Technology and Regulation

EU cross-regime enforcement, redundancy and interdependence. Addressing overlap of enforcement structures in the digital sphere after *Meta*

Author(s)	Prof. Paul de Hert, Paweł Hajduk
Contact	paul.de.hert@tilburguniversity.edu, p.hajduk@outlook.com
Affiliation(s)	Tilburg University; Vrije Universiteit Brussel, the Cardinal Stefan Wyszyński University in Warsaw, Poland

Keywords	accountability; cross-regime enforcement; cross-regime cooperation; interdependence; redundancy
Published	**Received**: 16 Jun. 2024 **Accepted**: 14 Nov. 2024 **Published**: 2 Dec. 2024
Citation	Prof. Paul de Hert, Paweł Hajduk, EU cross-regime enforcement, redundancy and interdependence. Addressing overlap of enforcement structures in the digital sphere after *Meta*, Technology and Regulation, 2024, 291-308 • https://doi.org/10.26116/techreg.2024.021 • ISSN: 2666-139X

Abstract

The post-GDPR EU's legal acts regulating digital technologies have increased the already significant number of enforcement authorities whose competence overlaps with data protection authorities (DPAs). The CJEU judgement in the Meta case is a step forward in managing this phenomenon by allowing other authorities to deal with data protection matters incidentally in close cooperation with DPAs. Such overlap might be seen from the public law postulate of the precise delimitation of authorities' competence or through a concept of extended accountability explored by Colin Scott. This paper examines the second concept, demonstrating the potential advantages of enforcement structures' fuzziness, redundancy and interdependence and sketching a path forward for cross-regime cooperation.

1. Introduction

The post-General Data Protection Regulation (the GDPR) EU legal acts, including the Data Governance Act (the DGA), Data Act, Digital Markets Act (the DMA), Digital Services Act (the DSA), and Artificial Intelligence Act (the AI Act), establish parallel enforcement structures. While these acts are declared "without prejudice" to the GDPR, they regulate matters falling within its scope, rendering the meaning of "without prejudice" clauses questionable.[1] This denotes an overlap between incumbent branches of law adjacent to data protection law, such as competition law, consumer protection law or anti-money laundering law.

1 Cf. the analysis of "without prejudice" clauses, cf. Konstantina Bania, 'Fitting the Digital Markets Act in the existing legal framework: the myth of the "without prejudice" clause' (2023) 19 European Competition Journal 116.

The legislative technique (including vague terms and open texture)[2] combined with the nature of the EU legal order and political considerations means that the burden of concretising the meaning of legal norms inferred from these acts lies mainly with the enforcement authorities – either the centralised one or national authorities clustered in networks usually coordinated by collegiate bodies at EU level. This will create a complex multi-level enforcement system. Although such overlap is not a new phenomenon – as it has been examined by the European Data Protection Supervisor (the EDPS) at least since 2014 in the context of data protection, competition, and consumer protection law[3] – it is amplified by an acceleration of the digitalisation of societies, probably due to the COVID-19 pandemic. This is compounded by rapidly deploying general-purpose generative Artificial Intelligence models trained on publicly available personal data.[3]

All these make effective enforcement of data protection,[4] consumer protection and competition law are more needed. Recent studies demonstrate that lack of effective enforcement is the Achilles' heel of the GDPR.[5] The Fundamental Rights Agency's report "*GDPR in practice – Experiences of data protection authorities*"[6] focuses on DPAs as a critical element of the EU data protection law. One of the concerns of DPAs is the overlap of their competence with other authorities and ensuring coherence between them.[7]

We believe effective enforcement can be achieved without necessarily striving to avoid overlap. Although we find the DPAs' concerns justified, we also consider that overlap provides an opportunity to develop a unique enforcement system that could work effectively through cross-regime cooperation.[8]

To introduce our arguments, we briefly discuss the overlap within the EU regulation of digital technologies (Section 2), different models of enforcement structures in post-GDPR legal acts (Section 3), and we propose working definitions of "competence", "remit" and "overlap of competence" in order to organise terminology (Section 4). With regard to the overlap of enforcement structures, conceptualisation from at least two perspectives is possible. The first is the classical public law requirement of the precise delimitation of the remit of public authorities in pursuit of vertical accountability. The second is a concept of extended accountability explored by Colin Scott, which seems more suited to the challenges of the regulatory state.[9] We discuss these threads in Sections 5 and 6, exploring the extended accountability by demonstrating the advantages of the fuzziness of the enforcement structures. We argue that it renders a chance to strengthen the protection of fundamental rights.[10]

2 Cf. Paul De Hert, 'Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law', in Deirdre Curtin and Mariavittoria Catanzariti (eds), Data at the Boundaries of European Law (Oxford University Press, 2023; online edn, Oxford Academic, 23 March 2023); Paweł Hajduk, 'AI Act and GDPR: On the Path Towards Overlap of the Enforcement Structures' (RAILS-Blogspot, 1 October 2023) <https://blog.ai-laws.org/ai-act-and-gdpr-on-the-path-towards-overlap-of-the-enforcement-structures/> accessed 27 May 2024; Paweł Hajduk, 'Divergence Between Authorities on Publicly Available Spatial Data in Poland' (2022) 2(2) GIS Odyssey Journal 115.

3 Cf. Pablo T. Kramcsák, 'Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?' (2023) 48 Computer Law & Security Review 105765; Sebastião B. Vale, 'Training large generative AI models based on publicly available personal data: a GDPR conundrum that the AI Act could solve' (The Digital Constitutionalist, 2024) <https://digi-con.org/training-large-generative-ai-models-based-on-publicly-available-personal-data-a-gdpr-conundrum-that-the-ai-act-could-solve/> accessed 27 May 2024.

4 David Wright, 'Enforcing Privacy' in David Wright and Paul De Hert (eds), Enforcing Privacy: Regulatory, Legal and Technological Approaches (1st edn, vol 25, Springer 2016) 13-49.

5 noyb, European Center for Digital Rights, GDPR: A Culture of Non-Compliance (Report, January 2024) <https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance.pdf> accessed 27 May 2024.

6 European Union Agency for Fundamental Rights, GDPR in Practice – Experiences of Data Protection Authorities (FRA, 11 June 2024) <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities> accessed 11 June 2024.

7 Interventions by Ulrich Kelber, Kate Jones, Alexander Hoefmans, and Paweł Hajduk during the panel discussion "Data-driven practices through a cross-regulatory lens: the future of digital governance" moderated by Brendan Van Alsenoy at CPDP - Data Protection Day Conference on 25th January 2024 in Brussels, Belgium.

8 CJEU, Judgment of the Court (Grand Chamber), Meta Platforms Inc and Others v Bundeskartellamt, Request for a preliminary ruling from the Oberlandesgericht Düsseldorf, Case C-252/21, [2023] ECLI:EU:C:2023:537, para 42.

9 Colin Scott, 'Accountability in the Regulatory State' (2000) 27 Journal of Law and Society 38.

10 Cf. Fabrizio Gilardi, Delegation in the Regulatory State: Independent Regulatory Agencies in Western Europe (Edward Elgar Publishing 2008) 1-181.

While redundant and interdependent enforcement structures should serve the same public interest and support each other's actions within the unified enforcement system, the question remains: how can their cooperation be shaped to work coherently? Hence, a mature EU-wide framework is needed. The GDPR is agnostic on cross-regime cooperation between enforcement authorities, whereas post-GDPR legal acts – although they recognise the need to align their relationship with GDPR and DPAs – only contain scattered cross-regime cooperation instruments, which are investigated in Section 9. The recent Court of Justice of the European Union (CJEU) judgment in the Meta case (2023)[11] is a significant step in shaping the path towards such a framework, paving the way for authorities other than DPAs to deal incidentally with data protection matters in cooperation with DPAs (Section 8). Although the CJEU judgment in the Meta case is a valid step, establishing such a framework is only at its beginning. Hence, in Sections 9 and 10, we sketch potential solutions for cross-regime cooperation.[12]

2. The Landscape of EU Regulation of Digital Technologies

The GDPR overlaps in material and subjective scope with most other legal acts within the EU regulation of digital technology. Insightful scholars have already devoted considerable work to this issue.[13] Also, both authors analysed, among others, the phenomenon of "mimesis of post-GDPR laws", "EU law brutality", and the overlap of competence of enforcement authorities within the EU regulation on digital technologies.[14] Hence, due to the volume limitations of this paper, we will not demonstrate in detail the overlap between the material scopes of these acts as well as the competences of the authorities but we want to go a step further by addressing extended accountability in EU digital regulation holistically and proposing a way forward.

For clarity, we start with a brief overview of the EU regulation of digital technologies. Regulation of digital technologies started at the EU level at least in the 1990s (thirty years ago) with the Data Protection Directive[15] (1995), followed by the milestones of the eCommerce Directive (2000),[16] the Information Society Directive[17] (2001) and the ePrivacy Directive[18] (2002). Over the following years, ground-breaking CJEU jurisprudence[19]

11 CJEU (n 8), para 42.

12 It is necessary to make disclaimers. Firstly, we only consider a selection of EU legal acts regulating digital technologies, acknowledging the notion of "digital technologies" is difficult to define (cf. Vagelis Papakonstantinou and Paul De Hert, The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play (Routledge 2024) 1-154); Secondly, this paper does not aim to analyse all of the legal acts in detail; its purpose is to make a general reflection; Thirdly, we acknowledge that the notion of "accountability" is broad (cf. Julia Black, 'Constructing and contesting legitimacy and accountability in polycentric regulatory regimes' (2008) 2(2) Regulation & Governance 137-164) and multidimensional (cf. Richard Mulgan, ''Accountability': an ever-expanding concept?' (2000) 78(3) Public Administration 555); In this paper, we use the meaning introduced by Scott without going into an in-depth discussion.

13 Cf. Gabriela Zanfir-Fortuna, 'Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's "Fit for the Digital Age" Legislative Package' (2024) EDPS at 20 Anniversary Volume (forthcoming) <http://dx.doi.org/10.2139/ssrn.4794182> accessed 20 June 2024; Martin Ebers and Karin Sein, 'Data-driven Technologies – Challenges for Privacy and EU Data Protection Law' in Martin Ebers and Karin Sein (eds), Privacy, Data Protection and Data-driven Technologies (Routledge, forthcoming 2024) <https://ssrn.com/abstract=4823823> accessed 20 June 2024.

14 Including De Hert (n 2); Hajduk (n 2); Papakonstantinou and De Hert (n 12); Vagelis Papakonstantinou and Paul De Hert, "The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'act-ification', 'GDPR mimesis' and 'EU Law brutality'" (2022) Technology and Regulation 2022, 48-60; Paweł Hajduk, 'A Walk in the Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research' in F. Bieker, S. de Conca, N. Gruschka, M. Jensen, I. Schiering (eds), Privacy and Identity Management. Sharing in a Digital World. Privacy and Identity (IFIP Advances in Information and Communication Technology, vol 695, Springer 2024) 3–17.

15 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 L281/31.

16 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1.

17 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

18 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 (Directive on privacy and electronic communications) [2002] OJ L 201/37.

19 Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238.

was rendered, as with the Data Retention Directive[20] (2006), and new legislation like the NIS 1 Directive[21] (2016) for cybersecurity. Sectoral legal acts supplement these core legal acts, such as the financial market, Payment Services Directive 2[22] (2015) and the anti-money laundering directives.[23] This phase culminated in the adoption of the GDPR (2016),[24] EUDPR (2018)[25] and the Law Enforcement Directive (2016).[26] The EU legislature then moved on to the next phase, which can be referred to as "*post-GDPR*" legislation after 2018 with the adoption, *inter alia*, of the Digital Markets Act,[27] Digital Services Act,[28] Data Act,[29] Data Governance Act,[30] NIS 2 Directive,[31] and AI Act.[32] This is not the end of the EU's legislative initiative in the digital area,[33] with the next step being the creation of EU data spaces,[34] including by the European Health Data Space Regulation.[35] A comprehensive overview of the regulation of digital technology in the EU is presented in tables annexed to the publication by Kai Zenner, Scott Marcus and Kamil Sekut, "*A dataset on EU legislation for the digital world*".[36]

20 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

21 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

22 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) [2015] OJ L337/35.

23 For example, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance) [2015] OJ L141/73.

24 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) (Text with EEA relevance) [2016] OJ L119/1.

25 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance) [2018] OJ L295/39.

26 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

27 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) (Text with EEA relevance) [2022] OJ L265/1.

28 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) (Text with EEA relevance) [2022] OJ L277/1.

29 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 L/2854.

30 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) (Text with EEA relevance) [2022] OJ L152/1.

31 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) [2022] OJ L333/80.

32 Text based on the draft AI Act as of 21 May 2024, available at Council of the European Union, 'Artificial Intelligence (AI) Act: Council Gives Final Green Light to the First Worldwide Rules on AI' (21 May 2024) https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ accessed 6 June 2024.

33 Legislation aimed at creating EU Data Spaces may be recognised as the next phase of EU digital regulation. The European Data Protection Supervisor Wojciech Wiewiórowski, during a panel discussion at the conference "Forum Prawa Mediów Elektronicznych" at the University of Wrocław on 21 March 2024, suggested such a division of EU digital regulation.

34 European Commission, 'Common European Data Spaces' (Digital Strategy, 2024) <https://digital-strategy.ec.europa.eu/en/policies/data-spaces> accessed 4 June 2024; The DGA and Data Act serve as a horizontal framework for EU data spaces.

35 European Commission, 'European Health Data Space' (EU Health Data Space, 2024) <https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en> accessed 4 June 2024.

36 K. Zenner, J. Scott Marcus, K Sekut, 'A dataset on EU legislation for the digital world' (16 November 2023, Bruegel) <https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world> accessed 20 April 2024.

The vital part of EU regulation of digital technology is still played by incumbent branches protecting the functioning of the internal market and consumers – competition law and consumer protection law.[37] Their objectives remain complementary to the objectives of data protection law and, in the post-GDPR legal acts, have been partially tailored to digital technologies through the Digital Markets Act and Digital Services Act.[38] The interplay between data protection, competition and consumer protection law in digital technologies was already recognised by the EDPS almost a decade ago.[39] It can be analysed from the perspective of their objectives.[40] Ultimately, these objectives, although different, are all ultimately directed towards protecting the individual (whether it is a consumer or data subject), as well as the internal market (while it is also about safeguarding consumers).[41]

Although all these branches employ distinctive concepts and have distinct enforcement structures, they achieve synergies when it comes to regulating digital technologies. For example, this might be sought to curb deceptive practices towards consumers (data subjects) and abuse of dominant position by Big Tech, which strengthens consumers' position (data subjects) and their ability to execute their fundamental rights. Their synergy might be sought under an overarching idea of public interest, aims of the EU in the light of Article 3 of the Treaty on European Union (the TEU)[42] and the obligation to apply the Charter of Fundamental Rights[43] (Article 51 of the Charter).

It might be argued that where an overlap of acts occurs, it is a symptom of a strengthened legislator's concern that translates into "redundant" (doubled) legal protection of the same matters from the perspective of different means towards achieving a common objective. For example, maintaining proper market power balance (via the competition law route) helps secure personal data protection by constraining the position of dominant undertakings, which confers more agenda to the individuals to exercise their rights. All this, however, would not be effective without enforcement structures.

37 The evolution of consumer protection law has been discussed in the literature; cf. Roger Brownsword, 'The E-Commerce Directive, Consumer Transactions, and the Digital Single Market – Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection', in Stefan Grundmann (ed), European Contract Law in the Digital Age, European Contract law and Theory (Intersentia, 2018) 165-204.

38 Although the classification of these two legal acts as competition law or consumer protection law is controversial. Cf. Oles Andriychuk, 'Shaping the new modality of the digital markets: The impact of the DSA/DMA proposals on inter-platform competition' (2021) 44 World Competition 3; Natalia Moreno Belloso and Nicolas Petit, 'The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove' (5 April 2023) 48 European Law Review 391 <https://ssrn.com/abstract=4411743> accessed 28 May 2024.

39 European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy' (EDPS, March 2014) <https://www.edps.europa.eu/sites/default/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 28 May 2024.

40 EU competition law aims "to enhance the efficiency of the internal market and the welfare of and choice available to consumers" (EDPS n 39); while consumer protection law seeks "to remove barriers to the internal market by building trust in products and services throughout the internal market, based on transparency and good faith" (EDPS n 39); whereas data protection law protects "the fundamental rights and freedoms of natural persons, in particular, their right to the protection of personal data" while maintaining "the free movement of personal data" (Article 1(1); Recitals (2), (4), (12) and (14) of the GDPR).

41 We recognise that this is a simplification of the objectives of competition law, but for the purposes of this paper we have taken this limited view.

42 Consolidated Version of the Treaty on European Union [2012] OJ C326/13.

43 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

3. Models of Enforcement Structures in Post-GDPR Legal Acts

Different models of enforcement structures can be distinguished in EU regulation of digital technologies. Their formation depends on various factors, such as the legislator's choice based on path dependency, the EU's constitutional framework, and political considerations[44] related to a specific sector.[45] We distinguish three models of enforcement structures in the EU regulation of digital technologies: 1) cooperative federalism, 2) a centralised model and 3) an intermediate ecosystem model.

Most legal acts regulating digital technologies in the EU (the GDPR, the DGA and the Data Act) introduce the model of a two-tiered enforcement structure[46] with an essential part vested with Member States' enforcement authorities complemented by Boards at the EU level.[47] These acts mandate Member States to establish national enforcement structures by designating either existing authorities or by establishing new authorities. It could be conceptualised as a cooperative federalism.[48] This means harmonising the obligations and penalties at the EU law level while leaving the establishment of the enforcement structures to the Member States.[49]

A centralised model is present in the post-GDPR legal acts as well. Almost complete centralisation of enforcement is limited to the DMA,[50] and partial centralisation has been introduced in the DSA.[51] This is justified by the specific subjective scope of these acts, which cover the most significant players in the digital economy. However, once the AI Act has taken its final shape, it is possible to argue that the enforcement model introduced both in the AI Act and the DSA can be distinguished as an ecosystem model.[52] The DSA introduces parallel enforcement at the Member State level combined with partially central enforcement vis-à-vis VLOPs (very large online platforms) and VLOSEs (very large online search engines) at the Commission level with the additional establishment of a collegiate coordinating body at the EU level, the European Board for Digital Services.[53] National authorities, so-called Digital Services Coordinators, are obliged to cooperate closely with the Commission[54] and procedures are established for the referral of cases from Member

44 An example is the establishment of the European Public Prosecutor's Office. It was a compromise between a centralised, supra-state vision by the Commission and a cooperative approach by the Member States concerned about their sovereignty; Cf. Valsamis Mitsilegas, 'European Prosecution Between Cooperation and Integration: The European Public Prosecutor's Office and the Rule of Law' (2021) 28(2) Maastricht Journal of European and Comparative Law 245.

45 The centralisation depends on the sector. For example, enforcement in the banking sector was centralised mainly as a response to the 2008 financial crisis. Cf. David Coen and John-Paul Salter, 'Multilevel Regulatory Governance: Establishing Bank-Regulator Relationships at the European Banking Authority' (2020) 22 Business and Politics 113-134; Jakub Gren, David Howarth and Lucia Quaglia, 'Supranational Banking Supervision in Europe: The Construction of a Credible Watchdog' (2015) 53 Journal of Common Market Studies 181.

46 Cf. Zanfir-Fortuna (n 13).

47 The European Data Protection Board and its mimics, like the European Data Innovation Board.

48 Paul De Hert, 'EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPRin the Spirit of Cooperative Federalism' in Stefano Montaldo, Francesco Costamagna and Alberto Miglio (eds), EU Law Enforcement (Routledge 2021) 291-324.

49 An exception is the ePrivacy Regulation Proposal, which indicates that DPAs should be designated as the competent authority (cf. European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM(2017) 10 final, 2017/03 (COD), art 18 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0010> accessed 7 June 2024.

50 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 (Digital Markets Act) [2022] OJ L 265/1, ch V.

51 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L 277/1, ch IV, arts 49, 56. The state of the DSA's implementation demonstrates that the Member States designated mostly competition, consumer protection, and telecom authorities as Digital Services Coordinators with the limited roles of DPAs (European Commission, 'Digital Services Act—Digital Services and Digital Markets' (European Commission Digital Strategy, 2022) <https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs> accessed 28 May 2024).

52 Intervention by Renate Nikolay during the discussion "Enforcement in an age of accelerating innovation" at the accompanying event of the CPDP Conference, co-organised by the International Center for Future Generations (ICFG) on 23 May 2024 in Brussels, Belgium.

53 Digital Services Act (DSA), arts 61-63.

54 Digital Services Act (DSA), arts 57.

States to the Commission.[55] In turn, in the final version of the AI Act,[56] similar complex structures have been introduced.[57] The European Artificial Intelligence Office (AI Office), being part of the Commission, is competent, *inter alia*, for enforcing provisions for general-purpose AI models[58] and for contribution to the coherent enforcement of the AI Act;[59] another collegiate body, the European Artificial Intelligence Board has been established as well;[60] and the EDPS is competent "*where Union institutions, bodies, offices or agencies fall within the scope*" of the AI Act.[61] National legislators[62] must designate at least "*one notifying authority and at least one market surveillance authority*" as national competent authorities at the national level.[63]

Whether the ecosystem model should be distinguished as a separate one or a sub-type of the centralised or cooperative federalism model (given the similarities with each of them) is a methodological matter. What is key is that post-GDPR legal acts introduce a trend towards at least partial centralisation of competence, which might contribute to EU integration. In such a scenario, an increasing role of the Commission may be problematic. It is not only a regulator but also a political institution, creating risks of political capture.[64] This trend, however, may reflect a compromise between the weakness of individual Member States vis-à-vis the most significant players and, on the other hand, maintaining competence at the national level where possible.

4. Organising Terminology: "Competence", "Remit", and "Overlap of Competence"

To proceed further, it is necessary to organise the terminological grid, i.e. "competence", "remit", and "overlap of competence". The terms "competence" and "remit" of authorities are used ambiguously in EU legal acts. We propose to define "competence" as the complete set of "powers" and "duties" vested to enforcement authorities to perform their "tasks". To enable the authorities to perform their "tasks", there is a need for an adequate alignment with their "competence."[65] The "competence" and "tasks" of the enforcement authorities should be interpreted from the perspective of their objectives. These objectives can be deduced from the wording of the provisions establishing authorities or from the objectives of the legal act. Such exercise allows us to determine their "remit", understood as the scope of the cases they are competent to decide.

55 Digital Services Act (DSA), arts 58-59.

56 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 21 May 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [2024] OJ L/1689.

57 An overview of the enforcement structure: Laura Pliauskaite, 'EU AI Act Stakeholder Map' (IAPP AI Governance Center, May 2024) <https://iapp.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf> accessed 7 June 2024; It has also been examined in Claudio Novelli, Philipp Hacker, Jessica Morley, Jarle Trondal, and Luciano Floridi, 'A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities' (2024) European Journal of Risk Regulation 1–25.

58 AI Act, arts 75, 88-94.

59 AI Act, art 3(47); See also: European Commission, 'Commission Decision of 24 January 2024 Establishing the European Artificial Intelligence Office' C(2024) 390 final, art 2.

60 AI Act, arts 65-66.

61 Limited by, e.g., Article 70(9) of the AI Act.

62 Article 74 of the AI Act instructs on establishing market surveillance authorities, which is welcomed but imperfect. An important provision is Article 74(8) of the AI Act which essentially suggests the establishment of DPAs as market surveillance authorities "for high-risk AI systems listed in point 1 of Annex III, in so far as the systems are used for law enforcement purposes, border management and justice and democracy, and for high-risk AI systems listed in points 6, 7 and 8 of Annex III".

63 AI Act, arts 28, 70; The EU legislator leaves discretion to the national legislator in shaping the national competent authorities due to the character of the AI Act in the vein of product safety laws.

64 Intervention by Maria Magierska, Intervention during the panel discussion 'Navigating the Maze of Overlapping Roles and Emerging Authorities in the New EU Data (Protection) Framework' at the CPDP Conference, Brussels, Belgium (22 May 2024) <https://www.youtube.com/watch?v=-TW5KqDMv2I&t=2813s> accessed 4 June 2024.

65 Marcin Matczak, ‚Rozdział VI. Kompetencja' in Roman Hauser, Andrzej Wróbel, and Zygmunt Niewiadomski (eds), System Prawa Administracyjnego, Tom 1: Instytucje Prawa Administracyjnego (C.H. Beck 2015) (in Polish); Michał Szyrski, ‚§ 1.II. Teoretyczne zasady podziału zadań i kompetencji organów właściwych w sprawach jawności i jej ograniczeń. Znaczenie podstawowych teoretycznych pojęć – zadanie i cel, kompetencja, właściwość i zakres działania' in Grażyna Szpor and Bogumił Szmulik (eds), Jawność i jej ograniczenia. Zadania i Kompetencje, Tom IX (C.H. Beck, Warszawa 2015) (in Polish).

Against this background, the overlap of competence of authorities might be defined as "*a legal situation in which at least two enforcement authorities, when performing their tasks, are vested with a set of powers and duties (competence) which exercise may lead to deciding the same case or addressing the same matter divergently*."[66] It might be desirable to distinguish between overlap in issuing soft law and issuing binding decisions (including fines). The different consequences of these types of overlap justify such distinction. The issuing of decisions involves determining the rights and obligations of individuals, which requires procedural safeguards and due process standards. Meanwhile, the issuing of soft law, such as opinions, although shaping compliance by influencing the behaviour of regulated entities, does not lead to direct legal effects and, as a rule, is also a subject of judicial review by itself[67]. Therefore, it would be prudent to differentiate between legal bases for cooperation depending on the type of overlap. It might be argued that cooperation in issuing soft law does not require an explicit legal procedure, while cooperation in issuing binding decisions should proceed unambiguously. Establishing a clear legal procedure for cooperation in decision-making would enhance due process standards, while adopting a flexible approach to the cooperation on soft law would allow authorities to be more agile.

One of the examples of such overlap is the launch of proceedings by the Commission (communication of 25 March 2024) against Meta to investigate the "Pay or Consent" model under the DMA.[68] Simultaneously, this model is under investigation by some DPAs at the national level,[69] and the EDPB issued an opinion on consent in the context of this model.[70] It shows that, in a short period, parallel actions are taken by different authorities[71] competent under the GDPR and the DMA concerning the same behaviour. In such a setting, the legal relationship between these actions, including the issue of considering (or being bound by) each other's position and legal arguments, the possibility of different decisions and duplicate sanctions, remains unclear.[72]

5. Extended Accountability: Redundancy and Interdependence

How may the overlap of competence between authorities be assessed? May this fuzziness be seen as a positive development, or can it be criticised as posing a risk of incoherence and duplication of activities, leading to overspending and legal uncertainty? The assessment depends on the perspective from which the overlap is analysed.

We have identified at least two perspectives that might be taken: the public law postulate of the precise delimitation of authorities' competence or a concept of extended accountability explored by Colin Scott (2000). The first perspective, associated with the critique of the overlap of competence, suggests it might be problematic because it makes it more difficult to precisely delimit the boundaries of competence. In this

66 Hajduk (n 14).

67 Although Meta Platforms challenged the EDPB's opinion on Pay or Consent to the CJEU; cf. Meta Platforms Ireland v European Data Protection Board (Case T-319/24) [2024] OJ C 4865, 12 August 2024, challenging the European Data Protection Board's opinion regarding Pay or Consent under the GDPR <http://data.europa.eu/eli/C/2024/4865/oj>.

68 European Commission, 'Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act' (European Commission Press Corner, 25 March 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689> accessed 28 May 2024.

69 Norwegian Data Protection Authority, 'Request for an EDPB opinion on consent or pay' (Datatilsynet, 2024) <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2024/request-for-an-edpb-opinion-on-consent-or-pay/> accessed 28 May 2024.

70 European Data Protection Board, 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' (Adopted 17 April 2024) <https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf> accessed 28 May 2024; The legal problems of the "pay or consent" model are not analysed in this paper.

71 The inaugural meeting of the High-Level Group took place in May 2024, following Article 40 of the DMA; cf. European Commission, 'Inaugural Meeting of DMA High-Level Group' (12 May 2023) <https://digital-markets-act.ec.europa.eu/inaugural-meeting-dma-high-level-group-2023-05-12_en> accessed 7 June 2024.

72 The GDPR and the DMA have parallel fines that can be imposed by the DPAs under the GDPR and, in the latter, by the Commission. It also touches on the issue of double jeopardy in EU administrative law. Cf. Case C-117/20 bpost SA v Autorité belge de la concurrence [2022] ECLI:EU:C:2022:202; see also: Alba Ribera Martínez, 'Hate the game, not the player: the double jeopardy principle in bpost and Nordzucker applied to the Digital Markets Act's enforcement' (24 June 2022) <https://ssrn.com/abstract=4145758> accessed 28 May 2024.

vein, the literature has discussed the disadvantages of overlap, which include increased legal uncertainty, higher costs, and inconsistency.[73] Conversely, the second perspective recognises the potential advantages of overlap of competence, which we investigate through the lenses of extended accountability in the EU digital regulation. We consider that these two perspectives exhaust the scrutiny of the phenomenon of overlap of competence, nor that the first perspective is purely critical and does not allow for a nuanced approach. However, we believe that extended accountability is less explored and that its framing is helpful by presenting such a dichotomy.

To better understand the extended accountability in digital regulation, we first provide a broader setting. The complexity of the EU regulation of digital technologies reflects the complexity of the socio-technical change brought by digital technologies. Andrew Murray introduced the concept of network communitarianism[74] to describe the interconnected networks that operate in cyberspace.[75] He argued that any individual in cyberspace is not a solitary entity but is instead part of intertwined networks with diverse values, intersecting with each other and governed by different forces (like law, social norms, dynamics of the market, and design).[76] It can be inferred that the regulation of such a complex socio-technical system must take this complexity into account; this leads to the establishment of an elaborate enforcement system. Not every complex enforcement system must lead to an overlap of competence, as it is conceivable that boundaries of competence are distinguished clearly from the other. However, this requires not only a clear division of competence but also the material scope of legal acts. If the material scope of legal acts is not clearly separated (e.g., the GDPR vis-à-vis the Digital Services Act), this will result in the competence of the authorities appointed to enforce them overlapping.

The overlap of enforcement structures within EU digital regulation may be recognised as a part of a decades-long debate about the evolution of the government within the modern state. At the turn of the Second World War, there was a prominent discussion between Carl Friedrich and Herman Finer on how government should function in the modern state.[77] Finer, in his publications, including "*Administrative Responsibility in Democratic Government*" (1941),[78] argued for a distinction between administration (accountability for administrative decisions) and politics (responsibility for political decisions), advocating that a hierarchy should be maintained to ensure democratic legitimacy. In turn, Friedrich, in his works, including "*Public Policy and the Nature of Administrative Responsibility*" (1940),[79] claimed that a rigid hierarchical governmental system was no longer sustainable due to the modern government's increasing complexity and size. He emphasised that essential functions not only in policy execution but also in policymaking have shifted from politicians to administrative agencies, making the model of vertical political responsibility deficient. This dynamic of change in modern government applies to the EU regulation on digital technologies, as it requires capturing the complexity of 1) the multifaceted, networked, and entangled subject of regulation, i.e. digital

73 Lachlan Robb, Trent Candy, and Felicity Deane, 'Regulatory Overlap: A Systematic Quantitative Literature Review' (2023) 17 Regulation & Governance 1131; This paper by academics in Australia provides a comprehensive review of the literature for the 'regulatory overlap' phenomenon, including its identified benefits and shortcomings.

74 The concept of "network communitarianism" draws from the Actor-Network Theory and Social Systems Theory; Cf. E. Kanellopoulou and N. F. Ntounis, 'Network Communitarianism as a tool for stakeholder engagement in places: The case of Rog Factory', presented at the Inclusive Placemaking - 4th Institute of Place Management International Conference, Manchester, UK, 7–8 September 2017 <https://e-space.mmu.ac.uk/619141/1/Network%20Communitarianism%20as%20a%20Tool%20for%20Stakeholder%20Engagement%20in%20Places%20(1).pdf> accessed 28 May 2024.

75 We do not discuss the term "cyberspace" or its relationship to the term "digital technologies". We assume that the establishment and development of cyberspace is an effect of the deployment of digital technologies.

76 Andrew D. Murray, 'Nodes and Gravity in Virtual Space' (2011) 5 Legisprudence 195, 204-210.

77 Overview of this debate in Michael Jackson, 'Responsibility versus Accountability in the Friedrich- Finer Debate' (2009) 15(1) Journal of Management History 66; T. Schillemans and M. Bovens, The Challenge of Multiple Accountability: Does Redundancy Lead to Overload?' in M. Dubnick and H. Frederickson (eds), Accountable Governance Problems and Promises (Routledge 2011) 3-21; References to the original works of Finer and Friedrich were based on these works.

78 Cf. Herman Finer, 'Administrative Responsibility in Democratic Government' (1941) 1(4) Public Administration Review 335; Herman Finer, 'Better Government Personnel' (1936) 51(4) Political Science Quarterly 569.

79 Cf. Carl J. Friedrich, 'Public Policy and the Nature of Administrative Responsibility' (1940) 1 Public Policy 1.

technologies; 2) the phenomenon of the regulatory state within the EU;[80] 3) the unique legal construction of the EU, situated between an international law entity and a federal state.

We investigated networked communitarianism and the Friedrich-Finer debate to give a context allowing us to segue into the concept of extended accountability explored by Colin Scott in a paper, "*Accountability in the Regulatory State*", written more than two decades ago (2000). Scott defines accountability[81] as "*a liability to reveal, to explain, and to justify what one does; how one discharges responsibilities, financial or other, whose several origins may be political, hierarchical or contractual,*" indicating that previously it has been applied by public lawyers narrowly to "*encompass the formal duties of public bodies to account for their actions to ministers, Parliament, and to courts*".[82]

He distinguishes three variables of accountability: 1) who is accountable? 2) to whom? and 3) for what?[83] He argues that the classic understanding of accountability is inadequate in the reality of the regulatory state.[84] Therefore, he explores the concept of extended accountability. He distinguishes three types of accountability: 1) horizontal accountability, referring to other entities at the same level of governance; and two vertical types, namely 2) upwards accountability, which includes accountability of regulatees to regulators, as well as lower-level bodies to higher-level bodies and courts; 3) downwards accountability understood as accountability towards the market and individuals, also in the face-to-face interactions with them.[85] These various types of accountability taken together create the possibility for the emergence of extended accountability in the context of "*the existing dense networks of accountability associated with both public and private actors concerned with the delivery of public service.*"[86]

Scott discusses two variants of extended accountability: interdependence and redundancy. Interdependence assumes that the actions of authorities are mutually dependent "*because of the dispersal of key resources of authority (formal and informal), information, expertise, and capacity to bestow legitimacy such that each of the principal actors has constantly to account for at least some of its actions to others within the space, as a precondition to action.*"[87] In turn, redundancy is understood as "*overlapping (and ostensibly superfluous) accountability mechanisms [that] reduce the centrality of any one of them.*"[88] If one of the regulators fails, the other will be in place to counteract the overall failure of the enforcement system.[89]

Interdependence and redundancy can intertwine and be applicable simultaneously. Therefore, they should be understood as variants rather than features of extended accountability because they are not indispensable elements of every extended accountability model. It is possible to have a redundancy without an interdependence or interdependence without a redundancy. Redundancy, however, usually induces interdependence. For example, since parallel enforcement structures are part of a system of EU administrative law, they are bound by general obligations of cooperation, such as the principle of sincere cooperation (Article 4(3) TEU) or because of the need to observe the *ne bis idem* principle.

Scott is attentive to the risks inherent in both interdependency and redundancy. Regarding interdependency, he points out the risk of regulatory capture by one or a few elements of the accountability system. Concerning redundancy, alongside the risk of regulatory capture, he notes the challenge of delineating between appropriate and excessive redundancy.[90] We believe these risks are also relevant in regulating digital technologies.

80 On the concept of regulatory state, cf. G. Majone, 'From the positive to the regulatory state: Causes and consequences of changes in the mode of governance' (1997) 17(2) Journal of Public Policy 139-167; G. Majone, 'The regulatory state and its legitimacy problems' (1999) 22(1) West European Politics 1-24.
81 Following E.L. Normanton's definition in Scott (n 9).
82 Scott (n 9) 41.
83 Scott (n 9) 41.
84 Scott (n 9) 41.
85 Scott (n 9) 41.
86 Scott (n 9) 40.
87 Scott (n 9) 50.
88 Scott (n 9) 52-53.
89 Scott (n 9) 52-53.
90 Scott (n 9) 60.

6. Extended Accountability in EU Regulation of Digital Technologies

Extended accountability can be employed to understand the enforcement structures of EU regulation of digital technologies. The overlap of EU legal acts regulating digital technologies leads to the overlap of enforcement structures, which creates a redundant and interdependent enforcement system.[91] This is because the overlap of the material scope of these acts causes the overlap of authorities established to enforce them. In other words, since the interpretation of principles-based and risk-based laws leads to more than one authority assessing the legality of a factual state, there is an overlap. The extended accountability allows for not leaving any of these authorities as an isolated point but positioning them as elements of the EU's enforcement system of digital technologies.

In this system, the position of data protection authorities (DPAs) remains unique as their independence and the role of protectors of fundamental rights is enshrined in the Charter of Fundamental Rights (CFR).[92] The structural and functional separation of DPAs from other elements of the executive branch is key for DPAs to exercise their role. Introducing new enforcement structures through adopting new legal acts, encroaching on the material scope of the GDPR, may weaken the DPAs' position by *de facto* carving out DPAs' competence.

This should be considered when discussing the relationships between these authorities. DPAs should remain a central point of this system due to their role in the CFR. However, this does not preclude the establishment of other authorities that are directly or indirectly (aimed at) protecting the rights to privacy and personal data protection. In fact, establishing new or using already existing authorities may strengthen such protection by utilising other tools, such as remedies under competition law, especially given the operational limitations of DPAs. More than five years of enforcing GDPR have revealed that the DPAs have limited resources to handle all cases effectively. As a result, the DPAs make decisions on priorities,[93] and they can address only selected cases, which they then use as examples for regulatees, leaving many matters inadequately enforced.[94]

This situation reveals an opportunity for improved protection of fundamental rights through the engagement of more authorities (redundancy). When DPAs struggle to enforce GDPR (i.e. protect fundamental rights), other authorities may assist, using their competence within their remit. It can be argued that since DPAs are obliged to safeguard fundamental rights, and yet they fail to do so, it cannot be assumed that other authorities can do what DPAs cannot. An alternative, therefore, could be to strengthen DPAs' funding. True, there is no guarantee that this model will be more effective. This, however, is the model that the EU legislator adopted in the post-GDPR laws, and there is no practical retreat from this; therefore, ways to benefit the protection of fundamental rights from this model should be sought.

Moreover, there are at least two reasons to assume that this model offers a chance for better protection. Firstly, issues concerning the practical functioning of DPAs arise primarily from how their budgets are allocated. While the GDPR was adopted at the EU level, budget decisions are made by individual Member States. Additionally, there is a noticeable trend in recent EU legislation (such as the DSA, DMA, and partially the AI Act) towards centralising enforcement at the Commission level, particularly for the biggest entities. This could facilitate more adequate funding at the EU level.

91 Cf. Section 2 and the literature cited therein.

92 Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 8; Cf. also Maria Magierska, 'What Role for the Data Protection Authorities During the COVID-19 Pandemic?' in Filipe de Abreu Duarte and Francesco Palmiotto (eds), Sovereignty, Technology and Governance After COVID-19: Legal Challenges in a Post-Pandemic Europe (Hart Publishing 2022) 193.

93 The challenges with GDPR enforcement include procedural differences between Member States, the partial harmonisation of which is currently the subject of a legislative initiative; European Digital Rights (EDRi), 'GDPR Enforcement: Rights, Redress, and Representation' (EDRi, May 2024) <https://edri.org/wp-content/uploads/2024/05/EDRi_GDPR-Procedural-position-paper.pdf> accessed 4 June 2024.

94 Cf. M. Koomen and R. MacDonald, 'Enforcement in an age of accelerated innovation' (The International Center for Future Generations, June 2024) <https://icfg.eu/enforcement-in-an-age-of-accelerated-innovation/> accessed 7 June 2024.

Secondly, it is unfounded to assume that all problems related to protecting fundamental rights to privacy and personal data can be solved by the tools in the GDPR. For example, attempting to balance the dominant position of the biggest entities through the tools of the DMA, competition law and consumer protection law can strengthen this protection, as breaches of data subjects' rights may also constitute an abuse of the dominant position and consumer rights. Furthermore, these authorities have complementary expertise to the DPAs, which makes it possible to achieve synergies using competition law theories or the experience of cybersecurity authorities in security-related data breaches. Finally, more speculatively, the activity of other redundant authorities within the same system may lead to positive pressure on other competent authorities to act so as not to be perceived as passive.

Ultimately, even if better protection is not achieved in the end, this does not preclude the efforts of undertaking a reflection on the nature of the relationship between these multiple enforcement structures, for what is postulated is not always achieved, which, however, as an experiment, might provide insights for the future.

7. Steps to Address Fragmented Cross-Regime Cooperation in Post-GDPR Legal Acts

The EU regulation of digital technologies creates a mosaic enforcement system with redundancies and interdependencies. However, if appropriately handled and developed, it could enhance the protection of fundamental rights. The risk of lack of coherence is the price for such hopes. DPAs should maintain a central role in this system, as demonstrated above. Hence, a mature framework for cross-regime cooperation is needed.[95] This section examines these cross-regime cooperation instruments in post-GDPR laws at the EU and national levels, focusing on the DSA, the DMA and the AI Act.

The legal instruments at the EU level for cross-regime cooperation are the collegiate bodies: the European Board for Digital Services (EBDS in the DSA),[96] the European Artificial Intelligence Board (EAIB in the AI Act),[97] and the High-Level Group (in the DMA).[98] The High-Level Group comprises "*European bodies and networks*", including EDPS and EDPB.[99] In turn, the EBDS[100] and the EAIB[101] are composed of national enforcement authorities' representatives and the Commission (without voting). The competence of the Boards is not homogeneous, but they are focused on harmonising enforcement and fostering cross-regime coherence by issuing guidance and recommendations[102] and, in the case of High-Level Group, reports assessing "*the interactions between (...) sector-specific rules*".[103]

95 Cf. remarks on "cross-sectoral fragmentation" in Mark Cole and Christina Etteldorf, 'The Implementation of the GDPR in Member States' Law and Issues of Coherence and Consistency' in Inge Graef and Bart van der Sloot (eds), The Legal Consistency of Technology Regulation in Europe (Hart Publishing 2024) 131 <http://dx.doi.org/10.5040/9781509968053.ch-007> accessed 16 June 2024.

96 Digital Services Act (DSA), art 61(1).

97 AI Act, art 65(1).

98 Digital Markets Act (DMA), art 40(1).

99 Digital Markets Act (DMA), art 40(1).

100 Digital Services Act (DSA), art 61(2).

101 AI Act, arts 65-66.

102 In the DSA, it is Article 63 in conjunction with Article 61(2); in the AI Act, it is Article 66, especially (h).

103 Digital Markets Act (DMA), art 40(5); Additionally, cf. Article 46(1)(g) DMA.

The Boards mimic the European Data Protection Board,[104] although they do not confer their unique powers.[105] While they will contribute to coherence within a given regime, they may be moderately effective for cross-regime coherence. First, surprisingly, at least some of the Boards (the EBDS)[106] do not include permanent representatives from either the EDPB or the EDPS, while in others (the EIAB), EDPS participates only as an observer.[107] Secondly, their work is generally based on voluntary participation and initiative, so it may take significant time to influence how individual authorities exercise their competence.

The situation appears more complex at the national level. The DMA does not provide for establishing enforcement authorities at the national level,[108] but the DSA and the AI Act (in the ecosystem model) envisage such authorities.[109] The provisions of the DSA are, nevertheless, rather succinct regarding cross-regime cooperation between Digital Services Coordinators (DSCs) and other enforcement authorities. Such instruments can be derived from the general provisions establishing DSCs, which acknowledge the possibility of establishing cross-regime cooperation at the national level.[110]

The AI Act introduces more elaborate cooperation provisions at the national level. We will only focus on a selected few aspects. Firstly, the AI Act mentions DPAs as a relevant reference point, including as an authority to be informed of each use of the real-time biometric identification system and an authority whose competence should remain without prejudice.[111] The legislator acknowledges the DPAs in the enforcement structures of the AI Act.[112] Secondly, the key instrument of cooperation is based on a fundamental rights lens, as market surveillance authorities are obliged to cooperate with authorities "*which (...) enforce the respect of obligations under Union law protecting fundamental rights.*"[113] DPAs should be counted as one.[114] Such cooperation includes exchanging information and "*full cooperation*" in the evaluation of AI systems "*where risks to fundamental rights are identified,*"[115] Market surveillance authorities are also obliged to inform about "*a serious incident*" leading to "*the infringement of obligations (...) intended to protect fundamental rights,*"[116] which should give knowledge to DPAs to act within their remit. Finally, the AI Act includes pinpoint references to cooperation with other authorities (including DPAs) regarding specific solutions, such as regulatory sandboxes,[117] as well as in issuing soft law "*in areas covered by other Union law*".[118]

104 On the concept of mimesis of post-GDPR lawmaking, cf de Hert (n 2).

105 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 (General Data Protection Regulation) [2016] OJ L 119/1, ch VII.

106 Digital Services Act (DSA), art 62; Recital (134) of the DSA admits the possibility of (at least incidental) cooperation with EDPB or EDPS: "In view of possible cross-cutting elements that may be of relevance for other regulatory frameworks at Union level, the Board should be allowed to cooperate with other Union bodies (...) with responsibilities in fields such as (...) data protection, electronic communications, (...) consumer protection, or competition law".

107 AI Act, art 65(2).

108 The Digital Markets Act (DMA) includes provisions for cooperation with national authorities; see Article 37 of the DMA. For a discussion on the relationship between the European Commission as the DMA's enforcer and national competition authorities, see: Alba Ribera Martínez, 'The Decentralisation of the DMA's Enforcement System' [2024] SSRN <https://ssrn.com/abstract=485723> accessed 9 November 2024.

109 While DPAs may be designated as competent authorities, Member States are expected to designate other authorities than DPAs.

110 Article 49(2) of the DSA supplemented by the Recital (110): "Moreover, in addition to the specific mechanisms provided for in this Regulation as regards cooperation at Union level, Member State should also ensure cooperation among the Digital Services Coordinator and other competent authorities designated at national level, where applicable, through appropriate tools, such as by pooling of resources, joint task forces, joint investigations and mutual assistance mechanisms."

111 AI Act, recital 157.

112 In addition, they have been explicitly designated as market surveillance authorities to a limited extent (n 62).

113 AI Act, art 77.

114 Hajduk (n 2).

115 AI Act, arts 79(2), 82(1).

116 AI Act, art Article 73(7) in conjunction with Article 3(49)(c).

117 For example, AI Act, art 57(4), see also: AI Act, recital 36.

118 AI Act, art 70(8).

Particularly noteworthy is the solution adopted in the NIS 2 Directive, a post-GDPR cybersecurity legal act.[119] Following the obligation to exchange information, Article 35(2) provides that if the DPAs impose a fine under the GDPR, the cybersecurity authorities cannot impose an administrative fine under the NIS 2 Directive to sanction the same conduct constituting a breach of obligations under the Directive.[120] This solution should be assessed as an uncommon but sound way to address how the relationship of other authorities to DPAs is shaped at the EU law level. Still, beyond the scope of this provision is, for example, how to decide whether a fine relates to the same conduct of a regulated entity, i.e. what criteria to adopt that this identity exists or not.

In conclusion, although post-GDPR legal acts recognise this risk, they offer only fragmented and overly broad cross-regime cooperation instruments. Specifically, it is unclear in which situations this cooperation should be initiated, how procedural actions should be executed, whether cooperation is mandatory, and what the consequences of failing to cooperate might be.[121] It would be beneficial to introduce precise instruments for cross-regime cooperation within these legal acts at the EU level. This includes specifying the situations in which cooperation should occur, the procedures, and the consequences of lack of cooperation. The EU legislator appears hesitant to regulate these matters, probably due to the procedural and institutional autonomy of the Member States, leaving blanks to be filled by them. However, this ongoing work by the Member States means that 27 legislators will be deciding on these issues, with the risk of deepening the patchwork enforcement system.

8. *Meta* Case: Shaping of the Cross-Regime Cooperation Framework

Cross-regime cooperation instruments have been introduced in an unsatisfactory manner. In such a case, jurisprudence comes to the fore. The judgement in the Meta case is a significant step in shaping the path towards a cooperation framework. It paves the way for authorities other than DPAs to deal incidentally with data protection matters in close cooperation with DPAs. It can be recognised as part of a broader trend emerging to establish extended accountability in the EU regulation of digital technologies, which supplements the actions of the EU legislator.

The case was rendered in response to a request for a preliminary ruling by a German court in proceedings between *Meta* and the German competition authority (*Bundeskartellamt*),[122] which identified Meta's practices as an abuse of dominant position.[123] We will not discuss substantive issues, only those relating to cooperation between competition authorities and DPAs.[124]

119 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80, arts 21, 23.

120 It should be interpreted with the obligations to exchange information under Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [2022] OJ L333/80, art 35(1).

121 Cf. Hajduk (n 14) for analysis of cross-regime cooperation instruments in the DGA, the Data Act, and the European Health Data Space Regulation Proposal.

122 It should be noted that the Bundeskartellamt's official summary of decision (Bundeskartellamt, Case Summary, 15 February 2019, 'Facebook, Exploitative Business Terms Pursuant to Section 19(1) GWB for Inadequate Data Processing' (Sector: Social Networks) (Ref: B6-22/16, Date of Decision: 6 February 2019), Bundeskartellamt <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3> accessed 28 May 2024) demonstrates that the German competition authority cooperated with the DPAs during the proceedings. This means that the German competition authority, even without the CJEU judgement, correctly interpreted the need to cooperate.

123 CJEU (n 8) paras 1-2, "concerning the decision by which that authority prohibited processing certain personal data as provided for in the general terms of use of the social network Facebook"; Cf. Inge Graef, 'Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment' (2023) 30(3) Maastricht Journal of European and Comparative Law 325; Maciej Barczentewicz, 'The CJEU's Decision in Meta's Competition Case, Part 2: Sensitive Data and Privacy Enforcement by Competition Authorities' (6 July 2023) <https://www.barczentewicz.com/post/the-cjeus-decision-in-metas-competition-case-part-2-sensitive-data-and-privacy-enforcement-by-competition-authorities/> accessed 28 May 2024.

124 The CJEU's reasoning in paras. 36-63 (n 8); "Subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding

From the *Meta* ruling, it follows that authorities other than DPAs may incidentally determine whether the processing of personal data complies with the GDPR if this is necessary to assess the prerequisites and take a decision that remains in their remit. The meaning of the term "*necessity*" of data protection matters for determining a decision by another authority remains elusive. However, such a determination cannot be made arbitrarily; it should be made in close cooperation with DPAs, following the duty of loyal cooperation.[125] This positions the DPA as the focal point in resolving all matters relating to the processing of personal data.[126]

The CJEU outlines how cooperation between DPAs and other relevant authorities should function. The requirements are as follows: (1) if a DPA issues a decision, other authorities should adhere to it without deviation; (2) however, if there is a doubt as to the scope of the DPA's decision, if a DPA is conducting an investigation or if another authority makes a preliminary finding of non-compliance with the GDPR, then that another authority is required to consult with the DPA for clarification or to request a decision from the DPA (in which case the first point applies); (3) if the DPAs do not respond within a reasonable timeframe, the other authority may decide at its discretion.

It is valuable that the CJEU provided guidance on cross-regime cooperation for the EU digital regulation enforcement system. However, several questions remain unresolved, including: How will the deviation from the DPA decision be assessed (how can the scope of *res judicata* of DPAs' decisions be determined)? What are the procedural implications if the DPAs determine that there has been no infringement of the GDPR?[127] Which matters will require DPA consultation, i.e. what is the limit of "*necessity*"? What defines "*a reasonable time*" if a pending case before the DPAs is delayed? By asking these questions, we can better reflect on how to establish more mature rules for cross-regime cooperation.

9. Developing Cross-Regime Cooperation via Hard Law (Option 1)

Although the judgement in the *Meta* is a significant step in shaping cross-regime cooperation between authorities, establishing a mature cooperation framework is only at its beginning. What is the path forward? Below, we discuss selected ways of straightening coherence: the role of national and EU courts, the actions that the EU and national legislators may take, and the role of the enforcement authorities themselves.

The role of national and EU courts should be considered separately. The judicial branch helps to harmonise different authorities' actions through judicial review, establishing a cohesive body of case law that all relevant authorities within different enforcement structures should follow. Achieving coherence this way has its limitations because it is applied *ex-post*, and due to procedural reasons, it takes a long time before a case is resolved.

is necessary to establish the existence of such an abuse. Given this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with Regulation 2016/679, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation."

125 Consolidated Version of the Treaty on European Union [2012] OJ C326/13, art 4(3).

126 As Graef underlines, the decisions of DPAs are binding on other authorities in personal data matters, but it is not a foregone conclusion that this works the other way round, meaning that decisions of other authorities are not binding to DPAs Cf. Graef (n 123).

127 Cf. Peter J. van de Waerdt, 'Meta v Bundeskartellamt: Something Old, Something New' (2024) 2023 European Papers-A Journal on Law and Integration 1077-1103.

Therefore, establishing procedures for cooperation directly within EU legal acts would improve cross-regime cooperation. However, this is constrained by the principle of procedural and institutional autonomy of the Member States.[128] After their adoption, post-GDPR legal acts are institutionally and procedurally integrated into the administrative law of Member States, resulting in a heterogeneous system across Member States. The establishment of national enforcement structures for post-GDPR legal acts is still in progress. In light of the *Meta* case, it may be beneficial to consider introducing cross-regime cooperation instruments at the Member State level to address individual cases and soft law. Below, this paper discusses how such instruments could be shaped.

Instruments of cooperation at the national level in individual cases are needed to reduce the risk of double jeopardy and to alleviate the risk of situations where certain behaviours are prohibited under one legal regime but considered lawful under another. It may be beneficial to discuss separately those legal acts inextricably linked to the right to personal data protection (such as the DGA and the Data Act). Under these legal acts, DPAs should be designed directly as the sole enforcement authorities. Conversely, for legal acts related to the regulation of digital platforms in the context of competition and consumer protection laws (such as the DMA and DSA), DPAs could have the power to provide binding opinions on individual cases involving data protection matters. This approach aligns with the *Meta* judgement and could prevent an overemphasis on the role of DPAs.

The challenge with this approach lies in determining the criteria for categorising a given legal act. This would necessitate an analysis of the main objectives associated with each legal act. Unfortunately, this determination may often be somewhat arbitrary. Identifying the primary objectives of a legal act can be complicated. However, it is hard to envision an alternative to this proposal, as a current unstructured approach poses a risk of creating a confusing array of enforcement structures across Member States.

10. Developing Cross-Regime Cooperation via Soft Law (Option 2)

To achieve more coherent legal interpretation across various legal regimes, it is needed to establish cooperation between authorities in issuing soft laws. It might be argued that such cooperation allows for more latitude as soft law documents do not entail direct legal consequences.

Initially, it is essential to map issues on which the authorities' remit overlap across the whole EU digital regulation. Following this, cooperation on soft law could occur, which may be issued, depending on the competence provisions, either separately or together. Additionally, establishing coordination bodies at the national level could serve as intermediaries between various legal regimes. Such solutions have already been adopted, for example, in the UK through the Digital Regulation Cooperation Forum[129] and in the Netherlands through the Digital Regulation Cooperation Platform[130] (*Samenwerkingsplatform Digitale Toezichthouders*). Such national coordinating bodies could help issue soft laws and coordinate actions. Cooperation instruments at the national level should not modify the remit or competence of individual enforcement authorities.

At first, it may seem counterintuitive. After all, if the challenge is that there are multiple bodies in the enforcement system, what is the purpose of setting up another one? It can be argued that, however, since the system is already extensive, introducing an additional body that focuses solely on coordinating existing ones to increase their coherence should benefit from removing the duplication of efforts, for example, by utilising a dedicated task force (of representatives) from different authorities dealing with the same issue within their remit. However, proving the effectiveness of this approach is challenging. An empirical,

128 Cf. Analysis of the principle of procedural autonomy by Diana-Urania Galetta, Procedural Autonomy of EU Member States: Paradise Lost?: A Study on the "Functionalized Procedural Competence" of EU Member States (Springer 2010) 1–145.

129 Information Commissioner's Office, 'Digital Regulation Cooperation Forum' (ICO, 2024) <https://ico.org.uk/about-the-ico/what-we-do/digital-regulation-cooperation-forum/> accessed 4 June 2024.

130 Autoriteit Consument en Markt, 'Digital Regulation Cooperation Platform (SDT)' (ACM, 2024) <https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt> accessed 4 June 2024.

qualitative study would be necessary to demonstrate that a coordinating body offers benefits compared to the jurisdiction in which such a body does not operate.

Given the numerous enforcement structures at the Member States and the EU levels, a similar coordinating body could also be established at the EU level. Indeed, the EDPS brought forward such a proposal almost a decade ago, calling for establishing a Digital Clearing House.[131] It was envisaged as a network of contact points for enforcement authorities in the digital sector (including the telecoms) at the national and EU levels with two criteria for membership: a common objective to promote the regular exercise of their competencies and a willingness to cooperate and exchange information. It would have five tasks: 1) Discussing (but not deciding) the application of the most appropriate legal act for specific cases and EU coordination of the application of individual acts; 2) Employing data protection law and consumer protection law to formulate theories of harm for competition law purposes; 3) Discussing the actions of authorities where personal data is a crucial asset as an alternative to new legislation for the sector; 4) Consulting on the consequences of the application of remedial powers in individual cases; 5) Fostering informal cooperation between European administrative networks, e.g., the European Competition Network and the European Consumer Protection Network. This proposal was based on the identified potential synergy between data protection law, competition law and consumer protection law concerning Big Data technology.[132] It would be worthwhile to revisit this idea.[133] The basic premise, i.e., achieving coherence and synergy, remains valid. National coordinating bodies could serve as contact points at the EU level. This would create an elaborate connecting point that could improve the handling of redundancy and strengthen the exercise of interdependencies.

Finally, an effective enforcement system goes beyond well-crafted legal acts. It also requires the authorities' appropriate, cooperation-oriented attitude, which partially depends on Member States' administrative cultures and might also be hampered by political goals. Finally, even the best laws can change little if authorities lack the human and financial resources.

11. Conclusions

The EU has been developing a comprehensive proposal in the post-GDPR legal acts regulating digital technologies. Problems with effective enforcement within the EU single market (digital technologies) are recognised as a serious challenge to be addressed.[134] Whether Europe will be *"fit for the Digital Decade"*[135] will depend on the effectiveness of the enforcement. This system could be envisaged as a coherent, cross-border, cross-regime cooperative system. It can be tempting to argue that this ambitious EU project of regulating digital technologies is destined to fail. In our view, such a statement would be premature as post-GDPR legal acts have strengths that need to be explored.

131 European Data Protection Supervisor (EDPS), 'Opinion on the coherent enforcement of fundamental rights in the age of Big Data' (23 September 2016) <https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 4 June 2024.

132 European Data Protection Supervisor (EDPS), 'Opinion on the coherent enforcement of fundamental rights in the age of Big Data' (23 September 2016) <https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf> accessed 4 June 2024; EDPS has launched an initiative to discuss the renewed idea of a Digital Clearinghouse 2.0 on the occasion of its 20th anniversary; EDPS, 'Towards a Digital Clearinghouse 20' (EDPS 20th Anniversary, 2024) <https://20years.edps.europa.eu/en/initiatives/towards-digital-clearinghouse-20> accessed 7 June 2024.

133 EDPS has launched an initiative to discuss the renewed idea of a Digital Clearinghouse 2.0 on the occasion of its 20th anniversary; EDPS, 'Towards a Digital Clearinghouse 20' (EDPS 20th Anniversary, 2024) <https://20years.edps.europa.eu/en/initiatives/towards-digital-clearinghouse-20> accessed 7 June 2024.

134 E. Letta, 'Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens' (Council of the EU, April 2024) <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf#page=4.14> accessed 4 June 2024.

135 European Commission, 'A Europe Fit for the Digital Age' (European Commission, 2024) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en> accessed 6 June 2024.

Therefore, in this paper, we analysed the concept of extended accountability to frame the proliferation of enforcement structures and propose a path forward. Based on the existing literature, this paper establishes that there is an overlap between the EU legal acts regulating digital technologies, which causes an overlap of the enforcement structures (with a diverse range of models) established to enforce these legal acts. At the same time, cross-border cooperation instruments adopted in these acts at the EU level seem unclear and insufficient.

The concept of extended accountability, inspired by the debate in the common law tradition, can be helpful to understanding the current situation and foster the evolution towards a more coherent system, in which redundancy and interdependence provide an opportunity to improve overall enforcement. Such a cooperation framework is already being developed following the CJEU judgement in the *Meta* case. Meanwhile, it is necessary to carefully structure instruments of cross-regime cooperation to maintain the unique position of DPAs enshrined in the CFR. In the final parts of the paper, we offered our proposal for developing more mature cross-regime cooperation instruments based on the *Meta* judgment as a starting point. It cannot be excluded that, in the coming years, there will be legislative initiatives at the EU level to clarify the situation of the enforcement system of the EU digital regulation. The activities of the new Commission on this are certainly worth following.

This paper invites further discussion on the redundancy and interdependence within EU regulation of digital technologies. This debate is still in its early stages, and several substantial issues are worth exploring in further research. First, it would be beneficial to analyse what quantitative tools could be used to measure the impact of cross-regime cooperation instruments on enforcement effectiveness. The second issue relates to the legitimacy of cross-regime cooperation. While such instruments may be welcome from the regulatory perspective, they may raise concerns among constitutional lawyers regarding the limitations of the executive branch to act within the confines of the law. The third issue involved the independence of these authorities in practice, including their financial autonomy in relation to the government's influence and the risks of their misuse to pursue political goals. The last issue may be investigated more clearly in the next year or two as the structures enforcing post-GDPR laws are established nationally.