Pisarkiewicz, Anna Renata; Parcu, Pier Luigi

Conference Paper

Empowering Regulatory Agility: Bridging the Technological Gap for Effective Digital Markets Oversight

24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Pisarkiewicz, Anna Renata; Parcu, Pier Luigi (2024) : Empowering Regulatory Agility: Bridging the Technological Gap for Effective Digital Markets Oversight, 24th Biennial Conference of the International Telecommunications Society (ITS): "New bottles for new wine: digital transformation demands new policies and strategies", Seoul, Korea, 23-26 June, 2024, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/302491

Empowering Regulatory Agility: Bridging the Technological Gap for Effective Digital Market Oversight

Anna Renata Pisarkiewicz, Centre for a Digital Society, EUI[1]

Pier Luigi Parcu, Centre for a Digital Society, EUI[2]

Keywords: Regulatory agility, digital markets, enforcement, VUCA framework, collaborative regulation, technological gap, technological proficiency, innovative policymaking, competences

1. Introduction

The digital economy, which keeps transforming how people and businesses interact and operate, has certain distinctive characteristics that pose unique challenges for regulators. It is highly dynamic and driven by innovation, which in comparison to the past, happens at a much faster pace and is more disruptive. It is technology-based and, more than before, data-driven, which means that it requires notable ICT and analytic capabilities and the ability to interpret and make decisions based on vast amounts of data. For example, to understand the economies of scale in search and the value of targeted advertising, the UK CMA requested and analysed over 4TB of data from Google and Bing during its market study on digital advertising (Hunt, 2022). Moreover, the digital economy with its corresponding digital regulations is increasingly complex and interconnected, making it difficult for regulators to understand and coherently regulate specific problems or components without examining entire digital and regulatory ecosystems. The digital economy also transcends traditional sectoral silos as well as territorial and jurisdictional limitations, thereby presenting challenges in terms of ensuring harmonized regulatory frameworks and effective compliance across different national authorities and different geographical realities. The German *Facebook (Meta)* case and the subsequent preliminary ruling from the EU perfectly illustrate both the increasingly blurred lines between data protection and competition law enforcement as well as a need for coordination and collaboration between the respective regulators. Finally, the global and interconnected nature of the digital economy creates important dependencies and vulnerabilities that regulators must understand and navigate, which exposes regulation to geopolitical tensions. The interplay between merger control and foreign direct investment (FDI) screening, for example, in cases involving semiconductors shows how regulatory frameworks must adapt to address these dependencies and vulnerabilities, ensuring that economic considerations are balanced with national security interests amidst rising geopolitical tensions.

All the above factors make the digital economy utterly unpredictable, raising questions about whether the traditional paradigms of market regulation need to be reevaluated and whether

[1] Dr. Anna Renata Pisarkiewicz: anna.pisarkiewicz@eui.eu

[2] Prof. Pier Luigi Parcu: pierluigi.parcu@eui.eu

existing regulatory authorities are well-equipped to ensure any kind of effective market oversight. Undoubtedly, regulation of digital markets has gained prominence as their pervasive expansions have unveiled a range of issues, varying from data privacy breaches, cybersecurity, and disinformation to monopolistic behaviors. In response to challenges and risks associated with the digital economy, many countries all over the world are engaging in discussions and reforms of their regulatory frameworks. The EU, in many respects, has led the way in this effort by adopting a comprehensive set of regulations and guidelines to address various aspects of digital market oversight. Today this set includes such diverse instruments as the Digital Market Act (DMA), the Digital Services Act (DSA), the Data Act, the Data Governance Act, the European Media Freedom Act (EMFA), the Cybersecurity Act, the General Data Protection Regulation (GDPR), and the recently approved Artificial Intelligence Act (the AI Act).

While these regulations pursue a variety of regulatory objectives, all of them will require effective implementation, monitoring, and enforcement, which involves a diverse array of EU and national authorities, spanning from national competition authorities to data protection authorities, cybersecurity authorities, sector-specific regulators, and consumer protection authorities. The multiplicity and variety of involved enforcement bodies point to the complexity of aligning inter-related or overlapping regulatory actions across different domains and jurisdictions, amplifying the challenges posed by the informational and technological gaps that exist between this quickly evolving business world and regulatory authorities. These gaps risk undermining the relevance and effectiveness of both the authorities and the regulations they are entrusted to implement.

As noted by Jin *et al* (2022), the technological core of the gap refers to the stark disparity in the adoption and use of advanced information and communication technologies (ICT). While transformative advancements in ICT have given rise to innovative business models and new forms of consumer engagement, facilitating a dynamic and complex ecosystem, regulatory authorities have been much slower in adapting to this fast-paced digital transformation.

With some notable exceptions, the increasing gap hinders the ability of regulatory authorities to effectively organize and provide effective market oversight. This is because still most of them grapple with excessive reliance on traditional data collection methods and inapt processes that might be simply too slow to provide effective regulatory intervention. This gap does not result solely from a deficit in technological tools, analytics, and expertise but can also be linked to a broader organizational and strategic misalignment of these authorities vis-a-vis the new complexity of the digital markets.

To explore this misalignment and the responses that have been developed to date, we apply a Volatility, Uncertainty, Complexity, Ambiguity (VUCA) framework adapted from the business literature, which we present in Section 2. We use this framework as a lens through which we dissect the dynamic nature of digital markets, characterized by rapid innovation, data-driven decision-making, and global interconnectivity, which collectively contribute to an unprecedented level of uncertainty and complexity. Next, in Section 3 we advocate for a paradigm shift towards regulatory agility, which is essential for navigating the VUCA features inherent in digital markets. To bridge the informational and technological gaps and ensure effective digital markets' oversight, regulatory bodies must develop and integrate specific competences. This can be achieved through competence mapping, which allows regulatory authorities to assess current skill levels, identify gaps, and develop targeted strategies to enhance their oversight capabilities. Key competences for innovative policymaking and science for policy, identified by the European Commission's Joint Research Centre (JRC), are particularly relevant in the context of this paper, and will be discussed in section 3. Section 4

explores the reconciliation of agility and collaborative enforcement with certain traditional tenets of good regulation, such as legal certainty, predictability, and coherence. In section 5, we discuss institutional responses to the technological gap by focusing on selected case studies that illustrate solutions already experimented with in a few countries. We conclude the exploration in section 6, in which we aim to shed some light on the pathways through which regulatory bodies may evolve and adapt in the digital age, in their challenge to pursue effective oversight while fostering innovation and protecting consumer interests.

2. Adopting the VUCA framework to digital regulations and regulatory authorities

Initially used in the context of the U.S. military following the 9/11 terrorist attacks in 2001, the VUCA framework has paved its way to the business world aiming to provide a nuanced understanding of the dynamic and often unpredictable nature of modern business environments (Bennett and Lemoine, 2014). The acronym, which stands for *Volatility, Uncertainty, Complexity, and Ambiguity*, describes the challenging conditions that organizations face in a complex and rapidly changing environment. Volatility refers to the pace of the change in an industry or market; uncertainty concerns the unpredictability of future events; complexity reflects the existence of multiple variables and forces affecting an organization, while ambiguity refers to the lack of clarity about how to interpret a given fact or trend due to incomplete or contradictory information. These four distinct yet interrelated elements are well-suited to capture the multifaceted challenges that regulators (and companies) face in the digital economy.

While the VUCA framework is popular for analyzing complex and rapidly changing environments, we are cognizant of the fact that it also has several limitations. For example, it assumes a relatively static basic environment and risks oversimplifying more complex evolutions. Still, despite its deficiencies, this framework can provide an interesting lens through which we can explore the characteristics of the present digital markets, offering a structured approach to understanding regulatory challenges and helping to formulate more adequate institutional responses.

Volatility in digital markets can be observed in the rapid changes in consumer behaviour and technology advancements. For example, the swift rise of new social media platforms and the decline of previously dominant ones, or the quick adoption of new technologies like blockchain, non-fungible tokens (NFT), and AI demonstrates market volatility and fluctuating market conditions that businesses must navigate. Furthermore, the inherent volatility of cryptocurrencies as well as the potential of private blockchains to foster collusion through smart contracts automatically punishing deviations by participants from cartel agreements, highlight the complexities faced by competition and regulation in deterring harmful behaviours in this area (Massarotto, 2019).

Uncertainty in digital markets can result from unpredictable regulatory changes and the difficulty in predicting the impact of new technologies or the emergence of disruptive business models. For example, the introduction of stringent data protection regulations such as GDPR or the DSA in Europe brings uncertainty to data-driven businesses. The emergence of blockchain technology, which spans beyond cryptocurrencies to diverse activities such as supply chain management or digital identities, is challenging regulators to foresee and prepare for its broad implications. Similarly, the unexpected rise of sharing economy platforms (e.g. Uber, Airbnb) and peer-to-peer transactions have disrupted traditional industries, creating uncertainty about future market

structures, which has been compounded by the fact that these platforms often operated in legal gray areas and regulatory vacuum.

Complexity has multiple dimensions. It is evident in the intricate network of stakeholders, including tech giants, disrupted firms, startups, national and international regulators, and consumers, each with their own interests and influences and their interdependence within and across digital ecosystems. However, complexity can also refer to different layers of the digital ecosystem that altogether represent complex dynamics and supply chains. This stakeholder and layer complexity is further compounded by the global nature of digital services, where actions in one part of the world can have significant repercussions elsewhere or, anyway, can induce geopolitical responses.

Ambiguity describes situations where the "rules of the game" are unclear. In digital markets, ambiguity can result from the lack of clear information depending on the rapid evolution of digital technologies that make it difficult to understand cause-and-effect relationships and, consequently, to develop quickly, where necessary, appropriate regulations. For example, the valuation of digital assets and cryptocurrencies often lacks transparency, leading to highly speculative and sometimes fraudulent investments. Also, the fast-paced innovation in areas like AI and quantum computing makes it difficult to predict the future capabilities of these technologies. Moreover, ambiguity is also likely to arise from unclear legal provisions in EU digital regulations as well as still largely untested interaction between various recently adopted legal instruments. For example, the concept of fairness, a key consideration underlying the DMA, while not new to competition law enforcement, remains vaguely defined, continuing to raise concerns that can jeopardize legal certainty and enforcement actions (Colangelo, 2023).

The above four VUCA elements characterize all digital markets, albeit to a different degree. Consider the degree of volatility, which varies across digital markets and reveals distinct dynamics. For example, the highly monopolized market for search engines seems to exhibit low to moderate volatility. The stability is partly due to the strong network effects and high entry barriers, which have allowed dominant players like Google to maintain a significant market share over an extended period of time. While there is ongoing innovation in algorithms and features, these changes often appear incremental and less likely to cause sudden market shifts. Also, regulatory changes and antitrust investigations can represent potential sources of volatility. However, also such events tend to unfold over extended periods. Digital marketplaces (e-commerce platforms) seem to be moderately volatile due to changing consumer preferences, and the expansion into new markets or product categories. Seasonal spikes in sales, such as during holiday seasons, can also introduce short-term volatility. Regulatory changes affecting online sales, taxation, and international trade can impact market dynamics, but again, like in the case of search engines, these changes are often anticipated and gradual. Higher volatility, instead, can be found in the more decentralized cryptocurrency market, where prices tend to swing dramatically within a short period of time, influenced by a range of factors, including speculative trading, technological developments, macroeconomic factors, and even regulatory developments.

Hence, while all digital markets are influenced by innovation and changes in the regulatory landscape, some markets are more volatile than others due to their speculative nature and sensitivity to technological and macroeconomic factors. This variation underscores the need for tailored regulatory and policy approaches to effectively navigate the different challenges presented by specific digital markets.

Also, it is important to bear in mind that VUCA factors may affect market participants differently even within the same digital ecosystem, based on their role and position. For example, in the search engine market, Google has enjoyed a

dominant position for a sustained period of time, as extensively discussed in the EU Google Shopping case. This long-held dominance contributes to the search engine market's general stability. Yet, the volatility in Search Engine Results Pages (SERP), pivotal for businesses dependent on online visibility, contrasts this stability. Hence, while search engine providers might not be affected by volatility, their customers are, which is why monitoring SERP volatility is important as it can help competition authorities in understanding these fluctuations, which is vital for ensuring fair competition in digital markets.

Despite its limitations, the adoption of the VUCA framework seems pertinent for assessing whether recent EU digital regulations, and competent regulatory authorities entrusted with their enforcement, can reasonably well address the volatility, uncertainty, complexity, and ambiguity of digital markets. As it is not feasible to examine within a single article the entire regulatory ecosystem, in this paper, we focus on five recently adopted and most analysed EU regulations: the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act, the Data Act, and the Data Governance Act.

Before applying the VUCA framework to these regulations, it becomes both useful and necessary to understand the multifaceted rationales that underpin these regulatory efforts. While regulations are frequently adopted to address market failures, as explained by Prosser (2006), such a view does not fully reflect the range of regulatory activities. Indeed, the EU's approach to digital market oversight extends well beyond traditional market failure paradigms, mirroring a broader vision of the digital transformation that seeks to harmonize market efficiency with the protection of fundamental rights, social solidarity, inclusiveness and cohesion, and European digital sovereignty. This holistic perspective is evident in the set of EU regulations that plan to govern the digital space and that have been designed with distinct yet complementary rationales.

The Digital Markets Act aims to ensure fair competition and contestability in digital markets by addressing the power of gatekeepers, i.e. large platforms that control access to significant market opportunities. The goal is to prevent these firms from abusing their dominant positions or otherwise engaging in conduct that would be harmful to consumers and smaller competitors, thereby fostering a more competitive and innovative digital environment. The Digital Services Act seeks to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. It focuses on regulating online platform's responsibilities regarding illegal content, transparent advertising, and disinformation, ensuring user safety and accountability online. The Artificial Intelligence Act seeks to manage the risks associated with AI systems and promote their safe adoption. Its rationale is to lay down a legal framework for trustworthy AI that respects fundamental rights and safety, ensuring AI systems that are ethical, transparent, and accountable. The Data Act is designed to facilitate data sharing and use across sectors and Member States. It aims to unlock the economic and societal benefits of data by establishing clear rules on data access and use, thereby fostering innovation and competition while ensuring privacy and security. Finally, the Data Governance Act aims to encourage the availability of public sector data for use, enhance data sharing mechanisms across sectors, and foster trust in data intermediaries. The DGA seeks to create a framework to enable better governance of data sharing, improve trust in data intermediation services, and facilitate the reuse of certain categories of protected public sector data.

These acts collectively, but not exclusively, aim to shape a digital economy that is competitive, fair, and respectful of fundamental rights, ensuring Europe's digital sovereignty and promoting its values and standards in the digital domain.

In Table 1 we illustrate how the mentioned regulations respond to the specific VUCA features of the digital markets, emphasizing their roles in creating a safer, more competitive, and innovative

digital environment.

The enforcement of these acts will be assigned to a diverse array of regulatory authorities, each bringing a different set of expertise and responsibilities. This diversity is reflective of the broad spectrum of issues these regulations aim to address, from competition and market fairness to data governance, artificial intelligence ethics, and user safety.

Table 2 provides an overview of the type of competent regulatory authorities and enforcement mechanisms for each regulatory act. It also illustrates the diverse regulatory landscape and hints at the importance of coordination and collaboration among various authorities within a single country and across borders to ensure effective oversight of digital markets and services.

Since regulations need to be enforced by competent regulatory authorities, in Table 3 we summarize how these authorities need to adapt and evolve to enforce regulations effectively in the VUCA setting of digital markets.

As is evident from Table 3, the rapidly changing digital landscape demands a paradigm shift in regulatory approaches and institutional structures. Agility, predictive planning, advanced data analytics, interdisciplinary collaboration, and transparency all point to the complex interplay between technological advancements and regulatory frameworks. All this is definitely not the state of the art for present sectoral regulation in the EU and elsewhere. However, these adaptations are not just necessary but vital for regulatory bodies to effectively navigate the volatility, uncertainty, complexity, and ambiguity that are inherent in digital markets.

3. The need for technological proficiency, collaborative regulation, and agility

Section 3 shifts the analysis of digital regulation and regulatory authorities under the VUCA framework to the exploration of practical challenges faced by regulatory authorities in the process of adaptation. In particular, regulatory bodies must develop a comprehensive set of competences to effectively oversee and govern digital markets. The European Commission's Joint Research Centre (JRC) has identified key competences for 'Innovative Policymaking' that are crucial for regulatory authorities to adapt and thrive. These competences are organized into seven clusters: (1) advise the political level, (2) innovate, (3) work with evidence, (4) be futures literate, (5) engage with citizens and stakeholders, (6) collaborate, and (7) communicate. Each cluster encompasses specific skills, knowledge, and attitudes necessary for effective policymaking (Fig. 1). In this section, we will explore technological proficiency, collaborative regulation, and agility and how they respectively link to Cluster C (Work with evidence), cluster F (Collaborate), and Cluster D (Be futures literate) but also B (Innovate) of the 'Innovative Policymaking' competence framework.

Technological proficiency

Considering the necessary adaptations identified earlier in the paper, it is quite evident that the technological gap emerges as the first critical challenge facing regulatory authorities. This gap refers to the stark disparity between the rapidly evolving digital markets and firms and the slower regulatory oversight in the adoption and use of advanced ICT. While Jin *et al* (2022) pointed to the existence of an informational and technological gap between the business world and antitrust agencies, such a gap is not specific to antitrust agencies but concerns most, if not all, public regulatory authorities.

Technological proficiency is fundamental for Cluster C (Work with Evidence) of the *Innovative Policymaking* competence framework as it enhances the ability of regulatory authorities to collect, analyze, and interpret data swiftly and effectively.

Closing technological gap requires regulatory authorities to undergo an internal process of digital transformation aimed at

enhancing their ability to organize and operationalize knowledge for enforcement purposes. This involves developing the type of technological proficiency required for monitoring digital markets, which is not a straightforward task as the gap has at least two major dimensions. The first concerns authorities' direct capabilities and expertise, while the second involves the broader organizational and strategic misalignment of the regulatory framework with the complexity of digital markets, pointing to a deeper, systemic issue that extends beyond mere expertise and proficiency in the use and analysis of data and technology.

A) Capabilities and expertise

With respect to data collection and data analytics, regulatory authorities might still excessively rely on traditional data collection methods and processes, such as manual processing, formal requests to parties, periodic reporting, and static datasets. Data units within regulatory authorities or at the authorities' disposal can help modernize the approach to data collection and analysis, moving beyond the traditional methods that have long been established in regulatory practices. In particular, data experts can leverage cutting-edge technologies to mine and analyze data in real-time, providing a dynamic and nuanced understanding of market conditions, and creating authorities' own data. As Jin et al (2022) explain:

"the agencies receive most legal information as documents comprising text and figures, rather than structured, numerical data fields. Often, these documents are left unused or underused because the agencies do not have the capability in terms of staff nor tools to process them comprehensively in real time. Similarly, whereas consumer can file complaints to the FTC in real time, their complaints are mostly used for low-frequency public reporting (e.g. once-a-year summary of most complained categories) or ex-post justification of some ongoing cases. There is little effort (and few staff dedicated) to proactively screening and identifying new trends and patterns concerning wrongdoing from the complaints data at a high frequency".

Technologically proficient authorities can employ advanced data acquisition techniques such as web scraping to gather vast amounts of public and proprietary data, far beyond what is typically accessible through traditional means. Web scraping, which is the process of extracting content and data from websites using software, can help regulators decide which companies to investigate in depth, detect suspicious patterns indicative of harmful practices, but also to check compliance with remedies imposed by the authorities (Hunt, 2022). Data engineers can also build bespoke digital products and solutions. For example, the CMA's data engineers, and eDiscovery specialists developed the authority's Evidence Submission Portal (ESP), which significantly increased the number of documents the CMA could take in (from a few hundred thousand to over seven million). ESP also streamlined the procedure as it automatically verifies whether documents are in the correct format and rejects those that are not. This, together with the automatic processing of the documents into the CMA's digital document review program, has allowed the CMA to reduce from four to one the number of days in merger cases between the submission of the documents and the beginning of the review process by the case team (Hunt, 2022).

Thus, in general terms, the ability to go deep into the data and technologies brings two key contributions. First, it allows the authority to understand the details and the implications of collected information more quickly and effectively than it could if it relied only on non-technical staff (Hunt, 2022:16). In developing a more nuanced understanding technologists, i.e experts with a range of data and technology skills, have an instrumental role to play as they can help formulate requests for information, and collaborate with case teams, predominantly consisting of lawyers and economists, to pose precise, understandable questions that help in the efficient collection and assessment of technical evidence.

Second, technical staff play a crucial role in

direct interactions with the involved parties. Hunt (2022) explains that members of the CMA's Data Technology and Analytics (DaTA) team have frequently participated in meetings, evaluated information on the spot, and questioned or contested interpretations, sometimes even identifying instances where information was technically misrepresented. Their involvement has often led to the discovery of new avenues in a case and substantially shaped the case team's approach.

The critical role of technological proficiency for regulatory authorities is evident in the enforcement of EU digital regulations, such as the DSA. As pointed out by Jaursch (2023), the DSA 'is a *"data-gathering machine", containing more than 50 references to mandatory or voluntary transparency and evaluation reports, databases, activity reports, guidelines, codes of conduct and standards"*. While a detailed list of these references can be accessed at the link in the footnote,[3] Table 4 summarizes the key elements that require scrutiny along with references to specific provisions in the DSA, highlighting the necessity for robust technological infrastructure and expertise to interpret complex datasets and ensure compliance.

Of course, technological expertise within regulatory authorities is only a component of the broader spectrum of expertise needed for effective market monitoring. The overall acumen of necessary expertise is inherently linked to the concept of regulatory independence. This independence, which is often enshrined in regulations, is crucial for maintaining the integrity of regulatory processes and ensuring that regulatory authorities make decisions in the best interest of the market and consumers, and that they are grounded in a comprehensive understanding of the regulated markets rather than being swayed by external pressures or the technical narratives shaped by the firms they regulate.

Technological proficiency, and, more in general, adequate expertise, together with regulatory independence, lay a foundational requisite for the effective monitoring of markets. This requisite is not merely theoretical but is foreseen in various regulations that usually are at least partially prescriptive with respect to the specific expertise required within regulatory authorities. For instance, the Data Act limits itself to a general requirement laid down in Article 37 that "Member States shall ensure that the competent authorities are provided with sufficient human and technical resources and relevant expertise to effectively carry out their tasks in accordance with this Regulation". In contrast, the AI Act is more specific and prescribes, in Article 30, that "Competent personnel shall have the necessary expertise, where applicable, for their function, in fields such as information technologies, artificial intelligence, and law, including the supervision of fundamental rights". This requirement reflects the broader acknowledgment that the depth and range of expertise within regulatory bodies must be sufficiently comprehensive to comprehend the multifaceted nature of the digital markets they oversee. By stipulating such standards, regulations reinforce the importance of regulatory bodies being well-equipped with adequate technical, legal, and economic acumen.

B) Organizational misalignment

The second dimension of the technological gap, as mentioned earlier, points to a deeper, systemic issue that extends beyond mere expertise and proficiency in the use and analysis of data and technology. This misalignment arises when the structures, procedures, and operational functioning of regulatory authorities are inadequate vis-à-vis the complex and rapidly evolving nature of digital markets.

Organizational misalignment may manifest itself in various forms, such as siloed departments that hinder cross-functional inter- and intra-agency

[3] https://www.stiftung-nv.de/sites/default/files/dsa_reporting_overview_0922.csv__0.zip

collaboration, crucial for understanding and regulating complex digital ecosystems, insufficient budget for upgrading the authority's expertise, but also management's resistance to change. Moreover, strategic misalignment can also take the form of overly prescriptive, rule-based approaches or red-tape processes that hinder comprehension of deeper or more technical issues, slow down decision-making, and deprive the authorities of the flexibility needed for adaptive regulation.

Addressing the existing technological gap in both dimensions requires a comprehensive reevaluation of the regulatory authority's organizational structure, strategic objectives, operational methodologies, and mapping of existing as well as missing skills and expertise as an initial step in a comprehensive reform of regulatory authorities. Such a comprehensive process should certainly include setting a data unit within the authority or securing access to data experts outside of the authority, fostering a culture of continuous learning and adaptation, encouraging cross-disciplinary as well as inter- and intra-agency collaboration, and leveraging data-driven insights to inform regulatory strategies. Moreover, regulatory authorities may need to re-evaluate whether they engage proactively with a sufficiently broad range of stakeholders.

Collaborative regulation

Technological proficiency within regulatory authorities, as explained in the preceding section, not only empowers authorities to adapt to the complexities of the digital economy but also provides a starting point for discussing the importance of collaborative regulation. Collaborative regulation directly supports cluster F (collaborate) of the 'Innovative Policymaking' competence framework by fostering collaboration and coordination among different regulatory bodies and stakeholders.

The ITU's Benchmark Report on fifth-generation collaborative digital regulation (2021), highlights a paradigm shift towards more integrated and cooperative regulatory frameworks, acknowledging that in a digital economy, where traditional silos between sectors continue to blur, the ability of regulatory bodies to harness the collective expertise and resources of diverse stakeholders becomes crucial. This collaborative approach not only amplifies the collective expertise available for regulatory authorities but can also help achieve regulatory responses that are more nuanced, proportionate, and agile.

Collaborative regulation, while not a novel concept, has gained new dimensions and more prominence with the advent of the digital economy, which amplified its complexity and breadth. Historically, collaboration existed, for example, between competition authorities and sector regulators that working together sought to ensure market fairness and protect consumer interests (OECD, 2022a). Collaboration between these authorities aimed to align competition law enforcement with sector-specific regulatory goals, ensuring coherent and effective oversight. In the digital realms, however, the scope of collaborative regulation extends well beyond traditional boundaries, encompassing a wider and, hence, more diverse array of regulatory bodies and stakeholders, with divergent interests and expertise. For example, the judgment of the EU Court of Justice in the *Meta* case addresses the complex interplay between competition and data protection laws within the European Union, focusing in particular on the responsibilities and powers of national competition authorities vis-à-vis national data protection authorities.[4] The case concerned the decision of the German competition authority, Bundeskartellamt that prohibited certain data processing practices based on the General Data Protection Regulation (GDPR). The core issue was whether a *competition authority* could determine that processing personal data as stipulated in a company's general terms of use and its actual

[4] Case C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, ECLI

practices were inconsistent with the GDPR, especially when such processing was linked to the abuse of a dominant position.

The Court emphasized the distinct but complementary roles of competition and data protection authorities, noting that while each has its specific mandate, their interventions can intersect, particularly in the digital economy where data plays a central role in competitive dynamics. Importantly, the judgment referred to the principle of sincere cooperation as enshrined in Article 4(3) of the TFEU, which mandates mutual respect and assistance among Member States and their respective authorities to comply with EU law obligations. The practical applications of this principle imply that when a competition authority considers it necessary to assess compliance of a given behavior with the GDPR when investigating an abuse of dominance, it should not act alone but in concert with relevant data protection authorities, ensuring a coherent interpretation and application of EU law. Only such a cooperative approach can effectively protect fundamental rights while ensuring competition.

Collaborative regulation extends not only in breadth, involving a wider group of stakeholders, but also in depth, encompassing various levels of cooperation, from informal exchanges to formalized collaboration and institutionalized collaborative bodies.

The rise of collaborative regulation by no means eliminates autonomous single-authority investigations. In fact, since the increased complexity also introduces challenges, particularly in coordinating efforts and resources across a wider array of authorities, each with its specialized mandate, it is important to resort to collaborative regulation only in those cases that no single authority could effectively manage alone. In those instances where a collaborative approach can lead to better enforcement outcomes, it is important to consider different cooperation models and their dimensions, while taking into account formal, legal, and procedural challenges that might obstruct their successful implementation.

While it is not the aim of this paper to exhaustively discuss all the dimensions of collaborative regulation, Table 5 highlights some of the most relevant aspects that need to be considered.

In the realm of EU digital regulations and considering competent authorities responsible for their enforcement, the sharing of data between regulatory bodies (government-to-government, G2G data sharing) emerges as particularly pertinent and possibly decisive for collaborative regulation. However, several challenges might obstruct such efforts. First, promoting collaborative regulation as well as technological proficiency and agile approach all require treating data as a strategic asset. However, as highlighted by the UK National Audit Office (NAO) report on 'Challenges in using data across government' (2019), the absence of a cohesive, government-wide strategy for data management indicates that this may not be the case. The diversity in data formats and standards across various authorities or even within the same (multi-mandate) regulatory authority hampers the exchange of data and information, calling for a more harmonized approach to data standardization and compatibility to ensure interoperability and enhance the effectiveness of joint regulatory initiatives. Second, the disparity in technical infrastructure and expertise among regulatory bodies across Member States can lead to inconsistent enforcement and regulatory practices. Bridging this gap necessitates significant investment in enhancing the digital capabilities of regulatory authorities, ensuring a uniform level of regulatory oversight across the board.

In the context of collaborative regulation, the diverse institutional choices made by EU Member States in the designation of Digital Service Coordinators under the DSA illustrate the multifaceted approach to digital governance. As shown in Table 6, the range from telecom and media, competition, and consumer protection regulators to newly established authorities reveals the adaptability of national regulatory frameworks to the specificities of digital market oversight and confirms the autonomy of Member States in

organizing their regulatory bodies. More importantly in the context of this section, this variety underscores the importance of inter-agency and cross-border cooperation to ensure coherent and effective enforcement of the DSA.

While Table 6 shows diverse solutions with respect to the appointment of the DSC under the DSA, the most prevalent option is the appointment of the telecom regulator. Historically, such authorities have been entrusted mostly with economic sector-specific regulation. In charge of carrying out market analysis under Article 7 of the Framework Directive such authorities have already had units with experts in fact based economic analysis. In any case, a decision to create a data unit requires an understanding of how a separate data unit can enhance and be integrated into an already existing in-house expertise.

Also, new powers under the DSA will require telecom regulators to consider fundamental rights and to interact with a wider and more diverse spectrum of stakeholders. In some countries, telecom regulators have also been designated as competent authorities for data intermediation and data altruism under respectively Art. 13 and 23 of the Data Governance Act (i.e. BNetzA in Germany or Traficom in Finland, see Table 7 for an overview of all competent authorities notified to date). These extended new powers might dilute the core mandate of telecom regulators, creating some risks and uncertainties about the correct and optimal use of newly gathered data.

To conclude, collaborative regulation is not just about sharing information or aligning enforcement actions but about creating synergies between different regulatory perspectives to foster a holistic understanding and oversight of digital ecosystems. This, in turn, requires a commitment from all involved parties to foster a culture of cooperation, supported by the necessary legal and procedural frameworks as well as skills and competences. In conclusion, while the concept of collaborative regulation is not new, its application within the digital economy requires a significant upgrade, implying a profound reevaluation of traditional regulatory approaches.

Agility

Another feature that emerges from the VUCA framework as particularly pertinent for effective oversight of digital markets is the concept of agile and responsive regulation, which hinges on the previously discussed technological proficiency of regulatory authorities. The notion of agility in regulatory governance, as delineated by the OECD's Recommendation for Agile Regulatory Governance to Harness Innovation, underscores the need for regulatory systems to be flexible, adaptable, and responsive to fast-paced technological advancements (OECD, 2021). The UK Department for Business, Energy & Industrial Strategy (2019), in its White Paper on *"Regulation for the Fourth Industrial Revolution"* posits that regulatory agility is crucial not only for fostering innovation but also for ensuring that regulation protects public interests without stifling technological advancements. In the context of the JRC 'Innovative Policymaking' competence framework, regulatory agility directly supports and relates to Cluster B (Be futures literate) and Cluster B (innovate).

According to Horsapple and Li (2008), *"agility is the result of integration alertness to changes – both internal and environmental – with a capability to use resources in responding (proactive/reactive) to such changes, all in a timely, flexible, affordable, relevant manner"*. As noted in the White Paper on Agile Regulation by Project Management Institute and the US National Academy of Public Administration (2022), agility *'begins by asking whether the current way of doing things is limited by statute or if innovation is allowable, but simply not currently utilized'*. This approach helps identify areas where regulatory agility can be improved without the need for legal changes, as well as areas where legislative amendments are necessary to enable more flexible and responsive regulation.

Some countries are already moving forward

to enhance their regulatory agility in the digital market. For example, in November 2020, Canada, Denmark, Italy, Japan, Singapore, UAE, and the UK signed the world's first "Agile Nations" agreement. Key initiatives within Agile Nations include sharing insights on innovation opportunities and risks to enable timely regulatory reforms, exploring joint regulatory experimentation through initiatives such as regulatory sandboxes, and assisting innovative firms in navigating the regulatory regimes of participating governments. For example, Denmark has focused on exploring regulatory sandboxes and testbeds, to foster innovation-friendly regulation in sector like AI, fintech, biotechnology, and health.

Initially, regulatory sandboxes have been used mainly in certain sectors, notably in finance, where they were pioneered to test new fintech innovations in a controlled environment while ensuring consumer protection and financial stability. This sector-specific adoption was largely driven by the high pace of innovation and significant risks associated with financial technologies. Over time, however, the use of regulatory sandboxes has expanded beyond the financial sector, becoming increasingly relevant in other areas, particularly in the digital economy.[5] For example, the French telecom regulatory authority, Arcep has introduced a regulatory sandbox to foster innovation in telecoms by easing certain obligations for up to two years for operators wishing to develop innovations supported by 5G technology. Similarly, the Thailand's National Broadcasting and Telecommunications Commission (NBTC), deployed a regulatory sandbox opened to interested stakeholders beyond the ICT industry to promote 5G technology trials in 700 MHz, 2600 MHz, and 26GHz frequency bands.

This expanding adoption reflects the recognition that the sandbox model offers a pragmatic way to balance the need for regulatory oversight with the imperative to foster innovation. In the digital economy, where technological advancements rapidly transform markets and consumer behaviours, sandboxes provide a valuable mechanism for regulators and innovators to collaborate, test, and learn about new technologies and business models in a real-world but controlled setting.

Examples mentioned above clearly demonstrate that regulatory agility is not just about the speed of regulatory responses but also about the capacity for anticipation, iterative learning, and integration of diverse stakeholders' views into the regulatory process. This perspective can be complemented with insights from Bennear and Wiener (2019) who emphasize the significance of instrument choice and the calibration of regulatory responses to match the evolving landscapes of risk and innovation. In their analysis, the authors distinguish between unplanned (e.g. ad hoc retrospective review, for example, in response to crisis) and planned adaptive (i.e. periodic reviews) regulations, and within the latter, between discretionary and automatic mechanisms.

Both the academic and policy-oriented discourse on agile and responsive regulation presents a compelling case for the evolution of regulatory frameworks in the digital economy. While benefits are noteworthy, the shift to more adaptive regulation is not devoid of deficiencies. As mentioned earlier, adaptive regulation requires technological proficiency and extensive data collection, which implies costs both in terms of time and resources that can be disproportionately burdensome on both those requiring data and those required to provide it (Sunstein, 2019).

To better understand and address the challenges, posed by the VUCA features of the digital markets in terms of their regulation, it is

[5] Also, the study by the Joint Research Centre of the European Commission on making energy regulation fit for purpose highlights the increasing adoption of regulatory experimentation across EU Member States as a tool for fostering innovation and adapting to rapidly changing environments driven by digitalization and decarbonization.

useful to map the necessary competences and adaptive capacities of regulatory authorities. By employing a 2x2 matrix, we can visualize the relationship between technological proficiency and adaptive capacity, and how these factors interact with the VUCA elements, providing a structured approach to enhancing the authorities' oversight capabilities (Table 8).

By integrating the 2x2 matrix on competence mapping and VUCA elements, we can clearly identify the specific areas where regulatory authorities need to enhance their capabilities. High technological proficiency combined with high adaptive capacity places regulators in the best position to manage the complexity and volatility of digital markets. Conversely, low technological proficiency and low adaptive capacity highlight the urgent need for targeted training and organizational reforms.

4. Reconciling the VUCA framework with traditional principles of good regulation

Reconciling the VUCA framework with principles of good regulation is crucial as it allows regulatory bodies to discharge their regulatory mandate in the volatile, uncertain, complex, and ambiguous setting of the digital markets while upholding the historical tenets of effective regulation aimed at guaranteeing legal certainty, predictability, and coherence.[6]

In digital markets characterized by volatility, uncertainty, and R&D-intensive innovation, ensuring sufficient flexibility required for agile regulation while ensuring legal certainty is paramount. This means that legislation must be both precise enough to provide clear guidance to all the stakeholders about their rights and obligations but also flexible enough to adapt swiftly to technological advancements and evolving market conditions. Incorporating adaptive regulatory mechanisms, such as sunset clauses or periodic review provisions, can provide a pathway for regulations to evolve without sacrificing clarity. In what could represent a good example, both the DMA and the DSA outline specific obligations for digital platforms while also allowing for adjustments based on evolving market trends, emerging risks, and technologies. For example, the DMA targets large online platforms acting as 'gatekeepers' to the digital market, setting out specific criteria for their designation and imposing obligations designed to ensure fair competition and innovation. By establishing quantitative thresholds and a framework for gatekeeper designation, the DMA combines specificity with the flexibility to adapt to market developments. This is seen, for example, in Articles 3 and 4 of the DMA, which lay out the criteria for gatekeeper designation and the framework for updating these criteria, highlighting the balance between specificity and adaptability. The AI Act, in turn, specifies dynamic compliance requirements, including continuous monitoring, post-market surveillance, and incidence reporting. These measures seek to ensure that AI systems remain compliant throughout their lifecycle, allowing for adaptive regulatory responses to new risks and issues as they arise (Larsson et al, 2024). Thus, in essence, the DMA, the DSA, and the AI show how EU digital regulations are designed to be both clear and adaptable, ensuring they remain effective in a rapidly evolving digital ecosystem.

While clear legal provisions can diminish uncertainty with respect to applicable rules, uncertainty in digital markets can also challenge the predictability of regulatory outcomes. To address this concern, regulators can, for example, employ forward-looking tools like horizon scanning and

[6] According to Baldwin *et al* (2011), good regulation must satisfy five key criteria. First, the regulatory regime should be based on a legislative mandate. Second, it must foresee an appropriate scheme of accountability, and third, it must have safeguards for guaranteeing due process. Fourth, the regulator entrusted with the enforcement of the regime must act with sufficient expertise, and, last but not least, the regime must be efficient.

stakeholder consultation to better anticipate future developments. For example, the recent EU Exploratory Consultation on *'The future of the electronic communications sector and its infrastructure'* (2023) illustrates the Commission's attempt to gather views on the changing technological and market landscape that would inform its decision-making process as to whether a new regulatory framework needs to be adopted.

The complexity of the digital ecosystem demands coherence in regulatory responses across different domains, ensuring that they do not create conflicting obligations. This may, again, involve greater inter-agency collaboration and the development of horizontal regulatory principles that apply consistently across the digital economy. The establishment of the Digital Regulation Cooperation Forum (DRCF) in the UK, discussed more in detail in section 5, which represents an important step towards enhancing coherence by fostering collaboration among different regulatory authorities involved in the oversight of digital markets, is a case in point. Also, a uniform understanding of Fair, Reasonable, and Non-Discriminatory (FRAND) terms across diverse regulatory landscapes, such as those governed by the DMA, the DSA, and the European Electronic Communications Code (EECC), could foster a consistent and equitable approach to access and usage of essential digital services, data, and infrastructure.

The intricate nature of the digital ecosystem necessitates a harmonized approach to regulatory responses across various sectors, ensuring the avoidance of conflicting obligations. This calls for enhanced inter-agency collaboration and the establishment of overarching regulatory principles that uniformly apply across the digital economy. The application of Fair, Reasonable, and Non-Discriminatory (FRAND) terms exemplifies such a horizontal principle that could bridge regulatory frameworks effectively. Such a shared understanding would not only enhance coherence in the digital regulatory landscape but would also ensure that regulatory authorities operate within a common framework, thereby facilitating collaborative regulation.

Last but not least, while ambiguity in rapidly evolving digital markets can challenge regulatory clarity, incorporating agile methodologies and innovative tools (such as hackathons, regulatory sandboxes, etc.) into regulatory practices can help in finding the right balance.

In conclusion, the challenge of regulatory governance in digital markets lies in striking a delicate and optimal balance between respecting the traditional principles of good regulation while creating and maintaining a surplus of flexibility and agility necessary to effectively respond to the challenges summarized by the VUCA framework.

5. Case studies and practical insights

In light of the proliferation and transformation of digital markets, most regulatory authorities have found themselves ill-equipped and lacking the skills necessary to ensure effective oversight of digital markets. While many authorities have undertaken efforts to reorganize and adapt, the chosen models vary, revealing diverse benefits, risks, and deficiencies.

In this section, we briefly recall a few selected case studies focusing on two main institutional adaptations: (a) the development and integration of data and technology expertise, and (b) collaborative regulation.

a. Developing data and technology expertise

To establish adequate technological infrastructure, authorities either have to develop internal technical expertise by setting up a data unit and hiring professionals with a deep understanding of digital technologies or collaborate with or outsource data analysis to external experts and organizations that can provide the necessary

insights and knowledge. The creation of a data unit requires important decisions to be made in terms of how such a unit should be integrated into an existing authority.

For example, the UK competition authority, CMA has set up a separate Data, Technology and Analytics (DaTA) unit, while Ofcom has created an Emerging Technology directorate and data science team. These units are responsible for leveraging technology and data analysis to inform regulatory decision-making.

The creation of the DaTA unit within the CMA is an example of a strategic initiative to integrate technological and data expertise into traditional competition and consumer protection roles. It was motivated by the recognition that a deep understanding of digital technologies and data-driven markets is crucial for effective regulatory oversight of digital markets. The unit was created to provide expert advice across the CMA's various functions, including market studies, antitrust investigations, consumer enforcement, and merger reviews, thereby enhancing the CMA's capacity to address complex digital economy cases.

Similarly, in December 2018, the US Federal Communications Commission (FCC) established the Office of Economics and Analytics (OEA) to promote more consistent quality and use of economic analysis in its decisions. The reorganization concentrated economists who were previously dispersed across different offices and bureaus into a centralized office managed by economists. This reorganization aimed to ensure that economic perspectives were systematically incorporated into the agency's policy work, enhancing the quality and relevance of the economic analysis. While this reorganization concerned economists, lessons drawn from it may also apply to managing other specialized or technical staff in large and complex organizations (Ellig et al, 2021).

However, while the evolution from traditional evidence-based regulation toward a data-driven regulation and development of adequate technological infrastructure and expertise might seem like an obvious and desirable choice, the cultural shift to such an approach requires a profound change in mindset and organizational structure within regulatory bodies. Indeed, the establishment of such specialized units requires several strategic choices. Key issues concern the unit's structure, the allocation of resources between immediate casework impact and longer-term innovation, and strategies for hiring and retaining skilled data scientists and engineers. Data scientists are currently in high demand and short supply, making it challenging for regulatory authorities to attract and retain top or even good talents in the field. For example, the OECD report (2022b) highlights challenges that regulators face in recruiting well-qualified staff, particularly IT and data specialists, which impacts their regulatory functions. Hence, a decision to establish a data unit will first require a government's commitment to provide sufficient investment in resources and competitive salaries to attract qualified data scientists and experts in digital technologies. Also, considering that different authorities will acquire additional powers and duties under various regulations governing the functioning of digital platforms (such as competition, privacy, antitrust, cybersecurity, AI, and data protection), EU Member states might consider establishing a centralized pool of data scientists.

For example, with a decree of 31st August, 2020, France has created the *Pôle d'expertise de la régulation numérique*, which operates as a national service. Its primary goal is to enhance the state's ability to regulate digital platforms by providing technical support in data processing, data science, and algorithmic processes to state authorities that have regulatory powers over digital platforms.[7]

[7] PEReN is administratively linked to the Directorate General for Enterprise. It is under the joint authority of the ministers responsible for the economy, communication, and digital sectors. It targets online platform operators, as defined by Article L. 111-7 of the French Consumer Code.

Moreover, France has also established a Digital Republic Fund that provides funding and resources for digital innovation projects, including the recruitment of data scientists. Such a centralized approach might not only allow the state to pool financial resources together, but it may also facilitate expertise building for data scientists who could work on projects for different authorities as well as cross-fertilization of ideas and knowledge-sharing among different regulatory authorities. However, as there is no one-size-fits-all approach, different regulatory authorities must carefully consider their specific needs and resources when deciding on the best strategy.[8]

Furthermore, the creation of a separate data unit should be accompanied by a careful evaluation of potential limitations concerning data collection, storage, and analysis to ensure compliance with all the applicable regulations. Also, considering that the amount of information collected by the authorities may increase exponentially, ensuring a standardized approach may be necessary to effectively manage and analyze the data. For example, in the UK, the Data Standards Authority, which forms part of the new Central Digital and Data Office (CDDO), plays a crucial role in promoting data standardization and harmonization across government agencies (UK CDDO, 2023).

b. Collaborative regulation

As already stressed throughout this paper, the paradigm shift towards more integrated and collaborative frameworks is essential for navigating the complexities of the digital economy. The selected examples discussed below illustrate the strategic moves taken by some countries towards harnessing collective expertise and resources, enabling a more nuanced, proportionate, and agile regulatory responses.

In July 2020, the UK established the Digital Regulation Cooperation Forum (DRCF) as a collaborative initiative between the Competition and Markets Authority (CMA), Information Commissioner's Office (ICO), and the Office of Communications (Ofcom), with the Financial Conduct Authority (FCA) joining in April 2021. The DRCF was created as a non-statutory body to enhance coordination among these regulatory authorities and to foster a more unified and coherent regulatory approach, acknowledging that isolated actions by individual regulators might not be sufficient to effectively address the multifaceted nature of digital markets. Its objectives extend to advancing a coherent regulatory approach, informing policymaking, enhancing regulatory capabilities, anticipating future developments, promoting innovation, and strengthening international engagement.

Since its inception, the DRCF has launched several initiatives aimed at addressing various key digital regulation challenges, such as algorithmic transparency, children's online safety, and the regulation of online advertising markets. It has also worked on developing shared understanding and capabilities among its members, exemplified by collaborative projects and joint statements on regulatory approaches.

While the DRCF represents a significant step towards more integrated digital regulation in the UK, it has faced criticisms related to its non-statutory nature, limited membership, lack of enforcement powers, and restricted accountability mechanisms. Limited membership, for example, raises concerns about the creation of a tiered regulatory landscape. Restricted and selective membership might lead to a scenario where certain regulators might be perceived as 'first-class' authorities with direct influence on digital regulation coordination, while others risk being seen as 'second-class' regulators,' with their roles and contributions potentially marginalized. This restrictive membership could have significant implications for the future budgets and resources of

[8] For the UK's CMA experience, see for example, Hunt, S. (2022), The technology-led transformation of competition and consumer agencies: the Competition and Markets Authority's experience.

the authorities within and outside the DRCF. Membership in the DRCF could, for example, provide a strategic advantage in terms of influence over digital regulation policies and priorities. This could translate into better access to government attention and potentially more favorable budget allocations, as their work is directly tied to the high-profile task of coordinating digital regulation and potential enforcement on high-profile cases. This, in turn, could also result in increasing disparity in terms of access to expert data scientists necessary to establish technological proficiency.

Critics argue that for the DRCF to be truly effective, it may need a statutory basis, broader membership encompassing more regulators with digital remits, and clearer mechanisms for accountability and enforcement (Vanberg, 2023).

In response to the complexities of digital regulation, several countries have established collaborative fora akin to the UK's DRCF. In the Netherlands, the Digital Regulation Cooperation Forum was launched in October 2021, comprising the Netherlands' Authority for Consumers and Markets (ACM), the Dutch Data Protection Authority, the Dutch Authority for the Financial Markets (AFM), and the Dutch Media Authority (CvdM). Similarly, Australia has created the Digital Platform Regulators Forum in March 2022, which includes the Australian Competition and Consumer Commission (ACCC), the Australian Communications and Media Authority, the Office of the Australian Information Commissioner, and the Office of the eSafety Commission.

In this context it is worth noting that a wider collaborative effort was undertaken already back in 2019 by several French regulators (the Competition Authority, AMF, Arafer, Arcep, CNIL, CRE and CSA) that signed a Memo on 'New Regulatory Mechanisms – Data-Driven Approaches' (Arcep, 2019). While wider collaboration may help ensure more regulatory coherence, if not well crafted and carefully planned it may also add complexity and result in slowness of the regulatory process, precisely when it needs to become more agile. The requirements for an improved collaborative regulation appear, therefore, themselves extremely challenging.

Altogether, the initiatives briefly discussed in this section reflect a global trend towards more collaborative and coherent regulatory strategies to address the complex challenges posed by the digital economy.

6. Conclusions

To conclude, the concepts discussed in this paper – technological proficiency, collaborative regulation, and regulatory agility - are interrelated and mutually reinforcing. Technological proficiency enhances an authority's ability to be agile and to adopt quicker and more informed responses. Collaborative regulation supports both agility and technological proficiency by pooling resources, knowledge, and expertise, ensuring that regulatory bodies can leverage each other's strengths to address complex and rapidly changing digital environments.

However, these trends can also give rise to potential conflicts. While agility demands rapid responses, collaborative regulation risks slowing down decision-making process by requiring coordination among multiple authorities. Technological proficiency is likely to vary across different regulatory authorities, leading to disparities in understanding and interpreting data-based and technological issues. Such disparities can create frictions rendering collaborative efforts counterproductive. Moreover, rapidly evolving technologies can outpace regulatory bodies' ability to develop and maintain technological proficiency. The faster the pace of change, the more disruptive the innovation, and the more challenging it becomes for the regulator to stay informed and effectively leverage new technologies in their regulatory practices. This problem is further compounded by the stark disparity in budgets available to major digital players and public regulatory authorities.

To address these potential conflicts, regulatory bodies must strike a balance between the

speed of response, the depth of technological understanding, and the breadth of collaboration. This will require flexible frameworks that allow for rapid adaptation to technological advancements and market changes; continuous investment in learning and professional development programs to keep pace with technological advancements; and developing mechanisms to enhance collaboration without compromising the agility of decision-making. Competence mapping can play a crucial role in achieving this balance. By systematically identifying, defining, and measuring the skills, knowledge, and behaviours required for effective performance, regulatory authorities can assess their current competence levels, identify gaps, and develop targeted strategies to enhance their oversight capabilities. Key competences for innovative policymaking identified by the European Commisison's Joint Research Centre (JRC) are particularly relevant in this context.

While regulatory work in the digital economy will undoubtedly become more challenging, the purpose of this exploration is to emphasize the essentiality of improving the quality of the "machinery" employed to achieve effective oversight. By developing the right set of competences, fostering collaboration, and embracing agility, regulatory bodies can navigate the complexities of the digital landscape while promoting innovation and protection consumer interests.

References

Agile Nations Overview, (https://www.gov.uk/government/groups/agile-nations)

Agile Nations Charter, (https://www.gov.uk/government/publications/agile-nations-charter)

Arcep (2019), New Regulatory Mechanisms: Data-Driven Regulation, available at: < https://en.arcep.fr/fileadmin/cru-1677573101/user_upload/grands_dossiers/La_regulation_par_la_data/note-aai-data-driven-regulation-july2019.pdf >

Attrey, A., Lesher, M., and C. Lomax (2020), 'The role of sandboxes in promoting flexibility and innovation in the digital age', Going Digital Toolkit Policy Note, No. 2, available at: https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf

Baldwin, Cave, and Lodge (2011), Understanding Regulation: Theory, Strategy, and Practice, Oxford University Press.

Bennear, L.S., & Wiener, J.B. (2019). Adaptive Regulation: Instrument Choice for Policy Learning over Time.

Bennett, N. and J.G. Lemone (2014), 'What a difference a word makes: Understanding threats to performance in a VUCA world', Business Horizons, vol. 57, no. 3, pp. 311-317,

Colangelo, G. (2023), 'In Fairness We (Shoult Not) Trust: The Duplicity of the EU Competition Policy Mantra in Digital Market', The Antitrust Bulletin, vol. 68, Issue 4.

European Commission (2022), Competences for Policymaking: Competence Frameworks for Policymakers and Researchers working on Public Policy, JRC Science for Policy Report.

Holsapple, C.W. and X. Li (2008), 'Understanding Organizational Agility: A Work-Design Perspective',

Hunt, S. (2022), The technology-led transformation of competition and consumer agencies: the Competition and Markets Authority's experience, available at:

<https://assets.publishing.service.gov.uk/media/62b9ab0d8fa8f5357862f49e/The_technology_led_transformation_of_competition_and_consumer_agencies.pdf>

ITU's Benchmark Report on fifth-generation collaborative digital regulation (2021).

Jaursch, J. (2023), 'Here is why Digital Services Coordinators should establish strong research and data units', DSA Observatory, https://dsa-observatory.eu/2023/03/10/here-is-why-digital-services-coordinators-should-establish-strong-research-and-data-units/

Jin, G.Z., Sokol, D. and L. Wagman (2022), 'Towards a Technological Overhaul of American Antitrust', Antitrust, vol. 37, no. 1.

Joint Research Centre of the European Commission. (2021). Making Energy Regulation Fit for Purpose: State of Play of Regulatory Approaches.

Larsson, S., Hildén, J., and K. Söderlund (2024), Between Regulatory Fixity and Flexibility in the EU AI Act, Draft paper available at: https://lucris.lub.lu.se/ws/portalfiles/portal/171573074/Larsson_Hild_n_S_derlund_Jan_2024_Between_Regulatory_Fixity_and_Flexibility_in_the_EU_AI_Act_draft_paper_2024-1-26.pdf

Massarotto, G. (2019), 'From Digital to Blockchain Markets: What Role for Antitrust and Regulation'.

OECD (2022a), Interactions between Competition Authorities and Sector Regulators.

OECD (2022b), Equipping Agile and Autonomous Regulators.

OECD. (2021). Recommendation for Agile Regulatory Governance to Harness Innovation.

Prosser (2006), 'Regulation and Social Solidarity', Journal of Law and Society, vol. 33, no. 3.

Sabel and Dorf (1998), "A Constitution of Democratic Experimentalism", Columbia Law

Sheikh, H. (2022), 'European Digital Sovereignty: A Layered Approach', Digital Society, vol. 1.

Sunstein, C. R. (2019), Sludge and Ordeals, Duke Law Journal 1843.

UK Central Digital and Data Office (2023), Data Standards Authority: operational model and processes.

UK Department for Business, Energy & , Strategy. (2019). Regulation for the Fourth Industrial Revolution.

UK Department for Business & Trade (2021), Agile Nations Charter, available at: https://www.gov.uk/government/publications/agile-nations-charter/agile-nations-charter-accessible-webpage-version.

US National Academy of Public Administration and Project Management Institute (2022), Agile Regulation: Gateway to the Future.

Vanberg, A.D. (2023), Coordinating digital regulation in the UK: is the digital regulation cooperation forum (DRCF) up to the task?, International Review of Law, Computers & Technology, 37:2, 128-146, DOI: 10.1080/13600869.2023.2192566.

Table 1. Adopting the VUCA framework to selected EU digital regulations

VUCA Framework	*Digital Markets Act*	*Digital Services Act*	*Artificial Intelligence Act*	*Data Act*	*Data Governance Act*
Volatility	Addresses the rapid changes in market dynamics and the emergence of gatekeepers by establishing clear rules to ensure fair competition.	Tackles the fast-evolving online platform environment by setting standards for content management and user protection.	Responds to the rapid development and deployment of AI technologies by creating a framework for their safe and ethical use.	Aims to manage the swift changes in data generation and usage by facilitating data sharing and access.	Seeks to stabilize the data sharing environment by establishing trustworthy mechanisms for data governance.
Uncertainty	Reduces uncertainty for smaller market players by defining gatekeeper obligations and permissible practices.	Decreases legal uncertainties for online services by providing a harmonized set of rules for content moderation.	Mitigates uncertainties around AI by specifying risk-based requirements for AI systems.	Clarifies rights and obligations regarding data access and use, reducing uncertainties for data holders and users.	Reduces uncertainties in data sharing by setting clear rules for data intermediation services and data altruism.
Complexity	Addresses market complexity by simplifying the regulatory environment for digital markets and ensuring transparency in gatekeeper operations.	Manages the complexity of online platforms by requiring clear terms of service, transparency in algorithms, and user recourse mechanisms.	Deals with the complexity of AI systems by categorizing them according to their risk level and imposing corresponding requirements.	Aims to simplify the complex data landscape by establishing a clear framework for data sharing across sectors.	Addresses the complexity of data governance by providing a structured framework for data sharing and reuse.
Ambiguity	Clarifies ambiguous practices by gatekeepers that could harm competition, ensuring that rules are clear and enforceable.	Reduces ambiguities in online content management by establishing clear responsibilities and accountability for platforms.	Reduces ambiguities in the ethical use of AI by establishing clear standards for transparency, accountability, and human oversight.	Clarifies legal ambiguities around data sharing and usage rights, ensuring clear and fair conditions.	Aims to dispel ambiguities in data sharing practices by establishing certified data intermediaries and frameworks for data altruism.

Table 2. Institutional enforcement of the DMA, DSA, AI Act, Data Act, and Data Governance Act

Regulatory aspect	DMA	DSA	AI Act	Data Act	Data Governance Act
Primary Regulatory Body	European Commission (NCAs may also have a role in enforcement, particularly in cases where local market conditions are affected).	Digital Service Coordinators (DSCs) at the national level.	A decentralized enforcement mechanism with national supervisory authorities responsible for enforcement, complemented by a European AI Board for coordination.	Each Member State designates one or more competent authorities for the application and enforcement of the Data Act, with the possibility to establish new authorities or rely on existing ones.	
Cross-border Coordination	The DMA facilitates cooperation among Member States and between Member States and the Commission through a central database for sharing information related to gatekeepers and their obligations.	The European Board for Digital Services facilitates cooperation between DCS of each Member State and the Commission.		Where multiple competent authorities are designated, a data coordinator facilitates cooperation between them and assists with the Act's application and enforcement.	
Enforcement Mechanism	The Commission has investigating powers, including the power to request information, conduct inquiries, and imposed fines and periodic penalty payments for non-compliance.	DSCs have the power to investigate, order compliance, and impose fines for non-compliance.	National authorities are responsible for ensuring compliance, conducting investigations, and imposing sanctions. The AI Board provides opinions and guidance, while the AI Office supports enforcement activities.	Competent authorities have the tasks and powers to promote data literacy, handle complaints, and conduct investigations concerning the Act's applications.	

Table 3. Adaptation required by regulatory authorities under the VUCA framework

VUCA Framework	*Volatility*	*Uncertainty*	*Complexity*	*Ambiguity*
Adaptation required by regulatory authorities	Develop agile regulatory frameworks that can quickly adapt to rapid technological advancements and market changes.	Enhance predictive capabilities and engage in scenario planning to better anticipate future regulatory needs and challenges.	Foster interdisciplinary collaboration and employ advanced data analytics to navigate and regulate complex digital ecosystems.	Promote transparency and clear communication to reduce ambiguities in regulatory expectations and enforcement.

Table 4. Monitoring and analysis activities under the DSA

Aspect	*Description*	*DSA Provision*
Annual Transparency Reports	Providers of intermediary services must publish annual reports detailing content moderation efforts and measures taken due to the enforcement of their terms and conditions.	Art. 15, 24
Notice and Action Mechanisms	Hosting service providers are required to implement user-friendly mechanisms for users to notify them of illegal content.	Article 14
Trusted Flaggers	The DSA recognizes the role of trusted flaggers in notifying illegal content, designated by the Digital Service Coordinators for their expertise and ability to provide high-quality notices.	Article 16, 22
Out-of-Court Dispute Settlement	The DSA provides for out-of-court dispute resolution mechanisms for resolving disputes between online platform and users concerning content moderation decisions. It also requires that certified out-of-court dispute settlement bodies shall report to the DSC that certified them, on an annual basis, on their functioning, specifying at least the number of disputes they received, the information about the outcomes of those disputes, the average time taken to resolve them and any shortcomings or difficulties encountered. They shall also provide additional information at the request of the DSC.	Art.21
Compliance with Terms and Conditions	Platforms are required to make their terms and conditions transparent, easily accessible, and understandable to users, and to inform users of significant changes.	Art. 14
Risk Assessments and Audits	Very large online platforms (VLOPs) and search engines must conduct risk assessments related to illegal content dissemination, negative effects on fundamental rights, and manipulation of their service.	Art. 34, 37
Data Access and Scrutiny	The DSA allows for data access by researchers to analyze systemic risks associated with online platform, offering empirical evidence of the DSA's impact.	Art. 40
DSA Coordinators Reports	National DSCs oversee and enforce the DSA, and their reports and findings on digital services compliance are crucial	General provisions on DSA coordinators and their powers.

Table 5. Key aspects of collaborative regulation

Analytical category	Description
Institutional scope of collaboration	• *Intra-agency:* between different units/directorates within a single regulatory body (particularly relevant for multi-mandate regulatory authorities (i.e. CNMC, BNetzA, etc); • *Inter-agency:* between different regulatory bodies within the same jurisdiction (i.e. between competition authorities and sector regulators or between competition and data protection authorities); • *Cross-border:* between regulatory bodies from different jurisdictions.
Nature of collaboration	• *Voluntary vs mandatory:* activated through mutual interests among regulatory bodies vs required by law; • *Formal vs informal:* established through formal agreements (like MoUs) vs ad hoc collaborations, including networks and temporary working groups (i.e. the Big Data Sector Inquiry, conducted jointly by the AGCM, AGCOM (respectively, competition and telecom regulatory authorities), and by the Data Protection Authority).
Substantive scope of collaboration	• *Information and data sharing:* exchange of insights and data, which can be facilitated by clear and explicit government-to-government (G2G) data sharing rules. • *Consultation and advice:* mutual assistance through advisory opinions to ensure coherent regulatory outcomes (i.e. remedies in competition cases that comply with privacy regulations, expert advice provided by ENISA to national telecom regulatory authorities) • *Joint monitoring:* coordinated actions for monitoring and enforcement.

Tab. 6. Designated Digital Service Coordinators by institutional model

Institutional Model	Country	Authority
Telecom or telecom and media regulator	Austria	RTR
	Belgium	BIPT
	Czech Republic	CTU
	Estonia	TTJA
	Finland	Traficom
	Germany	BNetzA
	Greece	EETT
	Hungary	NMHH
	Italy	AGCOM
	Lithuania	RRT
	Malta	MCA
	Poland	UKE
	Romania	ANCOM
	Slovenia	AKOS
	Sweden	PTS
Media regulator	Cyprus	CRTA
	Ireland	Media Commission
Competition authority	Denmark	Competition and Consumer Authority
	Luxembourg	Autorité de la concurrence
Multi-mandate	The Netherlands	ACM

(competition and sectoral regulation)	Spain	CNMC
Consumer protection authority	Latvia	PTAC
Newly created authority	France	ARCOM

Source: Table based on the official information from the Commission website,[9] where 17 countries features as having officially notified their DSC. For the other 10 Member States, information has been gathered based on draft laws that are mostly in the final stages of approval.

Table 7. Competent notified authorities under the DGA

Country	Competent body	Competent authority for data intermediation	Competent authority for data altruism
	Art. 7	Art. 13	Art. 23
Austria			
Belgium			
Bulgaria	Minister of e-Government, President of the National Statistical Institute (for reuse of statistical data)	Minister of e-Government	
Croatia	Central State Office for the Development of Digital Society		
Cyprus			
Czech Republic			
Denmark	Statistics Denmark	Agency for Digital Government	
Estonia			
Finland	Statistics Finland Finnish Social and Health Data Permit Authority Findata (for secondary use of social and health care data)	Finnish Transport and Communications Agency Traficom	
France		ARCEP	CNIL
Germany			
Greece			
Hungary	The National Data Asset Agency	The National Data Protection and Freedom of Information Authority	
Ireland	Central Statistics Office (Researcher Co-ordination Unit)	The Competition and Consumer Protection Commission	
Italy			
Latvia	Ministry of Environmental Protection and Regional Development Republic of Latvia		
Lithuania	The State Data Agency	The State Data Protection Authority	
Luxembourg		Ministry of State, Department of Media, Connectivity and Digital Policy	
Malta			

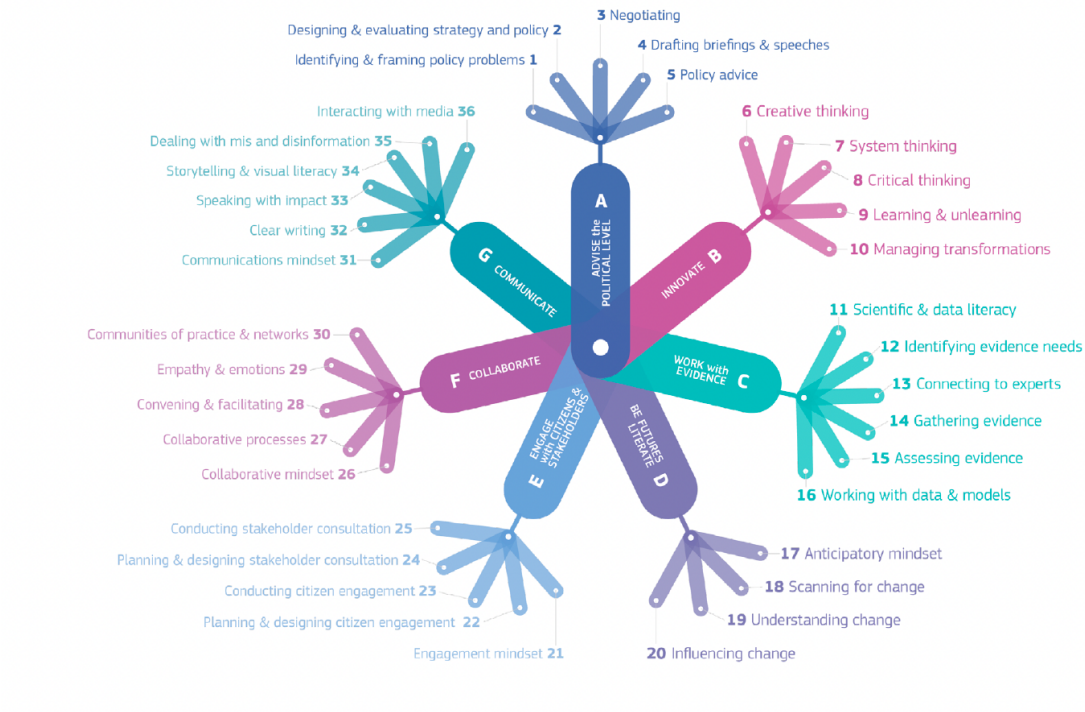
[9] https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs

Netherlands	Statistics Netherlands	The Authority for Consumers and Markets	
Poland			
Portugal		Administrative Modernization Agency	
Romania		Authority for Digitalization of Romania (ADR)	
Slovakia			
Slovenia			
Spain	Deputy Directorate General for Planning and Governance of Digital Administration General Secretariat for Digital Administration. State Secretariat for Digitization and Artificial Intelligence Ministry of Economic Affairs and Digital Transformation	Deputy Directorate General for Digital Society Directorate General for Digitization and Artificial Intelligence State Secretariat for Digitization and Artificial Intelligence Ministry of Economic Affairs and Digital Transformation	
Sweden			

Table 8. 2x2 Matrix on competence and VUCA mapping

	High adaptive capacity	**Low adaptive capacity**
High technological proficiency	Well-equipped, adaptable regulators (Manage complexity, volatility)	Technologically skilled, but rigid (Manage uncertainty, complexity)
Low technological proficiency	Adaptable but lacking technological skills (Manage volatility and ambiguity)	Least prepared regulators (struggle with all VUCA elements)

Fig. 1. Clusters and competences of the 'Innovative Policymaking' competence framework



Source: European Commission (2022), Competences for Policymaking.