monitor compliance with the regulation.

Another subset of such procedural meta-regulation is constituted by documentation and reporting requirements imposed on regulated subjects. For instance, Article 35 of the GDPR provides that, when personal data processing is likely to result in a high risk to the rights and freedoms of natural persons, the data controller needs to carry out a so-called 'data protection impact assessment' (DPIA). This is a structured way of identifying the impact of the processing on the data subject, of assessing the necessity and proportionality of the processing, and of mitigating the risks involved. While DPIAs do not need to be made public, data controllers are encouraged to publish (summaries of) DPIA 'to help foster trust in the controller's processing operations, and demonstrate accountability and transparency.'[24] The documentation and reporting approach of the GDPR was followed and developed in more recent digital legislation. Article 15 of the Digital Services Act, for instance, requires that all providers of intermediary services prepare an annual report on content moderation. Article 24 provides for additional information to be included in these reports by online platforms, and Article 42 adds additional information requirements for very large online platforms and search engines. As regards the Digital Markets Act, Article 11 provides that gatekeepers need to publish an annual report in which they describe how they comply with the obligations imposed on them. The Artificial Intelligence Act, finally, in some cases requires providers of high-risk AI systems to prepare a fundamental rights impact assessment (Article 27).

To be sure, EU digital legislation also permits public and private enforcement. For instance, the GDPR (Article 83), Digital Services Act (Articles 52 and 74), Digital Markets Act (Article 30) and AI Act (Articles 99 and 101) specifically provide for the possibility of regulators to impose fines on non-compliant regulatees. In terms of private enforcement, the Digital Services Act (Article 90), Digital Markets Act (Article 52) and AI Act (Article 110) explicitly provide for representative actions. Nevertheless, meta-regulation is pervasive throughout digital legislation, as has been noted by several other authors.[25]

IV. Lack of compliance

As indicated above, the discussion on the complexity of EU digital legislation has recently focused on the burden that this allegedly creates for businesses that have to comply with this legislation. Such a discussion is one-sided, since such a burden may well be acceptable for society if it is outweighed by the benefits

[24] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (4 April 2017), available at https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711.

[25] See, for instance, Raphaël Gellert, *The Risk-Based Approach to Data Protection* (OUP 2020), especially chapter 5 'Meta regulation in data protection law: the risk-based approach' (concerning the GDPR); Nicolo Zingales, *The DSA as a paradigm shift for onlineintermediaries' due diligence: Hail to meta-regulation*, Verfassungsblog 2 November 2022, available at https://verfassungsblog.de/dsa-meta-regulation (concerning the DSA); and Alexander Peukert, Copyright and the meta-regulation of intermediary services and artificial intelligence, Kluwer Copyright Blog 13 June 2024, available at https://legalblogs.wolterskluwer.com/copyright-blog/copyright-and-the-meta-regulation-of-intermediary-services-and-artificial-intelligence (concerning the DSA and AI Act).

created by the legislation. However, creating these benefits assumes that there is substantive compliance with the legislation. There are serious concerns that this is not the case.

In particular, there are several empirical studies that show that compliance with EU privacy laws is very poor. The most extensive one that I am aware of, was published in 2024 and conducted by researchers at ETH Zurich. They conducted an automated analysis of 85,443 of the most popular webpages in multiple European languages and of the cookie notices they provide to users.[26] They found that the vast majority of websites do not comply with the requirements of EU privacy legislation. First of all, they observed that of the 64,828 websites that use analytics and/or advertising cookies, a third simply does not provide a cookie notice, so does not even inform users of the existence of these cookies, let alone allows them to accept or reject them. Secondly, they found that, out of the 48,843 websites that do contain a cookie notice, 73% already started using analytics and/or advertising cookies even before the user had interacted with the cookie notice, so again without having accepted or rejected the use of cookies. Thirdly, they found that 57% of the 33,431 websites that provide an accept button in their cookie notice, did not provide a reject button, in other words, they did not give the user an option to not consent. Fourthly, they found that 65% of the 16,231 websites that do provide a reject button, continue using cookies even after the users has clicked on the reject button. These findings are consistent with many other studies that also conclude that the majority of websites fail to comply with the requirements of the GDPR and the ePrivacy Directive.[27]

Compliance with digital consumer protection rules is similarly poor. In 2025, the European Commission and the national consumer protection authorities of 25 EU Member States as well as Iceland and Norway announced that they found that half of the 356 online traders of second-hand goods they surveyed are not in compliance with EU consumer protection rules.[28] 40% of the traders concerned do not inform consumers of their right of withdrawal from the purchase contract, even though this right of withdrawal was introduced in EU law in 1997.[29] 45% do not correctly inform consumers of their right to return faulty goods or goods that do not look or work as advertised, and 57% do not respect the minimum period of one year legal guarantee for second-hand goods, even though both of these requirements were introduced in EU law in 1999.[30]

Another example is the P2B Regulation which prohibits certain practices of digital platforms that are considered unfair towards business users. The P2B Regulation provides that the Commission should conduct an evaluation of the regulation, including to assess the sector's compliance with its rules. Such an evaluation was performed by an external contractor and resulted in a study that was published in September 2023.[31] One of the topics of the study was the level of alignment of the platforms' terms and conditions with the P2B Regulation, in particular as regards the transparency obligations imposed on the platforms. The study concluded that, out of the 290 online platforms that were covered in the study, only 49 (17%) were 'significantly aligned' with the P2B Regulation. The alignment of 128 platforms (44%) was qualified as

---

[26] Ahmed Bouhoula, Karel Kubicek, Amit Zac, Carlos Cotrini, and David Basin, 'Automated Large-Scale Analysis of Cookie Notice Compliance' (2024) 33rd USENIX Security Symposium 1723.

[27] See, for instance, Michael Kretschmer, Jan Pennekamp and Klaus Wehrle, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web' (2021) 15(4) ACM Trans. Web 20, 16: 'The general consensus on studies investigating cookie banners in detail is that, whether provided by [Consent Management Platforms] or not, they are not fully compliant with the requirements set by the GDPR in the majority of cases'.

[28] European Commission, 'Investigation by the Commission and national consumer authorities finds that nearly half of second-hand online traders fail to correctly inform consumers of their return rights' (press release 7 March 2025), IP/25/706.

[29] By Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (1997) OJ L 144/19.

[30] By Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees (1999) OJ L 171/12.

[31] Vaida Gineikytė-Kanclerė, Luka Klimavičiūtė, Barbora Kudzmanaitė and Lucie Lechardoy, *Final report (D6) of Study on Evaluation of the Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (the P2B Regulation)* (2022), available at https://op.europa.eu/en/publication-detail/-/publication/d6a287b5-5116-11ee-9220-01aa75ed71a1/language-en/.

medium level, while 123 platforms (42%) were assesses as having a low level of alignment.[32] While the study noticed some improvements in the content of the terms and conditions compared to previous studies conducted on this topic, the conclusion of the study was clearly that compliance was low. For the second aspect of the P2B Regulation, the existence of effective redress mechanisms for users of online platforms, the results of the study were no different. Only 34% of the platforms that were required to introduce such a mechanism actually informed their business users that it existed.[33] To what extent the mechanisms that existed were actually effective was difficult to assess, since there was quite a lot of disagreement between the platforms and business users that were interviewed about this.[34]

It is too early to assess levels of compliance with more recent digital legislation, like the Digital Services Act, Digital Markets Act and the Artificial Intelligence Act.

V. The limits of meta-regulation

Obtaining compliance with legislation is obviously a complex task. The promise of meta-regulation is that part of the compliance efforts can be farmed out to regulatees themselves, thereby reducing the enforcement cost for the regulator. In addition, since meta-regulation provides regulatees with some discretion on how to tailor compliance tools to their specific situation, it is believed that it may actually achieve better compliance.

These 'advise and persuade' strategies, as Gunningham called them, are obviously important. If norms are clear and there is little disagreement between regulator and regulatee on what compliance entails, this will certainly enhance compliance.[35] This is also borne out by empirical evidence. Van der Heijden, for instance, refers to the Australian Taxation Office's Compliance Model which was introduced to tackle the widespread view that not paying taxes on cash income was acceptable. The Compliance Model relied on responsive regulation, meaning a mix of persuasive and repressive measures. Since 'most targets of tax regulation will have an accomodative posture [and] will be likely to comply when exposed to persuasion or education on why paying taxes matters, [they] can then be left to self-regulate.'[36] Only 'a small set of targets will be disengaged and will be likely only to comply when exposed to stringent enforcement and hefty fines requiring a traditional command-and-control approach.'[37] Van der Heijden refers to similar experiences with the US Environmental Protection Agency's Audit Policy. As regards digital policy, the data discussed in the previous section undoubtedly demonstrates that some level of compliance occurs through persuasive techniques.

However, the effectiveness of responsive/smart regulation is predicated on a number of conditions. One of them is that there is sufficient alignment between the regulatory objectives and the self-interest of the regulatee. Meta-regulation in particular provides regulatees with discretion on how to achieve the regulatory objective. If there is no alignment between regulatory objectives and the self-interest of the regulatee, then the latter's incentives will cause it to use its discretion to pursue its self-interest while skirting full compliance with the regulation. As Coglianese and Mendelson point out: 'a key challenge confronting self-regulation and meta-regulation will be ensuring that targets use the discretion afforded them in ways consistent with public regulatory goals rather than with their own private individual interests.'[38]

---

32 *Idem* 192.

33 *Idem* 105.

34 *Idem* 117.

35 Miroslava Scholten, 'Challenges and successes of enforcement of EU law' in Miroslava Scholten (ed.), *Research Handbook on the Enforcement of EU Law* (Edward Elgar 2023) (525) 532-533.

36 Jeroen van der Heijden, *Reponsive regulation in practice: a review of the international academic literature*, State of the Art in Regulatory Governance Research Paper (2020), available at https://apo.org.au/sites/default/files/resource-files/2020-07/apo-nid307316.pdf, 11.

37 *Idem*, 11-12.

38 Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave, and Martin Lodge (ed), *The Oxford Handbook of Regulation* (OUP 2010) 146.

In the case of the digital regulation mentioned above, there is often a conflict between the regulatory objectives and the incentives of the regulatees. For instance, for many digital companies, personal data are an (or even the most) important input for their services: they therefore have no incentive to minimize personal data collection and storage, even though these are precisely principles of the GDPR.[39] Requiring a firm to set up internal measures to comply with these principles will therefore inevitably clash with that firm's business model. The conflict of incentives is even more blatant in some provisions of the Digital Markets Act which, for instance, prohibit regulatees from treating their own services and products more favourably in ranking and related indexing and crawling than the services and products of third parties.[40]

In addition, like all forms of smart/responsive regulation, meta-regulation still assumes that, in addition to the compliance efforts put in by the regulatee, there is also a certain amount of public and/or private enforcement. Smart/responsive regulation is based on an enforcement pyramid, where persuasive compliance is backed up by the risk of more forceful sanctions. As Scholten points out, '[r]eactive mechanisms, such as sanctioning procedures, are thus important too'.[41] Gunningham fully recognized this when he said that soft 'advise and persuade' strategies in regulation 'can easily degenerate into intolerable laxity and fail to deter those who have no interest in complying voluntarily'.[42] He discusses the example of the Australian inspectorate of health and safety regulation whose oversight of an asbestos mine was inadequate: inspections were rare and announced in advanced, and merely resulted in reports with recommendations. Gunningham characterised this as 'negotiated non-compliance'.[43]

The same risk arises from meta-regulation: companies appoint a compliance officer and prepare the reports required by the legislation, but fail to actually comply with the substantive requirements of the legislation. A good example is provided by the ETH Zürich study of compliance with privacy laws mentioned above: the majority of webpage investigated show a privacy notice, but in most cases the company ignores the choice made by the user or starts collecting data before the user can give their consent. The companies have their paperwork in order, but breach the substantive obligations under the privacy laws. Along the lines of what Gunningham states above, one could call this 'documented non-compliance'. This risk arises if the focus of the regulator is more on the paperwork than on substantive compliance.

VI. The need for private and, especially, public enforcement

Smart/responsive regulation does not merely rely on the meta-regulation of compliance efforts by regulatees themselves; it also specifically values the role that can be played by third parties, such as customers or competitors of regulated firms, interest groups like NGOs, and the press. Third party monitoring of compliance and private enforcement can indeed constitute a significant sources of compliance pressure for recalcitrant businesses.

As indicated before, private enforcement has always played an important part in the enforcement of EU law. The fact that the majority of CJEU judgments are still delivered following a reference for a preliminary ruling under what is now Article 267 TFEU shows how important enforcement at the level of the Member States is for compliance with EU law – and in many instances this is enforcement by private actors.

In respect of EU digital legislation, private enforcement has played a particularly important role. Some of the key CJEU rulings on the E-commerce directive, such as *Google France*,[44] *Papasavvas*,[45] and *Uber Spain*,[46] were the result of private litigation. The same is true for several landmark CJEU rulings on the GDPR, such

[39] See in particular Article 5 of the GDPR.

[40] Article 6(5) of the Digital Markets Act.

[41] Miroslava Scholten, 'Challenges and successes of enforcement of EU law' in Miroslava Scholten (ed.), *Research Handbook on the Enforcement of EU Law* (Edward Elgar 2023) (525) 534.

[42] Neil Gunningham, 'Enforcement and Compliance Strategies' in Robert Baldwin, Martin Cave, and Martin Lodge (ed), *The Oxford Handbook of Regulation* (OUP 2010) 125.

[43] Neil Gunningham, 'Negotiated Non-Compliance: A Case Study of Regulatory Failure' (1987) 9 Law and Policy 69.

[44] CJEU, case C-236/08 Google France and Google v Louis Vuitton ECLI:EU:C:2010:159.

[45] CJEU, case C-291/13, Papasavvas v O Fileleftheros Dimosia Etairia ECLI:EU:C:2014:2209.

[46] CJEU, case C-434/15, Asociación Profesional Elite Taxi v Uber Systems Spain ECLI:EU:C:2017:981.

as *Planet49*,[47] *Schrems II*,[48] and *Lindenapotheke.*[49] In some of these cases, private litigation was instituted in light of the inability or unwillingness of regulators to ensure compliance with the rules in question.

But private enforcement has its limits.[50] Many victims of non-compliance lack the time and financial resources to start protracted litigation against regulated subjects, in particular if the latter are firms with deep pockets. This problem is particularly well known when it comes to the consumer protection rules: in virtually all circumstances, individual consumers prefer to cut their losses, rather than contest unfair treatment by professional traders. A second hurdle for private enforcement is that third parties are often at an informational disadvantage compared to the regulatee. While the latter should in principle dispose of the information needed to comply with the rules and therefore also to assess whether it complies with the rules, this is often not the case for third parties. Meta-regulation can be a help in this respect, in particular due to the reporting requirements, which may aid private litigants in their discovery process; but this of course assumes that the reporting requirements are themselves complied with. A third limit to private litigation is that it can usually only lead to an order to cease-and-desist and the payment of damages to the claimant. If non-compliance is very profitable, this may well be a risk that the regulatee is willing to run.

Public enforcement does not suffer from the limits described above (or at least not to the same extent). It is the regulator's very job to ensure compliance with the rules, so that is what it should devote its time and financial resources to (at least if these are sufficiently available). Regulators often have extensive investigative powers, which allow them to obtain information that is not available to private litigants. And regulators often have sanctioning powers that go beyond what can be obtained in private litigation: ranging from fines to the withdrawal of licenses.

Of course, public enforcement has downsides compared to private enforcement. First and foremost, it is costly for society and should therefore only be used if other compliance tools cannot achieved the desired compliance results. However, given the poor compliance results noted earlier, we are in this situation when it comes to compliance with the digital rules. Public enforcement of the digital rules is therefore absolutely essential, in addition to the compliance and documentation efforts undertaken by regulatees and private enforcement by third parties.

The effectiveness of public enforcement is clearly illustrated in the field of the digital consumer rules. The Consumer Protection Cooperation network (that brings together national consumer protection authorities in the EU) has reported that compliance with consumer protection rules very significantly increases once the network takes action (so-called 'sweeps') against websites that fail to comply with certain rules. In the 13 sweeps conducted between 2007 and 2019 (ranging from websites of airlines, over consumer credit, to telecommunications), compliance levels almost doubled from on average 41% before the sweep to 79% after the sweep.[51] The risk of sanctions immediately focused the mind of the websites in question. Perhaps the 41% compliance prior to intervention was the result of 'advise and persuade' policies, but the 38% additional compliance was only achieved after public enforcement action was taken.

In order to achieve its compliance-enhancing potential, public enforcement authorities need to dispose of sufficient resources to conduct enforcement action against recalcitrant regulated subjects. Such enforcement resources should not be tangled up in verification exercises in respect of documentary compliance of regulatees, which may be the case if there are extensive reporting obligations. Documentary compliance is indeed only part (and decidedly the minor part) of the compliance with the rules in question. Imposing procedural obligations on regulatees should not result in the regulators drowning in paperwork.

---

47 CJEU, case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49* ECLI:EU:C:2019:801.

48 CJEU, case C-311/18 *Data Protection Commissioner v Facebook Ireland and Schrems* ECLI:EU:C:2020:559.

49 CJEU, case C-21/23, *ND v DR* ECLI:EU:C:2024:846.

50 See, for a discussion of factors that affect the preference for public and private enforcement, Steven Shavell, 'The Optimal Structure of Law Enforcement' (1993 36(1) The Journal of Law & Economics (255) 266-270.

51 Statistics provided on the European Commission's website on the Consumer Protection Cooperation Network: https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.

VII. Conclusion and way forward

This paper has described how the meta-regulation approach played an important part in the digital legislation adopted by the EU over the last decade and a half. It also pointed out how compliance with this digital legislation is subpar. One of the explanations for this lacklustre performance may be that the meta-regulation approach was not well suited for digital legislation, due to the mismatch between the objectives of the legislation and the incentives of regulatees. Another explanation for non-compliance is the limited amount of public enforcement.

In order to ensure compliance with digital laws, additional public enforcement is needed. This implies that the necessary resources are made available to public enforcers. Public enforcement would also benefit from a regulatory framework that focuses less on procedure and documentation, and more on black-and-white rules. This will avoid that regulators are drowning in paperwork produced by regulatees for apparent compliance. From this perspective, regulatory simplification does not need to entail deregulation.