

cerre

Centre on Regulation in Europe




REPORT

January 2022

Giorgio Monti
Alexandre de Stree

**IMPROVING EU
INSTITUTIONAL DESIGN
TO BETTER SUPERVISE
DIGITAL PLATFORMS**



The project, within the framework of which this report has been prepared, was supported by the following members of CERRE: AGCOM, Airbnb, Arcep, BIPT, Booking.com, Huawei, Meta, Microsoft, and Ofcom.

As provided for in CERRE's bylaws and procedural rules from its 'Transparency & Independence Policy', all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of member of CERRE.

The authors would like to thank Pierre Larouche for his peer review and Vasileios Tsoukalas for his great work as a research assistant on this report. They are also grateful for the representatives of the European Banking Institute (EBI), the Netherlands Authority for Consumers and Markets (ACM), and the European Union Agency for Cybersecurity (ENISA) who attended the private workshop of this project.

© Copyright 2022, Centre on Regulation in Europe (CERRE)

info@cerre.eu

www.cerre.eu

Table of contents

About CERRE	5
About the Authors	6
Executive Summary	8
1 Introduction	13
2 Institutional Design to Supervise Digital Platforms	15
2.1 The national regulators and their characteristics	15
2.1.1 National regulators as the keystone of EU regulation	15
2.1.2 The EU’s continued strengthening of national regulators	16
2.2 Models of decentralised oversight and enforcement.....	17
2.2.1 Country of origin and countries of destination	17
2.2.2 The logic and the challenge of different models of decentralised enforcement.....	18
2.3 Cross-country coordination	20
2.3.1 Networks of regulators – an overview.....	20
2.3.2 Regulatory networks – issues for discussion.....	22
2.4 Cross-regime coordination	23
2.4.1 Coordination through legal mechanisms	23
2.4.2 Coordination through institutional mechanisms	25
2.5 Centralised oversight and enforcement.....	26
3 Coordination in Practice	30
3.1 Coordination with a policy dimension.....	30
3.1.1 The NIS Directive	30
3.1.2 Policy choices in cybersecurity: 5G Toolbox.....	31
3.2 Cross-country coordination	33
3.2.1 Data protection law: European Data Protection Board.....	34
3.2.2 The e-Commerce Directive	35
3.2.3 Consumer protection laws: Consumer Protection Cooperation Network	35
3.2.4 Competition law: European Competition Network.....	36
3.2.5 The European Electronic Communications Code: Body of the European Regulators for Electronic Communications.....	38
3.3 Cross-regime coordination	40
3.3.1 Coordination at the national level	40
3.3.2 Coordination at the EU level	42
4 An Example of Semi-centralisation: Banking Union	45
4.1 Origins	45
4.2 Operation	46
4.2.1 Significant banks	46
4.2.2 Smaller banks	47
4.3 Lessons learned.....	47

5 Conclusions and Recommendations..... 50

- 5.1 Characteristics of effective and legitimate regulatory authorities.....50
- 5.2 Coordination between national authorities and EU networks52
- 5.3 Semi-centralising enforcement at an EU body54
 - 5.3.1 Benefits and costs of centralisation..... 54
 - 5.3.2 Semi-centralisation at the European Commission 55
 - 5.3.3 Semi-centralisation at a European platform authority 57
 - 5.3.4 National authorities in support of the semi-centralised enforcement..... 60
- 5.4 Principles of good regulatory style62
 - 5.4.1 Principles of good regulation 62
 - 5.4.2 Participatory regulation 63

About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality; and
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of service providers, to the specification of market rules, and to improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims to clarify the respective roles of market operators, governments, and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the Authors



Giorgio Monti is a CERRE Research Fellow and a Professor of Competition Law at Tilburg Law School. He began his career in the UK (Leicester 1993-2001 and London School of Economics 2001-2010) before taking up the Chair in competition law at the European University Institute in Florence, Italy (2010-2019). While at the EUI he helped establish the Florence Competition Program which carries out research and training for judges and executives. He also served as Head of the Law Department at the EUI. His principal field of research is competition law, a subject he enjoys tackling from an economic and a policy perspective. Together with Damian Chalmers and Gareth Davies he is a co-author of *European Union Law: Text and Materials* (4th ed, Cambridge University Press, 2019), one of the major texts on the subject. He is one of the editors of the *Common Market Law Review*.



Alexandre de Streel is the Academic Director of CERRE and a Professor of European Law at the University of Namur and the Research Centre for Information, Law and Society (CRIDS/NADI). He is a Hauser Global Fellow at New York University (NYU) Law School, visiting professor at the European University Institute, SciencesPo Paris and Barcelona Graduate School of Economics, and also assessor at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence. Recently, he advised the European Commission and the European Parliament on the regulation of online platforms. Previously, Alexandre worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union and the European Commission (DG CONNECT). He holds a Ph.D. in Law from the European University Institute and a Master's Degree in Economics from the University of Louvain.



EXECUTIVE SUMMARY

Executive Summary

In recent years, the European Union (EU) has seen an important increase of new laws which apply to the providers of digital services, in particular to digital platforms (such as the 2016 Network and Information Security Directive, the 2018 European Electronic Communications Code, or the revised 2018 Audiovisual Media Services Directive). This tendency will continue with the forthcoming adoption of the Digital Markets Act (DMA), the Digital Services Act (DSA), and the Digital Operational Resilience Act (DORA). Those services specific laws apply in addition to the general laws applicable to all service providers such as competition law, consumer protection law, or data protection law. Each of those EU laws – general and services specific – come with their own oversight and institutional frameworks. As many laws overlap and apply at the same time, it is key for the effectiveness of oversight and enforcement that those institutional frameworks are coherent with each other and that the authorities in charge of the different EU laws cooperate.

The aim of this study is to take stock of existing institutional models of what we called 'EU platform laws', evaluate each model by studying its effectiveness and consistency, and recommend improvements to the overall system to ensure more enforcement coherence and effectiveness.

Models of institutional design and the importance of cooperation among regulatory authorities

The **national regulatory authorities play a key role** in enforcing EU platform laws. As they are 'an agent' for the enforcement of European law, EU law has progressively imposed more and more requirements on Member States to ensure that their regulatory authorities fulfil their task in an effective and legitimate manner. Those requirements are related in particular to their independence and resources as well as investigatory and sanctioning powers; they are very strictly enforced by the European Commission and the Court of Justice of the European Union (CJEU).

Three main types of institutional model are generally used for the enforcement of EU platform laws:

1. The first type is a **decentralised model based on the 'country of origin'**: in this case, the regulator of the Member State where the platform is legally established is the lead authority to regulate the platform for the whole EU; such model is used for e-commerce law, media law (Audiovisual Media Services Directive: AVMSD) and privacy law (General Data Protection Regulation: GDPR) applicable to services provided cross-borders.
2. The second type is a **decentralised model based on the 'countries of destination'**: in this case, the authorities of all the Member States where the platform provides its services can regulate the platform on their own national territories; such model is used for consumer protection, competition law or electronic communications law (European Electronic Communications Code: EECC).
3. The third type is a **centralised model**: in this case, an EU body (the European Commission or another EU independent authority) regulates the platform for the whole EU; such model is used for competition law.

Each of these models has its **pros and cons**:

- The first model gives a one-stop shop to the platform, thereby facilitating the expansion of the platform across countries and is a key factor for internal market integration. However, it requires mutual trust among Member States that the lead authority in charge will perform its tasks satisfactorily. This implies that lead authority has (i) the ability apply EU law effectively, i.e., it has sufficient legal powers and is fully independent and adequately resourced; and (ii) the incentives to apply EU law for the benefit of the EU as a whole and take into consideration the EU-wide spill-over effects of their decisions.

- The second model, which is the default one in international law, multiplies the number of regulators a platform must deal with, but ensures that each Member State could protect its users as it wishes. This could mean differentiated enforcement, which can be beneficial when there are national specificities but may also lead to different standards applied in comparable situations.
- The third model gives a one-stop shop to the platform and usually ensures that the EU regulator has the ability and the incentive to regulate for the whole EU. While the country of origin has been key over the last 30 years to integrate markets in the EU, centralisation may be the next step for EU integration with regard to global firms. However, the EU regulator may be less agile and further away from the market context, which may decrease the quality of its intervention.

Each of the three models could also benefit from strong cross-country cooperation between authorities:

- In the first model, the authorities of the Member States where the services are provided may support the lead authority and increase the trust between the national authorities; this is the goal for instance of the European Regulators Group for Audiovisual Media Services (ERGA) or the European Data Protection Board (EDPB).
- In the second model, a cooperation between each authority involved in regulating the platforms could ensure a common regulatory approach through all the EU as it is the case with the Body of European Regulators for Electronic Communications (BEREC) or offer a framework for a structured common dialogue between the different regulators and the regulated platforms as it is the case with the Consumer Protection Cooperation (CPC) Network.
- In the third model, the national authorities may support or complement the EU body in achieving its different regulatory tasks as it is the case for the enforcement of EU competition law by the Commission.

Next to the cross-country coordination among authorities in charge of the same EU legal regime, which is well established by now, another type of **cooperation is emerging, this time between authorities in charge of different legal regimes** which apply to the same digital services. Such cooperation has begun to take place at the national level with the establishment of fora among different national authorities (such as the Digital Regulatory Cooperation Forum (DRCF) in the UK) and might also take place at the EU level with more interactions among the different EU regulatory networks.

This cross-country and cross-regime forms of **cooperation may be of three types** which are not mutually exclusive: a reciprocal consultation before deciding individual cases; joint work on specific cases or joint work on technical policy making with the adoption of guidelines; or common positions.

Coordination and centralisation in action

Our report analyses in detail several case studies of cross-country and cross-regime cooperation. We show that **cross-country cooperation related to network security is a bit of an outlier** because it involves more political authorities than independent authorities and it only applies in a limited manner the principles of Better Regulation which have been developed by the European Commission.

If we assess the three models by reference to their ability to secure effective enforcement of the regime in question, then **cross-country cooperation among authorities which apply the country of origin enforcement model is challenging. For instance, the coordination among data protection regulators is still in its infancy and has certainly a lot to learn** from older cooperation fora which have been established for other legal regimes. While this system could work for small platforms and when platforms are not concentrated in a small number of Member States,

it remains to be seen whether the authority of one Member State will ever have enough ability and incentive to regulate the biggest platform for the whole EU.

Cross-country cooperation for enforcement among authorities which apply the country of destination enforcement model seems to work better. The CPC Network has created a legal system that facilitates joint case work and we are seeing the fruits of this effort in enforcement practices. The European Competition Network (ECN) has managed to allow a relatively effective system to allocate cases and carry out joint technical policy making. BEREC has devised a system of cooperation for consultation and for technical policymaking that works well to ensure a consistent enforcement across the EU.

Cross-regime cooperation in order to work coherently together in digital markets is more recent and is not always easy to achieve because different regulatory cultures meet and have to understand each other. At the national level, the British DRCF model which focuses on specific dossiers where cross-regulatory interests are engaged provides a pragmatic model for developing this form of cooperation. At the EU level, there are episodic references to the need for joined-up thinking which require further development. The cooperation between the three European Financial Supervision Authorities (European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA)), formalised through the establishment of joint committees, may serve as good practice.

A good example of centralised enforcement is the Single Supervisory Mechanism (SSM) under which the biggest banks of the Eurozone are supervised by the European Central Bank (ECB) in close cooperation with the national financial supervisors through the establishment of Joint Supervision Teams (JSTs). The SSM illustrates the advantages of centralisation which ensure a level playing field across the Eurozone as well as a holistic and effective regulatory assessment. It also illustrates the many challenges of centralisation. As the system is still in transition, there remain national differences in supervision culture that should be eroded as joint supervisory teams continue to work together. Moreover, sufficient transparency of SSM operation should be ensured to preserve the accountability of the system of supervision.

Policy Recommendations

Based on our analysis of the law on the books and the law in action, we make the following recommendations to improve the coherence and the effectiveness of the enforcement of the ever-increasing stable of EU platforms laws:

First, regarding the **characteristics of good regulatory authorities**, several key requirements on **independence, accountability, transparency as well as sufficient resources, power to collect and exchange information, and to sanction** are increasingly being applied to the national authorities. However, it may be desirable for the EU to agree on a template for the effective functioning of national authorities that could be applied across the range of regulatory regimes and tasks rather than incrementally amending every EU legal instrument in each legal regime.

Second, regarding the cooperation between regulators, the EU legal framework should maximise the potential benefits of cooperation, minimise the costs, and ensure that the former is higher than the latter. While cooperation has evolved dynamically in the past and we should expect this to continue to happen, we think that at this stage there is enough experience for authorities and legislators to **generalise flexible and pragmatic frameworks to organise authorities' cooperation**. This is useful as it creates a structure so that the authorities do not have to invent a procedure each time, hence should reduce the costs of cooperation. It is also important that those frameworks respect the fundamental rights of the parties under investigation. Our recommendation here is for legislative change to facilitate cooperation among regulators by:

- Embedding national authorities in networks to facilitate both **exchange of experience and exchange of information** with necessary safeguards to protect the rights of firms in particular with regard to the confidentiality and due process;
- Exploring processes to **facilitate joint work** when the conduct of one firm is implemented, or has effects in, multiple jurisdictions. When the country of origin model applies, the competent regulator should have the ability – in particular in terms of legal powers – and the incentives to act. The model in the DSA (requests for intervention) can be one way forward. When the countries-of-destination model applies, coordinated enforcement as provided in the CPC Regulation or as is emerging in some competition cases can be replicated;
- Empowering networks to come up with **soft laws** that result from sharing experiences and identifying best practices and that have some legal effects (such as comply or explain effects) as it is the case with BEREC.

These cooperation frameworks should continue to be developed for cross-country coordination, but more importantly they should now be **seriously considered for cross-regime coordination**. To be pragmatic, this second form of cooperation may have to be first developed at the national level where it is probably easier to implement. Then, it can be expanded more systematically at the EU level, in particular with more interactions among the several EU networks involved in platforms regulation and with the establishment of joint committees as seen in financial supervision.

Third, there are **some advantages in the centralisation of some enforcement tasks at the EU level with regard to the largest digital platforms which offer cross-border services**, as proposed by the DMA and the DSA. However, such centralisation requires good design, in particular: within the European Commission a joint taskforce of DG COMP and DG CONNECT is needed to secure effective enforcement; rules are needed to determine when and how information gathered about firms under one instrument (e.g., DMA) may be used for investigations under other instruments (e.g., DSA or competition law); the respective role of DMA and competition law needs also to be specified.

In the longer term, depending on how the regulatory practice under the DMA and DSA evolves, one might consider the case for an EU authority separate to the Commission, responsible for the enforcement of platform regulation (both the DMA and the DSA) against the largest cross-border digital platforms (a “European Platform Authority”). Were this to be pursued, however, it would have to be subject to the same governance principles as should apply to national authorities, as discussed above: independence (politically and of industry), adequate funding, robust information gathering/sharing and enforcement powers.

A centralisation model at the European Commission or a new European Platform Authority would **require the involvement and a close cooperation with national independent authorities** which have several comparative advantages to an EU body. The lessons from Banking Union reveal the usefulness of this connection. The degree of power sharing between the EU and national authorities can vary depending on which authority has a comparative advantage in addressing each task.

4. Fourth, regarding the style of enforcement, **key Better Regulation requirements related to effectiveness, proportionality, due process as well as participation, innovation and experimentation** are increasingly applied to the national authorities in charge of the different EU legislations applicable to digital platforms. However, it may be useful that the **EU agrees a template for the effective style of oversight and enforcement** for the national authorities that could be applied across the range of regulatory tasks and fields when overseeing digital platforms.

01

INTRODUCTION



1 Introduction

We are seeing a marked increase in the number of rules governing digital markets in the EU, aiming to correct market failures and ensure more contestability, innovation, and fairness as well as a safer cyberspace with less illegal and harmful content and products. These different legal tools can be complements and/or substitutes, they also may overlap and/or create frictions with each other. Moreover, while digital markets are borderless, the oversight and the enforcement of EU rules are often constrained territorially and carried out by national authorities.

The aim of this study is to take stock of existing institutional models of EU platform law enforcement, evaluate each model by studying its effectiveness and consistency, and recommend improvements to the system. The study focuses on a discussion of three main questions: (1) how can the current system of decentralised enforcement be enhanced in the EU? In discussing this question we focus, in particular, on how cooperation among regulators enforcing the same rules in different jurisdictions function and how it may be improved further; (2) is there cooperation among authorities involved in different spheres (e.g., data protection and competition law) desirable and how can this be facilitated?; and (3) is there a case, as foreseen by the DMA and DSA proposals, for centralised enforcement at EU level for the biggest digital platforms regarding certain activities? In writing this paper we also came across a fourth question, which is about the style of enforcement: are digital platforms to be regulated by a command and control model or by a model that focuses more on securing compliance by persuasion? This question is not addressed in full, but we observe a trend towards more enforcement efforts in the latter form. The paper focuses on cooperation within the EU, but it is likely that discussions will be needed to facilitate global cooperation as more jurisdictions enact rules targeting digital platforms which are active across borders.

The paper is structured in the following manner. In Section 2, we create a map of legal issues to explain the current system of institutional design and explore the key themes. In Section 2.1 we explore the powers of national regulators and their characteristics. Those have been strengthened by the EU and there is some increased convergence among the various regulatory fields under study. In Section 2.2 we explore different models of decentralised enforcement in a context where there are national regulators but the activity they regulate crosses national borders. This raises the question of how national authorities cooperate and how this may be enhanced. In Section 2.3 we examine forms of centralised enforcement, where the European Commission is the principal actor. This raises the question about how far this model might be extended for digital platforms. This discussion also shows that there may be multiple regulators addressing the same conduct. As a result, Section 2.4 sets out the modalities that may be designed to facilitate cooperation across regulators. This section serves largely as an exercise in mapping out the current framework.

Section 3 contains a set of case-studies that help us think about the three research questions posed above. Section 3.1 considers the regulation of cybersecurity and contrasts this with other regulatory frameworks discussed in this report. Section 3.2 considers a set of case-studies to examine the functioning of cross-border collaboration among national regulators in the same legal domain. Section 3.3 turns to collaboration across regulatory domains.

Section 4 contains a study on banking supervision. We considered it useful to explore a different system where major institutional realignments took place recently and which may have lessons for the regulation of digital platforms.

Section 5 contains our conclusions and recommendations. Section 5.1 discusses what more may be done to strengthen national regulators. Section 5.2 considers lessons from the cooperation case studies and Section 5.3 discusses the prospects of further centralisation of some aspects of the biggest digital platform regulation and how this might be designed. Finally, Section 5.4 makes a few recommendations on style of enforcement in digital markets.

02

**INSTITUTIONAL
DESIGN TO SUPERVISE
DIGITAL PLATFORMS**

2 Institutional Design to Supervise Digital Platforms

2.1 The national regulators and their characteristics

2.1.1 National regulators as the keystone of EU regulation

Generally speaking, the EU has developed a system where the regulation of digital markets and platforms is carried out by a range of independent national regulatory authorities.

These authorities are **asked to apply rules which are often open-ended and this requires that regulatory choices are made by the regulators**.¹ In particular, some laws set multiple goals and authorities have to make trade-offs. For example, the European Electronic Communications Code (EECC) is designed to achieve four main goals which are not prioritised: connectivity and access to very high-capacity network, competition, internal market, and citizens' interests.² Balancing these multiple objectives, which may at times be conflicting, requires judgment calls and thus requires the exercise of some discretion. This is legitimate, expected, and reserved to the regulators.³ A good illustration of both aspects is found in the work of Shortall and Cave on how to stimulate investment in Next Generation Access.⁴ The authors show that the position of regulators evolved and different jurisdictions made different regulatory choices. This is a helpful example for a number of reasons. First, it reveals that regulators have some latitude to decide how to best secure the goals set by the legislators in the regulatory framework they apply: this makes them responsive to technical changes but also poses challenges on how to best regulate. Second, it reveals the value of assessing the effectiveness of such choices *ex-post* as a means of developing future regulatory strategies. Third, it reveals the potential of collaboration with other regulators to identify superior solutions and the important contributions made by networks of regulators, as explained below.

Independent regulators generally draw their legitimacy from two main sources.⁵ The first is the quality of their performance (called output legitimacy). In this respect, networks of regulators serve also to facilitate the improvement of regulatory tasks. In some fields, it has been recommended that *ex-post* analysis of the regulator's work is a useful exercise to improve outputs further.⁶ **The second source of legitimacy may be termed input legitimacy: this means that the agency is accountable to others.** Accountability implies transparency about decisions so that the public can see what the agency does and its regulatory choices are transparent. It also implies that decisions are amenable to judicial review and that the agency is accountable to its Parliament. There is an inevitable trade-off between independence and accountability which has been discussed at length in the context of central banks. In brief, too much accountability risks allowing politicians

¹ L. Hancher and P. Larouche, 'The coming of age of EU regulation of network industries and services of general economic interest', in P. Craig and G. de Búrca (eds), *The Evolution of EU Law*, 2nd ed, Oxford University Press, 2011.

² Directive 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ [2018] L 321/36., Article 1(2).

³ In different cases regarding electronic communications rules, the Court of Justice condemned Member States because they curbed this regulatory discretion: Case C-424/04, *Commission v Germany – New Generation Networks* EU:C:2009:749, where the Court of Justice condemned Germany for having adopted a law restricting the power of the NRAs in analysing and regulating emerging markets; Case C-220/07 *Commission v France – Universal Service II* EU:C:2008:354, para.34 and Case C-154/09, *Commission v Portugal – Universal Service*, EU:C:2010:591, where the Court of Justice condemned France and Portugal for adopting a law restricting the power of the NRAs in designating the universal service provider, according to a procedure which is efficient, objective and non-discriminatory; Case C-518/11 *UPC Nederland v Gemeente Hilversum* EU:C:2013:709, para.54 and Case C-560/15 *Europa Way and Persidera v Autorità per le Garanzie nelle Comunicazioni et al.* EU:C:2017:593, para.57 where the Court of Justice considered that the Parliament and the government could not intervene in an on-going selection procedure organised by the Italian NRA for radio spectrum assignment.

⁴ T. Shortall and M. Cave, *Is Symmetric Access Regulation a Policy Choice? Evidence from the Deployment of NGA in Europe* (2015) 98(2) *Communications and Strategies* 17. The authors also observe that some experimentation with different regulatory models can help identifying the superior one.

⁵ In a pure legal setting, the legitimacy of the regulatory authorities also derive from the constitutional order of each Member State.

⁶ W.E. Kovacic, *Using Ex Post Evaluations to Improve the Performance of Competition Authorities*, 31 J. Corp. L. 503 (2006); W.E. Kovacic, *Using Evaluation to Improve the Performance of Competition Policy Authorities* OECD, DAF/COMP (2005)23. More generally, see J.B. Weiner and L.S. Benneer, *Institutional Roles and Goals for Retrospective Regulatory Analysis* (2021) (open access at: <https://www.rff.org/publications/working-papers/institutional-roles-and-goals-retrospective-regulatory-analysis/>).

to affect the regulatory enterprise while too little accountability risks delegitimising the regulators. This calls for a balance between these two aspects. Insofar as judicial review is concerned, there has been a trend towards more intense scrutiny of agency actions and debate on this has been particularly pronounced in the field of competition law.

2.1.2 *The EU's continued strengthening of national regulators*

As national authorities play a key role in enforcing European rules, **EU law increasingly sets minimum requirements that those authorities must meet** in order to ensure effective and consistent enforcement across the internal market. Those requirements relate to independence and accountability, investigation, sanctioning powers, as well as to the respect of due process and fundamental rights.⁷ The reason for this is that, increasingly, national authorities have greater enforcement powers, and this often requires procedural protections for firms and users. While EU law reveals a degree of convergence, variations still exist across legal instruments.

Notably, **when it comes to the independence of national authorities, secondary laws emphasise this requirement but in varied ways**. This depends on the subject matter to be regulated but also on the political process and the notions of independence at the time the legislation was adopted. In this respect, one of the most recent secondary law (the ECN Plus+ Directive) sets out one of the most comprehensive independence requirements of all the EU rules.⁸ At the other extreme, the independence of the authorities in charge of network security is under-specified in the NIS Directive.⁹ However, the proposal for the NIS2 Directive includes further specification for the resources and the powers of investigation and sanction for national authorities but still does not specify the duty to ensure that those authorities remain independent.¹⁰ Given that there is a general alignment in this respect in other fields of regulation, this gap points to the more national security aspects of cybersecurity. It is also worth noting that in this field many of the key choices appear to be left to national government.

The **CJEU has clarified the concept of independence found in secondary law** in several cases, in particular with respect to the electronic communications rules¹¹ or privacy rules.¹² From recent case law, it appears that for Germany the degree of independence required by EU energy law may have been at risk of going against German constitutional law. The ECJ pushed back against these arguments by noting that the requirement that regulatory authorities should be independent is not contrary to principles of democracy because these authorities are given well-defined tasks and the political choice as to what the tasks are and how they are to be discharged is for the political process.¹³ The Court is sensitive to the fact that decisions of independent regulators may sometimes have significant market impact and has taken the view that it may be acceptable to have members of ministries present during certain sensitive regulatory choices (e.g., the determination of energy tariffs) provided that at the end of the deliberation "the national regulatory authority is to adopt autonomous decisions, on the sole basis of the public interest, to ensure compliance with the objectives pursued by that directive, without being subject to external instructions from other public or private bodies."¹⁴ Some have suggested that even though this judgment focuses on the electricity

⁷ P. Larouche, C. Hanretty, and A. Reindl, *Independence, Accountability and Perceived Quality of Regulators*, CERRE Report, 2012. See for instance, AVMSD, Art.30; GDPR, Arts.51-59; CPC Regulation, arts.5-10; ECN+ Directive, arts. 4-16; EEC, Art. 6-9; NIS Directive, art.8.

⁸ Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, O.J. [2019] L 11/3, art.4.

⁹ Directive 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, OJ [2016] L 194/1, art.6.

¹⁰ Proposal of the Commission of 16 December 2020 for a Directive on measures for a high common level of cybersecurity across the Union, COM (2020) 823.

¹¹ Case C-424/15 *Ormaetxea Garai et al. v Administración del Estado* EU:C:2016:780 ; Case C-240/15 *Autorità per le Garanzie nelle Comunicazioni (AGCOM) v Istituto Nazionale di Statistica – ISTAT and Others* EU:C:2016:608.

¹² Case C-518/07 *Commission v. Germany*, EU:C:2010:125.

¹³ Case C-718/18, *Commission v Germany*, EU:C:2021:662.

¹⁴ Case C-378/19, *President of the Slovak Republic*, EU:C:2020:462, para.54.

directive, one can read into it a general principle of independence.¹⁵ This might go too far as the focus of the ECJ is on the specific directive but one can also see the advantages of the Court discovering general principles of independence which would facilitate the alignment of all regulators, in particular since often firms are regulated by more than one agency.

In addition to independence, EU legislation also provides that authorities should be **adequately funded and have the capacity to enforce** the rules. Clear example of this is found in the EECC or the Audiovisual Media Services Directive (AVMSD), which specify the importance of adequate staffing, expertise, and financial means.¹⁶ However, as with independence, the degree of specification varies across legal instruments. This is probably the result of the experience gained in designing authorities and identifying what further attributes should be addressed in EU rules. Furthermore, the European Commission's powers of oversight when it comes to institutional requirements like capacity and resources are more limited because proving inadequacy is problematic. It is relatively easier for the European Commission to identify the absence of independence (by comparing the manner in which it is specified in EU law and the way in which it is implemented in practice) and to bring infringement proceedings against the Member States that deviate. However, there seem to be some egregious instances of inadequate resourcing where European Commission pressure on Member States who make insufficient efforts to empower national authorities seems to be justified.¹⁷

When it comes to the powers that the authorities are expected to have, the **investigatory and sanctioning powers** that the EU harmonised for national competition authorities with Regulation 1/2003 have also been replicated in the General Data Protection Regulation (GDPR), the EECC, and are also found in the DMA and DSA proposals. The NIS Directive, in contrast, is less prescriptive when it comes to remedies. However, the proposal for the NIS2 Directive provides for stronger supervision and enforcement measures, establishing a list of administrative sanctions for infringing cybersecurity risk management and reporting obligations.

In sum, the **EU has invested significantly in facilitating and strengthening the independence and operation of national regulatory authorities**. An issue that we explore in the case studies and in the recommendations of this report is how far this has been fruitful and what more might be done. It is also worth exploring how far what emerges are a set of generally applicable attributes for all national authorities.

It is also worth noting that **in the field of consumer law some jurisdictions** (e.g., Germany, France, Austria, or Belgium) **do not have authorities** that can be compared to the Dutch, Italian, or British consumer bodies (which are integrated into competition authorities). In Germany, consumer law enforcement is largely a matter of private law litigation. This raises two broad questions: (i) how far the EU consumer law acquis should require the institutionalisation of regulators for consumer law matters and (ii) the impact that the absence of consumer bodies in some jurisdictions has on the operation of the cooperation mechanisms like the CPC Network which we discuss below.

2.2 Models of decentralised oversight and enforcement

2.2.1 Country of origin and countries of destination

National authorities are key because EU law is normally governed by the principle of 'indirect administration' under which **rules are decided at the EU level and then enforced at the national level**. In practice, the application of EU law is generally based on two main models of public enforcement:

¹⁵ Rizzuto, 'The Independence of National Regulatory Authorities: Is There Now an Autonomous EU Law Concept of Independence of General Application?', *European Competition and Regulatory Law Review* 5(1), 2021.

¹⁶ EECC, art.9; AVMSD, art.30(4).

¹⁷ A notable example (which we discuss further in Section 3) is the Irish data protection authority, which has been criticised for being ineffective and under-resourced.

1. A decentralised model where **enforcement is carried out by the authorities of the Member State where the company providing the regulated service is established (country of origin)**: this model is used in several EU platform laws such as the e-Commerce Directive,¹⁸ AVMSD,¹⁹ the GDPR,²⁰ and the NIS Directive.
2. A decentralised model where enforcement is carried out by the **authorities of the Member State where the company provides the regulated services (countries of destination)**²¹: this model is used for consumer protection law,²² the application of EU competition law by national competition authorities,²³ and electronic communications regulation.

The **country of origin model is most logical choice to stimulate firms active in many jurisdictions and contribute to the internal market, as it allows a one-stop shop for firms.** It is often found in legislation that creates some minimum harmonisation to limit the risk of forum shopping. However, this risk remains for at least two reasons: first, some Member States remain keen to adopt higher levels of protection, leading to some service providers moving to more *de iure* permissive jurisdictions; second, some national authorities may be less effective than others in enforcing EU harmonised law, which may also stimulate service providers to move to more *de facto* permissive jurisdictions.

While the countries of destination model removes the risk of forum shopping, firms might experience differences in the way the rules are applied. This risk can be addressed, albeit slowly, by litigation and preliminary rulings to the ECJ.

Moreover, **both models can be ameliorated by networks of regulators** which can ensure greater consistency in approach and level the playing field for firms across the digital single market.

2.2.2 *The logic and the challenge of different models of decentralised enforcement*

The **default model in international law is the countries of destination** under which each national authority is responsible for regulation on its national territory. However, this may be a serious obstacle to market integration as it multiplies the number of authorities with which a firm with cross-border operation has to deal with. **Therefore, the EU promoted the country of origin model.** Since the new approach to internal market regulation for goods in the 1980s, which enshrined the principle of mutual recognition of standards, home state control was seen as a mechanism to facilitate market integration by making easier exports to the EU by national firms: compliance with national standards sufficed.

However, the country of origin model can only be effective and acceptable if there are **minimum common standards and a mutual trust among countries that those standards would be enforced**: each Member State must believe that the national regulator of the country where the firm

¹⁸ Directive 2000/31 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), OJ [2000] L 178/1.

¹⁹ Directive 2010/13 of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ [2010] L 95/1, as amended by Directive 2018/1808.

²⁰ Regulation 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), OJ [2016] L 199/1.

²¹ We refer to 'countries of destination' since the firm may fall to be controlled by multiple regulators, each applying EU Law to their jurisdiction.

²² Directive 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ [2005] L 149/22, as amended by Directive 2019/2161; Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ [2011] L 304/64, as amended by Directive 2019/2161.

²³ Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, O.J. [2019] L 11/3.

is established applies the rules in a manner that is rational, and that regulators are well-resourced and independent. As we show below, these fundamentals are sometimes missing. For instance, some data protection authorities are severely under-resourced, some jurisdictions do not have regulators for some rules (e.g., consumer laws), and some regulators have no requirements of independence. Furthermore, the model only works when the lead national authorities act taking into consideration the interests of other jurisdictions when there are spill-over effects across Member States.

In sum, the **assumptions upon which the country of origin model is applied are: national authorities have (i) the ability to apply EU law (which defines common EU standards) effectively, i.e., they have sufficient legal power to do so and are fully independent and adequately resourced; and (ii) the incentives to apply EU law for the benefit of the EU as a whole, i.e. they take into consideration the EU-wide spill-over effects of their decisions.** This is by no means granted because the national authority is expected to provide a public good for all other Member States, but it is often not credited for doing this. In other words, the authority gains no monetary or other reward from other Member States if it acts to secure the interests of EU consumers or citizens in other Member States. It is also likely that the Member State where the authority is situated has little interest in increasing resources of its authority when that authority engages in extraterritorial enforcement that shows no direct return to the domestic market and may even entail a cost when it increases the incentives of the firms to move to other more 'complacent' jurisdictions.

The EU has addressed the first issue related to ability. On the one hand, as we have discussed in Section 2.1, the EU legislator updates requirements to further strengthen national authorities by giving them more enforcement and sanctioning powers, specifying in ever greater detail how to secure independence, and requiring increased resources. On the other hand, the European Commission can bring infringement proceedings against Member States who do not guarantee the independence of their national regulator and the ECJ has assisted in this effort by giving further specifications to the importance of the independence of regulators. However, there are limits to what can be achieved by these two routes and it is likely that we will continue with national authorities having asymmetric powers and skills and, in any case, this does not address the other issue related to the incentives.

It is not clear how much integration through law (i.e., ever more prescriptive secondary laws) can be implemented to convince national authorities to consider the interests of the EU more generally and take into account spill-over effects. Granted, these cross-border issues do not always arise, for example if the market failure is purely national and the sole spill-over effect is facilitating market access of firms not yet present in the jurisdiction, then effective enforcement which focuses only on national markets suffices. However, the issue is more pertinent when a national regulator is expected to act in ways that benefit others (the GDPR is the prime example) or when the regulator considers conduct that is cross-border and where anticompetitive effects manifest themselves in more than one jurisdiction (competition law serves as an example).

Looking at this issue more generally, it may be said that the ECJ has succeeded in making national courts realise that when they are applying EU law, they are acting as European Union courts. Thus, increasingly national courts make reference to the case-law of the ECJ in their rulings and the procedures by which national courts may make references for preliminary rulings serves to integrate them into a network of national courts enforcing EU law.²⁴ However, it seems **there are fewer routes by which national authorities can be compelled to act as EU authorities** when this is necessary to address cross-border infringements. In the case-studies we look into examples of how far cross-border considerations are addressed via legislative and non-legislative means.

²⁴ de Witte et al (eds) *National courts and EU law : new issues, theories, and methods* (2016).

2.3 Cross-country coordination

2.3.1 Networks of regulators – an overview

As we have noted above decentralised enforcement is facilitated by coordination between the national authorities when corporate practices have cross-border effects, which is often the case for digital services.

For the **country of origin model, in principle, one single authority is in charge of enforcing European law for the whole EU. However, this authority is often required to cooperate with the authorities of the Member States where the regulated services are provided**, and safeguards clauses sometimes allow those authorities to intervene. For instance, to enforce the GDPR, a 'lead authority' is designated by reference to the 'main establishment' of the company whose conduct is under review. The lead authority is required to cooperate with other Data Protection Authorities and its decision then affects the firm's conduct across the EU.²⁵ This scheme assumes that each lead authority is as capable and has the same incentive to act as any other. The lead authority is expected to work in close collaboration with other authorities and to consult them before making decisions; in some instances, the European Data Protection Board (EDPB) may arbitrate differences of opinion.²⁶ The purpose of these coordination devices is to provide a regulatory solution that is agreed by all authorities (ensuring uniformity) and which is perceived to address the infringement (ensuring effectiveness).

With the **country of destination model, several authorities are often in charge, hence the potential need for coordination among those is even more pressing** but arises for different reasons than under the country of origin model. For instance, **in EU consumer law, if there is concern about a widespread infringement that affects consumers in more than one Member State or has an EU-wide dimension, then the consumer protection authorities in charge have an obligation to coordinate enforcement by appointing a coordinator among them to ensure coherent investigation.**²⁷ The companies whose practices are under review may offer commitments that resolve the consumer law concern in all relevant jurisdictions and, absent this, each authority is obliged to take enforcement action in case an infringement has been found. The coordinator and the European Commission play a role in ensuring that the national authorities act consistently. The upshot is that a firm operating across the EU is *de facto* afforded a single regulator and may propose EU-wide commitments. This procedure has developed incrementally since 2007 and a number of decisions have been taken in the digital economy.²⁸ For instance, Booking.com made a number of commitments to modify the information that consumers see so that it complies with consumer law, for instance, offering explanations on how results are ranked and if hotels pay for higher ranking, as well as clarifying the total price of the rooms.²⁹ Obviously this kind of coordination is not always appropriate when national authorities take into account country-specific considerations.

In competition law, the job of securing consistency is on the European Commission. This is discharged by the European Commission issuing guidelines on substantive matters. The drafting process includes inputs from national competition authorities suggesting a degree of cooperation in the design of the rules, although the European Commission remains the lead agent. In practice, these soft law instruments are largely followed, but their formal legal force has been questioned and tested by litigants in a number of court cases. The European courts weakened somewhat the approach of the European Commission by emphasising the lack of binding effect of soft law

²⁵ GDPR, Arts 56 and 62 to 65.

²⁶ GDPR, Arts 60 and 63-65.

²⁷ Regulation 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ [2017] L 345/1, Articles 16 to 24.

²⁸ https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/coordinated-actions_en;
https://ec.europa.eu/internal_market/scoreboard/docs/2019/performance_by_governance_tool/cpc_en.pdf

²⁹ https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6812

instruments upon courts and other authorities than the European Commission itself.³⁰ In addition, Regulation 1/2003 contains a more granular mechanism to ensure consistency, found in Article 11. This allows the European Commission to be informed about likely decisions of national competition authorities and offers the option for them to guide national authorities. This provision includes a 'nuclear option' by which the European Commission takes over the case from a national competition authority. Such a practice is not reported but interviews with some stakeholders suggest that there have been instances where informally, cases started by a national competition authority were transferred to the European Commission.³¹ There are notable examples of cases handled by multiple national competition authorities or by the European Commission and national authorities that we discuss below in Section 3.2.3.

In **network security law, the coordination between authorities in charge of monitoring cybersecurity risks is more complex as it is a mix of political and regulatory bodies.** The EU Agency for Network and Information Security (ENISA) serves to help the EU and Member States to develop their cybersecurity policies.³² For the NIS Directive, a new cooperation forum was opened, the NIS Cooperation Group³³ where the Member States cooperate, exchange information, and agree on how to implement the directive consistently across the EU. This group includes ministries as well as cybersecurity authorities. The political aspect of this cooperation is also visible by the fact that it is chaired by the Presidency of the Council of the EU, and it is deliberately described as a group for strategic cooperation. There is also a more operational network, composed of computer security incident response teams (CSIRTs) which is designed to facilitate cooperation in case of a security incident, and which more broadly seeks to facilitate the exchange of information and good practices in addressing incidents.³⁴ In this context, the NIS Cooperation Group is somewhat of an outlier. While it resembles the European Competition Network (ECN) or Body of European Regulators for Electronic Communications (BEREC), its composition is more politicised, deliberately so considering the sensitive issues that it addresses. Indeed, its work on 5G security has even been discussed by the Council.³⁵ Recall as we noted above that the NIS Directive is also silent on the necessity for national competent authorities to be independent. This institutional setup might account for some of the concerns that we discuss below.

More generally, the coordination among national authorities tends to be formalised over the years with the establishment of EU networks of national authorities such as the European Regulators Group for Audiovisual Media Services (ERGA),³⁶ the EDPB,³⁷ the Consumer Protection Cooperation Network (CPC),³⁸ ECN,³⁹ or BEREC.⁴⁰ In general, the European Commission plays a very

³⁰ For instance, the CJEU insisted upon the non-binding nature of the *De minimis* notice (now at OJ 2014 No. C 291/1) (Case C-226/11 *Expedia* EU:C:2012:795 at para. 4), the Notices on cooperation within the ECN, OJ 2004 C101/43 and on leniency, OJ 2006 C 298/17 (Case C-360/09 *Pfleiderer*, EU:C:2011:389, at para. 21), the Guidance paper on Article 102 TFEU, OJ 2009 C45/7 (CJEU, 6 October 2015, Case C-23/14 *Post Danmark I*, EU:C:2015:651, at para. 52), the instruments produced by the ECN, especially the Model Leniency Programme (Case C-428/14, *DHL Express (Italy)*, EU:C:2016:27, at paras. 41-44).

³¹ The e-books commitment decision was originally handled by the then Office of Fair Trading but the Commission took over very early on. Formally the OFT explained that the case was not a priority one for it and the 'European Commission is currently well placed to arrive at a comprehensive resolution of this matter and will do so as a matter of priority.' Case Reference: CE/9440-11 Update - 6 December 2011.

³² Regulation 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) [2013] OJ L165/41, Article 2; now replaced by Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA, the "EU Cybersecurity Agency", and repealing Regulation 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), OJ [2019] L 151/15.

³³ NIS Directive, Article 11.

³⁴ NIS Directive, Article 12.

³⁵ Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G (3 December 2019) <https://www.consilium.europa.eu/media/41595/st14517-en19.pdf>

³⁶ AVMSD, art.30b.

³⁷ GDPR, arts.68-76.

³⁸ See fn.26.

³⁹ See fn.7.

⁴⁰ Regulation 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of the European Regulators for Electronic Communications, OJ [2018] L 321/1.

active role in those networks in organising and stimulating coordination as well as favouring the exchange of good practices among national authorities.⁴¹

2.3.2 Regulatory networks – issues for discussion

The establishment of EU networks of national authorities in all the fields covered in this study might be seen as a logical reaction to the decentralisation of enforcement in markets which are increasingly integrated and have the following advantages.

These networks enhance the performance of authorities in promoting discussion and the identification of best practices. For example, ECN functions as a network where best practices are identified by sharing experiences of different authorities and identifying good practices. This relates both to matters of procedure (where ECN formally publishes best practice documents) and also at the level of substantive assessment (where experience among competition authorities is shared). Similarly, BEREC adopts guidelines that defines regulatory best practices and technical implementing rules aiming at ensuring a consistent regulatory approach in the EU.⁴² The NIS Cooperation Group also issues soft laws.⁴³ The EDPB also provide guidance on best practices in applying the rules.⁴⁴ Thus, networks of national authorities facilitate cooperation in identifying superior solutions. This serves to strengthen regulators because they can refer to a united position of their fellow regulators when their enforcement stance is contested. This can be of particular importance for relatively new regulators in Member States where the culture of independent regulators is less well-developed.

Recommendations or other best practices documents issued by regulatory networks are not legally binding. Normally the expectation of such soft laws in other contexts of EU law (e.g., the open method of coordination) indicates that national authorities retain discretion to continue their policy as before: best practices give methods which may or may not be followed to achieve objectives and indicators set at the EU level. However, some of those guidelines have more influence when the legislators or the Court instruct the national authorities to comply with the agreed guidelines or explain why they want to depart from them. This is the case of BEREC Guidelines that have, according to the EECC, a 'comply or explain' legal effect.⁴⁵ There are also instances where the legislator may choose to codify best practices into binding standards. Below we will explore a specific example of this in the case of cybersecurity. A more well-known example is found in the field of competition law, where the ECN+ Directive codifies a set of procedures that were discussed by the ECN in working groups.⁴⁶ It has to be said however that the ECN+ rules largely correspond to the European Commission's own procedural practices and it is not clear whether any aspect of the directive reflects the best practice devised by a national competition authority.⁴⁷ This move from soft to hard law is evidence of the contribution that networks can make to make the regulatory enterprise more effective by identifying fields where further legislation is needed.

Thus, **regulatory networks allow for a harmonised approach to regulation**, which is particularly important when the countries of destination model applies so that the firm is subject to one set of rules for each jurisdiction it operates in as far as this is possible. In particular, networks help identify and ensure the application of best practices that all national authorities contribute to

⁴¹ The European Commission can also intervene by vetoing proposed actions of an individual regulator, see: EECC, arts.32-34.

⁴² https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/

⁴³ <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>

⁴⁴ https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

⁴⁵ EECC, art.10(2) and BEREC Regulation, art.4(4).

⁴⁶ Directive 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, O.J. [2019] L 11/3.

⁴⁷ G Monti, 'The Proposed Directive to Empower National Competition Authorities: Too Little, Too Much, or Just Right', *Competition Law and Policy Debate* 40(3), 2017.

developing. Regulatory networks are also important when the country of origin model applies as they incentivise the national regulators to see the EU-wide salience of their regulatory choices.

Some networks are more advanced than others and there may be lessons to be drawn from the practices of networks and from the legislative framework applying them. For instance, BEREC has the power to adopt general guidelines facilitating a common interpretation and enforcement of EU law as well as the power to adopt an opinion on individual decisions of National Regulatory Authorities (NRAs). The power of this network has constantly increased over the years. The CPC is the network that has moved more clearly beyond information sharing and into enforcement as a result of the CPC Regulation. This, in our view, is a model that could be replicated in other sectors and it is worth considering (i) whether this would be a helpful approach in other fields of platform law enforcement; and (ii) whether such a development requires legislation or if authorities can cooperate more deeply even absent additional legislation.

Networks' output suggests they can be useful in strengthening enforcement but there may be an input legitimacy gap worth exploring. At present, the only way to make a network legally accountable is to challenge a decision of a national authority that implements an agreed regulatory choice made by the network members. Networks, in general, have no legal personality and merely facilitate the work of the regulators. This indirect mode of reviewing soft laws agreed by network members is quite cumbersome and offers no relief when the best practice is to opt for non-enforcement, in which case there may be nothing to challenge.⁴⁸ The NIS Directive example also reveals that there is a concern about the scope of policy-making that networks can have and, in this context, there is a risk that the Toolbox developed by the network to evaluate cyber security risks shifts from analysing the technology to analysing the supplier in a manner that may be disproportionate.

A final issue to explore is the **balance between uniformity in the interpretation of EU law and regulatory choices made and experimentation allowed for each national authority.** When a best regulatory practice is found, there is a value to extend it to the whole EU, but to find such best practice, some experimentation and testing of different options may need to be done.⁴⁹

2.4 Cross-regime coordination

Next to a cross-country coordination among regulators in charge of the same EU legal regime, another type of coordination among regulators in charge of different – but related – EU regimes is also important. Indeed, the same corporate conduct could fall under more than one regulatory regime, hence could be regulated by more than one authority. Moreover, the regulatory choices made by one authority may affect the policy pursued by another authority. Cross-regime coordination may take place through legal or institutional mechanisms.

2.4.1 Coordination through legal mechanisms

To deal with overlaps among different EU laws, the legislator may create a system of priorities (such that one rule applies, displacing the others). In some situations, a general/specific laws articulation could be used. In such cases, both legal regimes are applied in a complementary manner as far as possible. For instance, in the electronic communications sector, the ECJ clarified that the sector-specific consumer protection rules of the EECC are complementary – and not substitute – to the general consumer protection rules. Therefore, those general consumer protection rules apply fully to the electronic communications sector and should be enforced by the

⁴⁸ For example, suppose the ECN determines that a complaint is best handled by the competition authority of one Member State. As a result, no other authority acts. The complainant may challenge the decision of the authority that takes the case but will find it more difficult to challenge the inaction of the others absent a decision not to enforce which is justiciable. Moreover, the legal challenge can only discuss the authority's choice to act or its failure to act and only indirectly challenges the approach agreed by the network.

⁴⁹ Examples of experimentation in electronic communications regulations include the regulation of next generation networks: see fn.4.

consumer protection authority.⁵⁰ When this is not possible, the more specific regime should apply first, but at the same time, it should not apply to contradict the more general regime, unless the more specific regime explicitly deviates from the more general one.

Another possibility would be a principal/accessory relation: for composite services which is potentially covered by different EU laws, instead of applying all those different legal regimes, only the one pertaining to the principal component would apply, leaving aside the law applicable to the accessory component. For instance, in *UPC Nederland*, a case concerning the delivery of audio-visual media content over electronic communications networks, the ECJ applied the legal regime of the principal component (electronic communications network) to the entire service and left aside the regime that only applied to an ancillary element of the service (audiovisual media service).⁵¹ A similar approach was followed by the ECJ in the collaborative economy cases to decide whether the sharing platform should be qualified as a provider of an information society service or as a provider of the intermediated service (such as transport for Uber or hosting for Airbnb).⁵² The Court sought to identify the main component of the service provided by the collaborative economy platform, and then applied the legal regime relating to that main component to the whole service provided by the platform.

A third approach to this issue comes via the application of the *ne bis in idem* principle (double jeopardy in common law parlance). This principle prevents the initiation of a second action if the conduct has already been sanctioned. It applies to criminal offences and to regulatory offences that are sanctioned in a manner equivalent to criminal law. The precise contours of this principle are presently being reconsidered in a spate of cases pending at the ECJ. For present purposes, *bpost vs Autorité belge de la concurrence* is the most helpful. In this case the defendant had been penalised by the Belgian postal regulator for offering discriminatory rebates and by the Belgian competition authority who considered the same conduct an abuse of dominance. *bpost* questioned whether the same conduct could be pursued also by the competition authority and argued that this infringed the principle of *ne bis in idem*. As Advocate General Bobek observed, the principle has not been applied uniformly in EU law. There is some uncertainty on how to determine if the two enforcement actions cover the same issue. His proposal is that for all fields of EU law the test is based on identifying “a triple identity: of the offender, of the relevant facts, and of the protected legal interest.”⁵³ The first two are self-explanatory, the third is defined by the Advocate General thus: “It is the societal good or social value that the given legislative framework or part thereof is intended to protect and uphold. It is that good or value that the offence at issue harms, or with which it interferes.”⁵⁴ Applying this to the facts, the Advocate General is of the view that postal services regulation and competition law safeguard different interests: the former seeks to open a market to competition and so harm to markets up or downstream is not an issue for the regulator. In contrast competition law necessarily focuses on the harm the rebates cause in up or downstream markets. This interpretation is in line with other judgments which allow the parallel application of sector-specific regulation and competition law.⁵⁵ If it is followed, then this method for coordinating overlapping regulation will not be very significant, necessitating cooperation among authorities.

⁵⁰ Joined Cases C-54/17 and C-55/17, *Autorità Garante della Concorrenza e del Mercato (AGCM) v Wind Tre and Vodafone Italia*, EU:C:2018:710.

⁵¹ Case C-518/11, *UPC Nederland v. Hilversum*, EU:C:2013:709.

⁵² Case C-434/15 *Asociación Profesional Élite Taxi v Uber Systems Spain*, EU:C:2017:981, at para. 40 ; Case C-320/16, *Uber France*, EU:C:2018:221, at para. 22 deciding that: “that the intermediation service (provided by Uber) had to be regarded as forming an integral part of an overall service the main component of which was a transport service and, accordingly, had to be classified, not as an ‘information society service’ (...) but as a ‘service in the field of transport’ (...)”; Case C-390/18, *Airbnb Ireland*, EU:C:2019:1112, at para. 69; Case C-62/19 *Star Taxi App v. Unitatea Administrativ Teritorială Municipiului București prin Primar General, and Consiliul General al Municipiului București*, EU:C:2020:980.

⁵³ Case C-117/20, *bpost SA v Autorité belge de la concurrence* EU:C:2021:680, para.133.

⁵⁴ *Ibid.*, para 136.

⁵⁵ Case C-17/10, *Toshiba et al. v. Úřad pro ochranu hospodářské soutěže*, EU:C:2012:72.

2.4.2 Coordination through institutional mechanisms

As explained by the work of Freeman and Rossi on US administrative law, there are different types of coordination among authorities who share a regulatory space.⁵⁶ We can adapt their model to discuss the EU system and take stock of existing cooperation among different regulators in the following section of this paper. Importantly, the types are descriptive and there is no indication that Type 3 cooperation is inherently superior to Type 1.

Type 1: Consultation

At this basic level, an authority consults others before reaching a decision, but each authority remains competent to apply its own regulatory framework. Consultation may be required by law, or it may be agreed by the authorities. Three benefits that arise from consultation may be distinguished:

- First, consultation among authorities helps to reach an agreed position on the nature of the infringement and the remedy.
- Second, it may improve the quality of decision-making. An example of this is the Bundeskartellamt's duty to consult the Commission on Concentration in the Media (KEK) in carrying out its analysis in mergers relating to the nationwide distribution of TV programmes by private broadcasters.⁵⁷ This consultation helps an identification of the level of concentration in media markets, something that the KEK specialises in carrying out. While both authorities make their decisions on these mergers independently, shared information can help improve the quality of decision-making.
- Finally, consultation may also trigger the other authority into action. An example of this is the protocol agreed between the Italian NCA and the Italian Medicines Regulator by which the two authorities undertake to inform each other of possible infringements of laws which are to be investigated by the other authority.⁵⁸ This protocol was signed in the aftermath of an excessive pricing case taken by the competition authority after the matter had been also reviewed by the medicines regulator.

Type 2: Joint case work

While in Type 1 each authority pursues the case independently with input from the others, **authorities work jointly in Type 2. This can happen at every stage of an investigation:** they might agree to share information that has been gathered (subject to proper procedural safeguards), they may also work jointly to design remedies when both agree on the market failures that arise from.⁵⁹ Another form of cooperation at this level is in the monitoring of remedies. In some merger decisions, for instance, the European Commission relies on national regulators to secure compliance.⁶⁰

The added value of this deeper form of cooperation is that the cooperating authorities retain the power to regulate the market. However, on the one hand, they maximise the synergies among their

⁵⁶ Freeman and Rossi, Agency Coordination in Shared Regulatory Space (2012) 125 *Harvard Law Review*, at 1131. For another proposal indicating three models, see Reyna, Optimizing Public Enforcement in the Digital Single Market Through Cross-Institutional Collaboration (January 31, 2020). Available at SSRN: <https://ssrn.com/abstract=3529198> where he proposes: (i) ad hoc dialogue; (ii) legislation mandating cooperation (e.g., information sharing); (iii) joint decisions and common remedies.

⁵⁷ Germany, Act Against Restraints of Competition S.40(4)(3).

⁵⁸ Article 1(1)(a) Protocollo d'intesa AGCM - AIFA, 19 gennaio 2017.

⁵⁹ See some examples in mergers in G. Monti 'The Global Reach of EU Competition Law' in Cremona and Scott (eds) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford, 2019) pp.174-196

⁶⁰ Case COMP/M.2876, *Newscorp/Telepiú* [2004] OJ L110/73 offers an example where the Italian Communications Authority was put in charge of the arbitration procedures and would oversee compliance with the commitments. In Case No COMP/M.3916 – T-Mobile Austria/Tele.ring (2006) the divestiture of UMTS frequencies was supervised by the Commission and the Austrian telecom regulator.

powers and expertise and, on the other hand, they avoid that any overlap in their powers leads to inconsistent decisions.

Type 3: Joint technical policy making

In Type 3, **authorities work on common regulatory document and guidelines** which may then be a useful common basis when each authority must decide individual cases. An illustration of such type of cooperation is the recent report on competition and data jointly made by the UK Competition and Markets Authority and Information Commissioner Office.⁶¹ Two aspects of this report stand out for our discussion. The first is that the report recognises at a high level the complementarities and the tensions that may arise with the parallel pursuit of competition policy and data protection objectives. While this aspect of the report is nothing new for those who have experience of the field (e.g., the report notes how a data access remedy might stimulate competition but go against data protection principles and how data protection obligations may be read in such a way as to generate entry barriers harming competition) what matters is that the two regulators agree that these tensions are best managed by coordination among the regulators. This points to the importance of the two authorities educating each other on the perspectives that each has on the issue.

Second, and building on this report, the regulators are working on two ongoing issues where the approach of each expects to be influenced by communication with the other: the Competition and Market Authority's (CMA) scrutiny of Google's privacy sandbox and the Information Commissioner's Office (ICO) investigation of real-time bidding in digital advertising. What the report anticipates is not joint action by both regulators – rather that the two will exercise their powers considering the knowledge and the policy ambition of the other. With respect to the Google privacy sandbox, the aim is to provide Google with a compliance pathway that ensures that this operates within the boundaries set by competition and data protection law.⁶² Regarding real-time bidding, the ICO will maintain a dialogue with the CMA regarding any competition issues that arise.⁶³ Given the CMA's recent work on the market failures in advertising markets, there may be scope for further regulation of this market.⁶⁴

2.5 Centralised oversight and enforcement

Next to decentralised enforcement, which is the standard practice in Europe, **EU law is sometimes enforced at the European level. Enforcement may be centralised at the European Commission.** This is the case for the control of the mergers having a 'community dimension'.⁶⁵ To determine such dimension, the Merger Regulation relies on quantitative criteria which are relatively simple to use.⁶⁶ This is also the case for the enforcement of Article 101 and 102 TFEU.⁶⁷ However here enforcement is shared with national competition authorities (applying a countries of destination principle) and soft law is in place to determine whether the European Commission is the best-placed authority or whether instead an issue is best dealt with by national competition authorities.⁶⁸ Generally speaking, if the matter has effects in more than three Member States, the European Commission is seen as the best-placed authority.

⁶¹ Competition and data protection in digital markets: a joint statement between the CMA and the ICO (19 May 2021) (<https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf>).

⁶² *Ibidem*, para 100.

⁶³ *Ibidem*, para 104.

⁶⁴ CMA Market study final report of 1 July 2020 on online platforms and digital advertising.

⁶⁵ Council Regulation 139/2004 of 20 January 2004 on the control of concentrations between undertakings [2004] OJ L24/1. The Treaty legal basis allowing such central enforcement is Article 103 TFEU.

⁶⁶ Merger Regulation, art.1(2): (i) Combined worldwide turnover of all undertakings concerned is more than € 5bn, and (ii) individual EU-wide turnover of at least two undertakings concerned is more € 250m, unless (iii) each of the undertakings achieve more than two-thirds of its EU turnover in the same Member State.

⁶⁷ Council Regulation 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, O.J. [2003] L 1/1, as amended.

⁶⁸ Commission Notice on cooperation within the Network of Competition Authorities [2004] OJ C101/43.

Of much less importance, the enforcement of the rules imposed for airlines' Computerised Reservation Systems is also centralised at the European Commission.⁶⁹ In this case, the providers of Computerised Reservation Systems should submit, every four years, an independently audited report detailing the ownership structure and governance model of their systems.⁷⁰ The European Commission can launch investigations and take infringement decisions following procedures that are very similar to the one followed in a competition law case.⁷¹

From a legal perspective, the logic behind these (semi) centralised systems is the same: an EU institution should look after market actors when their conduct may affect the EU market in a significant manner, while national regulators are better placed to supervise conduct whose effects are largely national in scope. There is a certain economic logic to this as well, as the EU-wide regulator is better placed to carry out a welfare assessment for the EU as a whole instead of a national regulator. Procedurally, provided the dividing line between EU and state regulation is clear and based on easy-to-use criteria, the system can allocate enforcement cases in an effective way.

Currently, we are seeing **more centralisation within the EU. As explained below, Banking Union with the centralisation of the supervision of the significant banks in the Eurozone provides an interesting case study.** An optimistic reading is that faced with under-performing national regulators, the EU centralised enforcement by identifying the banks that posed the highest risks and this was achieved by designing a supervisory scheme that continues to involve national financial supervisors (who normally have superior knowledge of the institutions in question) but which is administered by the ECB (which is independent and which takes into account the interests of the EU as a whole and not just the domestic interests of national supervisors). A pessimistic reading is that this institutional revolution was only possible because of two features: (i) a huge shock to the economic and financial stability of the EU during the 2008 financial crisis and 2010 Euro crisis, and (ii) a legal basis in the TFEU that allowed the EU to empower the ECB to supervise banks. In other words: while the Banking Union should logically have occurred much sooner (the systemic risks posed by large banks were clear before 2008), it took a major crisis of the EU to agree to centralised supervision.

The recent **DMA and DSA proposals, may also suggest a new pattern emerging where the European Commission takes charge of some big platforms.** Like in the Banking Union, the selection criteria are based on the economic significance and cross-border presence of the platform as a proxy for the firms that generate the greatest risks at the EU level. Unlike the Banking Union, however, the DMA proposal only provides for minimum standards: stricter prohibitions may continue to be imposed on gatekeepers by the application of EU and national competition law. The DSA proposal imposes a regime specifically for Very Large Online Platforms (VLOPS).⁷² However, it should be noted that, during the present legislative negotiations, Member States insist that national authorities should play more of a role in supporting the European Commission and in enforcement.

A more general question arises whether a **single EU-wide regulator for the biggest digital platforms might be considered.** This would be designed to take the EU interest into consideration and it would avoid differentiated enforcement. As the Banking Union reveals, there can also be productive synergies between the EU regulator and the national authorities on the model of the joint supervisory teams. However, there remain several issues to be considered before creating EU-wide regulators. One is constitutional, which is the limited powers that the EU has in delegating enforcement to agencies. The other is political, which is the reluctance of Member States to depart

⁶⁹ Regulation 80/2009 of the European Parliament and of the Council of 14 January 2009 on a Code of Conduct for Computerised Reservation Systems OJ [2013] L 35/47. This Regulation was adopted on the basis of Articles 71 and 80(2) TFEU.

⁷⁰ CRS Regulation 80/2009, art.12.

⁷¹ CRS Regulation 80/2009, arts.13-16: The Commission may act upon complaint or ex officio and sent to the undertakings concerned a statement of objections. If the Commission finds a violation of the Code of conduct, it adopts a decision requiring the undertaking to bring such violation to an end and it may impose a fine not exceeding 10% of the annual turnover

⁷² DSA proposal, Articles 27 to 33.



from a decentralised model. There is a third issue which is that centralisation requires a heavy investment in resources to make sure that any EU regulator has sufficient powers to enforce the rules effectively. One can also discuss whether to centralise only some of the tasks. For example, using the DMA as a model, the regulatory tasks are: designation of gatekeepers, a specification regarding the conduct expected of them, monitoring for compliance and enforcement. It may be that there are advantages in leaving the first two tasks to the EU-wide regulator, but more expedient to decentralise monitoring and enforcement. There may also be specific issues which are best handled at national level having regard to the interests protected.

03

**COORDINATION IN
PRACTICE**

3 Coordination in Practice

In this section, we discuss a set of case studies that help illustrate how the current system of enforcement cooperation operates and identify the strengths and weaknesses. First, we deal with coordination when there is a strong policy dimension, then we deal with the coordination at the EU level for the same legal instrument and finally, we deal with the coordination at the national and EU level across legal instruments.

3.1 Coordination with a policy dimension

3.1.1 *The NIS Directive*

Cybersecurity operates at a different level from many of the technical challenges that other regulators engage with. Its principal concern is the integrity of the network system which service providers like the online platforms use to reach consumers. The NIS Directive (concerning measures for a high common level of security of network and information systems across the EU) is the result of pre-existing exchange among Member States, and the Directive seeks to achieve two related objectives: on the one hand to formalise and strengthen cooperation among Member States and on the other to ensure that all Member States have upgraded capacities to deal with cybersecurity challenges (referred to as minimum capacity building).

At the substantive level, the Directive imposes that all Member States adopt a national strategy on the security of network and information systems. This strategy includes its priorities, risk assessments, and the roles and responsibilities of national actors. It is to be communicated to the European Commission.⁷³

The Directive also imposes security and notification requirements to operators of essential services and digital service providers (e.g., electricity networks, airports). Member States should designate the providers of essential service providers and they have done so in a very different manner.⁷⁴ The obligations include taking appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations.⁷⁵

At the institutional level, the Directive lays down obligations for Member States to designate national competent authorities, single points of contact, and CSIRTs with tasks related to the security of network and information systems. These three may be a single institution and if they are separate then they must cooperate to achieve the objectives of the Directive.⁷⁶ National competent authorities are tasked with monitoring the compliance of regulated firms with their obligations,⁷⁷ while single points of contact and CSIRTs are designed to facilitate cross-border communication of cybersecurity incidents.

A Cooperation Group is set up to support and facilitate strategic cooperation and the exchange of information among national competent authorities and to develop trust and confidence amongst them.⁷⁸ This group focuses on developing best practices and sharing experiences among the

⁷³ NIS Directive, Article 7.

⁷⁴ Report from the Commission of 28 October 2019 assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148 on security of network and information systems, COM(2019) 546.

⁷⁵ NIS Directive, Articles 14 and 16.

⁷⁶ NIS Directive, Article 10.

⁷⁷ NIS Directive, Articles 15 and 17.

⁷⁸ NIS Directive, Article 11 and Commission Implementation Decision 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, OJ [2017] L 28/73. See <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>

regulators. Also, a **CSIRTs network** is established to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation.⁷⁹

For the purposes of this report, three aspects stand out in this Directive.

1. The first, as discussed above, is that the **Directive requires Member States to make policy choices** in ways that other systems of platform regulation discussed in this report do not. As discussed earlier this is reflected in the more politicised institutional setup.
2. The second is that the **powers and independence of the national authorities are under-specified** in the NIS Directive. As previously noted, the NIS2 proposal includes further specification for the powers of investigation and sanction for national competent authorities (aligning these with the powers found in competition law and the GDPR as well as the DMA proposal) but still does not specify the duty to ensure that national competent authorities remain independent. Given that there is a general alignment in this respect in other fields of regulation, this gap points again to the more political role that cybersecurity plays as a matter of national security.
3. The third is that there are some **overlaps between cybersecurity and other EU rules relating to digital markets**, notably the rules on data protection. However, these were not foreseen explicitly at the time of the NIS Directive.⁸⁰ In this respect, ENISA has published a Handbook on Security of Personal Data Processing in 2017, but closer institutional cooperation between the regulators in charge of cybersecurity and data protection would be welcome. As we discuss further in the report, there is an increased recognition that cross-institutional networks are necessary.

3.1.2 Policy choices in cybersecurity: 5G Toolbox

An interesting specific aspect of cybersecurity regulation is the document issued by the Cooperation Group 'Cybersecurity of 5G networks EU Toolbox of risk mitigating measures', released in January 2020. This is a non-binding document aims to "identify a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks."⁸¹ Even before entering the technicalities of the Toolbox, the real aim seems to ensure that some foreign suppliers are vetted closely and perhaps even excluded from certain EU markets. For the purposes of this report, we focus on the institutional considerations that this Toolbox gives rise to.

In brief, **the concern is that 5G infrastructure can be the source of cybersecurity threats. The Toolbox is a call for Member States to align their assessment of these risks and the criteria to be utilised for this analysis.** More specifically mobile network operators are expected to strengthen their security requirements and Member States are expected to assess the risk profile of 5G suppliers and to exclude some suppliers if this proves necessary to mitigate cybersecurity risks. Furthermore, Member States are expected to ensure that operators do not depend on one supplier, in particular when this is a high-risk supplier, but rather source their equipment requirements from a diverse range of suppliers.⁸² The Toolbox distinguishes between technical and strategic actions that may be taken. Technical actions include ensuring the security of software and physical infrastructure or using EU 5G certifications for components. Strategic measures include audits, imposing requirements on buyers to purchase from a range of vendors, all the way up to excluding some suppliers.⁸³ It is important to bear in mind that many of the measures envisaged will require

⁷⁹ NIS Directive, Article 12. See <https://csirtsnetwork.eu/>

⁸⁰ For discussion see Markopoulou et al, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation (2019) 35(6) *Computer Law & Security Review* 105336 (<https://www.sciencedirect.com/science/article/pii/S0267364919300512#sec0012>).

⁸¹ 5G Toolbox, page 4.

⁸² Commission, Secure 5G deployment in the EU - Implementing the EU toolbox COM(2020) 50, pp.5-6.

⁸³ 5G Toolbox, pages 11-12.

legislative steps taken by Member States or the EU, while only some of these steps will require action by national authorities. Our focus in this report is on the latter only.

Insofar as this is part of a soft law document interpreting the powers that national authorities have under the NIS Directive, then this is a familiar approach whereby national regulators' efforts are aligned so that even if there is home state control each controller adopts similar criteria for assessment, and it is expected that results should converge.

One intriguing aspect of this Toolbox is the exhortation on Member States to ensure that national authorities have adequate powers to address 5G cybersecurity threats. This was probably designed as a second-best until the NIS Directive is revised, and in common with other fields of digital regulation it reveals that one of the challenges of EU-wide regulation is ensuring that all authorities have comparable powers and resources. The absence of a requirement of independence for these authorities remains, which may partly be driven by the national security issues at play.

A difference between this document and other soft law instruments drafted by other EU networks of regulators is that **there is a distinctly political tone to the document** as it touches issues related to national security. Consider for example the list of factors to determine if the supplier of 5G software is likely to be influenced by a non-EU country. Here the recommendation is that one considers if there is a strong link between the supplier and a government of a third country, which may be evidenced by the following: (i) the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country, (ii) the characteristics of the supplier's corporate ownership, and (iii) the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.⁸⁴

This is **different from the technocratic approach followed by other EU regulations of digital markets**. Obviously, legislation like the DMA has a policy ambition: to secure more open markets and facilitate the emergence of credible rivals to the Big Tech. However, there are several points of distinction between the 5G toolbox and the DMA proposal:

- Most obviously, the DMA is grounded in secondary law, not in a soft law document. There is thus nothing illegitimate for the EU legislator to seek to pass laws to accomplish the mandate that has been conferred upon it by the EU Treaty. In contrast, one might query how far soft laws can be designed to codify an aggressive cybersecurity policy such as that here, in particular one that risks going beyond the legal mandate in the NIS Directive.
- Even if the DMA may be seen by some critics as targeting specific US firms active in some markets, the legislation proposes that if a service provider is a gatekeeper, then there can be a challenge to that designation. This is important because EU legislation has to respect the principles of due process and of proportionality. This avoids the risk of over-enforcement. It follows that the absence of a procedural pathway by which a firm who is excluded from the EU market as a result of a finding that it is a high-risk vendor does not have a clear pathway to challenge that decision is problematic. This is even more worrying given that risk assessment is carried out by Member States rather than by an independent agency. Granted, there may be reasons for treating cybersecurity differently, but it is also arguable that risk assessment of even such sensitive fields should be based on objective factors and be justiciable.
- A theme that we observe emerging in other fields of digital regulation is that regulators engage in dialogue with the firms subject to regulation. In the DMA proposal, for example, this may be found in the provisions for regulatory dialogue.⁸⁵ In this context however, it does not look like there are any formal mechanisms by which a supplier of 5G equipment can

⁸⁴ 5G Toolbox page 42.

⁸⁵ DMA Proposal, Article 7.

propose adjustments to respond to the risk assessment carried out. It may well be that risk mitigation is a matter of dialogue between the countries.

Thus, for cybersecurity as for the other objectives pursued by EU laws in the digital economy, one might expect according to the European Commission's Better Regulation Guidelines⁸⁶ a procedure where the policy choices are discussed with the industry and where national authorities' decisions are based on transparent technical assessment, are justified and subject to appeal. While one might sympathise with the policy objectives pursued by the European Commission and the Coordination Group, it is **doubtful that the current approach of the 5G Security Toolbox is built in a manner that is entirely consistent with principles of good governance that EU laws have usefully imposed in other fields of digital regulation.**

In the **proposed NIS2 Directive, the European Commission tries to embed the 5G Toolbox more fully into hard law.** The proposal specifies that in drawing up a cybersecurity strategy, Member States shall adopt "a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services."⁸⁷ Likewise, entities that fall to be regulated by the Directive must carry out risk management measures vis-à-vis "supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services."⁸⁸ In carrying out risk assessments of the supply chains, the Member States are expected to make reference to the 5G Toolbox.⁸⁹

In sum, the proposal makes explicit the scope of risk assessment to include suppliers and it strengthens the obligation for Member States to consider the risk assessment measures in the 5G Toolbox. This NIS2 proposal comes less than a year after the Toolbox was adopted and indicates concerns that Member States might otherwise not take the necessary measures.

There is another aspect of the proposed NIS2 legislation which is linked to this: the proposal for coordinated risk assessments in Article 19: "The Cooperation Group, in cooperation with the European Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, taking into account technical and, where relevant, non-technical risk factors." As presently drafted, the legal value of this coordinated risk assessment is not clear. It is not for the Cooperation Group or for the European Commission to issue decisions to exclude suppliers or to identify other risk mitigation measures. Nevertheless, this risk assessment will be perceived as a factor that influences the choices Member States make themselves.

The proposed NIS2 legislation addresses the first concern we raised above: it confers powers on Member States to vet suppliers of 5G equipment for cybersecurity risks. However, it does not appear to address the second and third concerns identified above – while placing supply chain security onto a legislative footing serves to legitimise the policy consideration, the legislation fails to afford the parties who are potentially adversely affected a chance to question the risk assessment. It is also plausible to claim that the non-technical aspects of the Toolbox risk reaching arbitrary results and may also be questioned from the perspective of proportionality.

3.2 Cross-country coordination

In the section, we review the practical functioning and effects of the EU coordination mechanisms and networks which have been set up for the main EU laws applicable to digital platforms. First, we analyse the coordination mechanisms applicable to the laws following the country of origin model

⁸⁶ Commission Staff Working Document of 3 November 2021, Better Regulation Guidelines, SWD(2021)305.

⁸⁷ NIS2 Proposal, Article 5(2)(a).

⁸⁸ NIS2 Proposal, Article 18(2)(d).

⁸⁹ NIS2 Proposal, Recital 47.

(data protection and e-Commerce) and then the mechanisms applicable to the laws following the country of destination model (consumer protection, competition, and electronic communications).

3.2.1 Data protection law: European Data Protection Board

As we noted above, the GDPR sets up a system of enforcement where a single authority can issue decisions that impact a firm's conduct across the EU as a whole. But there is a mismatch between the law in the books and the law in action. The text of the **GDPR makes it clear that a lead supervisory authority is empowered to enforce the GDPR in close cooperation with other data protection authorities in cases of cross-border processing of data**. Authorities cooperate in gathering information and strive to reach a consensus in determining whether there has been an infringement. This creates a one-stop-shop where considerable efforts are made to ensure that the decision of the lead authority is one that has the agreement of other authorities.

However, even if the system is relatively new, its **effectiveness has been called into question by several studies**. Of particular significance is a report by the Irish Council for Civil Liberties which highlights not only the fact that while Ireland is the main enforcer for Big Tech firms it has not been active with sufficient vigour against these firms, but also that across the EU, authorities are under-resourced and under-staffed.⁹⁰ The European Parliament has voiced similar concerns.⁹¹

More recently the Belgian supervisory authority sought to act against Facebook and a preliminary ruling was sought by the Belgian Court. This confirmed that the only instances where an authority which is not the lead authority may only enforce the GDPR are limited to the circumstances foreseen by the Regulation itself.⁹² This judgment is of particular significance because the ECJ heard arguments about the risk of under-enforcement that could be inherent in the system. The Advocate-General, whose Opinion was followed by the Court, advised that the Court had received insufficient evidence of a risk of under-enforcement. However, he left the impression that there may be ways for the Court to interpret the GDPR to enhance the data subject's rights should there be a clear risk of under-enforcement. This leaves the door open for further attempts by national authorities to apply the GDPR to cover for the gaps of the lead agency. The judgment is also important for emphasising that the lead authority has a duty to take an EU-wide perspective and to cooperate with others. In this respect, it reveals the potential for the coordination procedure in the GDPR. This has also consequence that could go beyond the GDPR as the **ECJ may condemn a Member State for breaching its Treaty obligation of sincere cooperation when its national authority acts without paying sufficient attention to what is happening outside of its borders (no coordination) and fails to act as an EU actor (no incentive to rule for the rest of the EU)**.

Beyond such possible condemnation, if the lead authority is not effective enough in regulating for the whole of the EU, other consequences are possible. First, **the authorities of the Member States where the digital services are provided may rely other legal tools which are based on the countries of destination principle** to remedy the ineffectiveness of the lead privacy regulator, even if this is at the risks of mixing the goals of the different legal instruments. Different actions against Facebook/Meta have shown that the German competition authority is ready to condemn digital platforms for a violation of privacy rules which may also constitute a violation of competition law⁹³ or that the Italian consumer protection authority is ready to intervene when the violation of

⁹⁰ <https://www.iccl.ie/digital-data/2021-gdpr-report/> For a comparison of the resource of the different privacy regulators, see the EPBP Report of 5 August 2021 with an overview on resources made available by Member States to the Data Protection Authorities and on enforcement actions by the Data Protection Authorities. The report shows that the regulator from Ireland and Luxembourg which supervised most of the Big Tech are not the best financed in the EU.

⁹¹ European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, paras. 12-22.

⁹² Case C-645/19, *Facebook v. Belgian Privacy Authority*, EU:C:2021:483.

⁹³ Bundeskartellamt, Case B6-22/16 *Facebook*, 6 February 2019, available at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3600108>. Bundesgerichtshof, KVR 69/19 *Facebook*, ECLI:DE:BGH:2020:230620BKVR69.19.0, 23 June 2020, par. 104-105.

privacy rules also constitutes a violation of consumer protection law.⁹⁴ Second, **EU lawmakers may call for a centralisation of the oversight and enforcement of the GDPR against the largest platforms**, thereby following the path chosen for the DSA and DMA rules.⁹⁵

3.2.2 The e-Commerce Directive

The e-Commerce Directive encourages **cooperation and mutual assistance between Member States and with the European Commission** for the implementation of the rules on Information Society Services, in particular through the establishment of national contact points.⁹⁶ In 2005, EU expert group on electronic commerce, composed of the different national contact points and chaired by the European Commission,⁹⁷ has been set up to discuss the derogation to the internal market clause, codes of conduct, liability of intermediaries and national notice-and-takedown procedures.⁹⁸ In addition, national authorities use the multilingual secure online application Internal Market Information (IMI) System to facilitate communications and support cooperation between them.⁹⁹

However, **in contrast to other networks, the experience here has been negative**. According to the preparatory documents for the DSA, there are two reasons for the lack of success: there is an absence of a clear framework for coordination (e.g., lack of legal powers and duties to cooperate, absence of timeframes) and also a lack of responsiveness by the authorities.¹⁰⁰

3.2.3 Consumer protection laws: Consumer Protection Cooperation Network

One of the most promising examples of a system of cooperation among national regulators is found in the field of consumer law, with the CPC Network, even though there is a difference between the expected functioning of the network and its actual operation. The expectation was that the consumer protection authorities and the European Commission would identify instances where a firm is infringing some aspects of EU consumer law such that there is a 'widespread infringement', and then the authorities would cooperate by sharing information and coordinating enforcement action. This would have resulted in coordination at the stage of investigation and enforcement. The European Commission's position is that the system is successful in securing EU-wide commitments from a number of digital actors, and relevant cases are reported on its website. Of particular interest is that all coordinated enforcement actions have resulted in commitments from the firms and that no case has reached the stage where penalties are imposed. An analysis of the several commitment decisions gives the impression of a well-coordinated network that de facto yields EU-wide remedies that are consistent, without the need for a single, supra-national agency.

⁹⁴ Press release AGCM, 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook', 12 May 2017, available at <https://en.agcm.it/en/media/press-releases/2017/5/alias-2380>. N. Zingales, 'Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law', *Computer Law & Security Review* 2017, p. 555-556.

⁹⁵ As put by Commission Vice-President Jourova at the 11th Annual Conference on data protection & Privacy conference of 2 December 2021: "Either we will all collectively show that GDPR enforcement is effective, or it will have to change [...]. Any potential changes will go towards more centralisation, a bigger role for the EDPB or the European Commission": <https://dataprotection-conference.com/>. In the same vein, the EDPS will hold a conference in June 2022 to 'explore both constructive improvements that exist within the current framework, but also alternative models of enforcement of the GDPR, including a more centralised approach': https://edps.europa.eu/system/files/2021-11/21-11-15_the-future-of-data-protection-conference-leaflet_en.pdf

⁹⁶ e-Commerce Directive, art.19.

⁹⁷ Commission Decision 2005/752 of 24 October 2005 establishing an expert group on electronic commerce [2005] OJ L282/20. The composition of the group, the agenda of the meeting and the documents discussed are available at: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=1636>

⁹⁸ Commission Staff Working Document of 11 January 2012, Online services, including e-commerce, in the Single Market, SEC(2011) 1641, p.23.

⁹⁹ Regulation 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (the IMI Regulation), OJ [2012] L 316/1, as amended. Between 2013 and 2019, Member States exchanged 139 requests and 105 notifications related to the ECD via the IMI System: https://ec.europa.eu/internal_market/imi-net/statistics/2019/08/e-commerce/index_en.htm

¹⁰⁰ Impact Assessment Report of the Commission Services on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), SWD(2020) 348.

However, **a closer look at some of the procedures reveals that the system does not necessarily function as smoothly as it is portrayed either in the Regulation or in the European Commission's presentation of the results.** The following observations are the result of interviews with stakeholders and while they do not cover all instances of coordinated enforcement, they help illustrate how the system works in practice and where improvements may be made.

First, at a procedural level, some coordinated actions proceed very quickly while **in other instances it takes longer** for the national authorities to set up a coordination mechanism, with firms at times having to prompt the national authorities and the European Commission to set up a coordinated action. This also reveals that firms prefer coordinated action because it provides them, de facto, with a one-stop shop. At the same time, some concerns were expressed about the **limited transparency** of the system, both in terms of how it is activated and how its procedures play out from start to finish: actors reported different modalities.

Second, during the proceedings firms spoke favourably of the ability to communicate collectively to all national authorities at the same time, and the impression is that all authorities have an equal status around the table even if in certain circumstances some authorities are more vocal and take a leadership role, as might be expected. In this context, the impression (contrary to the impression in other fora, like the ECN) is that **the European Commission is not always exercising a leadership role** or perceived to be the most important actor. This might be explained by the distribution of legal powers, but nothing prevents the European Commission from stepping in more decisively to steer discussions.

Third, while a commitment binds the firm to act in a specific manner across the EU as a whole, this does **not prevent some national authorities from taking a harsher line than the EU line.** For instance, the Hungarian authority has imposed a high fine on Booking.com even though the firm agreed on a set of commitments under the CPC framework. This penalty was for other practices that the Hungarian authority identified as contrary to consumer law.¹⁰¹ While nothing prevents this, sustained divergence among jurisdictions could raise questions about the value of coordinated enforcement. On the other hand, as we will see in other contexts, different national authorities have their own enforcement priorities and styles, and these choices are not constrained by EU law.

3.2.4 Competition law: European Competition Network

The **ECN was originally an information-sharing platform.** It was expected that national competition authorities would use it to facilitate knowledge sharing about cases they were taking to identify the best-placed authority to investigate a suspected infringement. This was built on a model whereby the division of labour would be as follows: for infringements spanning more than three Member States, the European Commission would be the best-placed enforcer, and for other suspected infringements, the best-placed NCA would be the one where the firms are situated and where most of the evidence is found. However, in reality, the ECN proved both more and less powerful than the original design.

It has **become more powerful because it is now a forum where NCAs and the European Commission share knowledge about enforcement procedures as well as enforcement strategies.** The ECN+ Directive, for example, is the direct result of discussions in the ECN about the need to strengthen the powers of national competition authorities.¹⁰² Turning to substantive law enforcement, in the context of the pharmaceutical sector the ECN has served to facilitate enforcement across NCAs. This is a sector in which the European Commission prioritised its

¹⁰¹ Hungarian Competition Authority, 'Gigantic fine imposed on Booking.com by the GVH' (28 April 2020)

https://www.gvh.hu/en/press_room/press_releases/press-releases-2020/gigantic-fine-imposed-on-booking.com-by-the-gvh

¹⁰² However, a closer study reveals a less rosy picture because the Directive generally codifies the Commission's enforcement powers as the standard for all NCAs, seemingly ignoring any possible procedural innovations by NCAs. G. Monti 'The Proposed Directive to Empower National Competition Authorities: Too much, too little or just right?' *Competition Law and Policy Debate* 40(3), 2017.

enforcement efforts as a result of a market investigation and where the European Commission has focused on certain practices (pay-for-delay agreements) while national competition authorities have selected other types of infringements (e.g., the French NCA has taken some cases against product disparagement).¹⁰³ It may then be claimed that the enforcement of competition law in this sector collectively allows some authorities to establish precedents that may be utilised by others and that by coordinating activities in a specific sector one increases the deterrent effect of competition law in the sector.

However, its **limitations in facilitating cooperation when it comes to EU-wide infringements have become apparent**. The European Commission lacks the resources to go after every EU-wide infringement and that in digital markets in particular some NCAs have differing priorities and launch enforcement actions that potentially address practices that have EU-wide effects, with the Facebook decision by the German NCA being a notable case in point. However, nothing in Regulation 1/2003 prevents NCAs from acting autonomously from each other. Nevertheless, the remedies imposed by NCAs tend to remain national because no competition authority appears empowered to impose sanctions that have extraterritorial reach, and such powers are not, it seems, conferred upon NCAs by Regulation 1/2003.¹⁰⁴ Accordingly, unilateral action by one NCA when the conduct in question is EU-wide appears sub-optimal.

Furthermore, **there are instances where we have seen one NCA take action with respect to an infringement occurring in its territory and then subsequently the European Commission considering the same, or very similar, issue intervene in the rest of the EU**. The *Aspen* excessive pricing case was originally brought by the Italian NCA, which issued a decision finding an infringement and this was followed by the European Commission issuing a commitment decision on the same facts.¹⁰⁵ This practice has been challenged by Amazon which found itself subject of one investigation by the Italian NCA for infringements in Italy¹⁰⁶ and one by the European Commission for infringements in other Member States.¹⁰⁷ However, this challenge was unsuccessful. The General Court of the EU (ECG) held that the initiation of proceedings by the European Commission was not an act that could be reviewed judicially.¹⁰⁸ One of Amazon's arguments was that this meant that it would have to defend itself twice in respect of the same conduct and it is arguable that this enforcement action appears to nullify the one-stop-shop principle that appeared to be at the heart of Regulation 1/2003.¹⁰⁹ Amazon also pressed the point that this created the risk of different outcomes. But the ECG took the view that if such differences were to arise, they could be dealt with after the decisions were issued and at that time Amazon would be able to seek judicial review of the decision. More generally the Court held that "protection against parallel proceedings provided for by the case-law does not imply any right, for the benefit of an undertaking, to have a case dealt with in its entirety by the Commission."¹¹⁰ This is accurate insofar as one reads the Regulation literally, but a teleological reading might have led one to prevent multiple enforcement for the same or very similar practices across Member States.

From this perspective, the **efforts of NCAs to collaborate in the Booking.com saga concerning its agreements with hotels appeared to show that the NCAs could operate in a manner comparable to that found in the CPC Network**. Initially, three NCAs (French, Italian, and Swedish) led a coordinated discussion with the undertaking and among themselves to identify a set of commitments that would resolve the competition concerns that the NCAs identified. In brief, the NCAs considered that a wide price parity clause (prohibiting the hotel from offering rooms at lower

¹⁰³ European Commission, 'Competition Enforcement in the Pharmaceutical Sector 2009-2017' COM(2019) 17.

¹⁰⁴ This is the position of AG Bobek in *Nordzucker* (Case C-151/20 Opinion of 2 September 2021).

¹⁰⁵ Commission Decision of 10 February 2021, Case AT.40394 – *Aspen*.

¹⁰⁶ <https://en.agcm.it/en/media/press-releases/2021/12/A528>

¹⁰⁷ https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077

¹⁰⁸ Case T-19/21 *Amazon v Commission* EU:T:2021:730.

¹⁰⁹ However, it seems clear that this approach does not violate the *ne bis in idem* principle, see G. Monti, "Managing Decentralised Antitrust Enforcement: Toshiba", *Common Market Law Review* 51(1), 2014, 261-279.

¹¹⁰ Case T-19/21 *Amazon v Commission*, para.45.

prices than those on Booking.com on any sales channel) was anticompetitive but a narrow price parity clause (prohibiting the hotel from offering lower prices in its hotel website) were not problematic. Commitments were thus made not to impose wide price parity clauses.¹¹¹ Once these commitments were made, all other NCAs bar one accepted similar commitments. A unitary solution for the EU was not found as the German competition authority took the view that the commitments were insufficient and that even narrow price parity clauses were anti-competitive. Events following the enforcement actions complicate the picture. First, in France and Italy, the legislator intervened to overturn the commitment decision and banned all price parity clauses.¹¹² Judicial review of the commitment in Sweden generated some uncertainty but ultimately the courts approved of the approach.¹¹³ More recently the German Federal Supreme Court affirmed the decision of the German NCA that narrow price parity clauses are anti-competitive.¹¹⁴ As a result, a uniform approach to assessing this conduct has not arisen, in spite of coordination.

3.2.5 *The European Electronic Communications Code: Body of the European Regulators for Electronic Communications*

Regarding the regulation of electronic communications networks and services, a number of legal tools and institutional coordination mechanisms have progressively been established to ensure regulatory consistency. Regarding the legal tools, **the European Commission can adopt harmonisation recommendations when divergences in the implementation of EU rules by the national authorities create a barrier to the internal market.**¹¹⁵ Over time, the European Commission has adopted a few of those instruments, in particular regarding the remedies to be imposed on operators having significant market power.¹¹⁶ Those recommendations should be taken into the utmost account by the national authorities and, where authorities choose not to follow them because of the specificities of the national circumstances, they should inform the European Commission and give the reasons for deviating from them ('comply or explain').¹¹⁷ The ECJ decided that the national courts also have to take them into consideration, in particular where the recommendations cast light on the interpretation of national measures adopted in order to implement them or where they are designed to supplement binding EU provisions.¹¹⁸ Thus, a national court may depart from harmonisation recommendations only where it considers that this is required on grounds related to the facts of the individual case. If those harmonisation recommendations do not bring enough regulatory consistency, in some limited cases, the European Commission may go further and adopt binding harmonisation decisions.¹¹⁹

¹¹¹<https://webgate.ec.europa.eu/multisite/ecn-brief/en/content/french-italian-and-swedish-competition-authorities-accept-commitments-offered-bookingcom>

¹¹² Monti, 'Galvanising National Competition Authorities in Europe' In Gerard and Lianos (eds) *Reconciling Efficiency and Equity: a Global Challenge for Competition Policy* (Cambridge, 2019).

¹¹³ <http://antitrust-alliance.org/the-swedish-patent-and-market-court-of-appeal-not-established-that-narrow-parity-clauses-restrict-competition/>

¹¹⁴ Decision of 18 May 2021 - KVR 54/20 (an unofficial English language translation is available: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2021/18_05_2021_BGH_KVR_54-20_Booking.com.pdf?__blob=publicationFile&v=3).

¹¹⁵ EECC, art.38(1).

¹¹⁶ Commission Recommendation 2009/396 of 7 May 2009 on the Regulatory Treatment of Fixed and Mobile Termination Rates in the EU, O.J. [2009] L 124/67; Commission Recommendation 2010/572 of 20 September 2010 on regulated access to Next Generation Access Networks (NGA), O.J. [2010] L 251/35; Commission Recommendation 2013/466 of 11 September 2013 on consistent non-discrimination obligations and costing methodologies to promote competition and enhance the broadband investment environment O.J. [2013] L 251/13.

¹¹⁷ EECC, art.38(2).

¹¹⁸ Case C-55/06, *Arcor v Bundesrepublik Deutschland*, EU:C:2008:244, para.94; Case C-28/15, *KPN and Others v Autoriteit Consument en Markt (ACM)* EU:C:2015:610, para.41.

¹¹⁹ Those specific cases are issues regarding market definition and SMP designation (EECC, art.38.3a) or issues regarding numbering (art.38.3b). For instance, Commission Decision 2007/116 of 15 February 2007 on reserving the national numbering range beginning with 116 for harmonised numbers for harmonised services of social value [2007] OJ L49/30, as amended.

To ensure a good coordination among national authorities, a first discussion forum - the European Regulators Group (ERG) emerged from the practice and was formalised by a Commission Decision.¹²⁰ In 2009, this forum was dismantled and BEREC was established by a legislative Regulation, giving it a statutory advisory role in relation to Commission harmonisation instruments and certain NRA market review decisions, as well as giving limited legal effect to its (soft law) advice/opinions (by requiring those to whom it is addressed – the Commission or the NRAs themselves - to take utmost account of them). BEREC is a technical body composed of representatives of independent national regulatory authorities in the field of electronic communications which – among other missions – aims to ensure the consistent and coherent enforcement of the regulatory framework for electronic communications. To this end, BEREC is in charge of producing a number of different guidelines to NRAs and other competent authorities in order to ensure common criteria and a consistent regulatory approach.¹²¹ In the last review of the EU regulatory framework, the lawmakers gave a mandate to BEREC to adopt a number of guidelines to address technically complex issues such as those relating to the application of symmetric access obligations, the assessment of co-investment proposals or the criteria to be met for a network to be deemed of very high capacity.¹²² However, BEREC has no binding decision-making powers even though national regulators and the European Commission should take the utmost account of soft law instruments adopted by BEREC.¹²³

The **coordination and the harmonisation procedures are the most developed for the designation of the operators having significant market power and for the choice of the remedies** to be imposed on those operators. Regarding the designation, national authorities should start their market analysis on the basis of markets defined and selected by the European Commission¹²⁴ and should follow the methodologies of its guidelines.¹²⁵ Moreover, the European Commission has a right to veto draft designations proposed by the national authorities. Regarding the choice of remedies, the national authorities should follow European Commission and BEREC guidelines and a close dialogue between each individual national authority, the European Commission, and BEREC is organised to ensure consistency in remedies imposed across the EU.

Briefly, over time, the **successive reforms of the EU regulatory framework have strengthened the role of the European Commission and BEREC in particular in ensuring regulatory consistency across Europe**, mostly with soft law instruments which have a 'comply or explain' legal effect. However, regulatory decisions continue to be made by the national regulators themselves and the establishment of an EU regulator, which has been proposed at times,¹²⁶ has never been accepted by the EU lawmakers, in particular because the establishment of telecommunications networks remain a national business and is based on tangible assets, contrary to the provision of many digital services which are much more globalised and based on intangible assets.

¹²⁰ Commission Decision 2002/627 of 29 July 2002 establishing the European Regulators Group for Electronic Communications Networks and Services, OJ [2002] L 200/38.

¹²¹ BEREC Regulation, art.3(2).

¹²² See https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/

¹²³ BEREC Regulation, art.4(4) and EECC, art.10(2).

¹²⁴ Commission Recommendation 2020/1307 of 18 September 2020 on a common Union toolbox for reducing the cost of deploying very high-capacity networks and ensuring timely and investment-friendly access to 5G radio spectrum, to foster connectivity in support of economic recovery from the COVID-19 crisis in the Union, OJ [2020] L 305/33.

¹²⁵ Commission Guidelines of 27 April 2018 on market analysis and the assessment of significant market power under the EU regulatory framework for electronic communications networks and services, OJ [2018] C 159/1.

¹²⁶ For instance, Proposal of the Commission of 13 November 2007 for a Regulation establishing the European Electronic Communications Market Authority, COM(2007) 699.

3.3 Cross-regime coordination

While an EU coordination within each legal regime is important to ensure regulatory consistency and effectiveness across Europe, coordination among legal instruments is also key to maximise synergies and minimise conflicts across legal instruments and their associated regulators. This coordination may take place at the national level among different regulators of the same Member State or at the EU level among different regulators from different Member States.

3.3.1 Coordination at the national level

Cooperation among authorities is easier when they share common public policy objectives.

For instance, there is a long tradition of cooperation between competition authorities and authorities in charge of network industries regulation, through exchange of information or consultation on cases and regulatory choices.¹²⁷ Such forms of cooperation may be more or less formalised going from simple informal contacts, to specific legal cooperation obligations, to conclusion of Memorandum of Understanding, or even to the full integration of the authorities as seen in Spain with the establishment of the *Comisión Nacional de los Mercados y la Competencia* (CNMC), or in the Netherlands with the establishment of the *Autoriteit voor Consumenten en Markten* (ACM).¹²⁸

Cooperation among authorities which do not share such common public policy objectives may be more difficult to achieve. Yet this becomes increasingly necessary with the multiplication of laws applicable to digital platforms and possible as some recent experiences in the UK and the Netherlands show. The UK has been at the forefront of regulatory thinking since at least the 1980s and it is where considerable efforts have been made in the past to coordinate the work of regulators. For instance, it was one of the first jurisdictions to group consumer and competition policy in one agency, and mechanisms have been put in place to align the application of competition law and utility regulation on the other.¹²⁹ It is no surprise then that it is a first mover when it comes to stimulating further cross-agency coordination. In July 2020, the Government launched the **Digital Regulation Cooperation Forum (DRCF)** which originally included the CMA, the ICO, and Ofcom and which from April 2021 also includes the Financial Conduct Authority (FCA). This is a non-statutory network that builds on existing cooperation arrangements between the regulators. In light of further legislation to govern digital markets, it was felt necessary to deepen the degree of coordination among the regulators.¹³⁰ The DRCF may also consult with other regulators whose remit may also overlap, for example, the Advertising Standards Authority or the Gambling Commission – one of the tasks of the DRCF is understanding where connections need to be made as a result of overlapping regulation.

At a formal level, the DRCF has **six objectives**, all of which are based on the consideration that each regulator should take into consideration the perspective of the other and that sharing knowledge among the regulators can sharpen the performance of each to ensure that consumer benefits are maximised. Thus, even before any enforcement action is taken by any of its members, the DRCF foresees that knowledge and resources are pooled (objective 3); that the authorities develop a

¹²⁷ On the practical form of inter-authorities cooperation, the International Competition Network and the OECD did interesting surveys: International Competition Network, Working Group on Antitrust Enforcement in Regulated Sectors (2004) Report to the Third Annual Conference in Seoul; International Competition Network, Working Group on Antitrust Enforcement in Regulated Sectors (2005) Report to the Fourth Annual Conference in Bonn; OECD, Relationship between Regulators and Competition Authorities (1999) DAF/CLP(99)8; OECD, Relationships between Competition Authorities and Sectoral Regulators (2005) DAF/COMP/GF(2005)2.

¹²⁸ See P. Alexiadis and Pereira Neto, *Competing Architectures for Regulatory and Competition Law Governance*, EUI-FSR Energy Research Report, 2019.

¹²⁹ G. Monti 'Utilities Regulation and the Competition Act 1998' in B. Rodger and A. McCulloch (eds) *Ten Years of UK Competition Law Reform* (2010) for a discussion of how the early approach favoured the application of regulation, which was unintended. The current system is set by the Enterprise and Regulatory Reform Act 2013, which seems to have improved communication and cooperation between regulators see CMA, *Promoting competition in services we rely on - The annual concurrency report 2021* (22 April 2021).

¹³⁰ The launch document is available here: https://www.ofcom.org.uk/_data/assets/pdf_file/0021/192243/drcf-launch-document.pdf

shared understanding of emerging digital trends to anticipate future developments (objective 4); that they promote innovation by sharing knowledge and experience, including ideas about how to regulate. When enforcement action is foreseen by one of its members then the regulators should ensure open dialogue and joint work to ensure coherence in the manner each regulator applies its rules (objective 1). Regulators will also use their collective knowledge to inform policymaking (objective 2) and to pool this knowledge with global partners (objective 6).¹³¹

These high-level principles indicate that the first task of the **DRCF is to function as a network where information and knowledge are shared**. Globally, it has been observed that many regulatory networks start with information sharing, largely because bringing together regulators with differing perspectives requires a period of dialogue and the building of mutual understanding before any deeper coordination is attempted.

This is confirmed by the first plan of work published by the DRCF for 2021-22, which identifies **four projects** on which the members will work (design frameworks, algorithmic processing, digital advertising technologies, end-to-end encryption) by setting up project teams, sharing resources and expertise and publishing joint findings.¹³² It is worth noting that each of these four issues is related to projects that some regulators have worked on in the recent past. Whether in the future the DRCF will prioritise fields where no regulator has experience remains to be seen, but it is wise to start with policy domains where each regulator has identified some market failures.

At an operational level, the DRCF works by setting up **working groups** on the topics that have been elected and interested regulators as well as a lead organization is identified. Presently the forum works with a virtual secretariat from the various members and a CEO has just been appointed to create a single point of contact to facilitate the operation of the network.¹³³

The CMA-ICO report on competition and data mentioned above is a good illustration of the work the DRCF will seek to stimulate, namely **pooling information and ideas and facilitating an understanding of how other regulators see technological developments and the market failures that arise there**. This can then facilitate a more coherent regulatory output. A further issue where coordination of this kind might be expected is in relation to the protection of minors where the ICO has published a code of conduct on age-appropriate design so that firms comply with data protection laws specifically in relation to children,¹³⁴ while Ofcom regulates video-sharing platforms where one of the objectives is the protection of minors from unsuitable content.¹³⁵ Operationalising the latter may raise data protection issues and the application of the principles of the best interests of the child when designing data protection protocols might usefully make reference to Ofcom's position on the protection of minors. Observe how joint work does not need to involve all the members, but only those regulators whose powers overlap, and there can be synergies to exploit or conflicts of perspective to resolve. This makes for a more focused interaction on concrete issues.

There are obviously some **legal issues that may affect how much cooperation is possible** – sharing of information obtained through formal investigations will be limited by the legal framework unless the parties waive confidentiality, as often happens with cross-border merger control. Parties may find it advantageous to waive **confidentiality** in exchange for a coordinated regulatory approach. These legal issues will become more sensitive the more closely the regulators work

¹³¹ https://www.ofcom.org.uk/_data/assets/pdf_file/0021/192243/drcf-launch-document.pdf

¹³² Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022 (10 March 2021) <https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022#annex-1-the-drcf-objectives-and-operation>

¹³³ <https://www.ofcom.org.uk/news-centre/2021/gill-whitehead-appointed-digital-regulators-forum-chief-executive>

¹³⁴ ICO, Age appropriate design: a code of practice for online services (2 September 2020) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>

¹³⁵ Ofcom, Regulating video-sharing platforms (21 October 2020) https://www.ofcom.org.uk/_data/assets/pdf_file/0021/205167/regulating-vsp-guide.pdf

together on individual cases, and the DCRF is aware that the existing memoranda of understanding between regulators need to be upgraded to facilitate its work.

A second legal issue relates to **accountability**, which the DCRF seeks to address by reporting on its progress regularly. Whether this is sufficient remains to be seen. Insofar as the DCRF is merely about sharing information, then this might be proportionate. However, if the DCRF were to go further and discuss regulatory choices, then this might require greater levels of accountability through *ex-ante* public consultation.

Finally, two important **operational aspects** of DCRF and its members are worth noting. The first is the emphasis on developing skills and capacity in monitoring digital markets. One of the principal challenges with recent technology is understanding how it operates so as to regulate it effectively. The DCRF intends to facilitate knowledge sharing via secondment programmes and members are aware of the need to recruit experts, e.g., in data science and artificial intelligence to be at the forefront of technological developments. The second is that joint work can be about a change in culture among some of the regulators when it comes to enforcement in the digital economy: the DCRF stresses the role of stakeholder consultation and the importance of involving regulated firms so that products and services are designed in a manner that complies with the regulatory framework ('by design' frameworks). This moves away from the deterrence-based focus found for example in the work of competition authorities and towards a more co-regulatory model, with regulators providing high-level guidance for how firms can comply with public policy objectives but then engaging with them to secure that they implement workflows and protocols that achieve this. It will be useful to see how this develops as the work of regulators in the privacy sandbox and digital advertising concludes.

Following the UK pattern, the Netherlands has also just established the **Digital Regulation Cooperation Platform (SDT)** composed of the Authority for Consumers and Markets (ACM), the Data Protection Authority (AP), the Authority for the Financial Markets (AFM) and the Media Authority (CvdM).¹³⁶ Little is known at this time, but the idea behind this platform is closely aligned to the UK approach, focusing first on sharing knowledge and investing in the development of knowledge and expertise in understanding the technology. It is also foreseen that the authorities could deal with digital market failures collectively, however, as we have seen throughout, this report this is something that has yet to happen and may be a useful long-term goal for these networks.

3.3.2 Coordination at the EU level

The **coordination across legal regimes at the EU level is a much more difficult endeavour than at national level** because there is no EU authority for each legal regime to be coordinated.¹³⁷ Except competition law for which the European Commission is in charge, the other legal regimes are applied by national authorities often grouped into EU networks and it may be difficult to coordinate networks. However, **some forms of collaboration are emerging**. For example a member of the EDPB participates in the ENISA advisory group, which recognises the shared interest in matters of data protection.¹³⁸ At the same time, however, we see that the EDPB also responds more formally to draft documents proposed by ENISA, for example on cloud computing where it offered a set of recommendations to better align cybersecurity and data protection policies.¹³⁹ The DORA proposal provides for a cooperation between the European Financial Supervisory Authorities and ENISA in the composition of the oversight forum which should ensure the operational resilience of the digital

¹³⁶ <https://www.acm.nl/en/publications/dutch-regulators-strengthen-oversight-digital-activities-intensifying-cooperation>

¹³⁷ In general on EU coordination, see P. Larouche, 'Coordination of European and Member State Regulatory Policy: Horizontal, Vertical and Transversal Aspects', 5 *Journal of Network Industries*, 2004, 277 and P. Larouche and A. de Streel, 'The integration of wide and narrow market investigations in EU economic law' in M. Motta, M. Peitz and H. Schweitzer (eds) *Market Investigations: A New Competition Tool for Europe?* Cambridge University Press, 2022, 164-215.

¹³⁸ https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020-0051_enisa_ag_redacted.pdf

¹³⁹ https://edpb.europa.eu/system/files/2021-03/letteredpbtoenisa_feedbackooneucscheme.pdf

infrastructures used by the financial firms.¹⁴⁰ Another example is the advice on the data theories of harms and remedies given by the EDPB to the European Commission in the context of the *Google/Fitbit* merger review.¹⁴¹

Another form of (implicit) coordination is when **the European Commission uses EU competition law – which constitutes primary EU law – to indirectly ‘correct’ decisions by regulators based on secondary EU law.** The most well-known example is when the European Commission imposed a fine of €12.6 million against *Deutsche Telekom* (DT),¹⁴² the German telecommunications incumbent, for maintaining a margin squeeze between its wholesale charge for full unbundling of the local loop and its retail prices for access lines. The European Commission’s ex post condemnation of DT was particularly contentious because the company’s wholesale and retail charges had been subject to the ex ante control of the German regulator. The decision to sanction DT was thus an indirect critique of the national regulator’s work. However, as the retail tariffs were regulated with a price cap applying to a basket of services, DT still had some price discretion, and it could have alleviated or at least reduced the squeeze.

Following the European Commission and the General Court, the ECJ held that Article 102 TFEU remained applicable even if the German regulatory authority had already dealt with the case unless DT would have been positively compelled by the authority to act as it did (which it was not).¹⁴³ The underlying message was clear: a firm remains subject to competition law for its course of conduct, even if such conduct would not fall foul of sectoral regulation as applied by a national authority. Competition law therefore prevails.¹⁴⁴ In the subsequent *Spain v. Commission* case, a similar margin squeeze issue arose, with Spain arguing for the primacy of the decision taken by its sectoral authority. The General Court framed the issue more explicitly in terms of a conflict rule.¹⁴⁵ The rule arising from *Deutsche Telekom* and *Spain v. Commission*, therefore, flows from the primacy of competition law (specifically Article 102 TFEU) – as primary EU law – over sectoral regulation, which is secondary EU law.

¹⁴⁰ Proposal of the Commission of 24 September 2020 for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations 1060/2009, 648/2012, 600/2014 and 909/2014, COM(2020) 595, art.29(3).

¹⁴¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf

¹⁴² Commission Decision of 21 May 2003 in Case 37.451 – *Deutsche Telekom*, 2003 OJ L263/9.

¹⁴³ Case T-271/03 *Deutsche Telekom v. Commission*, EU:T:2008:101, at paras. 85-88; Case C-280/08P, at paras. 80-90.

¹⁴⁴ The reverse situation, where a firm would comply with competition law but not with sectoral regulation, has not yet been explored in the case law. In the 1998 Access Notice, the Commission states that in such a case, compliance with competition law does not prevent liability under sectoral regulation. In practice, such cases are unlikely to arise since the 2004 reform (Regulation 1/2003), the Commission has ceased to issue non-infringement decisions under Articles 101 or 102 TFEU, and national competition authorities do not have the power to issue such decisions. Unless a firm would somehow have obtained a court judgment on the issue, it will accordingly not be in a position where it can invoke an actual decision to support a claim that it complies with competition law, in the course of regulatory proceedings.

¹⁴⁵ Case T-398/07, *Commission v. Spain*, EU:T:2012:173, at para. 55: In any event, even if the sectoral regulation referred to by the Kingdom of Spain derives from European Union secondary legislation, it must be stated that, in view of the principles governing the hierarchical relationship of legal rules, such secondary legislation could not, in the absence of any enabling provision in the Treaty, derogate from a provision of the Treaty, in this case Article [102 TFEU].

04

**AN EXAMPLE OF
SEMI-CENTRALISATION:
BANKING UNION**

4 An Example of Semi-centralisation: Banking Union

The supervision of banks in the European Union furnishes a helpful case study to understand how EU-wide centralised regulation can come about and how it may operate. Based on the Single Supervisory Mechanism (SSM), which became operational in November 2014, the ECB has assumed extensive and wide-ranging powers to supervise banks.¹⁴⁶

4.1 Origins

At the substantive level, banking regulation in the EU was gradually harmonised but, at the institutional level, Member States continued to supervise banks in their territory. Cross-border mergers since the late 1990s led to pan-European banking groups and some calls for centralised supervision, but all that Member States agreed to was the creation of the Committee of European Banking Supervisors in 2004. Banking supervision remained based on the principle of home country control. The Committee focused its energy on supporting the European Commission's delegated rulemaking. It lacked the legal authority to have any real impact in facilitating supervisory coordination. Furthermore, there was little appetite for further centralisation: the banking systems were stable and different Member States had national preferences and interests about how this system should operate.¹⁴⁷

The financial crisis changed this consensus. Expert reports observed weak supervision as well as the failure of national supervisors to accounting for systemic considerations and cross-border risks.¹⁴⁸ In a first stage (starting in 2010) coordinated supervision was attempted by transforming the Committee of European Banking Supervisors into the European Banking Authority (EBA). However, even with this new system supervision remained in the hands of national authorities.¹⁴⁹ This was for legal and political reasons. From a legal perspective, doubts remained about how much power the EU could confer to EU regulators, from a political perspective Member States remained reluctant to allow the EBA to make decisions that may have consequences on the national budgets.

However, **as the banking crisis became a sovereign debt crisis (because Member States began to pour huge amounts of money to rescue their banking sector), the European Commission found a window of opportunity to centralise banking supervision further.**¹⁵⁰

The sovereign debt crisis called into question the financial stability of all banks in the EU as they were exposed by holding bonds issued by states experiencing deep financial and economic crises. This led to a huge transformation of the EU institutions: the ECB implemented a range of monetary policy instruments to safeguard the operation of the financial markets and the EU legislator set out a framework to rescue Member States and instituted a European Banking Union. The Banking Union is conventionally described as having three pillars: the Single Supervisory Mechanism (SSM), Single Resolution Mechanism (SRM), and the European Deposit Insurance System (EDIS).¹⁵¹

¹⁴⁶ Council Regulation 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions [2013] OJ L287/63 (hereafter SSM Regulation); Regulation 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation 1093/2010 [2014] OJ L225/1 (hereafter SRM Regulation).

¹⁴⁷ N Moloney, 'European Banking Union: assessing its risks and resilience' 51(6) *Common Market Law Review*, 2014, 1609-1670 for helpful background on the policy and legal issue.

¹⁴⁸ High level report of the group on financial supervision in the EU (2009), known as the de la Rosière Report.

¹⁴⁹ 2010 EBA Regulation, recital 9, describing the ESFS as an integrated network of national and EU supervisory authorities "leaving day-to-day supervision at the national level".

¹⁵⁰ European Commission, 'A Roadmap towards a Banking Union', COM(2012)510.

¹⁵¹ K. Alexander, 'European Banking Union: Effectiveness, Impact and Future Challenges' in D. Bush and G. Ferrarini (eds), *European Banking Union*, 2nd ed, Oxford University Press, 2020.

The takeaways from the origins of the Banking Union are the following.

- First, from the perspective of effectively governing pan-European banks, it was **logical that there should be EU-wide supervision**. However, it was naïve to consider that Member States would agree to centralised enforcement given the importance that national banking systems play in the domestic economy.
- Second, the banking union **came about because of a wider economic crisis** but even this led to a Banking Union that is only applicable to Member States who have the Euro as their currency. This shows how even when the economic logic for centralised EU-level enforcement is compelling, Member States remain unwilling to yield any retained powers until extreme circumstances arise. For the purposes of this report, therefore, institutional failures by national regulators may be insufficient to motivate Member States to move to centralised enforcement.
- Third, from a legal perspective, it is also worth bearing in mind that conferring supervisory powers on the ECB **proved possible because Article 127(6) TFEU allows the Member States to confer on the ECB the competence** to act as a supervisor for credit and other financial institutions.¹⁵² Thus the EU found a pre-existing institution to which it could confer broad discretionary powers. It is worth contrasting this with the establishment of the SRM. Given the narrow scope of the legislative powers in Article 127(6) TFEU, the ECB could not be entrusted with operating the resolution framework. The solution here was to create a new EU agency, the Single Resolution Board: this entity is in charge of determining if resolution should be triggered but the European Commission and the Council exercise residual control over this decision, thereby ensuring those policy choices are under the control of a political EU institution.

4.2 Operation

In banking law, a distinction is drawn between regulation and supervision. Regulation refers to the drafting of rules and standards that govern e.g., minimum capital levels, disclosure requirements, and conduct standards for bankers. Supervision means the monitoring and surveillance of compliance. When acting as a supervisor, the ECB has powers of investigation and enforcement against institutions that are suspected of infringing the regulations.¹⁵³ Much like a national regulatory authority or a national competition authority, the SSM Regulation confers considerable enforcement powers to the ECB so that it may carry out its supervisory tasks adequately.

4.2.1 Significant banks

The ECB discharges its supervisory functions via the Supervisory Board. The Supervisory Board is responsible for overseeing supervision of 'significant' banks, which constitute over 80 percent of banking assets in the euro area.¹⁵⁴ As with merger control, **simple quantitative criteria are used to determine which banks are significant and therefore subject to centralised supervision**: total value of assets; whether it is one of the top three largest banks in its home Member State; its importance to the economy of its home state or the EU as a whole; and whether it has requested or received direct public financial assistance from the European Stability Mechanism or the European Financial Stability Facility.¹⁵⁵

The Supervisory Board utilises Joint Supervisory Teams (JSTs) to oversee the operations of the significant banks. These teams are composed of members of the ECB and members of the national competent authorities of the home and host state supervisors in the member states where

¹⁵² "The Council, acting by means of regulations in accordance with a special legislative procedure, may unanimously, and after consulting the European Parliament and the European Central Bank, confer specific tasks upon the European Central Bank concerning policies relating to the prudential supervision of credit institutions and other financial institutions with the exception of insurance undertakings."

¹⁵³ Kern Alexander, *Principles of Banking Regulation*, CUP, 2019, pp.41-44.

¹⁵⁴ As of July 2021, the ECB directly supervises 114 credit institutions in the Banking Union. See European Central Bank, Banking Supervision webpage <https://www.bankingsupervision.europa.eu/banking/list/html/index.en.html>

¹⁵⁵ SSM Regulation, Article 6 (4)(i)-(iii).

banks operate. JSTs conduct the day-to-day supervision of ECB supervised credit institutions.¹⁵⁶ The size, overall composition, and organisation of a Joint Supervision Team are tailored to the size, business model, and risk profile of the bank it supervises. **All decisions are taken at the EU level by a Supervisory Board of the SSM** composed of a Chair appointed for a non-renewable term of five years and a Vice-Chair chosen from among the members of the ECB's Executive Board, four ECB representatives, and the representatives of national supervisors.

JSTs have been found to work well in establishing systems of cooperation between members of different authorities.¹⁵⁷ However, there are reports of some obstacles, including language barriers and different supervisory cultures.¹⁵⁸ When it comes to substance, it has been observed that the SSM has brought about a more formal and demanding standard of supervision.¹⁵⁹

4.2.2 Smaller banks

The **Supervisory Board is also responsible for overseeing the supervisory actions of participating national authorities who directly supervise small and medium-sized credit institutions in the SSM regime.**¹⁶⁰ The ECB has ultimate discretionary authority to decide whether to intervene and to take supervisory decisions that could supersede the decisions of national competent authorities with respect to smaller credit institutions that the ECB does not directly supervise. Essentially, the ECB's competence (based on article 127(6) TFEU and as defined more precisely in the SSM Regulation) is to ensure that its tasks (as enumerated in article 4 of the SSM regulation) are fulfilled by supervision of 'significant' credit institutions and the financial groups in which they operate and to be indirectly responsible for – and to have discretionary authority – ensuring that the supervisory tasks set forth in article 4 SSM Regulation are fulfilled, which may entail taking direct oversight of small and medium-sized institutions that are ordinarily subject to direct supervisory control by national competent authorities.¹⁶¹

4.3 Lessons learned

The centralisation of supervision for the most important banks is similar to the logic animating the DMA and to a certain extent the DSA. However, the comparison should not be extended too far. The DMA and DSA are examples of asymmetric regulation: the larger actors pose greater risks and thus merit stricter rules. Conversely in banking supervision, the logic is that those banks that operate across borders should be regulated in a coordinated manner by an independent agent to avoid the risk of regulatory capture and risks spill-over. However, all banks are regulated: the choice in the SSM is dictated by institutional than substantive considerations.

¹⁵⁶ See Kern Alexander, 'European Banking Union: Effectiveness, Impact and Future Challenges' in Danny Busch and Guido Ferrarini (eds), *European Banking Union* (2nd edn, OUP 2020) pp. 27-91, 64-65.

¹⁵⁷ European banking supervision: Compelling start, lingering challenges
Dirk Schoenmaker, Nicolas Véron 25 June 2016 VoxEU (<https://voxeu.org/article/early-assessment-single-supervisory-mechanism>).

¹⁵⁸ See S. Iwankowski and M. Guthausen, 'Two years of the SSM: a lot done, a lot more to do' (2016) BaFin Division for SSM/SB Coordination
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2016/fa_bj_1610_EinheitlicherAufsichtsmechanismus_en.html German Federal Ministry of Finance, 'The Single Supervisory Mechanism: Lessons learned after the first three years' (German Federal Ministry of Finance's Monthly Report, January 2018)
<https://www.bundesfinanzministerium.de/Content/EN/Downloads/2018-01-26-SSM.pdf>

¹⁵⁹ J. Binder, 'The Banking Union and National Authorities 2 Years Down the Line: Some Observations from Germany' 18 *European Business Organisation Law Review* 401, 2017.

¹⁶⁰ *ibid* art 6 (7)(a)-(c). See also art 25 (8) (the Supervisory Board shall adopt 'draft decisions' 'to be transmitted to the national competent authorities of the Member States concerned.').

¹⁶¹ *ibid* art 6 (5)(b), 'when necessary to ensure consistent application of high supervisory standards, the ECB may at any time, or on its own initiative after consulting with national competent authorities or upon request by a national competent authority, decide to exercise directly itself all the relevant powers for one or more credit institutions'.

However, the SSM illustrates well **two advantages of centralisation** which are:

1. It ensures a **regulatory level playing field** across the Eurozone. This is vital because before the reform national supervisory authorities tended to be relatively lenient towards their banks, which led to under-supervision and financial instability. The new system leads to less regulatory capture.
2. It leads to a **holistic and effective regulatory assessment**. Having JSTs supervising the entirety of a bank's operation across the Eurozone makes for a more effective system of supervision. There is useful information sharing among members of the JST; cooperation among national authorities' functions as they are all integrated into a single assessment procedure, led by the ECB. This element reveals the value of joint work between a supranational institution and national authorities. In developing rules like the DMA and DSA this suggests that we think about the optimal interaction between the EU and national levels.

The SSM also illustrates the **challenges of centralisation**, such as:

- The system is still **in transition and there remain national differences** in supervision culture that should be eroded as JSTs continue to work together; there will remain practical barriers to coordination (e.g., language barriers, formal legal requirements) which may slow down coordination.
- The system should ensure **sufficient transparency** of SSM operation to preserve the accountability of the system of supervision.
- The system is so far **less successful in aligning the supervision of non-significant banks**. This is explained by the weaker institutional design as the ECB may step in as a last resort but otherwise, supervision is left to the national authorities.

Another point is also interesting. The EU financial supervision laws provide for one of the closest forms of cooperation between different EU agencies and network as the three European Financial Supervision Authorities (i.e., EBA, European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA)) have established joint committees.¹⁶²

¹⁶² Regulation 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), O.J. [2010] L 331/12 as amended; Regulation 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), O.J. [2010] L 331/48 as amended; Regulation 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), O.J. [2010] L 331/84 as amended, arts. 54-57.

05

CONCLUSIONS AND RECOMMENDATIONS

5 Conclusions and Recommendations

As this report makes clear, an EU harmonisation of the rules as increasingly seen for the platform economy is just the first step. Absent an appropriate institutional design to enforce the rules and a system to coordinate or centralise the enforcement of those rules, one can have divergent enforcement undermining the digital single market as well as risks of under-enforcement (as it may be the case for GDPR enforcement) or risk over-enforcement when multiple regulators intervene and impose remedies or demand commitments that are unnecessary and, in some cases, discriminatory, disproportionate and unjustified. In this concluding section, we present policy recommendations to ensure an effective and legitimate institutional design to implement the rapidly expanding set of EU rules applicable to digital platforms. First, we deal with the **characteristics that any regulatory authority should have**; then we make **recommendations about how to implement a good cooperation system across regulators at the national and at the EU levels**; then we deal with the **pros and cons of centralising some enforcement tasks at the EU level with regard to the largest digital platforms**; and finally, we go beyond institutional design and make a few **recommendations on the enforcement style that regulatory authorities should adopt given the characteristics of the platform economy**.

5.1 Characteristics of effective and legitimate regulatory authorities

Regulatory authorities are the keystone of any regulatory process, and their quality is often the main explanatory variable for the regulatory output. In that regard, the mainstream regulatory scholarship¹⁶³ lists the **main characteristics that regulatory authorities should meet to ensure the effectiveness and the legitimacy of their interventions**. They are the following:

- **Independence, accountability, and transparency**. Regulatory authorities should be independent of the regulated platforms but also of the political institutions to guarantee their credibility in regulating for users long-term interests and ensure that they exercise their powers impartially.¹⁶⁴ To balance this double independence, regulatory authorities should have strict accountability requirements. They should report regularly and transparently to the lawmaker, inter alia, on the state of the digital economy, their decisions, the use of their human and financial resources, as well as on their future action plans. National authorities should also report to the European Commission so it can properly control whether EU law is correctly enforced in the Member States. More generally, the actions of the regulatory authorities should be guided by the objectives of the legal regime they enforce and comply with the good regulatory principles such as effectiveness, proportionality, respect for fundamental rights and due process.

- **Sufficient resources**. Regulatory authorities should have sufficient financial and human resources to exercise effectively their tasks in a complex and fast-evolving environment. Financial resources may come, totally or partially, from an annual fee to be paid by the regulated platforms. Human resources should include experts in data, algorithms, and AI given the increasing importance of those technologies in the functioning of digital platforms.¹⁶⁵

¹⁶³ In general, see R. Baldwin, M. Cave, M. Lodge, *Understanding Regulation: Theory, Strategy and Practice*, 2nd ed, 2012, Oxford University Press; L. Hancher, P. Larouche and S. Lavrijssen, 'Principles of Good Market Governance', *Jour. of Network Industries* 4, 2003, 355-389; Viscusi, Harrington and Shappington, *Economics of Regulation and Antitrust*, 5th ed, MIT Press, 2018. Also P. Larouche, Code of conduct & best practices for the setup, operations, and procedure of regulatory authorities, CERRE Report, May 2014.

¹⁶⁴ On the need of independence for good regulatory enforcement, see C. Decker, *Modern Economic Regulation: An Introduction to Theory and Practice*, Cambridge University Press, 2014, Ch. 7 and P. Larouche, C. Hanretty, and A. Reindl, *Independence, Accountability and Perceived Quality of Regulators*, CERRE Report, 2012.

¹⁶⁵ For instance, the French authorities have set up the Pôle d'expertise de la régulation numérique which offers digital expertise to the French regulatory administrations and the French Competition Authority has established a digital unit. In the UK, the CMA has set up CMA's a Data, Technology and Analytics (DaTA) unit and Ofcom has created an Emerging Technology directorate and data science team.

- **Sufficient powers to collect, process, and exchange information.** One obstacle to good regulatory enforcement has always been the asymmetry of information between the regulators and the regulated, but this obstacle is particularly pronounced in the digital sector which is new, complex and fast-moving. Thus, having a wide power to request information and data from the regulated platforms amplifies the authorities' capacity to act. Moreover, for the cooperation between different authorities (both within a single country and between authorities in different countries) to be effective, information - including confidential ones - needs to be able to be shared among those authorities.

- **Sufficient powers to sanction.** To be credible, regulatory authorities need to have sanctioning powers which are appropriate, effective, proportionate, and dissuasive. In urgent cases, authorities should also be able to adopt interim measures. In the case of a serious breach or repeated breaches of the law, authorities should be able, as last resort, to prevent the regulated platform from continuing to provide its services.

Good regulators are also key to reinforce EU-level principles and rules at the national and local levels consistently as illustrated by the example of short-term rentals. This sector shows an extreme hyper-local regulatory fragmentation such that national and local rules create diverging enforcement outcomes and entry barriers in this market. The European Commission's recent consultation on a harmonisation measure in this sector evidences a careful balancing of interests: on the one hand, this is an economic sector that can support economic growth and innovation; on the other, there are some negative externalities resulting from having too many properties available as short-term lettings.¹⁶⁶ So far, this balancing is left solely to political local authorities without much EU guidance and principles and is only subject to review by the national courts when the regulations are challenged as contrary to EU internal market law and the e-Commerce Directive. This is an unsatisfactory state of affairs. The proposal to generate a form of harmonised framework and principles to be applied by (local) authorities which meet the characteristics of a good regulator is a better option.

Recommendations

The **characteristics of good regulatory authorities (i.e., independence, accountability, transparency, as well as sufficient resources, power to collect and exchange information, and to sanction and enforce)** are increasingly required of the national authorities in charge of the different EU legal regimes applicable to digital platforms.

However, **it may be desirable for the EU to agree on a template for the effective functioning of national authorities that could be applied across the range of regulatory fields and tasks rather than incrementally amending every EU legal instrument in each legal domain.** To be sure, there may well be some powers that are only suitable for some authorities, so such applicable attributes should not furnish an exhaustive list.

Regulators which have those characteristics should contribute to the respect of EU law and principles at the national and local levels, thereby contributing to the effectiveness and proportionality of the regulation as well as to the strengthening of the digital single market.

¹⁶⁶ https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13108-Tourist-services-short-term-rental-initiative_en

5.2 Coordination between national authorities and EU networks

As explained in the previous sections of our report, **two forms of coordination among regulatory authorities are essential in the platform economy**. The first is a cross-country coordination at the EU level among authorities in charge of the same EU rules because the services provided by the digital platforms are often cross-border.¹⁶⁷ The second is a cross-regime coordination at national and EU levels among authorities in charge of different EU rules because the same service provided by the digital platforms are often subject to several rules which overlap to some extent. While both forms of cooperation are thus essential for regulating digital platforms, the analysis of the current institutional design and the case studies show that EU law has developed much more the first (cross-country) than the second (cross-regime) form of coordination.

Regarding cross-country cooperation, the case studies suggest that national authorities are generally eager to cooperate. This is because there are certain distinct advantages in sharing information, obtaining ideas about how to apply the law, and there may also be some useful peer pressure that results from participating in enforcement networks. At a global level, it has been observed that the EU networks of authorities tend to work pragmatically and to cooperate more intensely as a result of repeated interaction.¹⁶⁸ It is also clear that in the past twenty years, experiences in coordinating enforcement have been largely positive and have led to deeper collaboration among the authorities.

Case studies also show that this general willingness to cooperate is greatly facilitated and stimulated by the establishment of pragmatic and flexible framework - often through networks of authorities - which organise such cooperation. The GDPR, the BEREC Regulation, or CPC Network Regulation codify a series of procedures to govern coordination, while these are missing in the NIS and in the e-Commerce Directive, where cooperation has proven less satisfactory. It is worth noting that the European Commission is aware of this: the NIS2 proposal seeks to improve coordination mechanisms and the DSA proposal also specifies in detail how cross-border coordination is to take place. The DSA proposal contains two provisions that facilitate joint work. One is that an authority that lacks jurisdiction on a certain form of conduct may request that the authority who is competent to take the necessary investigatory and enforcement measures to ensure compliance. The authority receiving this request shall take utmost account of this request, it may request further information and is expected to investigate, a failure to do so may be challenged and the European Commission may then request that enforcement action is taken.¹⁶⁹ This addresses the incentive gap that we have identified in other legal frameworks. The second provision allows for joint investigations.¹⁷⁰

Regarding cross-regime cooperation, case studies show that it is not easy because different public policy objectives and regulatory cultures meet and have to understand each other; yet it is possible. At the national level, the British DRCF model which focuses on specific dossiers where cross-regulatory interests are engaged provides a pragmatic model for developing this form of cooperation. At the EU level, there are episodic references to the need for joined-up thinking which require further development. More interactions between the different EU networks of authorities in charge of regulating digital platforms are needed. The cooperation between the three European Financial Supervision Authorities (EBA, ESMA, and EIPOA) formalised through the establishment of joint committees may serve as good practice.

Thus, diversity of cooperation methods and frameworks provide a fantastic real-world experiment which allow us to find best practices which maximise the ability and the incentive for authorities

¹⁶⁷ As the digital services are often provided globally, a global coordination between regulatory authorities beyond the EU is also needed.

¹⁶⁸ A-M Slaughter, *A New World Order*, Princeton University Press, 2005.

¹⁶⁹ DSA proposal, Article 45.

¹⁷⁰ DSA proposal, Article 46.

cooperation of different types: consultation, joint case work and joint technical policy work. Of the case-studies we have seen, telecom regulators have devised a system of cooperation that works well at type 1 (consultation) and type 3 (technical policymaking). The CPC Network has created a legal system that facilitates type 2 coordination, and we are seeing the fruits of this effort in enforcement practices.

Recommendations

At the very general level, the **legal framework should maximise the benefits of cooperation, minimise the costs, and ensure that the former are higher than the latter**. While cooperation has evolved dynamically in the past and we should expect this to continue to happen, we think that at this stage there is enough experience for authorities and legislators to **generalise flexible and pragmatic frameworks to organise authorities cooperation**. This is useful as it creates a structure so that the authorities do not have to invent a procedure each time, hence should reduce the costs of cooperation. It is also important that those frameworks respect the fundamental rights of the parties under investigation. Our recommendation here is for legislative change to facilitate cooperation among regulators by:

- Embedding national authorities in networks to facilitate both **exchange of experience and exchange of information** with necessary safeguards to protect the rights of firms in particular with regard to the confidentiality and due process;
- Exploring processes to **facilitate joint work** when the conduct of one firm is implemented, or has effects in, multiple jurisdictions. When the country of origin model applies, the competent regulator should have the ability – in particular in terms of legal powers – and the incentives to act. The model in the DSA (requests for intervention) can be one way forward. When the countries-of-destination model applies, coordinated enforcement as provided in the CPC Regulation or as is emerging in some competition cases can be replicated;
- Empowering networks to come up with **soft laws** that result from sharing experiences and identifying best practices and that have some legal effects (such as comply or explain effects) as it is the case with BEREC.

Authorities will have limited incentives to participate in cooperative efforts unless they are sufficiently well-resourced, and they can see an individual gain from participation. This latter point might account for the relatively disappointing findings of a study of the application of the AVMSD where the Member States reported difficulties in securing assistance from regulators in the other Member States: from an incentives perspective, it is understandable that a regulator in Member State A will likely give little priority to enforcing the rules against a firm who is infringing the law in Member State B. Thus, while rules and procedures are necessary to secure effective collaboration these are not sufficient.

Those cooperation frameworks should continue to be developed for cross-country coordination, but more importantly they should now be seriously considered for cross-regime coordination. To be pragmatic, this second form of cooperation may have to be first developed at the national level when it is probably easier to implement. Then, they can be expanded more systematically at the EU level, in particular with more interactions among the several EU networks involved in platforms regulation and with the establishment of joint committees as seen in financial supervision.

5.3 Semi-centralising enforcement at an EU body

The DMA and DSA invite a reflection on the merits of centralising enforcement for some parts of platform regulation. We start by explaining the theory of fiscal federalism to explain the costs and benefits of centralisation (5.3.1), then we consider how far the European Commission can play a role as a regulator and make recommendations about the functioning of the DSA and DMA in this regard (5.3.2). We then discuss whether centralised enforcement of some digital platform regulation may be best carried out by an EU agency (5.3.3) and finally discuss the relationship between an EU-wide enforcer and national authorities (5.3.4).

5.3.1 Benefits and costs of centralisation

The optimal level of governance for rule setting and enforcement can be determined based on the theory of fiscal federalism which provides an economic interpretation of the principle of subsidiarity.¹⁷¹ This theory explains the **comparative advantage of centralised and decentralised enforcement**. The **main benefits of centralisation** are the following:

- The internalisation of the cross-country externalities or spill-over effects; they may be particularly important when intangible services, such as the digital ones, are traded across the Member States and on the whole internal market;¹⁷²
- The costs saved by regulated platforms, with the elimination of regulatory duplication (one-stop-shop);
- The economies of scale and transaction costs saved by the regulatory authorities in the design and the implementation of the rules; and
- The additional commitment and coherence as a centralised authority tends to be more independent and less prone to capture by local firms and individual governments.

However, **centralisation brings also some costs** which are due to:

- the information asymmetry which is generally higher at the central level than at the local level;
- a higher distance to local markets and local firms and users;
- the removal of the possibility for regulatory experimentation and innovation to find - and then possibly converge - towards the most efficient form of regulation and, in some cases, the lower responsiveness and flexibility at the central level compared to the local procedures; and
- the heterogeneity of preferences across the Member States which may originate among other from differences in culture, languages, habits, social preferences and which cannot be adequately reflected in a unique central policy.¹⁷³

Moreover, if the centralisation is only limited to some firms, there is an additional risk/cost of lack of consistency in regulatory approach among firms supervised at the central level and those supervised at the local level.

¹⁷¹ A. Alesina, I Angeloni, and L. Schuknecht, 'What does the European Union do?', 123 *Public Choice*, 2005, 275-319; W. Oates, 'Towards a Second-generation Theory of Fiscal Federalism', 12 *International Tax and Public Finance*, 2005, 349.

¹⁷² There is such externality when the regulation (or the absence of regulation) in country A has significant effect on the welfare of the consumers and/or firms in country B and that effect will not be taken into account by the regulator of country A. Those spill over effects are often less important for tangible goods which tend to be more localised such as the deployment of telecommunications networks. Therefore, the absence of EU Telecommunications Authority seems justified to us, but does not imply that an EU Platform Authority would not be justified.

¹⁷³ Those heterogeneity of preferences may be particularly high for media and content regulation, which may explain why the EU media rules are in a Directive and not a Regulation.

Applying this theoretical framework to the EU regulation of digital platforms is not straightforward and does not necessarily lead to unambiguous policy recommendations because the **size of the benefits and the costs of centralisation and decentralisation mentioned above depend on several factors**. Those include:

- The way centralisation is organised (with an EU body, an EU network of national authorities or a lead authority) and the relative quality, agility and performance of the EU vs. national institutions;
- The diverse types of regulatory tasks to be performed, such as (i) the designation of the platforms to be regulated, (ii) the design of the obligations and remedies to be imposed on those regulated platforms, (iii) the oversight of the platforms and the monitoring of their compliance, and (iv) the enforcement and sanctions in case of non-compliance.

Having said that, there are a number of **arguments in favour of opting for a centralised model for some regulatory tasks against the largest platforms being active in several Member States**:

- First, those largest platforms are likely to operate globally, hence with lots of cross-country externalities. Moreover, they operate broadly the same systems across all Member States, due to the economies of scale involved in designing and operating these systems.¹⁷⁴ Therefore, if different national authorities were to require different tailor-made remedies, this could lead to an important reduction in effectiveness and may be difficult to justify based on proportionality.
- Second, monitoring compliance is likely to be costly and may require large-scale data analysis or direct review of algorithm design. It is unlikely that every individual national authority would be well set up to do this, and even if they were it would be duplicative to do it more than once.
- Third, the largest platforms have deep pockets, and securing compliance is more likely if they face a single, well-resourced regulator than a multitude of small authorities who might even disagree with each other on the appropriate course of action. Moreover, a single regulator can benefit from managing a set of cases in parallel and learning across the different cases.

To be sure, this centralised oversight and enforcement does not imply that national authorities will have no role with regard to the largest platforms. It merely means that oversight and enforcement would be centralised at the EU level and that national authorities come in support of such centralised enforcement as explained below in Section 5.3.4. For the other (smaller) platforms, decentralisation has more advantages than centralisation. As explained above, the coordination among national authorities, in particular to exchange information and best practices, may bring economies of scale and reduce transaction costs in rules implementation.

5.3.2 Semi-centralisation at the European Commission

Ensuring effectiveness and legitimacy

If the European Commission wants to become an EU regulator on the model of national authorities in other areas of EU sector-specific regulation, it should rely on a combination of independence, accountability, and expertise. Thus, the European Commission should be independent not only from the regulated platforms but also from political power. However, this need for independence comes in sharp tension with the legislative role that the European Commission plays in proposing legislation. In addition, there is a tension between this need for independence and the (geo)-political role that the European Commission is increasingly eager to play.¹⁷⁵ Thus, the old

¹⁷⁴ A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

¹⁷⁵ U. von der Leyen, *Political guidelines for the next Commission 2019-2024*.

debate on the independence of DG COMP and the need to establish a separate EU antitrust agency¹⁷⁶ may return with a vengeance as the European Commission acquires new regulatory powers and, at the same time, wants to become more political. Moreover, with those increasing powers, the European Commission should also be increasingly accountable, which may imply more hearings of the European Commission department in charge of the DMA and DSA enforcement before the European Parliament and strict judicial review of its decisions by the EU courts.¹⁷⁷

The European Commission should also have **sufficient budgetary and human resources**. For instance, to enforce the DMA, the European Commission foresees a team that should increase over time from 20 FTEs in 2022 to 80 FTEs by 2025.¹⁷⁸ The DMA Impact Assessment is not clear on how the size of the team has been calculated¹⁷⁹ but this low number can partly be explained by the fact that the European Commission expects that most of the DMA obligations would be self-executing because they are detailed. However, the experience of applying the detailed prohibitions of the Unfair Commercial Practice Directive against Big Tech shows how difficult the implementation of such rules is and that the self-execution is a kind of a mirage in the digital economy.¹⁸⁰ Moreover, lots of new issues will be raised at the very beginning of the implementation of the new rules, hence it is important to have sufficient staff from day one and not over time. Finally, the composition of the staff is as, if not more, important than its number as a key, yet challenging task of the European Commission would be analysing databases and algorithms requiring specific human and technical capability to review and interpret the large volumes and variety of data provided by the platforms.¹⁸¹

Maximising synergies between the European Commission powers

With the enactment of the DMA and the DSA, **the European Commission would add to its existing antitrust power important new regulatory powers and is set to become a 'concurrent' regulator. It is key that this palette of powers is used in the most effective way by maximising the synergies between them and in the most transparent manner by justifying why one power is chosen over another.** This has several practical implications.

First, given those synergies between the DMA and the DSA enforcement, it may be best that, within the European Commission, a **joint task force** composed of DG COMP and DG CONNECT would be in charge of enforcing the DMA and the DSA.¹⁸² Such joint task force should contribute to cross regime coordination within the Commission.

Second, the DMA and the DSA should clarify **how the information received during an investigation done under one law** (say the DMA) **could be used for investigation under another law** (the DSA or antitrust). This would require a dedicated legal basis allowing for such an exchange of information.¹⁸³ Legislation should also clarify how the obligations which could be

¹⁷⁶ C-D. Ehlermann, 'Reflections on a European Cartel Office', *Common Market Law Review* 32(2), 1995, 471-486.

¹⁷⁷ However, some commentators submit that such judicial review may not be effective enough because the DMA does not place meaningful constraints on administrative action of the Commission: P. Ibáñez Colomo, 'The Draft Digital Markets Act: a legal and institutional analysis', *Jour. of European Competition Law & Practice*, 2021.

¹⁷⁸ Commission Explanatory Memorandum to the DMA Proposal, p. 71.

¹⁷⁹ DMA Impact Assessment, paras.352-354. Additional indications may be found in Annex of DMA Impact Assessment Study, pp.61-70.

¹⁸⁰ See fn.17.

¹⁸¹ For instance, for the *Google Shopping* antitrust investigation, the Commission had to analyse very significant quantities of real-world data including 5.2 terabytes of actual search results from Google (around 1.7 billion search queries): Commission press release IP/17/1784 of 27 June 2017. As an interesting benchmark, the UK CMA has set up a team of data analysts and AI experts of nearly 50 FTEs.

¹⁸² Similar to the joint Article 7 task force with CONNECT and COMP in telecom in 2003-2006. See also P. Marsden and R. Podszun, *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*, Konrad-Adenauer-Stiftung, 2020, ch.4.

¹⁸³ A similar provision to exchange information between NCA and NRA is included in the EECC, Art. 11. Such sharing of information should comply with the fundamental principles of procedural fairness guaranteed by Article 41 of the Charter of Fundamental Rights of the EU. To do so, Schweitzer explains that two conditions must be met: "(i) the transfer of information must be provided for by law; and (ii) the information transferred must not have been obtained under an investigatory regime that provides for a lower degree of procedural protection than the one that is applicable in the context in which the information shall be used after the transfer": H. Schweitzer, *The New Competition Tool: Its institutional set up and procedural design*, Expert Study for the European Commission, October 2020.

imposed under the DSA (in particular the new transparency requirements on online advertising and on recommender systems) would complement and support the objectives and obligations imposed under the DMA and vice-versa.

Third, the **respective role of the DMA and competition law in policing the conduct of the digital gatekeepers should be clarified**. To intervene against the conducts of the digital gatekeepers which would be regulated by the DMA, the European Commission should rely on its DMA powers as the obligations and prohibitions are compulsory and (supposedly) self-enforcing. The interesting question, however, is which enforcement route the European Commission would follow when intervening against courses of conduct that are not (yet) covered by the DMA. Given the concurrency of powers, the European Commission could choose between competition law or the DMA. Under the former, it would open abuse of dominance case and build a theory of harm to the requisite legal standard imposed by the EU Courts. Under the latter, the European Commission would launch a market investigation and then adopt a delegated act to add the course of conduct under consideration to the list of the DMA obligations. To ensure legal predictability, it should explain in advance the criteria it will use to choose between its competition and regulatory powers.¹⁸⁴ To do that, the European Commission may, for instance, rely on the criteria it uses to select markets for *ex-ante* regulation in telecommunications.¹⁸⁵ On that basis, possible criteria to favour a DMA over competition law enforcement could comprise the recurrence or the prevalence a conduct by different types of gatekeepers, or the need to intervene quickly or with remedies that require an extensive monitoring.

5.3.3 *Semi-centralisation at a European platform authority*

Legal and policy considerations

If the benefits of centralising enforcement of EU rules against the biggest platforms are higher than the costs and if a centralisation at the European Commission were to prove insufficiently effective or legitimate, centralisation at a new independent EU agency - a European Platform Authority (EPA) - could be explored.¹⁸⁶

From a legal perspective, the position today is more welcoming to the creation of such agencies than at the origin of the EU project in the fifties. On the one hand, the EU Treaties provide an unsystematic approach to EU agencies, such that the powers of the EU to create agencies were challenged by the UK. In the resulting *ESMA Short Selling* judgment, the CJEU was confronted with a regulation that empowered ESMA to ban certain short-selling operations to ensure financial

¹⁸⁴ In the UK where most of the regulators have concurrent power, they have concluded MoU with the competition authority which clarify how concurrent powers will be exercised. See for instance, Memorandum of understanding of 8 February 2016 between the CMA and Ofcom on concurrent competition powers. Also P. Crocioni, Ofcom's Record as a Competition Authority: An Assessment of Decisions in Telecoms, EUI Working Paper RSCAS 2019/93.

¹⁸⁵ The selection is based on three criteria, and the third one in particular indicates that: 'Competition law interventions are likely to be insufficient where for instance the compliance requirements of an intervention to redress persistent market failure(s) are extensive or where frequent and/or timely intervention is indispensable. Thus, *ex-ante* regulation should be considered an appropriate complement to competition law when competition law alone would not adequately address persistent market failure(s) identified': EECC, Article 67(1) clarified by Commission Recommendation 2020/2245 of 18 December 2020 on relevant product and service markets within the electronic communications sector susceptible to *ex-ante* regulation, OJ 2020 No. L 439/23, recital 17. On those criteria, see H. Never and B. Preissl, 'The three-criteria test and SMP: how to get it right', *International Journal of Management and Network Economics*, 2008, 100. The Commission could also rely on the criteria proposed by Motta and Peitz to determine when a new EU market investigation tool (the so-called New Competition Tool) would be a better route than an Article 102 TFEU enforcement action. This may be the case when a competition law assessment is long, complex and uncertain or when a competition law assessment would not solve a generalized problem, but just deal with one specific conduct or firm: M. Motta and M. Peitz, *Intervention trigger and underlying theories of harm*, Expert Study for the European Commission, October 2020.

¹⁸⁶ The establishment of such EU authority was already proposed by the High-Level Group on the Information Society chaired by the then European Commissioner Bangemann nearly thirty years ago: Recommendations of the high-level group on the information society to the Corfu European Council (Bangemann group), p.17, available at: http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf Similar call for a Federal Platform Agency is also been made in the US: T. Wheeler, Ph. Verveer and G. Kimmelman, *New Digital Realities; New Oversight Solutions in the U.S. The Case for a Digital Platform Agency and a New Approach to Regulatory Oversight*, Harvard Kennedy School, August 2020.

stability. The CJEU confirmed that on the basis of Article 114 TFEU the legislature could 'deem it necessary to provide for the establishment of an EU body responsible for contributing to the implementation of a process of harmonisation.'¹⁸⁷ In particular, the Court held that such bodies would be useful when specific professional and technical expertise was required. The Court placed some limits: the agency should not make policy decisions and its rulings should be subject to judicial review. This judgment has been regarded by several commentators as opening the door for powerful agencies. A recent judgment confirms this indirectly. Germany has been slow in implementing certain aspects of the EU energy directives, in particular those provisions requiring the establishment of an independent national regulatory agency. In confirming that independent regulatory authorities comply with general EU law principles if they are tasked with a specific mandate (which can be defined politically), then it is legitimate for the EU to require the Member States to create independent regulators. In reaching this conclusion the Advocate General and the Court read these principles as further specifying the Meroni doctrine, thereby implicitly endorsing the option of creating EU agencies with executive powers.¹⁸⁸

The trends in the development of EU agencies suggest that increasingly they are conferred powers to make decisions (and not just powers to offer expert advice). This is coupled with safeguards: EU agencies must have clearly defined tasks (tolerating some exercise of regulatory discretion but agencies should not be making political trade-offs) and their decisions must be susceptible to judicial review. Commentators generally agree that this new legal framework generated by the EU Courts adapts the old Meroni case-law to the necessities of the current regulatory needs of the EU and facilitates the development of new EU agencies.

From a policy perspective, the case studies discussed above also reveal that a system where trust is placed on national regulators to apply EU law may be overly optimistic when it concerns the largest platforms: some national authorities are insufficiently resourced or do not have enough legal power to take into account spill-over effects and coordination among authorities may not be always optimal. This may partly explain the **observable trend towards centralisation for the enforcement some EU legal regimes against those largest online platforms.** The DMA is an example of a legislative project which is premised on the view that centralised enforcement of platforms that operate EU-wide is more likely to yield effective results than decentralised enforcement at a national level. A similar pattern emerges in the DSA with the proposal that very large online platforms may also be regulated by the European Commission. The powers the European Commission is expected to secure under both DSA and the DMA are comparable. While this option may be the best in the short run, once we have experience of the practice of regulating the platforms we might consider whether, in the longer run, the Commission will be the most appropriate body to enforce these rules or whether a specialised EU agency would be preferable.

One advantage of empowering a separate EU regulatory agency is that one might aspire to a greater degree of independence in its operation provided of course that strict independence requirements are imposed to such agency as it is the case for the ECB which supervise the significant banks. The European Commission is increasingly playing a more geo-political role in policymaking.¹⁸⁹ This may create the perception that it risks prioritising policy choices based on considerations that have less to do with the effectiveness of policy and more to do with responding to geo-political considerations. An independent agency should be more technocratic in

¹⁸⁷ Case C-270/12, *UK v Parliament and Council (ESMA Short Selling)* EU:C:2014:18, para 104.

¹⁸⁸ Case C-718/18, *Commission v Germany*, EU:C:2021:662, paras.131 which summarises the Meroni case-law as follows: 'it is not permissible to delegate to administrative bodies a margin of discretion which may, according to the use which is made of it, make it possible to take political decisions in the true sense, by substituting the choices of the delegator by those of the delegatee, and thus bring about an 'actual transfer of responsibility'. However, a delegation of clearly defined executive powers, the exercise of which can, therefore, be subject to strict review in the light of objective criteria determined by the delegating authority, is permitted'.

¹⁸⁹ Nugent and Rhinard, *The 'political' roles of the European Commission (2019)* 41(2) *Journal of European Integration* 203 painting a more subtle picture but observing that in relation to economic and market regulation the Commission has gained political power.

composition and given the legal constraints described above, it would necessarily have a very well-defined mandate.¹⁹⁰ While we are not naïve to suggest that agencies are pure technocracies, firms subject to regulation are likely to prefer dealing with an agency that is formally independent. More generally, development of agencies at the EU level can also serve the long-term interests of the EU by allowing the European Commission to focus more on developing policies while leaving implementation to agencies.¹⁹¹ It has also been suggested that in certain policy fields, Member States may prefer delegating tasks to an agency than to the European Commission.¹⁹² Furthermore, a separate agency can be **staffed appropriately** and can be expected to operate with fewer of the frictions that sometimes occur when different DGs have competing priorities.

However, certain general improvements are needed to legitimise EU agencies further. First, it remains to be seen how robust judicial review is. The CJEU has conferred a fairly wide margin of appreciation to agencies that consider complex economic or scientific evidence: complex assessments mean limited review.¹⁹³ This case law may need to evolve further the more powers agencies obtain. Second, the more powerful the agency is, it is legitimate to require that the independence safeguards that the EU increasingly requires of national authorities are also stipulated for EU agencies. A number of studies reveal that EU agencies are in-between the EU and the Member States and are at times dependent upon one or the other side. Increased powers require increased independence.

Scope of competences and organisation

Given the costs and the benefits of centralisation explained above, the role of an **EPA should be limited to supervision the largest digital platforms** which would be designed on the basis of some simple quantitative criteria that should be used as is the case for the determination of the significant banks supervised by the SSM (or the Community dimension mergers decided by the European Commission).¹⁹⁴ Those criteria could be the annual European turnover, the market capitalisation and the number monthly active users as well as the presence in several Member States as proposed in the DMA and the DSA.¹⁹⁵

The next key question is **which EU laws an EPA should enforce against the significant platforms**. Again, this issues should be determined on a law by law basis according to the costs and the benefits of centralisation.

- One option would be to limit the competence of an EPA to **core economic regulation which mostly aim to make the markets work better** (ensuring efficiency, contestability, and innovation) for which the homogeneity of preferences among the Member States is probably the highest. Under this option, the enforcement of the DMA would be an obvious candidate. The EPA could also be in charge of other economic regulation such as the consumer protection when applied to the significant platforms.
- Another more expansive option would be to also include in an EPA competences **other legislations which mostly aim at protecting broader users' interest and rights, in particular fundamental rights** (such as privacy and pluralism), for which the heterogeneity of preferences across Member States may be higher. Under this option, the

¹⁹⁰ See generally, G. Majone, 'The Rise of the Regulatory State in Europe' (1994) 17(2) *West European Politics* 77.

¹⁹¹ E. Vos, *EU agencies on the move: challenges ahead*, Sieps 2018-1.

¹⁹² *Ibidem*, p.17.

¹⁹³ See e.g., Case T-187/06 *Schröder v CPVO*, EU:T:2008:511; Case T-94/10 *Rütgers Germany v. ECHA*, EU:T:2013:109. This is also the general standard in the review of Commission decisions in the field of competition law, see Kalintiri What's in a name? The marginal standard of review of "complex economic evaluations" in EU competition enforcement. (2016) *Common Market Law Review*.

¹⁹⁴ See fn.64.

¹⁹⁵ Interestingly, similar quantitative criteria have been proposed in the US in the Big Tech Bills, see M. Schnitzer et al., International coherence in digital platform regulation: An economic perspective on the US and EU proposals, Yale Tobin Center of Economic Policy: Digital Regulation Project Policy, 2021, Discussion Paper 5, available at: <https://tobin.yale.edu/digital-regulation-project>

EPA could also be in charge of the DSA as well as other instruments such as the GDPR when both instruments are enforced against the significant platforms.

The **structure and the governance of an EPA** could be inspired by the Common Approach on decentralised agencies agreed by the European Commission, the European Parliament, and the Council in 2012, but with important adaptations to ensure that an EPA meets the characteristics mentioned in Section 5.1 above, in particular independence and agility. Therefore, an EPA should be managed by a Board composed of members with enough expertise in platforms economy and/or digital regulation and fully independent from the EU institutions as well as from the Member States. Moreover, the structure and the staff of an EPA should ensure that it develops a geek – and not a bureaucratic – work culture.

5.3.4 National authorities in support of the semi-centralised enforcement

Next to the benefits of centralisation, there are also **benefits of decentralisation that should be exploited with the involvement of the national authorities**. Two main models are possible.

In the minimalist model, the EU **platform laws would remain enforced centrally against the significant platforms and the national independent authorities would come in support** of the European Commission or an EPA, as it happens for the supervision of the significant banks with the establishment of the Joint Investigation Teams.¹⁹⁶ National authorities are particularly helpful for the tasks for which they have a comparative advantage vis-à-vis an EU body: first, they are more localised, hence may receive more easily complaints from small and local business users; second, national independent authorities have expertise and experience which can usefully support the EU body in designing obligations and remedies to be imposed;¹⁹⁷ third, they are closer to the 'field' and more easily monitor compliance, in particular, the national independent authorities may play a key role in running a mechanism to resolve a dispute between the designated gatekeepers and their business users.

In the maximalist model, **the EU platform laws would be enforced centrally against the significant platforms but they could also be enforced locally against the largest platforms by the national independent authorities** as it happens for EU competition law.¹⁹⁸ Different versions – more or less maximalist - of this model are possible depending on which regulatory tasks would be decentralised. National authorities could do all the regulatory tasks (i.e., designation of the platforms to be regulated, design of the obligations and remedies to be imposed, monitoring of compliance and sanction in case of non-compliance) or only some of them.

It is also key that the **national authorities supporting the European Commission, or an EPA, are independent** of political power and have sufficient expertise. This is by no means guaranteed as several cases seen in this report illustrate. For instance, in the DMA Proposal, the proposed Digital Market Advisory Committee (DMAC) is a comitology committee whose members should be representatives from the Member States, but not necessarily from their independent (competition or

¹⁹⁶ For the enforcement of the DMA, this option is favoured by BEREC: BEREC Proposal of 11 June 2021 on the set-up of an Advisory Board in the context of the Digital Markets Act, BoR (21) 93. Such advisory board would be composed of national independent authorities whereby the different national authorities would be involved in its meetings *ratione materiae*. BEREC mentions for instance *ex-ante* national regulatory authorities in the field of electronic communications, national competition authorities, national data protection authorities. This option is also supported by A. de Streel, R. Feasey, J. Krämer and G. Monti, *Making the Digital Markets Act More Resilient and Effective*, CERRE Recommendations Paper, May 2021.

¹⁹⁷ Indeed, several national authorities have expertise in dealing with digital platforms as well as data and algorithms; they also have experience in implementing some of the obligations of the proposed DMA such as interoperability, access to data or data portability.

¹⁹⁸ For the enforcement of the DMA, this option, this option is favoured by the ECN: Joint paper of the Heads of the National Competition Authorities of the EU of 22 June 2021 on how national competition authorities can strengthen the DMA. This option is also supported by H. Schweitzer, 'The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal', *ZEUP*, 2021.

regulatory) agencies.¹⁹⁹ In practice, national representatives in comitology committees are often coming from ministries which are not independent from the political power and often have less expertise than the regulatory authorities.

To deal with this issue, EU competition law and most EU sectoral economic regulation provide for an additional instance next to the comitology-type committee, namely, a network of independent national authorities. In the same vein, the DMA should establish, next to the DMAC, a network of independent national authorities as proposed by the European Parliament.²⁰⁰ It would then be up to the Member State to decide which (existing or new) national authorities should be designated as their National Digital Markets Authority in such network. In the NIS Directive, semi-political bodies such as the NIS Coordination Group establish recommendations outside the formal legislative process and unlike other EU regulatory networks without independence in the meaning as defined by the CJEU.

Recommendations

There are some **advantages in centralisation some enforcement tasks at the EU level regarding the largest and cross-borders digital platforms**, as proposed by the DMA and the DSA. However, such centralisation **requires good design**, in particular: within the European Commission a joint taskforce of DG COMP and DG CONNECT is needed to secure effective enforcement; rules are needed to determine when and how information gathered about firms under one instrument (e.g., DMA) may be used for investigations under other instruments (e.g., DSA or competition law); the respective role of DMA and competition law needs to be specified.

In the longer term, depending on how the regulatory practice under the DMA and DSA evolves, one might consider the case for an EU authority separate to the Commission, responsible for the enforcement of platform regulation (both the DMA and the DSA) against the largest cross-border digital platforms (a **“European Platform Authority”**). Were this to be pursued, however, it would have to be subject to the same governance principles as should apply to national authorities, as discussed above: independence (politically and of industry), adequate funding, robust information gathering/sharing and enforcement powers.

Either centralisation model at the European Commission or a new European Platforms Authority would require the **involvement and the cooperation with national independent authorities which have several comparative advantages to an EU body**. The lessons from banking union reveal the usefulness of this connection. The degree of power sharing between the EU and national authorities can vary depending on which authority has a comparative advantage in addressing each task.

It might be **considered whether the model of centralised enforcement should go beyond only the DMA and DSA to other aspects of digital platform regulation**. This should not happen without a close study of the costs and benefits of centralisation as indicated by the theory of fiscal federalism and consideration should be given to centralisation not only according to legal instruments but also according to the regulatory tasks. For example, it may be that obligations are set at the EU level, but oversight and enforcement is carried out by national authorities.

¹⁹⁹ Regulation 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission’s exercise of implementing powers OJ [2011] L 55/13, Art. 2.

²⁰⁰ The European Parliament DMA Resolution of 16 December 2021 foresees (at am.208-209) the creation of a European High-Level Group of Digital Regulators consisting of representatives of the Commission, relevant EU bodies and national competent authorities, including in specific sectors such as electronic communications.

5.4 Principles of good regulatory style

Next to the institutional design, which is the focus of this report, the regulatory style is also key for the success of the EU regulatory framework applicable to digital platforms. This final section of the report only briefly with this issue. The mainstream regulatory scholarship²⁰¹ show that authorities should also abide by a number of principles to ensure the effectiveness and the legitimacy of their interventions. Many of those principles are now part of the Better Regulation Guidelines of the European Commission²⁰² and increasingly imposed by the different EU legislation applicable to digital platforms. The case studies have shown that the application of those principles is particularly important for security politically loaded issues, such as network security.

5.4.1 Principles of good regulation

Any regulatory intervention should apply the following three good governance principles which are also mentioned in the EU primary laws:

- **Effectiveness**: any action taken by the regulatory authorities should aim to achieve the objectives of the enforced legislation. This should be demonstrated for every intervention and monitored *ex-post* after the interventions.²⁰³

- **Proportionality**: the content and form of regulatory obligations should not exceed what is necessary to achieve the objectives of the enforced legislation.²⁰⁴ In particular, this principle implies that the regulatory authorities adopt risk-based enforcement and tailor their intervention to the risks created by the services provided by the regulated platforms.

- **Respect of fundamental rights and due process**: the regulatory intervention might impact the fundamental rights of the regulated platforms (such as the freedom to conduct a business or a property right)²⁰⁵ as well as the fundamental rights of their users (such as the respect for private and family life, the protection of personal data, or the freedom of expression and information).²⁰⁶ Hence, authorities should take into consideration the need to protect and balance these fundamental rights. The legal framework should also require the authorities to respect due process and allow interested parties to be heard and to challenge a regulatory decision in court.²⁰⁷

Digital markets are also very innovative, and their evolutions are often unknown to regulated platforms and regulators alike. This implies that the regulators should promote innovation and be experimental in their approach.

- **Innovation friendly**: the regulatory authorities should provide support for innovations at the design, proof of concept, and testing stages, or for the further ongoing development of existing innovative products/services. To achieve such an objective, the legislator may directly provide in the law innovation exemptions or experimentation clauses.²⁰⁸ Another possibility is that the regulatory

²⁰¹ See above fn 161. Also World Economic Forum, *Agile Regulation for the Fourth Industrial Revolution A Toolkit for Regulators*, Dec 2020.

²⁰² Commission Staff Working Document of 3 November 2021, Better Regulation Guidelines, SWD(2021)305.

²⁰³ Commission Better Regulation Toolbox, November 2021, pp.401-402.

²⁰⁴ Proportionality is a general principle of EU law: TEU, art.5(4).

²⁰⁵ Charter of Fundamental Rights of the EU, arts.15-16.

²⁰⁶ Charter of Fundamental Rights of the EU, arts.7-8-11.

²⁰⁷ Charter of Fundamental Rights of the EU, arts.47-50.

²⁰⁸ For instance, to allow innovation in the development of Autonomous Vehicle while ensuring safety, the new Approval and Market Surveillance of Vehicles Regulation, includes a procedure for manufacturers to obtain, under specific cumulative conditions, a type-approval if they use new technologies or new concepts that prevent from complying with the relevant requirements. These type-approvals can only be issued if the manufacturer (i) justifies why new technologies or concepts prevent compliance with the relevant requirements; (ii) ensures a level of safety equivalent to that provided by the relevant requirements, and (iii) provides test results to ensure a similar safety level: Regulation 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, OJ [2018] L 151/1, art.39.

authorities offer regulatory sandboxes to innovators to experiment with new products or services with a temporary exemption of regulation.²⁰⁹

- **Experimental:** Given the novelty of many regulatory issues and remaining unknowns, errors of Type I (over-intervention) and Type II (under-intervention) are inevitable, but they should be minimised. One way to minimise errors is to learn from experience. In this regard, NESTA, a UK innovation foundation, calls for an 'anticipatory regulation' stating that: "When regulators have to take on new functions for which they lack an established playbook, or need to deal with uncertain market developments, a flexible, iterative learning approach is needed rather than a 'solve-and-leave' mentality. Where regulations are being developed for a new area or introduce substantial changes, it is difficult to know exactly what the impacts will be. Utilising a more experimental, trial and error approach, at least at the beginning, rather than immediately creating definitive rules can help build evidence on what works to achieve the desired outcomes. Standards, testbeds/sandboxes, or exhorting best practice are different ways in which regulators can provide more flexible interventions."²¹⁰

Experimentation can be done *ex-ante* before the adoption of a regulatory decision by running A/B testing of different types and designs of the intervention.²¹¹ Such A/B testing may take place in different manners. One possibility is that the regulatory authorities require when necessary and proportionate the regulated platforms to test with their users' different product changes and report the results for them to decide the best course of action. Another possibility is to allow the regulatory authorities to access the algorithm to analyse the outcome delivered by such an algorithm of different courses of action.²¹² More generally, any form of regulatory intervention is an experiment that should be evaluated *ex-post* by assessing the relevance, effectiveness, and efficiency of the intervention after some time of implementation.²¹³

5.4.2 Participatory regulation

Regulating markets always requires a good knowledge base of the relevant industry, but with digital markets, the importance of knowing the industry and its technology becomes even more important because one is regulating an ever-changing environment and regulators often lag behind the industry. In this context, the EU regulatory framework can be developed further by adding a richer set of **regulatory practices that help to bridge the informational asymmetry between the regulator and the regulated.**

In **some fields, the regulatory framework facilitates self and co-regulation.** In practice, there are ample examples of codes of conduct/practice developed at the EU level, for instance for online content moderation.²¹⁴ Codes of conduct can either serve to translate existing legal obligations into operational measures or can be developed to address further issues not (yet) covered by the legislation. As codes of conduct should be developed and complied with by regulated platforms, there is a risk that self-regulation becomes self-serving and/or is not well enforced. Therefore, those codes should comply with the principles for better self-and co-regulation proposed by the European

²⁰⁹ Such sandboxing has also been proposed by the Commission for the use of distributed ledger technology in financial services: Proposal of 24 September 2020 for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, COM (2020) 594. See also, UK Financial Conduct Authority has a sandboxes programme: <https://www.fca.org.uk/firms/innovation/regulatory-sandbox-prepare-application>; France Experimentation, a department of the French administration, can suspend the application of regulation for innovators: <https://www.modernisation.gouv.fr/nos-actions/france-experimentation/france-experimentation-le-registre-des-experimentations-ouvertes>

²¹⁰ Armstrong et al, Renewing regulation 'Anticipatory regulation' in an age of disruption, NESTA, March 2019, p.27.

²¹¹ One of the advantages of digital technologies is that such experiments are less costly to run than before and indeed, online platforms now commonly run A/B testing before launching new products or services.

²¹² G. Parker, G. Petropoulos, and M. Van Alstyne, [Platform Mergers and Antitrust](#), January 2021.

²¹³ On *ex-post* regulatory evaluation: Commission Staff Working Document of 3 November 2021, Better Regulation Guidelines, SWD (2021)305, Chapter IV.

²¹⁴ See A. de Streel et al., *Online Platforms' Moderation of Illegal Content Online*, Study for the European Parliament, June 2020, Chapter 2.

Commission.²¹⁵ Those principles ensure, on the one hand, that rules are prepared openly and by as many as possible relevant actors representing different interests and values and, on the other hand, that they are monitored in a way that is sufficiently open and autonomous and are sanctioned when violated.²¹⁶

In particular, the **DSA proposal promotes codes of practice** to be developed by the firms subject to regulation and involving civil society and other interested parties, including citizens.²¹⁷ There is no reason why this approach should not be replicated across all regulatory initiatives. The DMA proposal also proposes something similar with reference to a 'regulatory dialogue' although the precise role that this has remains somewhat unclear and is platform specific.²¹⁸

To ensure compliance, many rules discussed in this report are enforced by punitive measures: it is expected that penalties provide specific and general deterrence. However, this expectation may not always work, even studies in the field of antitrust law (where penalties could be very high) suggest that these have limited deterrent effects. There may be some differences of detail depending on the economic activity and the risk being managed however the academic literature on responsive regulation suggests that the key element of this approach is, to begin with, the assumption that the firms wish to comply with the rules and from that perspective, a **legal framework that facilitates an ex-ante design of compliance pathways can be useful** across all areas surveyed here.

Some improvement is however required in the procedural design of a participatory mode of regulation. At a high level, procedural safeguards are needed to constrain the regulator by setting out the following: when it is appropriate to encourage participative regulation, what the rights of the parties are and what obligations regulatees have during the process by which obligations and remedies are designed, the procedures by which third parties can participate, the degree of transparency in the process, and the options for judicial review. In general, the purpose of these procedural rules and rights is to avoid a situation where the regulator can secure unnecessary commitments on the one hand, while the firms being regulated are incentivised to provide as much information as possible to demonstrate that their self-regulatory initiative is satisfactory.²¹⁹

Furthermore, participatory regulation means **more reliance on internal compliance mechanisms** within the digital platforms. Internal oversight tools are methods developed by the platforms themselves to make sure they respect the rules in place. The EU law applicable to digital platforms already imposes some of those mechanisms such as:

- **Risk assessments:** Platforms could be required by law or incentivised²²⁰ to conduct risk assessments to review whether their products and services comply with the regulatory requirements or whether users are particularly exposed to certain risks. The GDPR contains such a requirement²²¹ and the proposed DSA foresees that VLOPS should conduct risk

²¹⁵ Those principles are available at : <https://ec.europa.eu/digital-single-market/en/best-practice-principles-better-self-and-co-regulation>. See also M. Finck, *Digital co-regulation: designing a supranational legal framework for the platform economy*, 43 *European Law Review*, 2018, 47-68; M.A. Cusumano, A. Gawer, D.B. Yoffie, 'Can Self-Regulation Save Digital Platforms?', *Industrial and Corporate Change*, 2021.

²¹⁶ In this respect, the governance of standardization is instructive: see J. Baron, J. Contreras, M. Husovec and P. Larouche, *Making the Rules: The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights*, JRC Report, 2019.

²¹⁷ DSA proposal, arts.35-36.

²¹⁸ DMA proposal, art.7.

²¹⁹ For example, a concern arises with the Commission's recent practice of extending its settlement procedure to vertical restraints: it appears that parties agree to a reduced fine in exchange for altering their distribution agreements, however not all of their vertical restraints appear to infringe EU competition law, revealing a risk of over-enforcement. G. Monti Keeping Geo-Blocking Practices in Check: Competition Law and Regulation (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789176

²²⁰ A platform could be incentivised to carry out risk assessments where for instance, the sanctions could be reduced or delayed if a risk assessment has been made.

²²¹ GDPR, art.35.

assessments of how their services are used to disseminate illegal content, of any negative effects for the exercise of fundamental rights and the intentional manipulation of their services harming the protection of public health, minors, civic discourse or on electoral processes and public security.²²² It may also be possible to request platforms to carry risk assessments with the help of independent auditors,²²³ experts and/or with the involvement of users, and civil society. In any event, regulators should provide a clear framework on risk assessments concerning frequency, reporting and involvement of third parties.

- **Appointment of compliance officer:** Compliance officers already exist to monitor and ensure compliance with the GDPR²²⁴ and are also foreseen in the proposed DSA for VLOPS²²⁵ Among the important tasks linked to oversight, we highlight a duty of cooperation with the regulator in charge,²²⁶ and a duty to inform the management and the employees of the obligations to be complied with.

Finally, it is important that **participatory regulation is dynamic**, in two ways: first, it anticipates what happens if there is an infringement: here the regulator has the right to take punitive measures; second, it anticipates that technological change may necessitate a revision of the agreed-upon steps to be taken.

Recommendations

The **principles for good regulatory actions (i.e., effectiveness, proportionality, due process as well as participation, innovation, and experimentation)** are increasingly imposed to the national authorities in charge of the different EU legislations applicable to digital platforms.

However, **it may be desirable that the EU agrees a template for the effective style of oversight and enforcement for the national authorities that could be applied across the range of regulatory tasks and fields when overseeing digital platforms.**


²²² DSA proposal, art.26.

²²³ This possibility is foreseen in article 13 of the proposed DMA.

²²⁴ GDPR, arts.37-39.

²²⁵ DSA proposal, art.32.

²²⁶ Platforms and regulators may need to take urgent action in certain circumstances which will require excellent collaboration between platforms and regulators. Crisis protocols could be established between regulators and platforms which could be activated rapidly in case of need. The regulator could identify potential areas where urgent cooperation may be needed (such as online disinformation) and establish a framework for collaboration with the help of platforms, civil society, and other experts. Article 37 of the proposed Digital Services Act foresees that the European Commission can initiate the drawing up of crisis protocols to coordinate a rapid and cross-border response in extraordinary circumstances such as acts of terrorism, pandemics. Compliance officers can be the point of contact for these crisis protocols within platforms.



cerre

Centre on Regulation in Europe

📍 Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

☎ +32 2 230 83 60

✉ info@cerre.eu

🌐 cerre.eu

🐦 @CERRE_ThinkTank